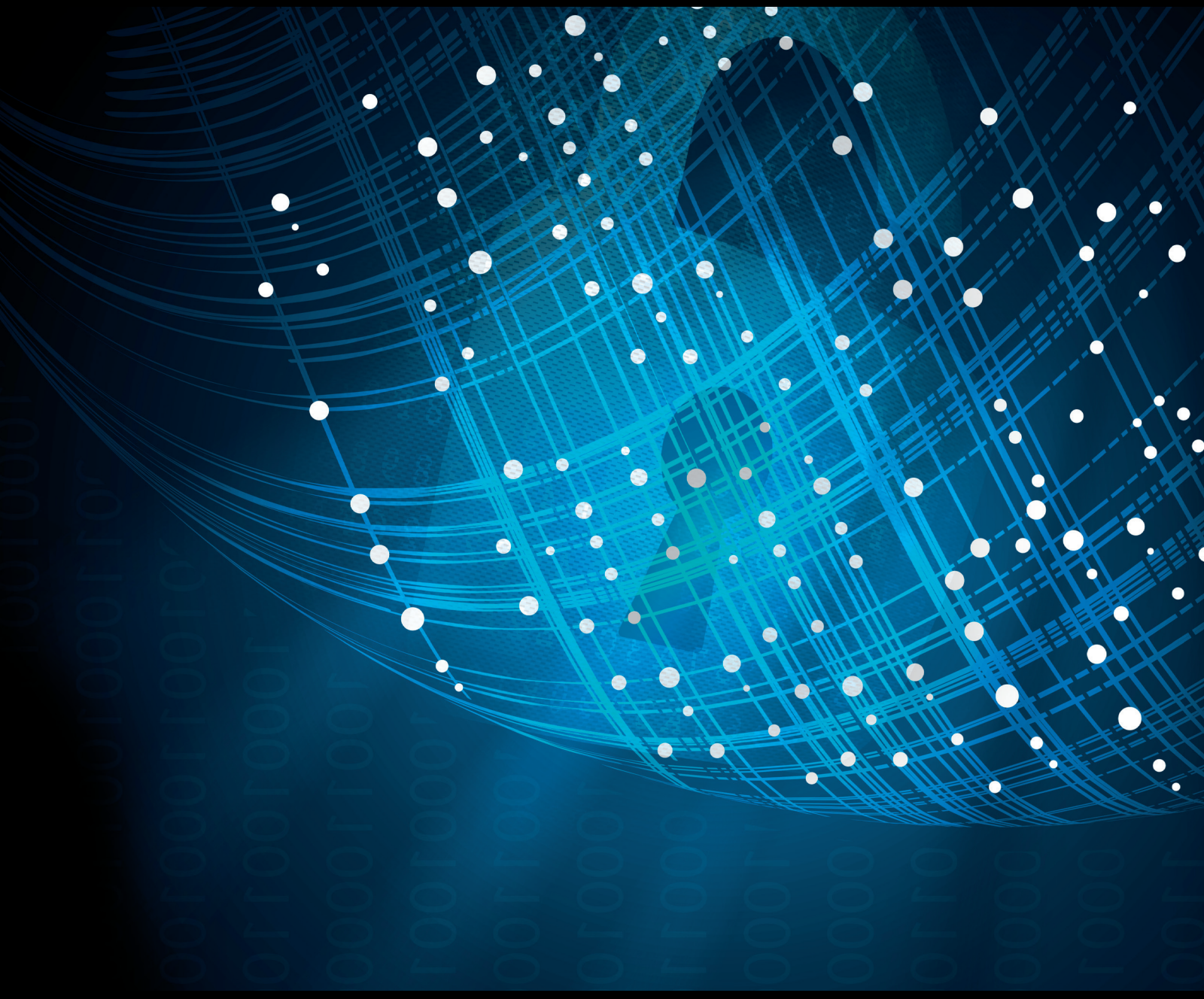
Security and Communication Networks

Application-Aware Multimedia Security Techniques

Lead Guest Editor: Manjit Kaur
Guest Editors: Ahmed A. Abd El-Latif, Jialiang Peng, Jiawen Kang, Robertas Damaševičius, and Vijay Kumar



Application-Aware Multimedia Security Techniques

Security and Communication Networks

Application-Aware Multimedia Security Techniques

Lead Guest Editor: Manjit Kaur
Guest Editors: Ahmed A. Abd El-Latif, Jialiang Peng, Jiawen Kang, Robertas Damaševičius, and Vijay Kumar

Contents

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9968275, 11 pages
https://doi.org/10.1155/2021/9968275

Review Article

A New Speech Enhancement Technique Based on Stationary Bionic Wavelet Transform and MMSE Estimate of Spectral Amplitude

Mourad Talbi[1] **and Med Salim Bouhlel**[2]

[1]*Laboratory of Nanomaterials and Systems for Renewable Energies (LaNSER), Center of Researches and Technologies of Energy of Borj Cedria, Tunis 952050, Tunisia*
[2]*Sciences and Technologies of Images and Telecommunications, Higher Institute of Electronics and Telecommunication of Sfax, Sfax University, Sfax, Tunisia*

Correspondence should be addressed to Mourad Talbi; talbi1969@yahoo.fr

Received 2 April 2021; Revised 26 April 2021; Accepted 10 October 2021; Published 24 December 2021

Academic Editor: Manjit Kaur

Speech enhancement has gained considerable attention in the employment of speech transmission via the communication channel, speaker identification, speech-based biometric systems, video conference, hearing aids, mobile phones, voice conversion, microphones, and so on. The background noise processing is needed for designing a successful speech enhancement system. In this work, a new speech enhancement technique based on Stationary Bionic Wavelet Transform (SBWT) and Minimum Mean Square Error (MMSE) Estimate of Spectral Amplitude is proposed. This technique consists at the first step in applying the SBWT to the noisy speech signal, in order to obtain eight noisy wavelet coefficients. The denoising of each of those coefficients is performed through the application of the denoising method based on MMSE Estimate of Spectral Amplitude. The SBWT inverse, $SBWT^{-1}$, is applied to the obtained denoised stationary wavelet coefficients for finally obtaining the enhanced speech signal. The proposed technique's performance is proved by the calculation of the Signal to Noise Ratio (SNR), the Segmental SNR (SSNR), and the Perceptual Evaluation of Speech Quality (PESQ).

1. Introduction

In many speech-related applications, an input speech signal is frequently corrupted by environmental noise and needs further processing using a speech enhancement technique for ameliorating the associated quality before being employed [1]. Generally, speech enhancement techniques can be grouped into two groups which are supervised and unsupervised. Unsupervised techniques include spectral subtraction (SS) [2–4], Wiener filtering [5, 6], short-time spectral amplitude (STSA) estimation [7], and short-time log-spectral amplitude estimation (logSTSA) [8]. Concerning the supervised speech enhancement techniques, they employ a training set for learning diverse models for noisy and clean speech signals, and examples include codebook-based methods [9] and Hidden Markov Model (HMM)-based techniques [10]. Classical speech enhancement techniques are frequently processing a noisy utterance in a frame-wise way, that is, for enhancing each short-time period of the utterance nearly in independent manner. Some research works showed that considering the inter-frame variation over a relatively long span of time can contribute to superior performance in enhancing speech [1]. Famous approaches along this direction include modulation-domain spectral subtraction [11], Kalman filtering, and modulation-domain Wiener filtering [12, 13]. Moreover, when we compare the discrete wavelet transform (DWT) to the Fourier transform (FT) where only the frequency parts are taken into consideration, though, in the expression of the DWT [14], both temporal and frequency

characteristics of the signal to be analyzed are taken into consideration. The DWT has become a well-known method in speech analysis. In Wavelet Thresholding Denoising (WTD) [15], the wavelet transform is applied for splitting the time-domain signal into sub-bands. After that, thresholding of the obtained wavelet coefficients (sub-bands) is performed. In [16], the DWT [17, 18] was applied to the speech signal to simply conserve the obtained approximation portion, which simultaneously attains data compression and noise robustness in recognition. In [1], the DWT was employed for analyzing the spectrogram of a noisy utterance along the temporal axis, and then the resulting detail portion was devalued with an expect of reducing noise effect in order to promote speech quality. Despite the ease of its implementation, the preliminary evaluation results indicate that the technique proposed in [1] permits to have input signals with better perceptual quality. It was proved that this technique [1] can be paired with many well-known speech enhancement approaches for achieving even better performance [1]. In this work, a novel speech enhancement technique based on the Stationary Bionic Wavelet Transform (SBWT) [19–21] and Minimum Mean Square Error (MMSE) Estimate of Spectral Amplitude [22] is proposed. In this paper, this approach is evaluated and compared to four other speech enhancement approaches which are as follows:

(i) Unsupervised speech denoising via perceptually motivated robust principal component analysis [23].

(ii) The speech enhancement technique based on MSS-SMPO [24, 25].

(iii) The denoising technique based on MMSE Estimate of Spectral Amplitude [22].

(iv) Our previous speech enhancement technique based on LWT and Artificial Neural Network (ANN) and using MMSE Estimate of Spectral Amplitude [26].

The fourth technique which is based on LWT and ANN [27–29] and uses MMSE Estimate of Spectral Amplitude [26] can be summarized by the following steps:

(i) **First step**: applying the LWT to the noisy speech signal for obtaining two noisy details coefficients, $cD1$ and $cD2$, and one approximation coefficient, $cA2$.

(ii) **Second step**: denoising *cD1 and cD2* by soft thresholding, and for their thresholding, suitable thresholds, $thr\,j, 1 \leq j \leq 2$, have to be used. Those thresholds are determined by using an Artificial Neural Network (ANN). This soft thresholding is performed for having two denoised coefficients, $cDd1$ and $cDd2$.

(iii) **Third step**: applying the denoising approach based on MMSE Estimate of Spectral Amplitude [22] to $cA2$ for obtaining a denoised coefficient, $cAd2$.

(iv) **Fourth step**: applying the inverse of LWT, LWT^{-1}, to $cDd1$, $cDd2$, and $cAd2$, for finally obtaining the enhanced signal.

As a future work, we will develop a novel speech enhancement approach using ANN [30–36] or deep learning [37, 38] for thresholding the noisy stationary bionic wavelet coefficients. Those coefficients are obtained by applying the *BWT* to the noisy speech signal.

In Section 2 of this paper, materials and methods are presented. Section 2.4 describes the speech enhancement technique proposed in this work. In Section 3, results and discussion are presented. Finally, Section 4 concludes the paper.

2. Materials and Methods

2.1. The Stationary Bionic Wavelet Transform (SBWT). In [19], the *SBWT* has been proposed as a novel wavelet transform. This transform was initially introduced for solving the problem of perfect reconstruction that exists with the Bionic Wavelet Transform (BWT). Its application was performed for speech enhancement [19, 20] and also for ECG denoising [21].

2.2. The MMSE Estimate of Spectral Amplitude. In the literature, it was proposed to estimate the noise power spectral density employing MMSE (Minimum Mean Square Error) optimal estimation [22]. It was proved that the obtained estimator can be considered as a VAD (Voice Activity Detector)-based noise power estimator, and the noise power is updated alone if speech absence is detected, compensated with a required bias compensation [22]. It was proved that the bias compensation is not needed if the VAD is substituted by a soft SPP (Speech Presence Probability) with fixed priors [22]. When choosing fixed priors, this has the benefit of decoupling the noise power estimator from subsequent steps in a speech enhancement algorithm, such as the estimation of the speech power and that of the clean speech [22]. Gerkmann and Richard [22] proved that the proposed SPP approach permits to maintain the quick noise tracking performance of the bias-compensated MMSE-based technique while exhibiting less overestimation of the spectral noise power and an even lower complexity of calculation.

2.3. Signal Model. In [22], Gerkmann and Richard considered frame-by-frame processing of time-domain signals where the Discrete Fourier Transform (DFT) is applied to these frames. Let the complex spectral noise and speech coefficients be given, respectively, by $N_k(l)$ and $S_k(l)$, where l is the time frame index and k is the frequency bin index [22]. In [22], it was assumed that in the short-time Fourier domain, both noise and speech signals tend to be additive. Therefore, the complex spectral noisy observation has the following expression:

$$Y_k(l) = S_k(l) + N_k(l). \tag{1}$$

In [22], it was supposed that the noise and speech signals own zero mean and are independent so that

$$E\left(|Y|^2\right) = E\left(|S|^2\right) + E\left(|N|^2\right), \tag{2}$$

where $E(\bullet)$denotes the statistical expectation operator.

The spectral noise and speech power are expressed as follows:

$$E\left(|N|^2\right) = \boldsymbol{\sigma}_{\mathrm{N}}^2, \quad E\left(|S|^2\right) = \boldsymbol{\sigma}_{\mathrm{S}}^2. \tag{3}$$

Then, both a posteriori SNR and a priori SNR are expressed as follows:

$$\gamma = \frac{\left(|\mathrm{Y}|^2\right)}{\sigma_N^2} \text{ (a posteriori SNR)}, \quad \xi = \frac{\sigma_{\mathrm{S}}^2}{\sigma_{\mathrm{N}}^2} \text{ (a priori SNR)}. \tag{4}$$

All details about MMSE-based noise power estimation are given in [22].

2.4. The Proposed Speech Enhancement Technique. The speech enhancement technique introduced in this work is based on the SBWT [19–21] and the MMSE Estimate of Spectral Amplitude [22]. The novelty of this approach consists in applying the speech enhancement method based on *MMSE* Estimate of Spectral Amplitude [1, 22] in the SBWT domain. In fact, this technique [22] is applied to each noisy stationary bionic wavelet coefficient for its denoising. Those noisy coefficients are obtained by applying the SBWT to the noisy speech signal. Then, the inverse of SBWT ($SBWT^{-1}$) is applied to the obtained denoised coefficients in order to obtain finally the enhanced speech signal. Figure 1 illustrates the flowchart of this proposed technique.

According to Figure 1, the first step of the proposed approach is to apply the *SBWT* to the noisy speech signal for obtaining eight noisy stationary bionic wavelet coefficients. Those coefficients are named wb_i, $1 \le i \le 8$, and each of them is denoised by the speech enhancement technique based on *MMSE* Estimate of Spectral Amplitude [1, 22]. and we obtain eight denoised coefficients, wd_i, $1 \le i \le 8$ (Figure 1). In those coefficients, wd_i, $1 \le i \le 8$ inverse is applied for SBWT (SBWT-1) in order to obtain the enhanced signal finally.

2.5. Minimum Mean Square Error (MMSE) Estimate of Spectral Amplitude in the SBWT Domain. In general, classical speech enhancement approaches based on thresholding in the wavelet transform domain can introduce some distortions to the original speech signal. This particularly occurs for the unvoiced sounds. Consequently, a great number of speech enhancement techniques based on wavelet transforms are employing other tools such as spectral subtraction (SS), Wiener filtering, and MMSE-STSA estimation [39, 40]. This is the reason why we apply the Minimum Mean Square Error (MMSE) Estimate of Spectral Amplitude in the *SBWT* domain in our speech enhancement system. The application of the *SBWT* permits to solve the problem of the perfect reconstruction existing when we apply the BWT [19]. Furthermore, the SBWT among all wavelet transforms [41, 42] tends to uncorrelated data [43] and facilitates the noise suppression. The fact that the Minimum Mean Square Error (MMSE) Estimate of Spectral Amplitude [22] is applied to each noisy stationary bionic coefficient permits to have a better adaptation for speech and noise estimations compared to the application of this technique [22] to the whole noisy speech signal.

2.6. Unsupervised Speech Denoising via Perceptually Motivated Robust Principal Component Analysis [23]. To overcome the shortcomings in the existing sparse and low-rank speech denoising technique that the auditory perceptual properties are not fully exploited and the speech degradation is simply perceived, a perceptually motivated robust principal component analysis (ISNRPCA) technique was presented. In order to reflect the non-linear property for frequency perception of the basilar membrane, cochleagram is employed as inputs of *ISNRPCA*. The latter employs the perceptually meaningful Itakura–Saito measure as its optimization objective function. Furthermore, non-negative constraints are also compulsory for regularizing the decomposed terms with respect to their physical meaning [23]. In [23], Min et al. proposed an alternating direction technique of multipliers (ADMM) for solving the optimization problem of ISNRPCA. The latter is completely unsupervised, and neither the noise nor the speech model requires to be trained beforehand. Experimental results under diverse kinds of noise and different SNRs prove that the ISNRPCA is showing promising results for speech denoising [23].

2.7. The Speech Enhancement Technique Based on MSS-SMPO [25]. In [25], a two-step enhancement technique based on spectral subtraction and phase spectrum compensation was presented for noisy speeches in diverse environments requiring non-stationary noise and medium to low levels of SNR. In the first step of the technique proposed in [25], the magnitude of the noisy speech spectrum is modified by a spectral subtraction technique, where a noise estimation approach was introduced. The latter is based on the low-frequency information of the noisy speech. This noise estimation technique is able to estimate precisely the non-stationary noise. In the second step, the phase spectrum of the noisy speech is modified consisting of phase spectrum compensation, where an SNR-dependent technique is incorporated for determining the amount of compensation to be compulsory on the phase spectrum [25]. A modified complex spectrum is obtained by aggregating the magnitude from the step of spectral subtraction and the modified phase spectrum from the step of phase compensation, which is found to be a better representation of enhanced speech spectrum.

3. Results and Discussion

In this work, the evaluation of the proposed technique is performed by its application to ten Arabic speech sentences pronounced by a male speaker and ten others by a female speaker (Table 1). Those speech signals are degraded in

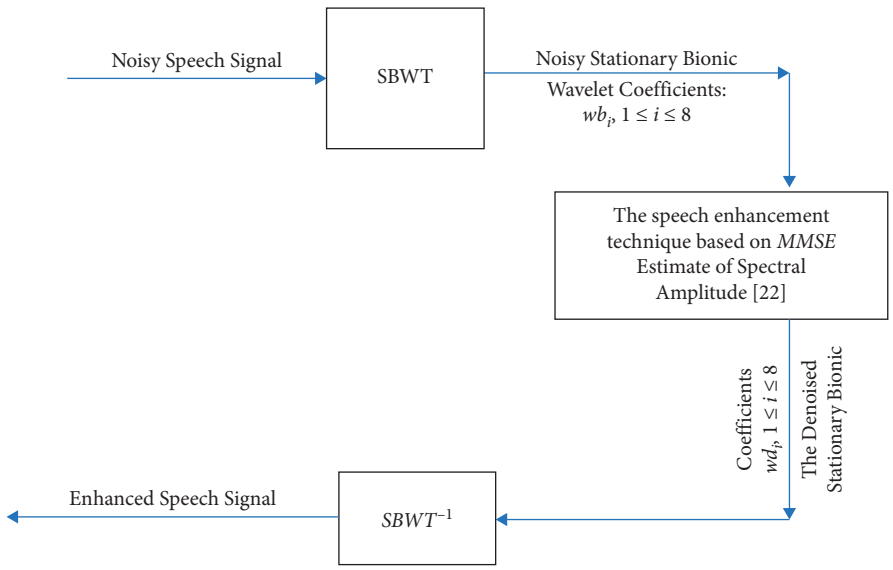


Figure 1: The flowchart of the proposed speech enhancement technique.

Table 1: The list of the used Arabic speech sentences.

Female speaker	Male speaker
أحفظ من الأرض: signal 1	يذي عبخ الن ال: signal 1
أين السم الفرين: signal 2	كتالسر امالسالب لمكأ: signal 2
م عتمتسي بهشم ال: signal 3	قطت إبرقس: signal 3
سانانزم مميذوي: signal 4	من لم تفتني: signal 4
مم ل دوة قتنك: signal 5	فل عن لضحكاتاغ: signal 5
اازار صاامئ: signal 6	و: signal 6
شبكل طبغ و لاك: signal 7	أين زوايا ق و انانان: signal 7
ول قبه تعذل ل: signal 8	د: signal 8
ادئاق و ايالو فرع: signal 9	به آبائكمن: signal 9
امكن انالب الاخ: signal 10	أظمره و قم: signal 10

artificial manner by an additive noise at different values of $SNRi$ (before denoising). In order to corrupt those speech signals (Table 1), we have chosen four kinds of noise which are white Gaussian, car, F16, and tank noises. Those twenty speech signals are sampled at 16 kHz and are listed in Table 1.

Also, for evaluating the proposed technique, it is compared with other three speech enhancement approaches which are as follows:

(i) The denoising approach based on MMSE Estimate of Spectral Amplitude [22].

(ii) The unsupervised speech denoising technique via perceptually motivated robust principal component analysis [23].

(iii) The speech enhancement approach based on MSS-SMPO [24].

This evaluation is performed through the computations of the SNR (Signal to Noise Ratio), the Segmental SNR (SSNR), and the PESQ (Perceptual Evaluation of Speech Quality). The results obtained from these computations are presented in Tables 2–16.

According to these tables, the best results are the values in italics and they are practically obtained from the application of the proposed technique. Therefore, this technique outperforms the other speech enhancement approaches [22–25] applied for this evaluation.

Figure 2 illustrates an example of speech enhancement applying the proposed technique to the clean speech signal (Figure 2(a)) corrupted in additive manner by a car noise (Volvo) with $SNR = 0dB$ (Figure 2(b)). According to this figure, this technique permits to considerably reduce noise and to obtain an enhanced speech signal (Figure 2(c)) with little distortions despite the fact that the value of the SNR is low (0 dB). Figure 3 illustrates the spectrograms of the clean, noisy, and enhanced speech signals.

The spectrogram in Figure 3(b) shows that the type of noise corrupting the speech signal is localized in low-frequency parts. The spectrogram in Figure 3(c) shows that the car noise is considerably reduced by using the proposed speech enhancement technique. Moreover, this technique permits to have an enhanced speech signal with low distortions compared to the clean speech signal (Figure 2(a)).

In the following, we will compare the proposed technique with our previous speech enhancement approach which is based on LWT and ANN and uses MMSE [26]. The first difference between the speech enhancement technique proposed in this work and our previous approach is that they use two completely different wavelet transforms which are the $SBWT$ for the technique proposed in this paper and the LWT for our previous approach proposed in [26]. The second difference between these two techniques is that the denoising approach based on MMSE Estimate of Spectral Amplitude is applied [22] to all stationary bionic wavelet coefficients for the technique proposed in this paper. However, we apply this approach [22] only to the approximation coefficient for our previous speech enhancement technique proposed in [26]. The latter also uses an

Table 2: Results obtained from the computation of SNR (signal 7 (female voice) corrupted by Gaussian white noise).

	SNRf (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**2.7870**	**8.1682**	*8.4026*	**6.3331**
0	**6.9200**	**11.5437**	*12.4447*	**10.4737**
5	**11.0291**	**14.7845**	*15.9887*	**14.2200**
10	**14.1329**	**18.2255**	*19.3911*	**17.6035**
15	**16.7798**	**21.3456**	*22.4836*	**20.8019**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 3: Results obtained from the computation of SSNR (signal 7 (female voice) corrupted by Gaussian white noise).

	SSNR (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**−2.4187**	**0.8504**	*1.3313*	**1.2531**
0	**−2.4610e − 04**	**3.1099**	*3.9607*	**2.7508**
5	**2.7044**	**5.4567**	*6.2536*	**5.1757**
10	**5.0003**	**8.6660**	*8.9350*	**7.4637**
15	**7.7230**	**11.7670**	*12.1193*	**10.4470**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 4: Results obtained from the computation of PESQ (signal 7 (female voice) corrupted by Gaussian white noise).

	PESQ			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**1.0636**	**1.4235**	*1.4884*	**1.2531**
0	**1.4606**	**1.8776**	*1.9593*	**1.7421**
5	**1.9352**	**2.2374**	*2.3747*	**2.1773**
10	**2.3212**	**2.5908**	*2.7116*	**2.5503**
15	**2.7461**	**2.9835**	*3.0695*	**2.8944**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 5: Results obtained from the computation of SNR (signal 5 (male voice) corrupted by F16 noise).

	SNRf (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**1.2722**	**2.5071**	*3.7283*	**2.3837**
0	**5.1589**	**6.2402**	*8.2589*	**7.1434**
5	**8.9032**	**9.5351**	*11.9891*	**11.1435**
10	**12.9517**	**14.0785**	*15.5901*	**14.6596**
15	**15.9880**	**17.9726**	*19.6030*	**18.3975**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Artificial Neural Network (ANN), and this fact differentiates this technique [26] from our technique proposed in this paper. The comparison of these two techniques is also in terms of SNR, SSNR, and PESQ. These two techniques are applied to a speech signal degraded by a car noise with diverse values of SNR before denoising (*SNRi*). Tables 17–19

Table 6: Results obtained from the computation of SSNR (signal 5 (male voice) corrupted by F16 noise).

	SSNR (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**−4.0510**	**−3.7447**	*−3.0533*	**−3.6560**
0	**−2.2335**	**−1.9010**	*−0.7847*	**−1.3701**
5	**−0.4451**	**−0.1214**	*1.0887*	**0.6802**
10	**1.7251**	**2.7250**	*3.1337*	**2.6493**
15	**3.7474**	*6.0977*	**5.9488**	**5.0968**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 7: Results obtained from the computation of PESQ (signal 5 (male voice) corrupted by F16 noise).

	PESQ			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**1.2831**	**1.2227**	*1.2951*	**1.2593**
0	**1.6378**	**1.5769**	*1.8125*	**1.7017**
5	**2.0750**	**2.1242**	*2.2982*	**2.1889**
10	**2.4313**	**2.5673**	*2.7291*	**2.6444**
15	**2.8416**	**3.0733**	*3.1164*	**3.0182**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 8: Results obtained from the computation of SNR (signal 3 (male voice) corrupted by tank noise).

	SNRf (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**1.8657**	**2.8506**	*4.5261*	**3.0084**
0	**5.2569**	**6.0328**	*8.2533*	**6.6513**
5	**8.8912**	**9.7367**	*12.5241*	**10.7510**
10	**12.5670**	**13.6433**	*16.6318*	**14.7634**
15	**15.9158**	**18.2296**	*21.0643*	**19.0401**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 9: Results obtained from the computation of SSNR (signal 3 (male voice) corrupted by tank noise).

	SSNR (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	*−3.0742*	**−4.1830**	**−3.6883**	**−4.2203**
0	*−1.2104*	**−2.2805**	**−1.7476**	**−2.6546**
5	*1.0990*	**−0.0078**	**0.9546**	**−0.1952**
10	**3.6778**	**2.6210**	*3.8260*	**2.5252**
15	**6.2864**	**6.0870**	*7.2508*	**5.7392**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 10: Results obtained from the computation of PESQ (signal 3 (male voice) corrupted by tank noise).

	PESQ			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**0.9941**	**1.3792**	*1.5538*	**1.3848**
0	**1.3492**	**1.8875**	*2.0085*	**1.8400**
5	**1.7720**	**2.3089**	*2.3781*	**2.2503**
10	**2.2027**	**2.5906**	*2.6361*	**2.5094**
15	**2.6084**	**2.7785**	*2.8201*	**2.7240**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 11: Results obtained from the computation of SNR (signal 8 (female voice) corrupted by factory noise).

	SNRf (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**3.0176**	**3.7705**	*4.9624*	**3.4404**
0	**6.6901**	**7.8983**	*9.0631*	**7.2378**
5	**10.4536**	**11.7369**	*12.5889*	**11.2022**
10	**13.5863**	**14.9194**	*15.7971*	**14.4791**
15	**16.0742**	**19.2111**	*20.1601*	**18.6555**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 12: Results obtained from the computation of SSNR (signal 8 (female voice) corrupted by factory noise).

	SSNR (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**−2.6512**	**−2.3588**	*−1.4115*	**−2.1701**
0	**−0.5142**	**0.0580**	*0.8899*	**−0.0307**
5	**1.6661**	**2.4913**	*2.9617*	**2.1659**
10	**3.5242**	**5.0128**	*5.3739*	**4.4255**
15	**5.5958**	**8.6024**	*8.9245*	**7.7369**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 13: Results obtained from the computation of PESQ (signal 8 (female voice) corrupted by factory noise).

	PESQ			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**0.6882**	**0.5311**	*0.8818*	**0.7038**
0	**0.9916**	**0.9724**	*1.1770*	**1.0327**
5	**1.4558**	**1.6078**	*1.7891*	**1.5358**
10	**1.9024**	**2.1297**	*2.3493*	**2.1484**
15	**2.4498**	**2.6051**	*2.7664*	**2.6077**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 14: Results obtained from the computation of SNR (signal 2 (male voice) corrupted by Volvo noise).

	SNRf (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**4.5435**	**3.3737**	*5.4782*	**4.2192**
0	**8.3623**	**7.4176**	*9.9016*	**8.3451**
5	**12.4591**	**12.8324**	*14.4917*	**12.6024**
10	**16.1163**	**17.5726**	*18.9803*	**17.4120**
15	**18.1761**	**20.6149**	*22.9204*	**21.4578**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 15: Results obtained from the computation of SSNR (signal 2 (male voice) corrupted by Volvo noise).

	SSNR (*dB*)			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**−1.1159**	**−1.2951**	*−0.1793*	**−1.1347**
0	**1.2097**	**1.3262**	*2.9410*	**1.7861**
5	**4.0138**	**5.1028**	*5.9979*	**4.7166**
10	**6.8442**	**8.3857**	*9.1966*	**7.8228**
15	**9.5287**	**10.9227**	*12.4662*	**10.9850**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 16: Results obtained from the computation of PESQ (signal 2 (male voice) corrupted by Volvo noise).

	PESQ			
	The speech enhancement technique			
SNRi (*dB*)	Unsupervised speech denoising via perceptually motivated robust principal component analysis [23]	The speech enhancement technique based on *MSS-SMPO* [24, 25]	The proposed speech enhancement technique	The denoising technique based on *MMSE* Estimate of Spectral Amplitude [22]
−5	**2.3027**	**2.2235**	*2.5406*	**2.4021**
0	**2.6867**	**2.5464**	*2.8408*	**2.7163**
5	**3.0848**	**2.8339**	*3.1719*	**3.0184**
10	**3.3970**	**2.9781**	*3.4203*	**3.2461**
15	**3.5439**	**3.0602**	*3.6435*	**3.4789**

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

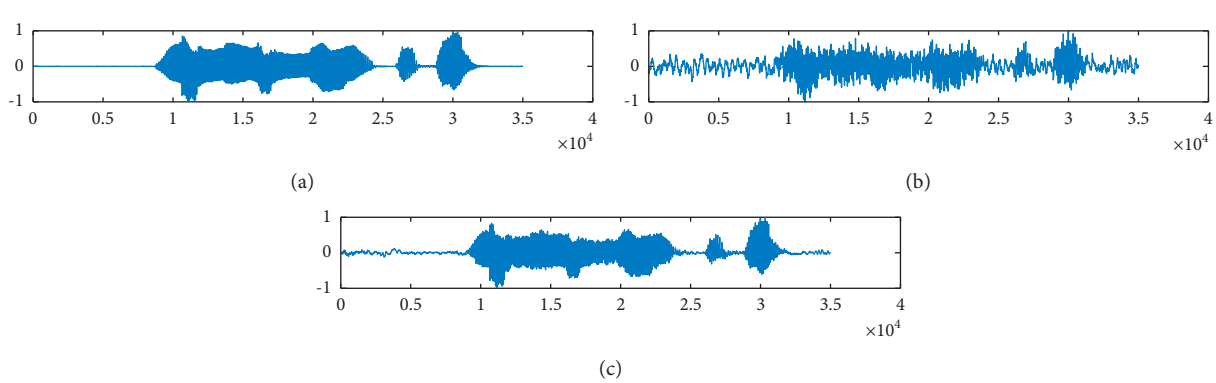


Figure 2: An example of speech enhancement applying the proposed speech enhancement approach. (a) Clean speech signal (male voice (signal 4)). (b) Noisy speech signal (clean signal degraded by additive car noise with $SNRi = 0\,dB$). (c) Enhanced speech signal with $SNRf = 13.2999$, $SSNR = 4.3802$, and $PESQ = 3.0888$.

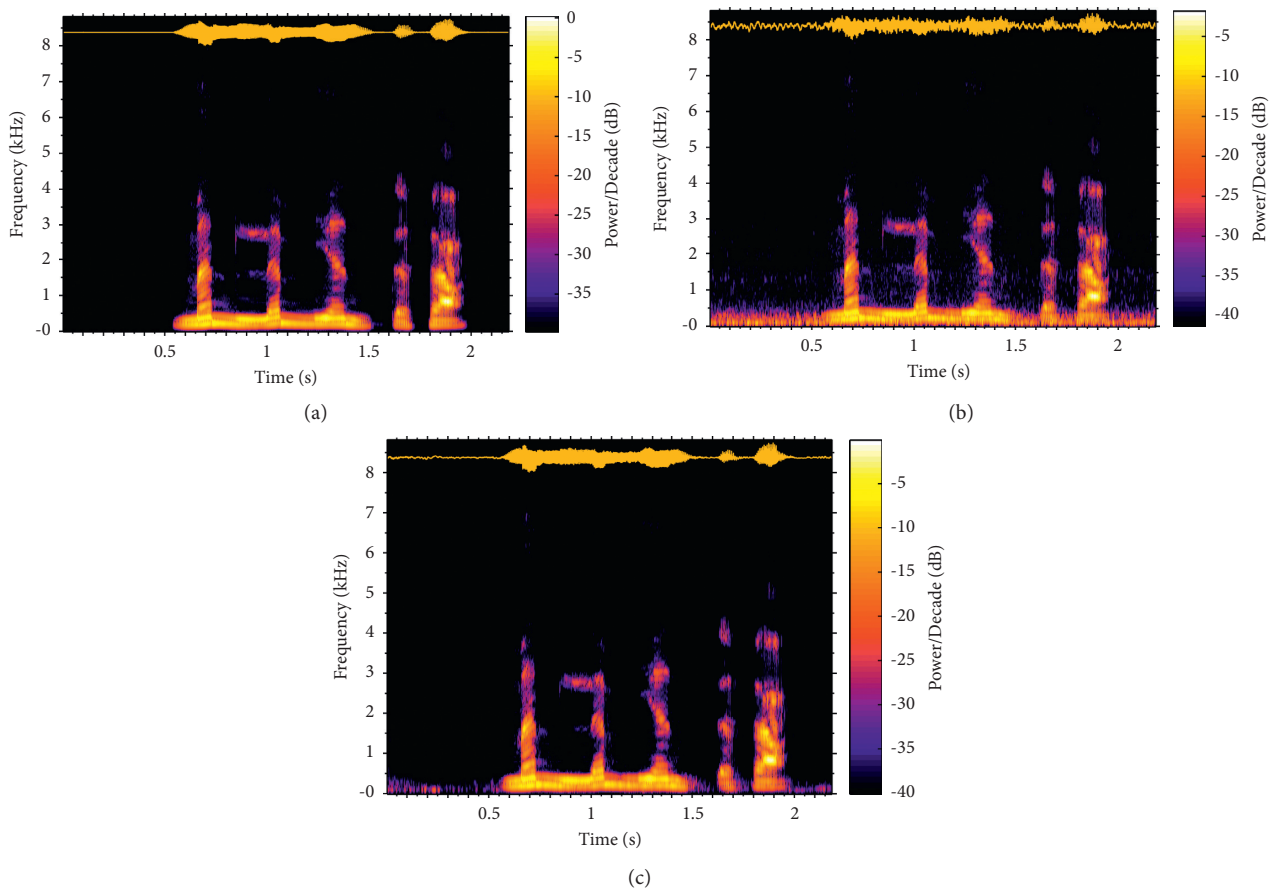


Figure 3: (a) The spectrogram of the clean speech signal (Figure 2(a)). (b) The spectrogram of the noisy speech signal (Figure 2(b)). (c) The spectrogram of the enhanced speech signal (Figure 2(c)).

Table 17: Results obtained from the computation of SNR (signal 2 (male voice) corrupted by Volvo noise).

SNRi (*dB*)	*SNRf* (*dB*) The speech enhancement technique	
	Speech enhancement based on *LWT* and *ANN* and using *MMSE* Estimate of Spectral Amplitude [26]	The proposed speech enhancement technique
−5	*5.8737*	**5.4782**
0	9.8414	*9.9016*
5	14.1647	*14.4917*
10	18.5308	*18.9803*
15	22.5102	*22.9204*

The bold values show the values obtained from the application of the proposed speech enhancement technique, and they are the best values.

Table 18: Results obtained from the computation of SSNR (signal 2 (male voice) corrupted by Volvo noise).

SNRi (*dB*)	*SSNR* (*dB*) The speech enhancement technique	
	Speech enhancement based on *LWT* and *ANN* and using *MMSE* Estimate of Spectral Amplitude [26]	The proposed speech enhancement technique
−5	**0.2145**	−0.1793
0	2.7478	**2.9410**
5	5.6644	**5.9979**
10	8.8942	**9.1966**
15	11.9663	**12.4662**

The bold values are the best values: for the SNRi values, 0, 5, 10, and 15 dB, these best values are obtained from the application of the proposed speech enhancement technique.

Table 19: Results obtained from the computation of PESQ (signal 2 (male voice) corrupted by Volvo noise).

SNRi (*dB*)	*PESQ*	
	The denoising approach	
	Speech enhancement based on *LWT* and *ANN* and using *MMSE* Estimate of Spectral Amplitude [26]	The proposed speech enhancement technique
−5	2.2837	*2.5406*
0	2.5999	*2.8408*
5	2.8709	*3.1719*
10	3.1190	*3.4203*
15	3.3590	*3.6435*

present the results obtained from the computation of SNR, SSNR, and PESQ for the two techniques.

According to these tables, the best results are the values in italics and they are obtained from the application of the proposed technique. Therefore, this technique outperforms the other speech enhancement approach proposed in [26].

4. Conclusion

In this paper, we propose a new speech enhancement technique based on *SBWT* and *MMSE* Estimate of Spectral Amplitude. In the first step of this technique, the SBWT is applied to the noisy speech signal for obtaining eight noisy stationary bionic wavelet coefficients. The denoising of each of those coefficients is performed through the application of the denoising approach based on MMSE Estimate of Spectral Amplitude. Finally, the inverse of $SBWT$ ($SBWT^{-1}$) is applied to the obtained stationary wavelet coefficients, for obtaining the enhanced speech signal. An evaluation of this technique is performed by its comparison with four other speech enhancement approaches where the first one is the denoising technique based on MMSE Estimate of Spectral Amplitude. The second one is the speech enhancement technique based on MSS-SMPO. The third one is the unsupervised speech denoising approach through perceptually motivated robust principal component analysis. The fourth one is the speech enhancement technique based on *LWT* and ANN and using *MMSE* Estimate of spectral amplitude. This evaluation is performed through the computations of Signal to Noise Ratio (SNR), the Segmental SNR (SSNR), and the Perceptual Evaluation of Speech Quality (PESQ). The results obtained from these computations show that the proposed technique outperforms the other previously mentioned techniques. Furthermore, the technique proposed in this work permits to considerably reduce the noises corrupting the clean speech signal and to have an enhanced speech signal with good perceptual quality.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] S.-K. Lee, S.-S. Wang, T. Yu, and J.-W. Hung, "Speech enhancement based on reducing the detail portion of speech spectrograms in modulation domain via Discrete wavelet transform," in *Proceedings of the 2018 11th International Symposium on Chinese Spoken Language Processing (ISCSLP)*, Taipei City, Taiwan, November 2018.

[2] S. Boll, "Suppression of acoustic noise in speech using spectral subtraction," *IEEE Transactions on Acoustics, Speech, & Signal Processing*, vol. 27, no. 2, Article ID 113120, 1979.

[3] M. Berouti, R. Schwartz, and J. Makhoul, "Enhancement of speech corrupted by acoustic noise," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 208–211, Washington, D. C., USA, April 1979.

[4] S. Kamath and P. Loizou, "A multi-band spectral subtraction method for enhancing speech corrupted by colored noise," in *Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing*, Orlando, Florida, USA, May 2002.

[5] C. Plapous, C. Marro, and P. Scalart, "Improved signal-to-noise ratio estimation for speech enhancement," *IEEE Transactions on Audio Speech and Language Processing*, vol. 14, no. 6, Article ID 20982108, 2006.

[6] P. Scalart and J. V. Filho, "Speech enhancement based on a priori signal to noise estimation," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 629–632, Atlanta, GA, USA, June 1996.

[7] Y. Ephraim and D. Malah, "Speech enhancement using a minimum-mean square error short-time spectral amplitude estimator," *IEEE Transactions on Acoustics, Speech, & Signal Processing*, vol. 32, no. 6, Article ID 11091121, 1984.

[8] Y. Ephraim and D. Malah, "Speech enhancement using a minimum mean-square error log-spectral amplitude estimator," *IEEE Transactions on Acoustics, Speech, & Signal Processing*, vol. 33, no. 2, pp. 443–445, 1985.

[9] S. Srinivasan, J. Samuelsson, and W. Kleijn, "Codebook driven short-term predictor parameter estimation for speech enhancement," *IEEE Transactions on Audio Speech and Language Processing*, vol. 14, no. 1, Article ID 163176, 2006.

[10] D. Y. Zhao and W. B. Kleijn, "HMM-based gain modeling for enhancement of speech in noise," *IEEE Transactions on Audio Speech and Language Processing*, vol. 15, no. 3, Article ID 882892, 2007.

[11] K. K. Paliwal, K. K. Wojcicki, and B. Schwerin, "Single-channel speech enhancement using spectral subtraction in the short-time modulation domain," *Speech Communication*, vol. 52, no. 5, pp. 450–475, 2010.

[12] C.-C. Hsu, K.-M. Cheong, J.-T. Chien, and T.-S. Chi, "Modulation Wiener filter for improving speech intelligibility," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 370–374, Queensland, Australia, April 2015.

[13] S. So and K. K. Paliwal, "Modulation-domain Kalman filtering for single-channel speech enhancement," *Speech Communication*, vol. 53, no. 6, pp. 818–829, 2011.

[14] O. Rioul and M. Vettertui, *Wavelets and Signal Processing*, Springer, Berlin Heidelberg, Germany, 1991.

[15] S. G. Chang, B. Bin Yu, and M. Vetterli, "Adaptive wavelet thresholding for image denoising and compression," *IEEE Transactions on Image Processing*, vol. 9, no. 9, pp. 1532–1546, 2000.

[16] S.-S. Wang, P. Lin, Y. Tsao, J.-W. Hung, and B. Su, "Suppression by selecting wavelets for feature compression in distributed speech recognition," *IEEE/ACM Trans. on Audio, Speech, and Language Processing*, vol. 26, no. 3, pp. 564–579, 2018.

[17] D. Huang, K. Lanyan, B. Mi, G. Wei, J. Wang, and S. Wan, "A cooperative denoising algorithm with interactive dynamic adjustment function for security of stacker in industrial internet of things," *Hindawi, Security and Communication Networks*, vol. 2019, Article ID 4049765, 16 pages, 2019.

[18] M. Ali Nematollahi, C. Vorakulpipat, and H. G. Rosales, "Optimization of a blind speech watermarking technique against amplitude scaling," *Hindawi, Security and Communication Networks*, vol. 2017, Article ID 5454768, 13 pages, 2017.

[19] T. Mourad, "Speech enhancement based on stationary bionic wavelet transform and maximum a posterior estimator of magnitude-squared spectrum," *International Journal of Speech Technology*, vol. 20, no. 1, pp. 75–88, 2017.

[20] M. Talbi and M. S. Bouhlel, "A novel approach of speech enhancement based on SBWT and MMSE estimate of spectral amplitude," in *Proceedings of the 2020 4th International Conference on Advanced Systems and Emergent Technologies (IC_ASET)*, Hammamet, Tunisia, March 2020.

[21] M. Talbi, "New approach of ECG denoising based on 1-D double-density complex DWT and SBWT," *Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization*, vol. 8, no. 6, pp. 608–620, 2020.

[22] T. Gerkmann and C. H. Richard, "Unbiased MMSE-based noise power estimation with low complexity and low tracking delay," *IEEE Transactions on Audio Speech and Language Processing*, vol. 20, no. 4, pp. 1383–1393, 2012.

[23] G. Min, X. Zou, W. Han, X. Zhang, and W. Tan, "Unsupervised speech denoising via perceptually motivated robust principal component analysis," *Shengxue Xuebao/Acta Acustica*, vol. 42, no. 2, pp. 246–256, 2017.

[24] Y. Lu and P. C. Loizou, "Estimators of the magnitude-squared spectrum and methods for incorporating SNR uncertainty," *IEEE Transactions on Audio Speech and Language Processing*, vol. 19, no. 5, pp. 1123–1137, 2011.

[25] M. T. Islam, A. Asaduzzaman, C. Shahnaz, W. P. Zhu, and M. O. Ahmad, "Speech enhancement in adverse environments based on non-stationary noise-driven SpectralSubtraction and SNR-dependent phase compensation," arXiv preprint https://arxiv.org/abs/1803.00396, 2018.

[26] M. Talbi, R. Baazaoui, and M. Salim Bouhlel, "Speech enhancement based on LWT and artificial neural Network and using MMSE estimate of spectral amplitude," *Deep Learning Applications*, 2021.

[27] T. Chen, N. Kapron, and J. C.-Y. Chen, "Using evolving ANN-based algorithm models for accurate meteorological forecasting applications in vietnam," *Hindawi, Mathematical Problems in Engineering*, vol. 2020, Article ID 8179652, 8 pages, 2020.

[28] E. Vilavicencio-Arcadia, S. G. Navarro, S. G. Navarro et al., "Application of artificial neural networks for the automatic spectral classification," *Hindawi Mathematical Problems in Engineering*, vol. 2020, Article ID 1751932, 15 pages, 2020.

[29] K.-C. Yang, C. Yang, P.-Y. Chao, and Po-H. Shih, "Applying artificial neural Network to predict semiconductor machine outliers," *Hindawi Publishing Corporation Mathematical Problems in Engineering*, vol. 2013, Article ID 210740, 10 pages, 2013.

[30] B. Ramesh Murlidhar, R. K. Sinha, E. T. Mohamad, R. Sonkar, and M. Khorami, "The effects of particle swarm optimisation and genetic algorithm on ANN results in predicting pile bearing capacity," *International Journal of Hydromechatronics*, vol. 3, no. 1, p. 69, 2020.

[31] M. Safa, M. Ahmadi, J. Mehrmashadi et al., "Selection of the most influential parameters on vectorial crystal growth of highly oriented vertically aligned carbon nanotubes by adaptive neuro-fuzzy technique," *International Journal of Hydromechatronics*, vol. 3, no. 3, p. 238, 2020.

[32] C. Zhu, W. Yan, X. Cai, S. Liu, T. H. Li, and G. Li, "Neural saliency algorithm guide bi-directional visual perception style transfer," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 1–8, 2020.

[33] T. Sangeetha and G. Mary Amalanathan, "Outlier detection in neutrosophic sets by using rough entropy based weighted density method," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 2, pp. 121–127, 2020.

[34] Z. Ali and T. Mahmood, "Complex neutrosophic generalised dice similarity measures and their application to decision making," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 2, pp. 78–87, 2020.

[35] T. Goehring, F. Bolner, J. J. M. Monaghan et al., "Speech enhancement based on neural networks improves speech intelligibility in noise for cochlear implant users," *Hearing Research*, vol. 344, pp. 183–194, 2017.

[36] R. Birok, R. Kapoor, and M. Singh Choudhry, "ECG denoising using artificial neural networks and complete ensemble empirical mode decomposition," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 2, pp. 2382–2389, 2021.

[37] J. Llombart, D. Ribas, A. Miguel, L. Vicente, A. Ortega, and E. Lleida, "Progressive loss functions for speech enhancement with deep neural networks," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2021, no. 1, 2021.

[38] P. Karjol, M. Ajay Kumar, and P. K. Ghosh, "Speech Enhancement Using Multiple Deep Neural Networks," in *Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Canada, April 2018.

[39] H. Tasmaz and E. Erc¸elebi, "Speech enhancement based on undecimated wavelet packet-perceptual filterbanks and MMSE– STSA estimation in various noise environments," *Digital Signal Processing*, vol. 18, no. 5, pp. 797–812, 2008.

[40] Y. Ephraim and D. Malah, "Speech enhancement using a minimum-mean square error short-time spectral amplitude estimator," *IEEE Transactions on Acoustics, Speech, & Signal Processing*, vol. 32, no. 6, pp. 1109–1121, 1984.

[41] A. Biswas, P. K. Sahu, A. Bhowmick, and M. Chandra, "Feature extraction technique using ERB like wavelet subband periodic and aperiodic decomposition for TIMIT phoneme recognition," *International Journal of Speech Technology*, vol. 17, no. 4, pp. 389–399, 2014.

[42] S. Singh and A. M. Mutawa, "A wavelet-based transform method for quality improvement in noisy speech patterns of Arabic language," *International Journal of Speech Technology*, vol. 19, no. 4, pp. 677–685, 2016.

[43] M. Bahoura and J. Rouat, "Wavelet speech enhancement based on time-scale adaptation," *Speech Communication*, vol. 48, no. 12, pp. 1620–1637, 2006.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9984453, 10 pages
https://doi.org/10.1155/2021/9984453

Research Article

A Cost-Efficient Autonomous Air Defense System for National Security

Fazle Rabby Khan,[1] **Md. Muhabullah**,[1] **Roksana Islam**,[1] **Mohammad Monirujjaman Khan**,[1] **Mehedi Masud**,[2] **Sultan Aljahdali**,[2] **Avinash Kaur**,[3] **and Parminder Singh**[3]

[1]*Electrical and Computer Engineering Department, North South University, Dhaka 1229, Bangladesh*
[2]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[3]*School of Computer Science and Engineering, Lovely Professional University, Phagwara, India*

Correspondence should be addressed to Mehedi Masud; mmasud@tu.edu.sa

Received 22 March 2021; Revised 16 May 2021; Accepted 18 June 2021; Published 25 June 2021

Academic Editor: Jialiang Peng

In a country, air defense systems are designed to reduce threats efficiently. An air defense system is a fundamental part of any country because it provides national security. This study presents an autonomous air defense system (AADS) development that will automatically detect aerial threats (e.g., drones) and target them without any human intervention. The AADS is implemented using radar, camera, and laser gun. The radar system dynamically emits microwaves and detects moving objects around it. It triggers the camera system if it senses the frequency of any aerial threat. The camera receives the radar's signal and detects using a neural network algorithm whether it is a threat or not. Neural network algorithms are used for the detection and classification of objects. The laser gun locks its target if the live video feed classifies an object as a more than 75% threat. In the detection stage, an average loss of 0.184961 was achieved using YOLOv3 and 0.155 using the Faster-RCNN. This system will ensure that no human errors are made while detecting threats in a region and improve national safety.

1. Introduction

The autonomous air defense system (AADS) is an integrated defensive unit capable of detecting aerial threats and reducing the manpower needed to defend the country. Currently, Bangladesh military uses tanks, armored vehicles, artillery, and rocket projectors for defense. These require a lot of human resources and training, which are costly and inefficient, respectively. At present, military personnels are facing several problems due to the existing defense system's rigidity. Most importantly, tanks, artilleries, and other machines require around three to four people to use [1]. It is expensive as it needs training and it is inefficient as well. Additionally, the people who operate these machines can go through many disturbances depending on the area, and aerial threats are harder to target since they are moving objects. As a result, the chance of human errors may increase to a great extent while shooting the targets. Last, to cope with the latest electronic warfare, the autonomous air defense system is a must for national security.

We need this system to compete with global defense industries as it is currently being deployed in other countries. Also, this system can be exported to other countries and increase foreign exchange. This system can be deployed in frigates, tanks, towers, or even aircraft to block incoming hits.

According to Figure 1, there have been an increasing number of internal and internationalized conflicts [2]. Also, it can be seen that battle-related deaths were a bit less during 2010 but had a sudden increase around 2016 [2]. An internal conflict is regarded as internationalized if one or more third-party governments are involved with combat personnel

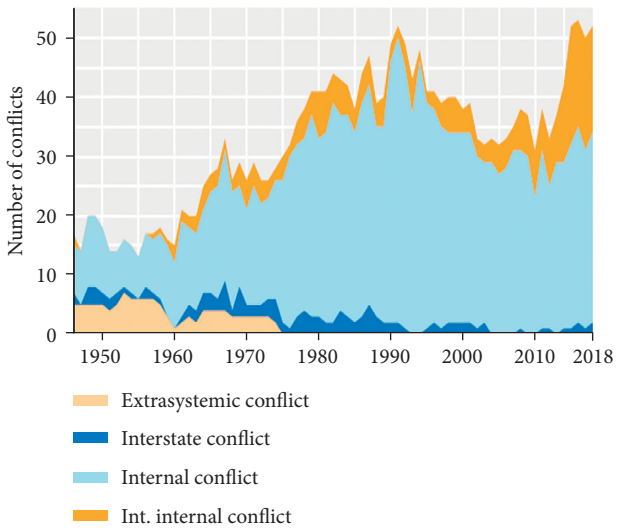


Figure 1: Number of national and international conflicts.

supporting the objective of either side [2]. From the research, it is also evident that countries are only increasing the number of troops sent to other countries for battling conflicts. It shows urgency for Bangladesh to find efficient ways to prevent these conflicts [2] and the importance of an automated system to handle this situation.

The study is organized as follows: Section 2 describes the existing works related to the AADS. Section 3 presents methods which include procedures and algorithms for training and detection. Section 4 describes the result and analysis, and Section 5 presents the conclusion.

2. Related Works

At the moment, all defense systems have manual controls over the systems. Eventhough many sensors and radars are used for detection now, there are fewer implementations of systems with cameras locating the targets and automatically firing them by image processing.

In [3], thermal cameras and acoustic sensors are used to detect and track drones automatically. Sensor fusion has been used to make the system more robust and avoid false detection, but they did not use any deep learning methods. The study by Unlu et al. [4] presents YOLO convolutional neural network-based autonomous drone surveillance and tracking architecture. Thermal images are used to classify drones into 4 categories (drone, bird, plane, and background). In [5], synthetic radar data and real image data are used to track a moving target. Tracking performance is improved using data fusion and agile edge processing. In [6], PTZ (pan, tilt, zoom) camera and optical and thermal sensors are used to detect boats. YOLOv3 is used on the COCO dataset for detecting boats. In [7], YOLOv3 and Faster-RCNN are used to detect power transmission towers. Also, this study indicates that Faster-RCNN has better detection performance, and YOLOv3 has better detection speed which can be used in real-time object detection [7]. In [8], a dual camera is used to develop a multiple target zooming system. Cameras used for this system are wide-view cameras and ultrafast mirror drive pan-tilt cameras [8].

In [9], turrets on the tanks can be controlled via eye movements and blinking. Images of the eyes are taken as controls, so that four people are no longer needed, and it is easier to control the system. In [10], camera surveillance is used to look for targets, and remote controls are used to target the threats. Lots of kinematics are used in this system. In [11], an automatic detection of the target using a camera at the gun's point is proposed. They use image processing techniques to detect targets from a distance from pictures that the gun points to. In [12], a very similar proposal for automatically detecting missiles using image processing and targeting aerial threats is proposed. The study by Anwar et al. [13] is the most recent study that proposes an automatic targeting system for gun turrets using deep learning methods.

The last system that was proposed did not have any automatic detection of nearby objects. It still needs manually moving the camera towards the target for detection. Our system proposes a radar that detects any nearby moving objects. The camera will automatically point towards the target for detection and verify whether the target is a drone or not.

The authors in [14–16] illustrates that secure data replicas in distributed management of identity and authorization policies in smart city applications can be mitigated by blockchain technology. In [15], a novel algorithm using synergetic neural networks to ensure the robustness and security of digital image watermarking is proposed. In [17], an innovative infrastructure of secure scenario combining Internet of Things (IoT) with cloud computing which operates in a wireless-mobile 6G network for managing big data on smart buildings is proposed. Authors in [18, 19] focus on the security architecture of the Internet of Things (IoT). Radio frequency identification (RFID) and wireless sensor network (WSN) can be the enabling factors in IoT development. In [20], the multifeature fusion paradigm of images is presented and helps describe the image pattern more clearly. The study [21] shows that if digital fingerprint image quality degrades to a certain level, it decreases the fingerprint recognition accuracy. Unlike fingerprint recognition accuracy, the object detection accuracy of YOLOv3 depends on how much area the object covers in a particular image. In [22], four-image encryption scheme is proposed as an image encryption technique that can protect users' privacy in online platforms such as cloud computing or social networks.

This study focuses on building autonomous air defense systems combining deep learning methods alongside a cheap camera and microwave sensors. The performance between the Faster-RCNN and YOLOv3 has been considered, and the real-time detection speed is given the most priority. Microwave radar sensors are used for the early detection of drones.

3. Method and Methodology

The AADS is a system that would provide safety from incoming aerial threats (e.g., drones) by locking targets. This device would detect and classify incoming aerial intruders by

image processing, lock multiple targets at a time, and shoot sequentially nearby threats. The area coverage by the AADS will be 360 degrees. This device will work in a short range (20 meters) and can also be used for a particular area or building's safety system.

3.1. Procedure. At first, a radar system will be integrated by the radar modules for getting early warnings to the system and direction. This custom radar system can detect aerial movement. After the detection, our camera and gun/laser will be activated and turned in that direction. Only drones will be classified and detected for this device and will not point to innocent birds, humans, or any natural beings. The device will check whether the classified object is a drone or not. When this device detects and classifies the drone, the target will be locked. Finally, a laser gun will point/fire the moving drones. The operation of the AADS is shown as a flowchart in Figure 2.

We used an HB100 X-band microwave sensor and an RCWL-0516 microwave radar sensor module, as shown in Figure 3. RCWL-0516 radar module only gave the result of the detected object. However, we needed a radar module to determine the frequency of moving objects. From HB100, we got the frequency of moving objects.

The pi camera has been used for drone detection and classification. This camera can be used to take pictures for image processing and identify whether the object is a drone or not. For moving the camera and laser, we have used 2 servo motors. One is used to rotate horizontally, and the other is used to rotate vertically. Therefore, the coverage area of the AADS will be 360 degrees.

3.2. YOLO (You Only Look Once) Algorithm. The AADS uses the YOLOv3 algorithm for drone detection and classification. The architecture of the YOLOv3 algorithm is shown in Figure 4. For feature extraction, we have used Darknet-53. It has 53 convolutional layers, which is an improved version of YOLOv2, Darknet-19. 1×1 and 3×3 convolutional layers are used in YOLOv3. At first, it resizes the image, then runs a convolutional neural network (CNN) to an image, and at the end, the resulting detection is constrained by the confidence of the model [24]. Batch normalization and stride-2 convolutions are used in YOLOv3. Inputs are normalized by batch normalization within the deep network [23]. In filter size $3 \times 3/2$, here "/2" is represented by stride-2. It basically resizes the input into half. For example, if the input size is 256×256, then the output size will be 128×128.

For bounding box prediction, 4 coordinates are used to predict for each bounding box. Coordinates for each bounding boxes are t_x, t_y, t_w, t_h. The cell in which the bounding box's center falls is offset from the top left corner of the image by (c_x, c_y) [23]. The width and height of the bounding box are calculated by k-means which are p_w and p_h. b_x, b_y, b_w, b_h are the actual coordinates of the prediction bounding box, which can be determined using the formula:

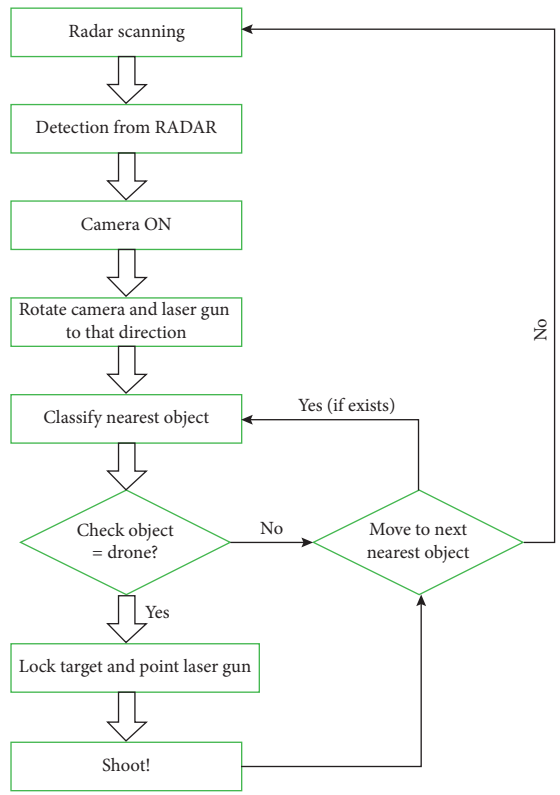
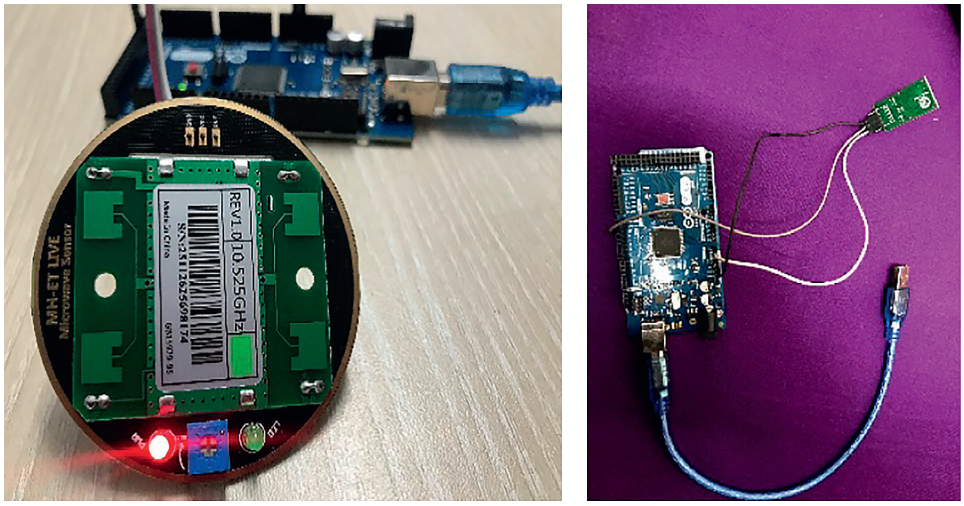


Figure 2: Flowchart of the AADS.

$$\begin{aligned} b_x &= \sigma(t_x) + c_x, \\ b_y &= \sigma(t_y) + c_y, \\ b_w &= p_w e^{t_w}, \\ b_h &= p_h e^{t_h}. \end{aligned} \tag{1}$$

3.3. Faster-RCNN. The Faster-RCNN [25] is a state-of-the-art object detection algorithm that is based on deep neural networks. In recent years, it is used widely because of its efficiency, taking less time for testing, and better performance. For the AADS, the Faster-RCNN is also used for real-time object detection for fast detection of drones. The Faster-RCNN is an improvisation of the Fast-RCNN [26], which had a computational bottleneck in the region proposal network (RPN). The RPN is the first stage of the RCNN [27], where regions of an object could be found which is also known as regions of interest (ROI). Then, features are extracted using different architectures (VGG or ResNet) of convolutional neural networks (CNN). The architecture used in this system for detecting drones is the Faster-RCNN ResNet-50 FPN, consisting of 50 layers [28, 29]. Figure 5 shows the Faster-RCNN architecture. The ROI pooling layer is the classification process and takes as input the region of interests and convolutional features. It generates a bounding box of the objects as well as their class names.



(a) (b)

Figure 3: Microwave radar sensor module. (a) HB100 X-band microwave sensor. (b) RCWL-0516 microwave radar sensor module.

	Type	Filters	Size	Output
	Convolutional	32	3 × 3	256 × 256
	Convolutional	64	3 × 3/2	128 × 128
1×	Convolutional	32	1 × 1	
	Convolutional	64	3 × 3	
	Residual			128 × 128
	Convolutional	128	3 × 3/2	64 × 64
2×	Convolutional	64	1 × 1	
	Convolutional	128	3 × 3	
	Residual			64 × 64
	Convolutional	256	3 × 3/2	32 × 32
8×	Convolutional	128	1 × 1	
	Convolutional	256	3 × 3	
	Residual			32 × 32
	Convolutional	512	3 × 3/2	16 × 16
8×	Convolutional	256	1 × 1	
	Convolutional	512	3 × 3	
	Residual			16 × 16
	Convolutional	1024	3 × 3/2	8 × 8
4×	Convolutional	512	1 × 1	
	Convolutional	1024	3 × 3	
	Residual			8 × 8
	Avgpool		Global	
	Connected		1000	
	Softmax			

Figure 4: Architecture of Darknet-53.

3.4. Training and Detection. The dataset collected of drones consists of 1359 images from the Kaggle dataset [30]. Then, those images were labeled into ".txt" format using "labeling" for the YOLOv3 algorithm. At first, a pretrained coco model was fetched for built-in classes (in total, 80 classes). Then, a custom object detector for drone detection was trained in "Google Colab." This custom object detector model was built for one class (drone). Also, 2000 iterations were completed for the drone class.

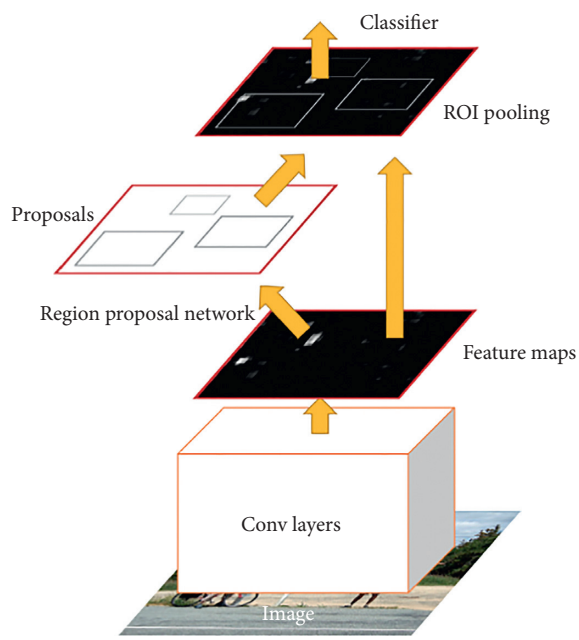


Figure 5: Faster-RCNN network.

4. Result and Analysis

The AADS was tested on 20% of total image data, completely different from the training dataset. We achieved a low average loss of 0.184961 for our custom object (drone) detector using the YOLOv3 algorithm. Loss is defined as a bad prediction in image processing. The number of losses indicates the bad prediction in every image. A training model has an overfitting problem when the loss is zero. A high value of loss also causes errors in prediction. Therefore, the value of loss should be close to zero. "Google Colab" has been used

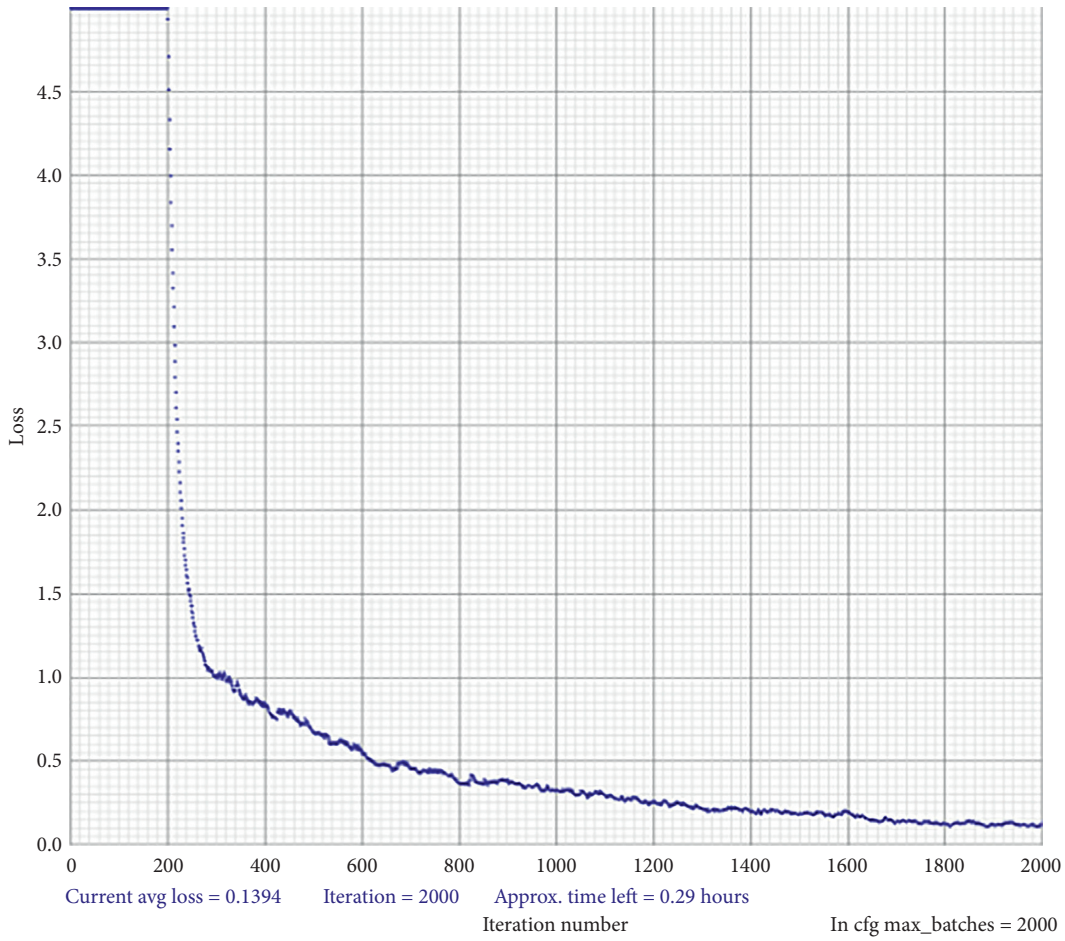


Figure 6: Loss chart for YOLOv3. The overall loss was 0.18496.

to train the model. During the training period, we generated the graph of loss dynamically in "Google Colab." The total loss chart for the YOLOv3 algorithm is shown in Figure 6. Initially, the loss was 5. After 2000 completed iterations, the loss dropped from 5 to 0.1 (approximately).

A Faster-RCNN algorithm was also applied to our dataset to compare the result between YOLOv3 and Faster-RCNN. Again, the AADS was tested on 20% different image data, and it achieved a low average loss of 0.155 for the custom object (drone) detector. Initially, the loss was 0.151, and the final loss was 0.155. The total loss chart is shown in Figure 7.

From Figures 6 and 7, we can see that the Faster-RCNN has better detection performance than YOLOv3. But for real-time moving objects, YOLOv3 is faster. Therefore, we chose the model of YOLOv3 for the AADS over the Faster-RCNN. The AADS was able to detect and classify drones and lock the target successfully, as shown in Figure 8. The rotation of servos towards the X-axis and Y-axis was also tested. The AADS was able to move in any direction using servos and track moving drones towards it. The custom drone detector model was tested using test image data, and it can classify drones successfully in Figure 8.

The two radar modules HB100X and RCWL-0516 detect using the Doppler radar principle [31, 32]. Both of them have different detection distances. HB100X can sense 2–16 meters and RCWL-0516 can sense 5–7 meters [31, 32]. These two modules were used in parallel to get the absolute moving object's data. RCWL-0516 sets a Boolean variable TRUE, and HB100X measures the distance and velocity of its target if any object passes through within range. These values are generated by the following Doppler equation

$$F_d = 2V\left(\frac{F_t}{c}\right)\operatorname{Cos}\theta, \tag{2}$$

where F_d stands for the Doppler frequency, V is the velocity of the target, F_t stands for the transmitting frequency, c is the speed of light (3×10^8 m/sec), and θ is the angle between the moving target direction and the axis of the module [33]. Transmit frequency (F_t) for HB100 is 10.525 GHz. We calculated the speed by using the frequency received from HB100. The following equations (equations (3) and (4)) are used to calculate the speed.

$$\text{speed}\left(\frac{km}{h}\right) = \frac{hz}{19.49}, \tag{3}$$

$$\text{speed}\left(\frac{m}{h}\right) = \frac{hz}{31.36}. \tag{4}$$

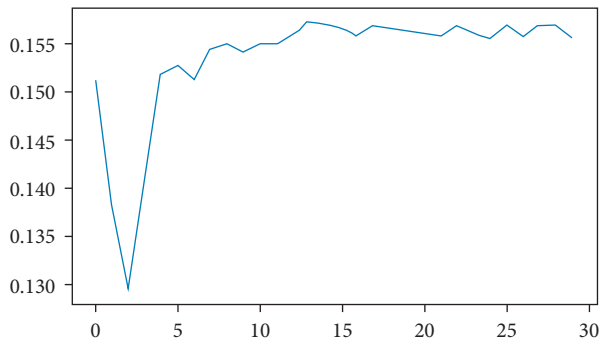


Figure 7: Loss chart for the Faster-RCNN. The overall loss was 0.155.

(a) (b)

Figure 8: (a) Drone detection using YOLOv3. (b) Drone detection using the Faster-RCNN.

The radar system is smart enough to work efficiently. It ignores the output if the object's velocity is between 20 and 30 mph as it is the average velocity of birds [34].

From RCWL-0516, we got the output that only detects the movement. For any object moving towards its range (5–9 m), the radar module can easily detect moving objects. Figure 9 shows the output received from the RCWL-0516 microwave radar sensor module.

Similarly, from the HB100 X-band microwave sensor, we got the detected drone's output and the measured Doppler frequency. Figure 10 shows the output received from the HB100 radar module. (2) and (3) are used to calculate the speed of moving drones.

The purpose of using these radar modules (RCWL-0516 and HB100) is to get an early warning of moving aerial threats. In the AADS, radar received signals from moving objects, and then, the camera and laser gun started their function. The camera was used to classify the object, whether it was a drone or not. The camera and the laser get activated only after getting the positive signal from the radar system. So, the AADS does not need to turn the camera and laser on all the time. The radar modules we used were very cheap and required less power to run compared to the camera and laser. Thus, the AADS can provide all-time security with less power which indicates less cost. As the camera remained off during its idle period, the life span of the AADS will also increase. Table 1 provides the comparison with other articles.

The AADS was built with a pan-tilt kit. The laser and camera were connected on the top of the frame, connected with a Y-axis rotating servo (horizontal). The X-axis servo was connected vertically, which allowed the upper portion of the AADS to move right or left. Radar modules were connected with Raspberry Pi. The AADS is shown in Figure 9.

Some drones are built using electric motors and plastic. We could have used the thermal camera for detection in the AADS as shown in Figures 11 and 12. But in the case of detecting plastic drones, it will not be effective. The competency of small drones is increasing, which is alarming. Drones are nowadays integrated with cameras, infrared detectors, thermal detectors, and many smart sensors and are being used for surveillance and bombing. It is difficult to maintain privacy in the drone-filled age. Competitors, thieves, or even just neighbors could be spying on every move using a remote-controlled flying camera. All these kinds of problems can be prevented using the AADS. The AADS is able to detect the smallest drones within its range

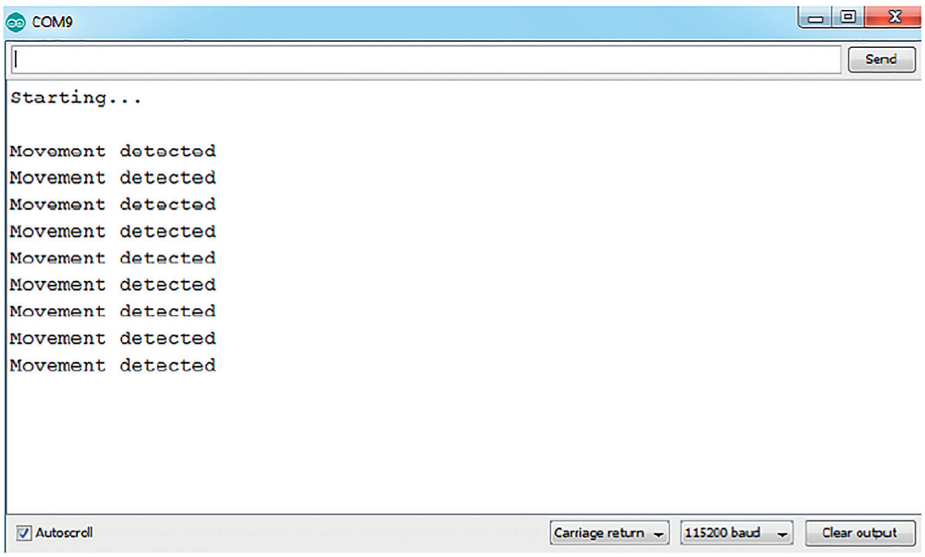


Figure 9: Output received from RCWL-0516.

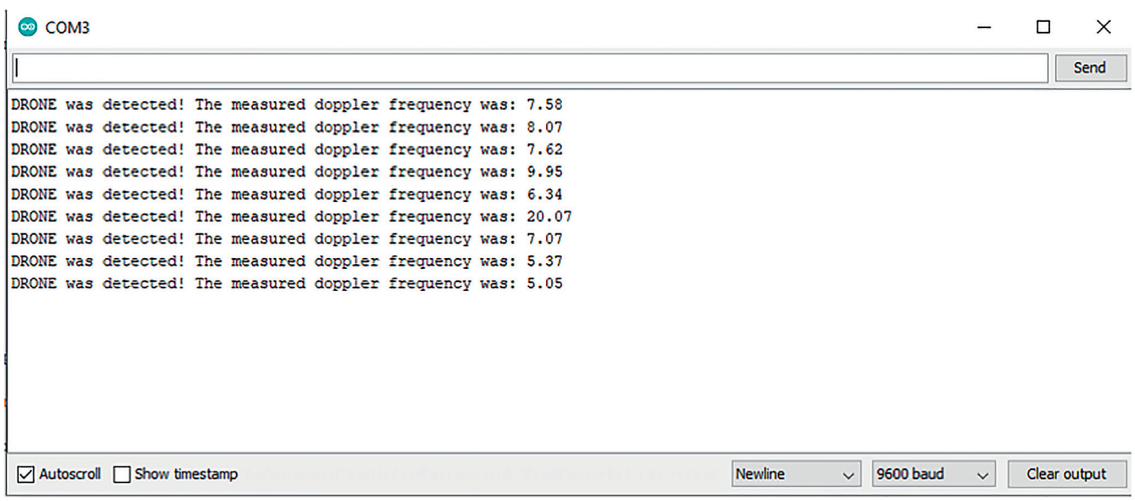


Figure 10: Output received from HB100 radar module.

Table 1: Comparison with other articles.

No.	Name	Sensors	Method	Deep learning	Images	Radar
1	This study	Camera HB100 RCWL-0516	YOLOv3 Faster-RCNN	Yes	RGB	Yes
2	Reference [3]	Camera Acoustic	Sensor fusion	No	Thermal	
3	Reference [4]	Camera	YOLO	Yes	Thermal	No
4	Reference [5]	Camera	Data fusion Agile edge processing	No	RGB	Synthetic radar data
5	Reference [6]	Camera Optical and thermal sensors	YOLOv3	Yes	Yes	No
6	Reference [7]	Camera	YOLOv3 Faster-RCNN	Yes	RGB	No

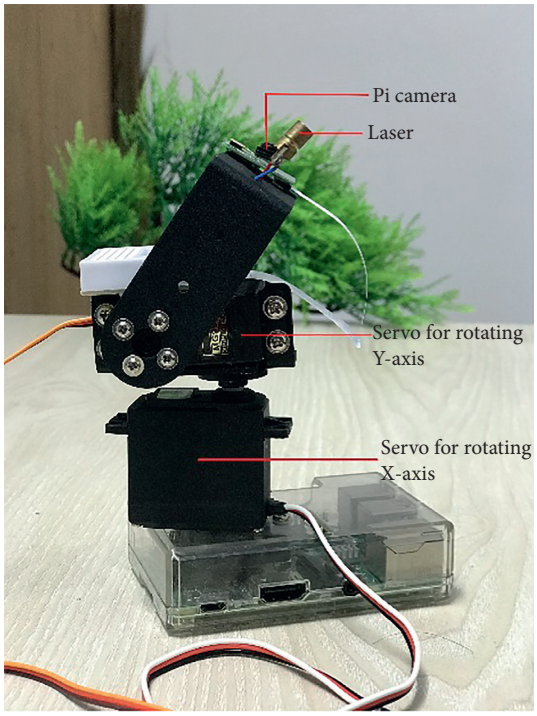


Figure 11: AADS (autonomous air defense system).

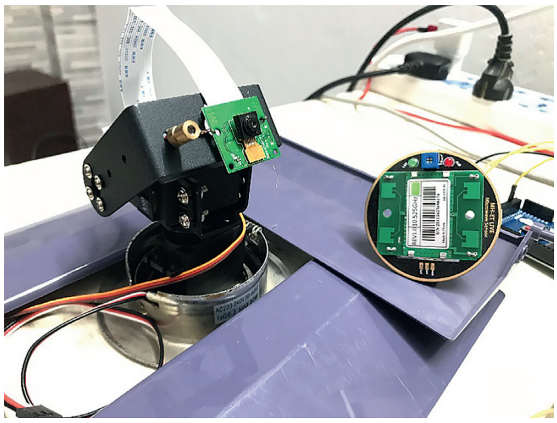


Figure 12: Main prototype of the AADS (autonomous air defense system).

and can be used as a strong defensive unit against surveillance drones. These drones are coated with plastic and stealthy materials which are difficult to detect for traditional radio wave radars. But that would not work if a drone is programmed to fly without radio uplinks and downlinks. Since we used microwave Doppler radar, detecting a movable object is our first task, and the camera is to determine whether it is a drone or not afterward. However, the old-fashioned Doppler radar is more effective against these stealth drones. Therefore, all kinds of mini drones, plastic drones, and drones coated with other elements (e.g., artificial leather) can be detected easily using this system.

5. Conclusion

The AADS is a modern technology that is very much needed in Bangladesh because of several efficiency and training problems. Recently, Bangladesh army tested their newly imported Swiss air defense system named Oerlikon Twin Gun GDF009 [35]. This defense system is similar to the AADS prototype from some standpoints such as hardware design, and the electronic components used are costly and as well as not fully automated because four persons are needed to operate this system. The cost of the AADS is only around 25,000 BDT. The cost is very low compared to the existing system such as Oerlikon Twin Gun because of the availability of parts and cheap Doppler modules.

However, to recover these problems and gain efficiency, the AADS prototype was developed to compete with global defense industries. To ensure national security, secure restricted areas from invasion, our AADS can be deployed. If we think economically, this system can save military expenses and be exported to earn substantial foreign currency. This system is also quite versatile as it can be deployed in different weapons such as frigates, tanks, and towers. Also, it can be used to predict the position of moving objects such as drones and planes. However, the most important fact about the AADS prototype is that it was developed with the current century's latest technologies. We used the YOLOv3 algorithm for detecting the target, which is considered one of the fastest detection algorithms, and it proved its efficiency compared to the Faster-RCNN for detecting real-time moving objects. The AADS is smarter than all other traditional air defense guns because of its autonomic activities, portability, and accuracy. We made this prototype version because of our low budget, and we hope to develop the original AADS with more innovative features in the future.

Data Availability

The data used to support the findings of this study are freely available at https://www.kaggle.com/dasmehdixtr/drone-dataset-uav.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank for the support from Taif University, Taif, Saudi Arabia, Taif University Researchers Supporting Project number (TURSP-2020/73).

References

[1] R. G. Vickers, "Gun turrets," 1967, https://patentimages.storage.googleapis.com/b9/7c/f9/43f8b6588314d4/US3348451.pdf In United States Patent Office [Online] Available:.

[2] R. Strand and N. Urdal, "Trends in armed conflict, 1946–2018," in *Conflict Trends 3-2019*PRIO, Oslo, Norway, 2019, https://www.prio.org/utility/DownloadFile.ashx?id=1858&type=publicationfile [Online]. Available:.

[3] F. Svanstrom, C. Englund, and F. Alonso-Fernandez, "Real-time drone detection and tracking with visible, thermal and acoustic sensors," in *Proceedings of the International Conference on Pattern Recognition (ICPR)*, Milan, Italy, January 2021.

[4] E. Unlu, E. Zenou, N. Riviere, and P. E. Dupouy, "An autonomous drone surveillance and tracking architecture," *IPSJ Transactions on Computer Vision and Applications*, vol. 11, pp. 1–13, 2019.

[5] P. Tsiantis, S. A. Purryag, and I. Kyriakides, "Target tracking using radar and image IoT nodes," in *Proceedings of the 16th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 418–422, Marina del Rey, CA, USA, May 2020.

[6] C. P. Simonsen, F. M. Thiesson, Ø. Holtskog, and R. Gade, "Detecting and locating boats using a PTZ camera with both optical and thermal sensors," in *Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics cs Theory and Appplications VISIGRAPP*, pp. 395–403, Valletta, Malta, February 2020.

[7] H. Wang, G. Yang, E. Li, Y. Tian, M. Zhao, and Z. Liang, "High-voltage power transmission tower detection based on faster R-CNN and YOLO-V3," in *Proceedings of the 2019 Chinese Control Conference (CCC)*, pp. 8750–8755, Guangzhou, China, July 2019.

[8] S. K. Sivanath, S. A. Muralikrishnan, P. Thothadri, and V. Raja, "Eyeball and blink-controlled firing system for military tank using labview," in *Proceeding of the 2012 4th InternationalConference on Intelligent Human Computer Interaction (IHCI)*, pp. 1–4, IEEE, Kharagpur, India, Decenber 2012.

[9] S. Hu, K. Shimasaki, M. Jiang, T. Takaki, and I. Ishii, "A dual-camera-based ultrafast tracking system for simultaneous multi-target zooming," in *Proceedings of the IEEE International Conference on Robotics and Biomimetics (ROBIO)*, pp. 521–526, Dali, China, December 2019.

[10] R. Bisewski and P. K. Atrey, "Toward a remote-controlled weapon equipped camera surveillance system," in *Proceedings of the Tools with Artificial Intelligence (ICTAI), 2011 23rd IEEE International Conference on*, pp. 1087–1092, IEEE, Boca Raton, FL, USA, November 2011.

[11] E. Iflachah, D. Purnomo, and I. A. Sulistijono, "Coil gun turret control using a camera," *EEPIS Final Project*, 2011.

[12] A. Garg and R. Raziur Rouf, K. N. Hafiz, M. Sharna, and N. Hasan, Automated detection, locking and hitting a fast moving aerial object by image processing (suitable for guided missile)," *IOSR Journal of Electronics and Communication Engineering*, vol. 11, no. 4, pp. 60–68, 2016.

[13] M. K. Anwar, A. Risnumawan, A. Darmawan, M. N. Tamara, and D. S. Purnomo, "Deep multilayer network for automatic targeting system of gun turret," in *Proceedings of the 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, pp. 134–139, Surabaya, Indonesia, September 2017.

[14] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Computers & Electrical Engineering*, vol. 93, 2021.

[15] D. Li, L. Deng, B. B. Gupta, H. Wang, and C. Chang, "A novel CNN based security guaranteed image watermarking generation scenario for smart city applications," *Information Sciences*, vol. 479, pp. 432–447, 2018.

[16] P. Singh, M. Masud, M. Shamim Hossain et al., "Cross-domain secure data sharing using blockchain for industrial IoT," *Journal of Parallel and Distributed Computing*, 2021, In press.

[17] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-based big data secure management in the fog over a 6G wireless network," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2021.

[18] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, 2021, inpress.

[19] M. Masud, G. S. Gaba, S. Alqahtani et al., "A lightweight and robust secure key establishment protocol for Internet of medical things in COVID-19 patients care," *IEEE Internet of Things Journal*, vol. 99, 2020.

[20] H. Wang, Z. Li, L. Yang, B. B. Gupta, and C. Chang, "Visual saliency guided complex image retrieval," *Pattern Recognition Letters*, vol. 130, pp. 64–72, 2020.

[21] M. A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh, and B. Gupta, "Impact of digital fingerprint image quality on the fingerprint recognition accuracy," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3649–3688, 2019.

[22] S. Ibrahim, H. Alhumyani, M. Masud et al., "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, Article ID 160433, 2020.

[23] A. Farhadi and R. Joseph, "Yolov3: an incremental improvement," in *Proceedings of the Computer Vision and Pattern Recognition*, Salt Lake, UT, USA, June 2018.

[24] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: unified,real-time object detection," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 779–788, Las Vegas, NV, USA, June 2016.

[25] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN Towards real-time object detection with region proposal networks," *In IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137–1149, 2017.

[26] R. Girshick, "Fast R-CNN," in *Proceedings of the 2015 IEEE International Conference on Computer Vision (ICCV)*, pp. 1440–1448, Santiago, Chile, December 2015.

[27] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Region-based convolutional networks for accurate object detection and segmentation," *In IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 38, no. 1, pp. 142–158, 2016.

[28] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN Towards real-time object detection with region proposal networks," in *Proceedings of the Neural Information Proceesing System*, vol. 1, pp. 91–99, Montreal, Canada, December 2015.

[29] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770–778, Las Vegas, NV, USA, June 2016.

[30] https://www.kaggle.com/dasmehdixtr/drone-dataset-uav Kaggle dataset. [Online].

[31] Spark Fruit Electronics, "HB100 X 10.525GHZ microwave sensor 2-16M Doppler radar human body induction switch module for arduino," 2020, https://sparkfruit.ph/product/mh-et-live-hb100-x-10-525ghz-microwave-sensor/ [online] Available:.

[32] T. K. Hareendran, "How to get started with a microwave radar motion sensor," [Online]. Available:https://www.electroschematics.com/get-started-microwave-radar-motion-sensor/, 2017.

[33] https://www.limpkin.fr/public/HB100/HB100_Microwave_Sensor_Application_Note.pdf AgilSense, 2020. [Online] Available:.

[34] E. Moore and C. Ryan, "How fast do birds fly? https://www.jaysbirdbarn.com/fast-birds-fly/ [Online]. Available:.

[35] Newsroom, "Skyguard anti-aircraft gun to boost bangladesh army's air defense capability," in *Bangladesh Army*Dhaka, Bangladesh[Online]. Available: https://bdnewsnet.com/bangladesh/bdmilitary/skyguard-anti-aircraft-gun-to-boost-bangladesh-armys-air-defense-capability, 2019.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 6653430, 14 pages
https://doi.org/10.1155/2021/6653430

Research Article

Detecting Abnormal Social Network Accounts with Hurst of Interest Distribution

Xiujuan Wang, Yi Sui, Yuanrui Tao, Qianqian Zhang, and Jianhua Wei

Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

Correspondence should be addressed to Yi Sui; 17864307856@163.com

Received 8 December 2020; Revised 19 May 2021; Accepted 27 May 2021; Published 9 June 2021

Academic Editor: Manjit Kaur

With the rapid development of the Internet since the beginning of the 21st century, social networks have provided a significant amount of convenience for work, study, and entertainment. Specifically, because of the irreplaceable superiority of social platforms in disseminating information, criminals have thus updated the main methods of social engineering attacks. Detecting abnormal accounts on social networks in a timely manner can effectively prevent the occurrence of malicious Internet events. Different from previous research work, in this work, a method of anomaly detection called Hurst of Interest Distribution is proposed based on the stability of user interest quantifiable from the content of users' tweets, so as to detect abnormal accounts. In detail, the Latent Dirichlet Allocation model is adopted to classify blog content on Twitter into topics to calculate and obtain the topic distribution of tweets sent by a single user within a period of time. Then, the stability degree of the user's tweet topic preference is calculated according to the Hurst index to determine whether the account is compromised. Through experiments, the Hurst indexes of normal and abnormal accounts are found to be significantly different, and the detection rate of abnormal accounts using the proposed method can reach up to 97.93%.

1. Introduction

With the rapid development and popularization of the Internet, people have become increasingly more interested in using social media. Online social platforms enable people to share their daily lives, express emotions, and access global news hotspots without leaving home. Owing to the convenience offered by such platforms, the number of social network users has increased dramatically. Statistics show that more than 1.3 million new users on average joined social media platforms every day during 2020, with nearly half a billion new users taking the global user total to almost 4.2 billion by the start of 2021 [1]. However, with the complexity and diversification of social networks, several problems have emerged. The terabyte (TB) level user data and high user traffic generated by social platforms present criminals with opportunities.

After manipulating social robots to hijack real accounts, criminals steal personal privacy data or implement Telecom fraud by spreading malicious links and sending spam and phishing e-mails. According to statistics, the share of spam in e-mail traffic amounted to 50.37% in 2020 [2]. Even social robots make negative comments or post false news on specific topics to control the direction of public opinion and affect social stability or political elections [3, 4]. In Ref. [5], it is pointed out that 9%–15% of active Twitter accounts are robots, so it is a challenging task to detect such robots. In addition, it is of great significance to create a green and safe network environment, protect users' privacy and security, and maintain political and social stability.

In previous cases of compromised accounts on social platforms, account thieves usually made a large number of repeated statements through the software to achieve dissemination. It was easy to distinguish whether the account had been stolen based on the content and language features. Today, the behaviors of social robots are more similar to those of real human beings [6, 7]. Therefore, it is no longer effective to determine whether an account has been compromised by robots simply based on the virtue of the grammatical and semantic features of the content.

As an increasing amount of behavior patterns of users on social platforms is quantified as features for abnormal detection, results have been achieved in the early stage of applications. At the same time, the information acquisition of criminals has gradually become symmetrical. Through the learning and imitation of normal user characteristics, a number of accounts that are difficult to distinguish between true and false are gradually constructed to evade abnormal detection.

To solve the aforementioned problems, it is argued herein that the psychological characteristics of human beings are not easy to change rapidly and are difficult to imitate, which can effectively help detect compromised accounts. The characteristics of human beings mainly refer to the uniqueness of the user, such as their personality, hobbies, and emotional tendencies. It takes a long time for one person to get to know another person intimately in daily communication [8]. It is even harder for an attacker to mimic a person's human characteristics through a single online message. If one can grasp the changes in user characteristics of human beings, it will contribute to a new approach of achieving abnormal detection. It is considered that most accounts with stable features are normal accounts, those with disordered features are robot accounts, and those with features that change at some point in time are compromised.

The main difference between our work and existing models lies in the detection based on the judgement of stability of user interest distribution. The contributions of this paper are described in detail as follows.

First, a new feature for anomaly detection is introduced. According to the individual differences of users and the stability of psychological characteristics, the user interest distribution is extracted from the content of users' tweets. Compared with the features used in previous studies, the process of extracting user interest distribution is easier to carry out, and the features that can reflect individual differences are not easy to imitate and will not mutate.

Then, an interest presentation algorithm with the Latent Dirichlet Allocation (LDA) model is proposed. There are too many points of the characteristics of human beings to investigate, and it is even more difficult to describe and quantify them. In the work described in this paper, hobbies, one of the characteristics of human beings, were chosen to detect compromised accounts since they can be easily quantified.

Finally, a compromised-account-detection algorithm is proposed in this paper. The Hurst of Interest Distribution (HoID) is introduced to measure the stability of user hobbies. Stability refers to whether the changing trend of user preferences is within an acceptable range, while the status update of abnormal accounts hijacked by robots is random, which is inconsistent with the previous psychological characteristics. Therefore, the stability of the distribution of hobbies of social accounts is used to identify the existence of abnormal accounts.

The rest of this paper is organized as follows. In Section 2, the related work is divided into two parts: the first part is abnormal-account-detection methods based on user characteristics, and the second part is characteristics of mining of human beings based on LDA. In Section 3, the detection method based on the HoID algorithm is elaborated. In Section 4, the experiments and corresponding analysis are described. Conclusions are drawn in Section 5.

2. Related Work

With the rapid development of the Internet era, social networks provide a significant number of conveniences for work, study, and entertainment but also bring various information-security problems. Cyberspace threats emerge endlessly and cause huge losses to Internet users. In the field of information security, to prevent illegal attacks and protect the security of private data in the process of transmission and storage, information-encryption technology is constantly improving and great progress has been made.

In recent years, many image-encryption approaches have been proposed on the basis of chaotic maps, in which it is very crucial to assign value to chaotic map parameters. The existing solutions are based on metaheuristics, which have the problems of slow computing speed and falling into local optima. Aiming to resolve this issue, Kaur et al. proposed a strength Pareto evolutionary algorithm-II-based metaheuristic approach to tune the hyperparameters of a four-dimensional chaotic map [9]. Comparative analyses showed that the proposed approach outperformed the competitive approaches in terms of entropy. Furthermore, dual local-search-based multiobjective optimization (DLS-MO) was used to obtain the optimal parameters of a hyperchaotic map and encryption factors in another study, which also achieved good performance [10]. In addition, the parameter estimation of hyperchaotic maps involves extensive computational search. Kuar et al. proposed a minimax differential evolution-based seven-dimensional hyperchaotic map to generate secret keys for image encryption [11]. The fitness of the parameters was evaluated using correlation coefficient and entropy. The proposed approach achieved significantly good encryption results compared to the competitive approaches. In addition, the proposed approach resisted various security attacks.

Although encryption technology ensures the privacy and security of information to a large extent, in view of the openness and sharing concept of cyberspace, in addition to the application of encryption technology, one should also combine an anomaly-detection algorithm to further purify the network environment and enhance network security. Detecting abnormal accounts on social networks in a timely manner can effectively prevent the occurrence of malicious Internet events. There are many studies on abnormal account detection on social platforms, and the LDA model has also been applied to the field of abnormal account detection.

The detection of social robots must process a pre-collected dataset and then select some representative and distinguishing features from the content information, behavior information, and social relationship graph. Finally, a supervised-machine-learning algorithm is used to classify the features to obtain a more accurate detection effect [12]. Earlier researchers include Wang [13], who extracted graph-

and content-based features and designed an algorithm to detect spam robots in Twitter. Efthimion et al. [14] proposed a new machine-learning algorithm that utilized a series of features, including the length of user name, time pattern, emotional expression, and the ratio of followers to friends. Logistic regression (LR) as a classifier could effectively detect robots with an error rate of 2.25%.

In recent years, with the development of big data and the improvement of computer performance, deep learning has gradually become popular. Cai et al. proposed a behavior-enhanced deep model (BeDM) for bot detection [15]. BeDM fused content information and behavior information and regarded user content as temporal text data to extract latent temporal patterns. They combined convolutional neural networks (CNNs) with a long short-term memory (LSTM) model, and the garbage robot of tweets was detected efficiently and accurately. Sneha et al. proposed a deep neural network based on the LSTM model that extracted context features from user metadata that were fed as auxiliary input into a LSTM deep network to process tweet text [16]. In addition, a technique based on synthetic minority oversampling (called SMOTE) was proposed to generate a large-scale labeled dataset suitable for deep network training from the minimum number of labeled data. Experiments showed that this structure could achieve high classification accuracy (AUC > 96%, where AUC denotes area under the curve) in the process of detecting bots through only one tweet.

2.1. Abnormal-Account-Detection Methods Based on User Characteristics. Feature representation is commonly adopted to detect abnormal accounts. Because there are significant differences between abnormal and normal accounts in some characteristics, the accuracy of account classification can be effectively improved by selecting features with a large degree of differences. The existing feature representation is mainly divided into features including attribute features, content features, network features, and activity features.

Attribute features include user name, avatar, number of followers, and other basic information, which are easily obtained. The user's age, educational background, e-mail address, emotional status, and other characteristics are also involved, which are not easily obtained due to the influence of user-privacy settings. Teams in the 2015 DARPA (Defense Advanced Research Projects Agency) Twitter Bot challenge used the users name, user avatar, geographical location, and other attributes to detect abnormal accounts in Twitter [17]. Results of these experiments indicated that a bot-detection system must be semisupervised, but all teams used human judgement to augment automated bot-identification processes. The credibility features of some social platforms (such as Twitter) can also be used for abnormal detection.

Content features refer to the features extracted from content information posted by users, which can be mainly divided into grammatical and semantic features [18, 19]. The semantic features refer to the subjects or emotions of the published content items, while the grammatical features refer to the features including sentence structure, word frequency statistics, and punctuation. Several special features are also used, such as the use of "#," "@," and "http://." Kumar et al. built an automatic classification system that used features such as text length and text composition ratio to detect abnormal users in Wikipedia [20]. Results of the experiments showed that the algorithms could utilize these additional signals rather than article appearance features to accurately identify hoaxes.

Network features mainly refer to the correlations between social users, which are quantified by scholars into indicators such as degree, clustering coefficient, and centrality. Most of the normal accounts have social circles, there are many friends who follow each other, and the number of followers and followees is relatively balanced, while abnormal accounts have great differences in the above aspects. Graph data are generally used to represent the feature and structure information of nodes. With the rise of deep learning, a large number of researchers have considered using deep-learning models to automatically model graph data, including graph embedding [21] and graph neural networks [22]. Kirill et al. used a graph-embedding model to extract node representations from social network user profiles and used different classifiers to classify features, such as Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), and Gradient Boosting (GB) [23]. In addition, a stacking-based ensemble was created, which not only extracted graph features but also utilized text features. Empirical evaluation proved the effectiveness of the proposed method for bot detection and showed that stacking of first-layer classifiers with graph-embedding features allowed boosting the best single-classifier scores by 1%–4% in AUC accuracy.

To better detect malicious accounts and social bots, Seyed Ali and others think that account classification should employ a feature set and social graph at the same time. Therefore, a detection model based on a graph CNN was proposed, which effectively gathered the features of a node neighborhood [24]. Experimental results showed the superiority of the method, which increased the AUC accuracy by 8%. Given the growing scale of social networks, it will consume a significant amount of computing resources to construct the Twitter graph structure based on the follower and friend relationships in social accounts.

Activity features refer to a user's behavior patterns, such as active time, frequency of information published, and common clients [3, 25, 26]. Xin et al. divided users' social behaviors into two categories: extroversive behavior features such as activity sequence and introversive behavior features such as request latency [27]. European distance is used to quantify the differences between the incoming clickstream and the behavior pattern represented by the behavioral profile, so as to identify whether the clickstream is from real users or abnormal users. This method is applicable to users that directly access Online Social Network (OSN) pages, but it is difficult to trace the behavior patterns of users who access OSNs solely through application programming interfaces. Wu et al. used the published information quantity matrix feature to detect abnormal users in Sina Weibo [28]. Yamak et al. used the time intervals between user registration and first posting to detect fake accounts in Wikipedia [29]. The results from several machine-learning algorithms were compared to show that new features and training data

enabled the detection of 99% of fake accounts, improving previous results from the literature.

In addition, some studies have combined the above features. Chavoshi et al. illustrated that the presence of highly synchronous cross-user activities revealed abnormalities and thus developed the DeBot system to identify bots in Twitter's network [30]. DeBot is an unsupervised method that calculates cross-user activity correlations to detect bots in a parameter-free fashion. Its evaluation showed that DeBot detected bots at a rate higher than the rate Twitter was suspending them.

2.2. Characteristics of Mining of Human Beings Based on LDA. LDA is a document theme model, through which the thematic tendency of an article can be obtained, and thus the expression of users' interests can be obtained. Some scholars have used a LDA model to carry out some studies related to the characteristics of human beings. Liu et al. proposed the probabilistic topic model (PT-LDA model) to predict personality characteristics under the framework of the five-factor model and considered that each topic not only has the multinomial distribution of words but also has the Gaussian distribution of personality, which provides a new method to reveal user behaviors in social networks [31]. Zhang et al. proposed the concept of GROUP-LDA, which integrates book-related information into the LDA model to describe the subject relevance among documents to accurately detect the book audience [32]. According to the evaluation results, it outperformed Latent Semantic Analysis (LSA), LDA, the author-topic model (ATM), and several other collaborative filtering methods in terms of precision, recall, $F1$-score, and mean average precision (MAP) for book-audience detection. Shinjee et al. combined the LDA theme model of television viewers with the LDA theme model of program descriptors to effectively improve the user-prediction accuracy of new TV programs [33]. Gao et al. proposed a mechanism called SECO-LDA to construct service co-occurrence (SECO) documents by studying the potential topic model in the history of service collaboration to extract potential SECO topics. The derived knowledge of these topics will help reveal the tendency of service composition, aid the understanding of the cooperation behaviors between services, and provide a better service recommendation [34]. Yan et al. considered that traditional search engines only collect documents containing keywords in the query without considering the real intention hidden by users. To solve this problem, a personalized retrieval algorithm based on query-intention recognition and a subject model is proposed. A LDA topic model is used to model the historical search data of users. When a new query appears, the underlying topic of the query is identified by the topic model of its user-history search, and the appropriate document is recommended [35].

3. Materials and Methods

In this paper, a method of detecting abnormal accounts on social platforms based on the judgement of stability of user interest distribution is proposed. The LDA model is adopted to calculate the distribution of users' interests based on body content items published by users, and the Hurst parameter is used to measure the stability of interest distribution. In detail, the aforementioned HoID algorithm detects compromised accounts on social platforms through four steps: sorting out user tweets, training the LDA model, obtaining user interest distribution, and determining whether the interest distribution is stable, as shown in Figures 1 and 2. Among them, Ω refers to user tweets, L refers to the LDA model, D refers to the interest distribution, H refers to the stability of interest, and $L = f(\Omega)$, $D = g(\Omega, L)$, and $H = h(\mathrm{D})$.

3.1. Sorting Out User Tweets. The content items published by users on social platforms in a certain period of time were summarized and sorted out. Taking users as a unit, statistics on the word usage frequency of each tweet were generated, and then the tweets were transformed into the form of word vectors, with stop words removed. The Baidu English stop word list, which contains 891 stop words, was used in this work.

3.2. Interest Distribution. It is considered that the contents posted by users on social platforms are closely related to their interests, and the topic distribution of tweets can reflect the distribution of users' interests and hobbies. Consequently, the processed tweets are input into the LDA model for training, which is used to predict the topic of the blocking tweets to obtain the interest distribution of users.

An article can cover more than one topic, and the words in the article reflect the specific set of topics it covers. In the proposed method, each topic is taken as a probability distribution on the word, and the document is taken as a probability mix of those topics. If one has N topics, the probability of the word i in a given document can be written as

$$P(w_i) = \sum_{j=1}^{N} P(w_i|z_i = j)P(z_i = j), \tag{1}$$

where z_i is the potential variable representing the topic of the ith word. $P(w_i|z_i = j)$ is the probability of word w_i being under the jth topic. $P(z_i = j)$ represents the probability of selecting a word from the jth topic in the current document, which varies from document to document. The jth topic is represented as a polynomial distribution $\varphi_{w_i}^{j} = P(w_i|z_i = j)$ of V words in the word list. The text is represented as a random mix of $\varphi_j^d = P(z_i = j)$ on K implied topics. Thus, the probability of word w "occurring" in text d is

$$P(w|d) = \sum_{j=1}^{N} \varphi_{w_i}^{j} \cdot \theta_j^d. \tag{2}$$

The maximum-likelihood estimators α and β of the maximum-likelihood function (equation (3)) are obtained by the expectation-maximization algorithm, and the parameter values of α and β are estimated, so as to determine the LDA model:

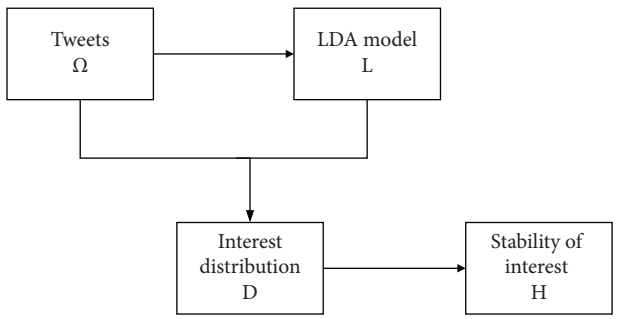


Figure 1: Module diagram of account interest mining.

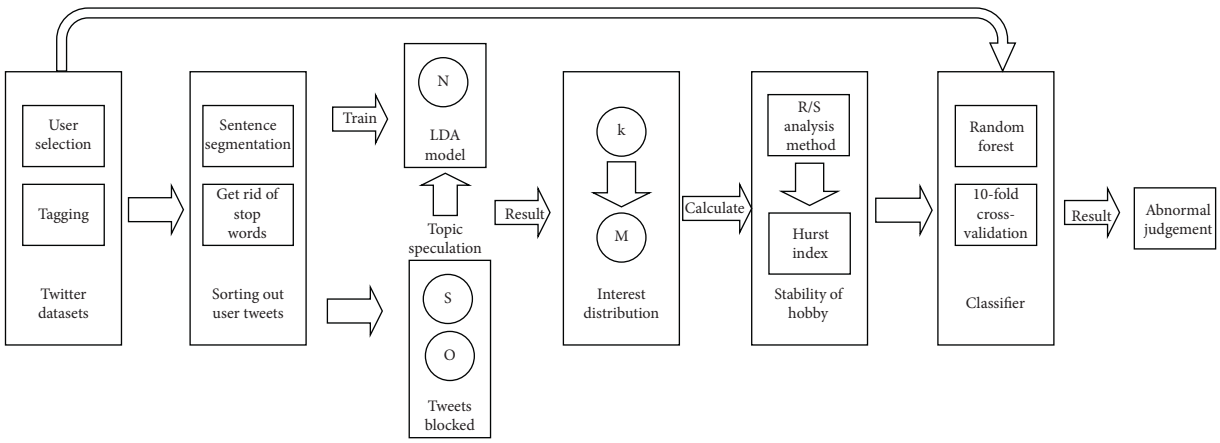


Figure 2: Account interest mining.

$$l(\alpha,\beta)=\sum_{i=1}^{M}\log\ p(d_i|\alpha,\beta), \tag{3}$$

where the conditional probability distribution of the "occurrence" of text d can be obtained from

$$p(d|\alpha,\beta)=\frac{\Gamma\left(\sum_i a_i\right)}{\prod_i\Gamma(a_i)\int\left(\prod_{i=1}^{k}\theta_i^{a_i-1}\right)\left(\sum_{n=1}^{N}\sum_{i=1}^{k}\prod_{j=1}^{V}\left(\theta_i\beta_{ij}\right)^{w_n^j}\right)\mathrm{d}\theta}. \tag{4}$$

Since the paired variables θ and β exist in equation (4), the analytical equation cannot be calculated and an approximate solution is required. Griffiths et al. proposed that Gibbs sampling is better in terms of confusion and running speed. Gibbs sampling as proposed by Griffiths et al. is a better way in terms of perplexity and running speed.

Because of the 140-word limitation of a single tweet, the users' interests cannot be precisely reflected by so few words. To solve this problem, user tweets must be divided into blocks. Each tweet block includes user tweets in a certain period, so as to reflect the distribution of user interests and hobbies in that period. The concepts of tweet-block size S and tweet-block overlap degree O are introduced here. Tweet-block size refers to the number of tweets in a single tweet block, while tweet-block overlap degree refers to the overlap degree of two adjacent tweet blocks. Figure 3 shows an example of $S=20$ and $O=10$.

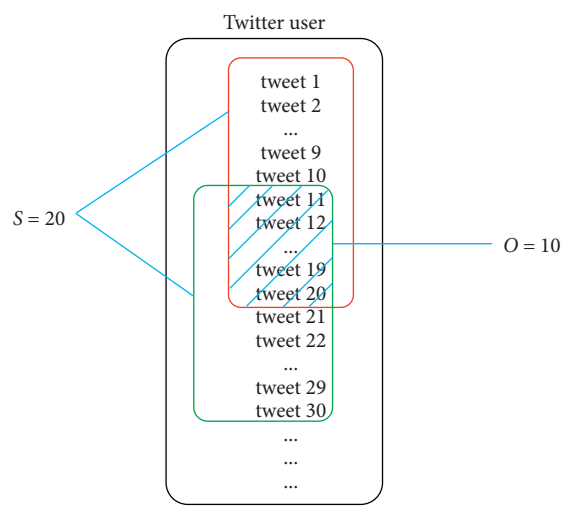


Figure 3: Example of user tweet separation when $S=20$ and $O=10$.

T is defined as the total number of tweets of the user. Taking K tweet blocks as an example, where $K=T/(S-O)+1$, tweet block k contains $((k-1)\cdot(S-O)+1,(k-1)\cdot(S-O)+S)$ tweets. Those tweets in one block are jointed as one text.

The LDA model is used to calculate the topic distribution of K tweet blocks. The topic distribution of the kth tweet block is represented as $\vec{k}=(P_{k1},P_{k2},P_{k3},\ldots,P_{kN})$. So far, the interest distribution matrix M of order $K*N$ has been obtained. Each row of the matrix represents the distribution

of the user tweets on N topics in a certain period, and each column represents the variation of users' interest on a certain topic over time:

$$M = \begin{pmatrix} (P_{11}, P_{12}, P_{13}, \ldots, P_{1N}) \\ (P_{21}, P_{22}, P_{23}, \ldots, P_{2N}) \\ (P_{31}, P_{32}, P_{33}, \ldots, P_{3N}) \\ (P_{41}, P_{42}, P_{43}, \cdots, P_{4N}) \\ \ldots \\ \ldots \\ (P_{K1}, P_{K2}, P_{K3}, \ldots, P_{KN}) \end{pmatrix}. \quad (5)$$

3.3. Stability of Interest. Stability refers to whether the changing tendency of user preferences is within an acceptable range. Since the characteristics of human beings are not easy to imitate and not easy to change in a short time, it is considered here that the distribution of hobbies of a healthy account user should be stable. If there is a mutation, the account may be compromised. The method of analyzing the stability of a group of data is different in terms of application backgrounds. In this paper, the Rescaled Range Analysis (R/S analysis) method is used to calculate data stability.

R/S analysis is usually used to analyze the fractal characteristics of time series and the long-term memory process. It was originally proposed by British hydrologist Harold Edwin Hurst when he was studying the Nile Dam project. It was later used in the analysis of various time series.

In this study, the Hurst index is used to indicate the degree of stability of user interest. From the user-interest distribution matrix obtained above, the interest distribution sequence $\overrightarrow{n}$ of a user under the topic n is shown in equation (6). It is divided into $[k/10]$ subintervals. For each subinterval, the cumulative dispersion $X_{t,l}$ is calculated according to equation (7), where M_L is the average value of P in the interval l:

$$\overrightarrow{n} = (P_{1n}, P_{2n}, P_{3n}, \ldots, P_{kn}), \quad (6)$$

$$X_{t,l} = \sum_{u=1}^{10} (x_u - M_L), \quad (7)$$

$$R = \max\left(X_{t,l}\right) - \min\left(X_{t,l}\right). \quad (8)$$

The fluctuation range R is defined by equation (8) and is equal to the difference between the maximum and minimum values of the accumulated deviation. The standard deviation of the subinterval is denoted as S, and the rescaled range (R/S) is defined, which increases with increasing sequence length. Through a long period of practice, Hurst established the relationship as shown in in the following equation:

$$\frac{R}{S} = Kl^H. \quad (9)$$

Taking the logarithm of both sides of equation (9), one obtains

$$\log\left(\frac{R}{S}\right)_l = H\ \log(l) + \log(K). \quad (10)$$

The least-squares regression analysis of $\log(l)$ and $\log(R/S)_l$ in equation (10) can be used to calculate H, which is called the Hurst exponent. The corresponding Hurst exponent of the nth topic is denoted as H_n. So far, N Hurst exponentials have been obtained, i.e., $H = (H_1, H_2, H_3, \ldots, H_n)$. H represents the stability of the user's interests, and it is a group of characteristics of human beings that are affected by parameters N, S, and O in this study. Classifiers can be used to complete classification work through traditional machine-learning methods.

4. Results and Discussion

In this section, the H feature defined at the end of the preceding section is used to classify each user.

4.1. Dataset. There are no public datasets that were used in the related research on the detection of compromised accounts, so it is difficult to accurately determine whether an account has been compromised or not. The varol-2017 dataset used by Varol et al. [36] was selected in the present work. Varol et al. monitored approximately 10% of the public tweets in Twitter for a period of three months starting from October 2015 and selected users who sent at least 90 tweets during the three-month observation period and sent more than 200 tweets overall. This dataset has since been adopted by many researchers and offers tweets in terms of users. It is easy to observe a user's interests change by analyzing their tweets over time.

Our study uses Twitter official API interface Tweepy [37] to crawl user data, including user's published tweets and user metadata. This dataset comprised 940 original accounts. After data screening and cleaning, 616 users were selected as normal accounts. These original data are used to depict normal users and construct compromised accounts.

4.2. Compromised-Account Construction. A method proposed by Trang et al. in [38], which first obtained the data of normal users, then randomly paired 616 normal accounts several times, and exchanged some tweets in the paired accounts, was adopted to construct abnormal accounts. As shown in Figure 4, the top m tweets of account U_1 itself were selected as the normal data before being hijacked. The $(m+1)$th tweet to the Nth tweet is exchanged with the same part of the account U_2 matched with the user, as the abnormal data after being hijacked. Accordingly, the "compromised" accounts, U_1^* and U_2^*, are constructed.

Based on the above method, the raw data were used to construct the compromised accounts using $N = 190$ and $m = 171$. Thus, 190 tweets from each of the 616 normal accounts were selected as experimental data. The first to 171st tweets served as original tweets, and the 172nd to 190th tweets were exchanged from paired accounts and served as the abnormal part. What is more, any two accounts in the normal accounts can be paired, and the pairing process is

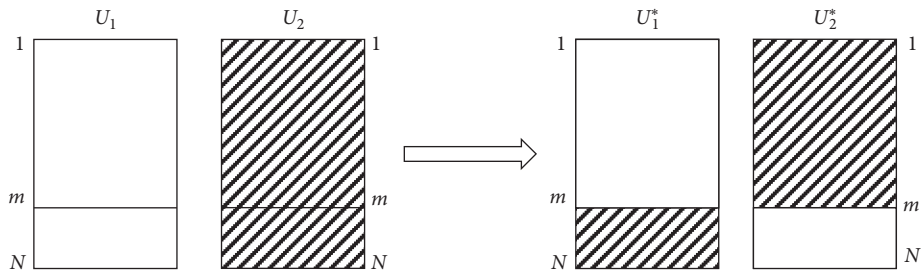


Figure 4: Compromised-account construction.

random and nonrepetitive. As a result, a total of 8,340 abnormal accounts were constructed.

4.3. Data Preprocessing. The above-described 940 normal accounts and 8,340 abnormal accounts exhibit a serious class-imbalance problem that will affect the correctness of the experimental results. Therefore, the SMOTE algorithm was used in this work to solve the class-imbalance problem [39].

SMOTE is an upsampling algorithm in which M samples are randomly selected from the k-nearest neighbors of each few samples, where M is the sampling multiplier. For each randomly selected neighbor b, a new sample c is constructed with its original sample a as follows:

$$c = a + \text{rand}(0, 1) * (b - a). \tag{11}$$

Since it is impossible to carry out SMOTE sampling on tweets, in this experiment, after calculating the N-dimensional Hurst value of the normal accounts, the above sampling was carried out on the tweets, and finally 8,340 normal and 8,340 abnormal accounts were constructed.

4.4. Evaluation Metrics. In this experiment, abnormal accounts were taken as positive samples. A random-forest classifier was used to conduct ten-fold cross-validation classification. Accuracy, precision, recall, and $F1$-measure were used as the evaluation indexes of the classification effect, calculated, respectively, as follows:

$$\begin{aligned} \text{precision} &= \frac{\text{TP}}{\text{TP} + \text{FP}}, \\ \text{accuracy} &= \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}, \\ \text{recall} &= \frac{\text{TP}}{\text{TP} + \text{FN}}, \\ F1 &= \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}}. \end{aligned} \tag{12}$$

Here, TP refers to true positive, which equals the number that is correctly divided into a positive example. TN refers to true negative and is the number that is correctly divided into a negative example. FP refers to false positive and shows the number that is judged to be a positive sample of a negative sample. FN refers to false negative and indicates the number that is judged to be a negative sample of a positive sample.

4.5. Experiment 1. This experiment explored the influence of different topic numbers N and overlap degrees O on the classification effect when the tweet-block size was fixed to $S = 20$. The number of topics was taken as $N = 2, 3, \ldots, 10$, and the overlap degree of tweet blocks was taken as $O = 0, 1, \ldots, 9$. Thus, a total of 90 sets of classifications with different N and O values were involved.

Figures 5–8 depict the classification metrics with varying parameters. It can be seen from these figures that the changing tendency of different evaluation indexes is similar.

Longitudinal observation shows that when O is constant, the accuracy/precision/recall/$F1$-measure is the lowest when $N = 2$, which indicates that interest distribution among two topics cannot accurately depict the interests of users. The performance becomes better when $N = 7, 8, 9, 10$. Almost each metric reaches the maximum when $N = 8$. This means that the interests of users distribute among approximately eight topics.

O refers to the degree of overlap between two adjacent tweets. When the degree of overlap is high, the proportion of repeated content between two tweets is high, and the change of a user's topic tendency is small. In contrast, when the degree of overlap is low, the change of a user's topic tendency is large. The change of topic tendency will be reflected in the change of Hurst value and, in turn, will affect the experimental results.

N refers to the number of topics. Different numbers of topics will lead to different distributions of user topic preference. When N is small, the user's tendency to assign each topic is relatively large. When N is large, the tendency to assign each topic is relatively small, which will also lead to the change of Hurst value and affect the experimental results.

Transverse observation shows that when N is constant, with increasing O, each index bounces back at several nodes, but the overall change tendency is downward. This means that if the overlap between blocks is too large, the change of user interests is less obvious to be quantified, thus affecting the "judgement" of the HoID algorithm.

In abnormal detection, missing an abnormal account can be fatal. Therefore, recall is considered the most important index in the present work. Figures 9 and 10 show the average recall rates of $O = 1$–9 when N is constant and the average recall rate of $N = 2$–10 when O is constant.

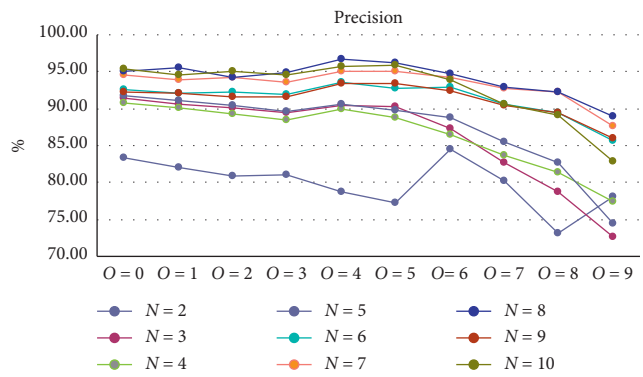


Figure 5: Precision for different N and O values.

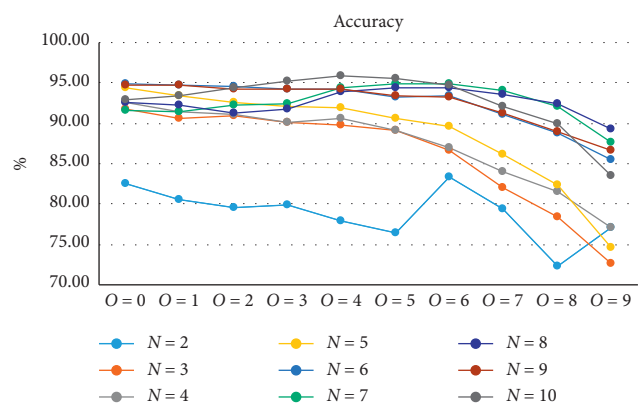


Figure 6: Accuracy for different N and O values.

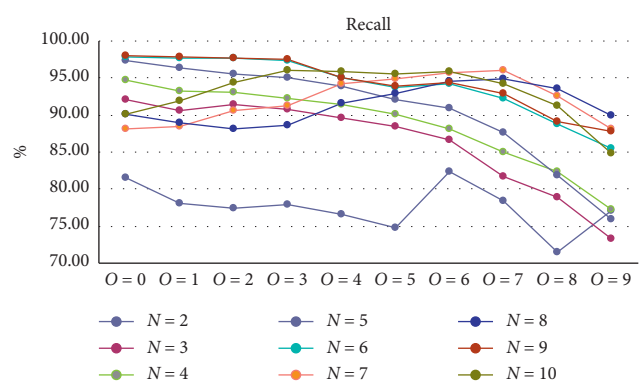


Figure 7: Recall for different N and O values.

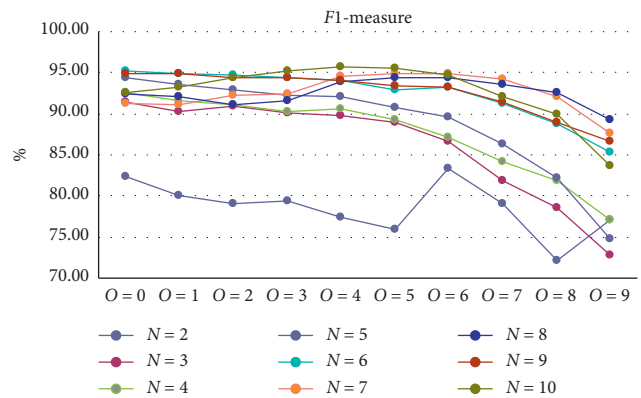


Figure 8: $F1$-measure for different N and O values.

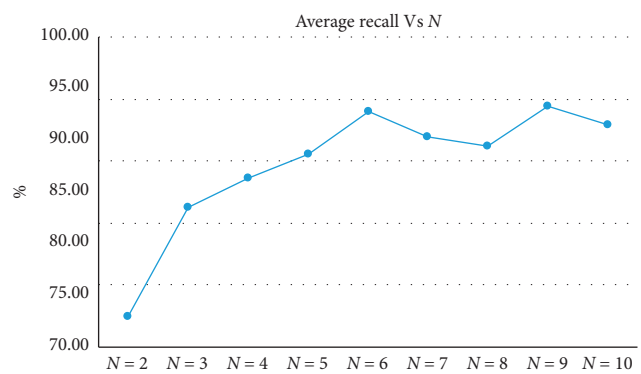


Figure 9: Average recall rate of $N = 2$–10 when O is certain.

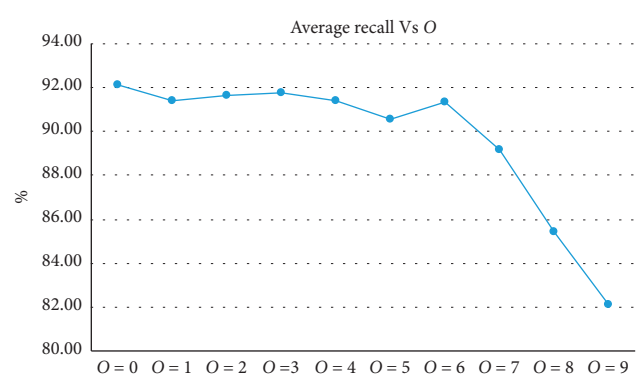


Figure 10: Average recall rate of $O = 2$–9 when N is certain.

As can be seen from Figures 9 and 10, when O is constant, the abnormal-account recall rate increases with increasing N, and when N is constant, the abnormal-account recall rate shows a downward tendency with increasing O. This confirms the previous conclusion; that is, low topics cannot classify users' interests, and large overlap cannot reflect the tendency change of user interests. By comparing the data among groups, it can be concluded that, in this dataset, $N = 9$ and $O = 0$ are the best parameters to achieve a maximum recall rate when $S = 20$, with a precision of 92.12%, accuracy of 94.77%, recall of 97.93%, and $F1$-measure score of 94.93%. This group of parameters was used for the experiment.

4.6. Experiment 2. This experiment was designed to visually examine the Hurst-index distribution of normal and abnormal accounts.

Table 1 shows the differences between normal and abnormal accounts in the mean and variance of H.

The results in the table indicate that in the majority of cases, the H mean of normal accounts is larger than that of abnormal accounts. This is consistent with the feature of the

Table 1: Mean and variance of H.

Hurst index	H mean		H variance	
	Normal	Abnormal	Normal	Abnormal
$H1$	1.037	0.919	0.469	0.285
$H2$	1.105	0.831	0.319	0.469
$H3$	0.445	0.684	0.989	0.670
$H4$	1.075	0.905	0.346	0.328
$H5$	0.979	0.898	0.544	0.327
$H6$	0.841	0.825	0.744	0.515
$H7$	1.094	0.967	0.360	0.207
$H8$	0.990	0.926	0.556	0.293

Hurst exponent, namely, the larger the exponent, the greater the stability. The H variance of normal accounts is also larger than that of abnormal accounts. The smaller difference in H of abnormal accounts is due to the similar ways the abnormal accounts are constructed.

Limited by the difficulties in visualizing high-dimensional data, Figures 11 and 12 only illustrate the two-dimensional joint distribution in normal and abnormal accounts, taking $H1$ and $H2$ as examples. It can be seen that the $H1$ and $H2$ values of most normal accounts are between 1.0 and 1.5 at the same time, while those of the abnormal accounts are between 0.8 and 1.2. The distribution of normal accounts is quite different from that of the abnormal ones, which proves the assumption of HoID, i.e., most accounts with stable features are normal accounts.

In order to verify the difference between abnormal and normal accounts, an independent samples t-test was adopted on the Hurst index of abnormal and normal accounts. The P values are shown in Table 2.

All P values are less than 0.05, which proves that there are significant differences between the Hurst indexes of normal and abnormal accounts.

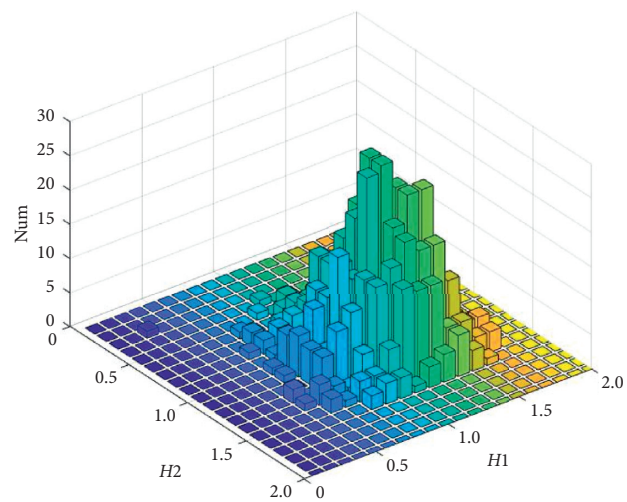


Figure 11: Normal-account joint distribution of $H1$ and $H2$.

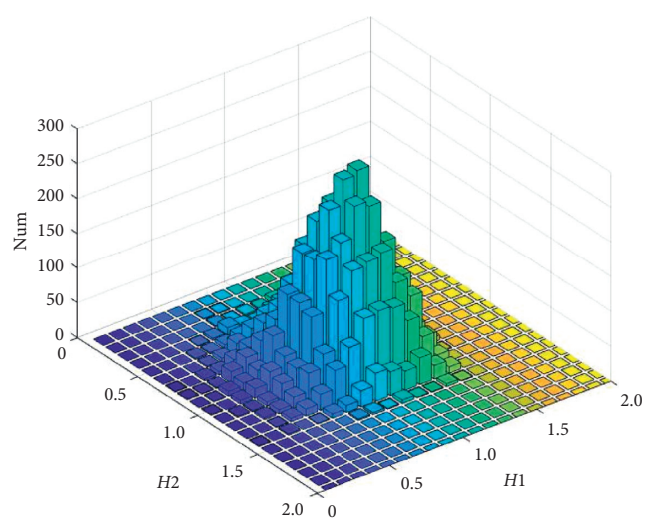


Figure 12: Abnormal-account joint distribution of $H1$ and $H2$.

4.7. Experiment 3. This experiment explored the influence of different tweet block sizes, $S = 5$, 10, 15, 20, and 25, on the classification effect when the number of topics was $N = 9$ and the overlap degree of tweet blocks was $O = 0$. The results are shown in Figure 13.

It can be seen from Figure 13 that the recall rate is the best at $S = 20$, and when $S = 15$ and 25, the comprehensive level of the four indexes is better, while when $S = 5$ and 10, all evaluation indicators are at a low level. It can be considered that the classification effect becomes better with increasing tweet block size S. It seems that 15 tweets in one block is the best way to judge user interest distribution in a certain timeframe.

Different classifiers were used to conduct ten-fold cross-validation classification. Results for accuracy, precision, recall, and $F1$-measure in classification by random forest (RF), support vector machine (SVM), and KNN are shown in Figure 14. The results show that KNN performs the best followed by RF, while SVM performs the worst.

4.8. Contrast Experiment. Egele et al. proposed COMPA, a method to detect compromised accounts on social networks [40]. The features selected by COMPA include terminal situation, user-mention situation, link-addition situation, time-point situation, language situation, and topic-participation situation. COMPA extracted features from the message flows published by users in chronological order and established a behavioral model to observe whether the new

Table 2: T-test results on normal and abnormal accounts.

Hurst index	P value
$H1$	4.075×10^{-111}
$H2$	0.0
$H3$	9.417×10^{-78}
$H4$	1.090×10^{-298}
$H5$	2.432×10^{-34}
$H6$	0.025
$H7$	3.136×10^{-202}
$H8$	1.311×10^{-30}
$H9$	2.603×10^{-22}

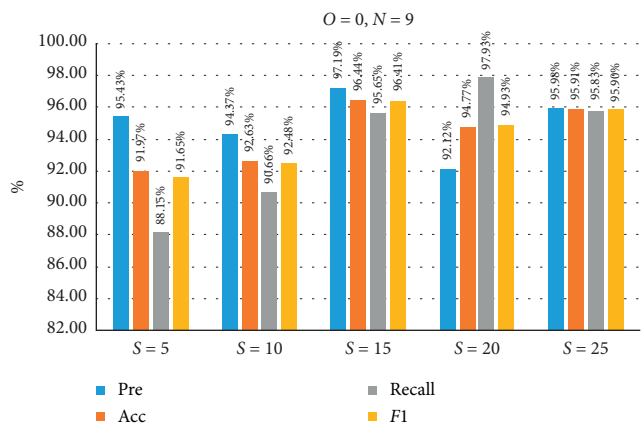


Figure 13: Results for $N = 9$, $O = 0$, and $S = 5$, 10, 15, 20, and 25.

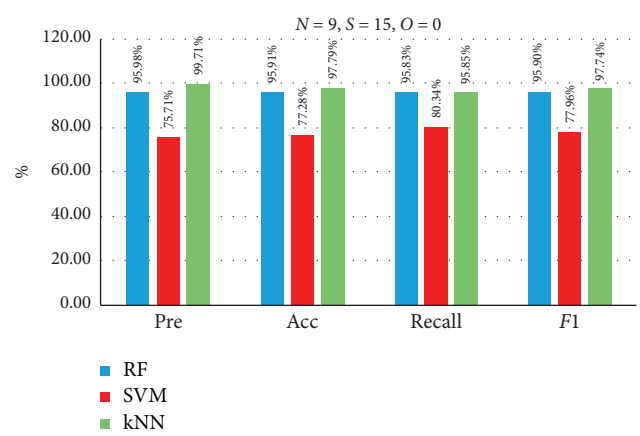


Figure 14: RF, SVM, and KNN classification results.

message flows conformed to the expected behavior and evaluate the abnormal score of each individual feature. Finally, the outlier scores of each feature were combined to obtain the global score of each message. The accuracy of the test results depended largely on the established behavioral profile and threshold value of selection.

Tang et al. proposed the supervised analytic hierarchy process (SAHP) for abnormal user detection [41]. In the process of abnormal user detection, different characteristics often reflect different degrees of user abnormality. Compared with COMPA, to establish more comprehensive profile features, SAHP took user expression habits into account and combined information gain rate with an analytic hierarchy process to ensure the accuracy of feature weight. SAHP then made detection decisions according to different thresholds. At high thresholds, the accuracy of the method is high, but it is slightly worse when a lower threshold is selected.

Kaur et al. utilized text-based continuous authentication (TB-CoAuth) for detecting compromised accounts in social networks [42]. Four categories of features, namely, content free, content specific, stylometric, and folksonomy, are extracted and evaluated by TB-CoAuth. In addition, various statistical and similarity-based feature-selection techniques are used to rank and select optimal features for each user, which are further combined using a popular rank-aggregation technique called Borda Count. Moreover, performance of various supervised-machine-learning classifiers is analyzed on the basis of different evaluation metrics.

HoID (parameters $S = 25$, $N = 9$, and $O = 0$), COMPA, and SAHP were tested separately on the same dataset. Furthermore, in the face of one of the most significant challenges in the domain of compromised accounts, i.e., the non-availability of ground-truth data consisting of the point of compromise and the compromised tweets, Kaur also used the artificial practice of creating ground-truth data to verify the model, manually injecting spam and randomness into the accounts. Therefore, the proposed method was also applied as a baseline model for performance comparison, and the results of HoID, TB-CoAuth, COMPA, and SAHP are compared and shown in Figure 15.

In previous research work, several researchers started from the user's external information, network features, content features, and activity features using active duration, commonly used devices, account update status, and text characteristics based on the content of tweets as the main features for anomaly detection. Results have been achieved in the early stage of applications, but there is no reasonable use of tweet content, which truly expresses the characteristics of individual user differences. However, these traditional characteristics are considered to be easier to imitate and have a high degree of deception, which affects the prediction effect of the model. More information of the features that these models used is provided in Table 3.

However, as per Pariser's filter theory, every user unknowingly builds their own bubble space based on their interests and search patterns. Hence, social users will be active in different social spaces, and their tweet patterns, interest topics, and social circles have established their own unique patterns. Even if user interests fluctuate, this will evolve over time, without a sudden change. In view of the uniqueness and stability of personal style, even if criminals use personal data to obtain user interests to maintain the active status of the account after hijacking it, it cannot fit with the exclusive mode of real users, so this behavior pattern earns an automatic strict violation.

Based on the above reasons, the distribution of interests and hobbies implicit in the content of user tweets was fully investigated and the main characteristics of users were quantified. The stability of the distribution of user interests

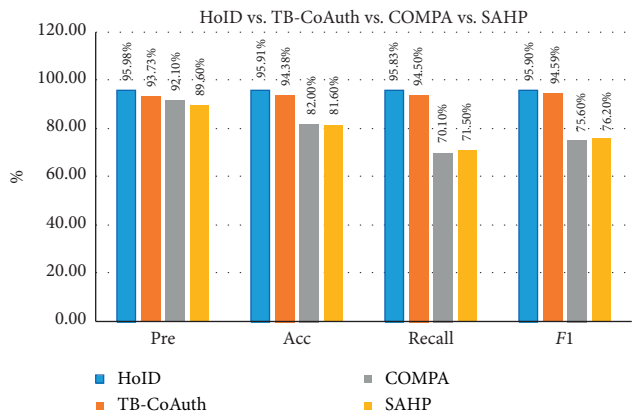


Figure 15: Results comparison of HoID, TB-CoAuth, COMPA, and SAHP.

Table 3: Comparison of feature selection with competitive methods in field of abnormal-account detection on social networks.

Model	Feature types	Feature used	Technique	Replicability of features	Remarks
Spot 1.0	Attribute features	Including the number of followers and followees, reputation, frequency of tweets, average number of URLs, hashtag, and trends	Machine-learning classification and statistical analysis	Easy	(1) Presented a tool developed for scoring suspicious profiles on Twitter through a three-dimensional indicator (2) Limited features for each category were examined (3) Text and semantics in tweets were completely ignored
OddBall	Network features	Number of nodes, number of edges, weights, eigenvalues, and number of friends	Unsupervised method to detect abnormal nodes in weighted graphs	Easy	(1) Discovery of new patterns that egonets follow (2) Huge size of social network made it difficult to expand and gather network features
DARPA	Attribute features, network features, and content features	User name/avatar, geographical location, and number of followers/ followings; tweet syntax and tweet semantics, such as frequent topics; sentiment inconsistency; average number of tweets per day, average clustering coefficient of retweet, and number/ percentage of bots in cluster	Step 1: initial bot detection by manually inspecting Step 2: clustering-based outlier detection (non-negative matrix factorization and KNN search) and network analysis Step 3: classification/outlier analysis (SVMs)	Easy	(1) Algorithm detected all bots in set scene (2) System needed to be semisupervised, with help of human judgement to augment automated bot-identification processes (3) Powerful visualization tools were needed to help analysts capture suspicious robots
COMPA	Activity features and content features	Time (hour of day), message source, message text (language), message topic, links in messages, direct user interaction, and proximity	Based on user behavioral profile, anomaly detection used content and URL similarity measures	Easy	(1) Created behavioral profiles of users to detect deviation from normal model (2) Compared to previous version, COMPA looked at isolated compromises that affect high-profile accounts (3) It took a significant amount of time and computational resources to collect profile information from users (4) Accuracy of detection results depended on established behavioral profile and selected threshold

Table 3: Continued.

Model	Feature types	Feature used	Technique	Replicability of features	Remarks
SAHP	Activity features and content features	Active time, message source (terminals), message topic, link, stop word, keyword, and mention (@)	Combines information gain ratio with analytical hierarchy process algorithm	Easy	(1) Presented profile features of users more comprehensively (2) Improved on previously established COMPA methods for detecting compromised accounts (3) Detection behavior of proposed algorithm was highly dependent on threshold value, selection of which may introduce bias
TB-CoAuth	Content features	Content free, content specific, stylometric, and folksonomy	Continuous authentication of textual content, incremental learning, and supervised-machine-learning classifiers	Hard	(1) Various features are selected: content free and content specific (2) Best classifier: SVM with RBF (radial basis function) kernel (3) $F1$-score: 94.57% (4) In the era of big data, it was inappropriate to rely on statistical and manual selection of features
HoID	Content features	Hurst of Interest Distribution	Machine-learning classification (LDA) and statistical analysis (Hurst)	Hard	(1) Feature selection is novel and precise, with personal uniqueness (2) Detection process does not need investment of human resources, which greatly improves algorithm efficiency and accuracy (3) Best classifier: KNN (4) $F1$-score: 95.90%

and hobbies to detect abnormal users was then analyzed. Experimental results show that the modeling based on the distribution of user interests can improve the effect of detecting abnormal accounts.

It is found that HoID performs better than COMPA, SAHP, and TB-CoAuth on a similar dataset. It is evident from Figure 15 that the four HoID indicators are all above 95%. Each classifier's precision is similar, while the accuracy, recall, and $F1$-measure of HoID are more the 10% higher than those of COMPA and SAHP. In addition, HoID's performance also increased by approximately 1% compared with that of TB-CoAuth.

5. Conclusions

In this paper, the detection methods based on user characteristics in social platforms are simply classified and summarized, and the potential hidden dangers are identified. HoID, an abnormal detection algorithm, is proposed to quantify the distribution of user hobbies over a period of time through the LDA model, and the stability of user interests and hobbies is quantified by the Hurst index. Experiments prove that the proposed method has a good effect in abnormal-account detection, which is an improvement over previous research in which the recall rate of abnormal accounts reaches up to 97.93%. It is concluded that with increasing tweet size S, decreasing tweet-block overlap O, and increasing topic number N, the classification effects become better.

While periodic research results are obtained in this paper, several areas for improvement remain. First, the LDA model can be trained with more theme-specific text than just tweets from Twitter users. Because the length of tweets is limited and the topic is not clear enough, the topic classification effect of the LDA model is limited. Second, in terms of the selection of datasets, due to the lack of datasets in the detection of compromised accounts, the method of cross-construction is used to generate abnormal accounts, which are not very close to negative samples used in actual situations.

Data Availability

Previously reported varol-2017 data were used to support this study and are available at https://botometer.osome.iu.edu/bot-repository/datasets.html. These prior studies and datasets are cited at relevant places within the text as references [36, 37].

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the National Key R&D Program of China (grant no. 2017YFB0802803), Beijing Natural Science Foundation (grant no. 4202002), and Research Project of the Department of Computer Science in Beijing University of Technology (BJUT) (grant no. 2019JSJKY004).

References

[1] "Digital 2021: global overview report," 2021, http://datareportal.com/reports/digital-2021-global-overview-report.

[2] "Spam and phishing in 2020," 2021, http://securitylist.com/spam-and-phishing-in-2020/100512.

[3] R. Björn, P. Laura, C. Benjamin et al., "Are social bots a real threat? An agent-based model of the spiral of silence to analyze the impact of manipulative actors in social networks," *European Journal of Information Systems*, vol. 28, no. 4, pp. 394–412, 2019.

[4] H. Brian, D. P. Joseph, and M. K. Taghi, "The impact of malicious accounts on political tweet sentiment," in *Proceedings of the 4th IEEE International Conference on Collaboration and Internet Computing*, pp. 197–202, Philadelphia, PA, USA, October 2018.

[5] O. Varol, E. Ferrara, C. A. Davis et al., "Online human-bot interactions: detection, estimation, and characterization," in *Proceedings of the 11th International Conference on Web and Social Media, ICWSM 2017*, pp. 280–289, Montréal, Canada, May 2017.

[6] K. C. Yang, O. Varol, C. A. Davis et al., "Arming the public with artificial intelligence to counter social bots," *Human Behavior & Emerging Technologies*, vol. 115, 2019.

[7] L. Luceri, A. Deb, S. Giordano et al., "Evolution of bot and human behavior during elections," *First Monday*, vol. 24, no. 9, 2019.

[8] L. Luceri, S. Giordano, and E. Ferrara, "Detecting troll behavior via inverse reinforcement learning: a case study of russian trolls in the 2016 US election," in *Proceedings Of the International AAAI Conference On Web And Social Media*, pp. 417–427, Atlanta, GA, USA, June 2020.

[9] M. Kaur, D. Singh, and R. S. Uppal, "Parallel strength pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2020.

[10] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 208–301, 2021.

[11] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B: Lasers and Optics*, vol. 126, no. 9, 2020.

[12] E. Alothali, N. Zaki, E. A. Mohamed et al., "Detecting social bots on twitter: a literature review," in *Proceedings of the International Conference on Innovations in Information Technology*, pp. 175–180, Al Ain, UAE, November 2018.

[13] A. H. Wang, "Detecting spam bots in online social networking sites: a machine learning approach," *Lecture Notes in Computer Science*, vol. 6166, pp. 335–342, 2010.

[14] P. Efthimion, P. Scott, and P. Nicholas, "Supervised machine learning bot detection techniques to identify social twitter bots," *SMU Data Science Review*, vol. 1, 2018.

[15] C. Cai, L. Li, and D. Zengi, "Behavior enhanced deep bot detection in social media," in *Proceedings of the 2017 IEEE International Conference On Intelligence And Security Informatics (ISI)*, Beijing, China, July 2017.

[16] K. Sneha and F. Emilio, "Deep neural networks for bot detection," *Information Sciences*, vol. 467, pp. 312–322, 2018.

[17] V. S. Subrahmanian, A. Azaria, S. Durst et al., "The DARPA Twitter bot challenge," *Computer*, vol. 49, no. 6, pp. 38–46, 2016.

[18] J. Im, E. Chandrasekharan, J. Sargent et al., "Still out there: Modeling and identifying russian troll accounts on twitter," 2019, https://arxiv.org/abs/1901.11162.

[19] A. Addawood, A. Badawy, K. Lerman et al., "Linguistic cues to deception: identifying political trolls on social media," in *Proceedings Of the International AAAI Conference On Web And Social Media*, Münich, Germany, June 2019.

[20] S. Kumar, R. West, and J. Leskovec, "Disinformation on the web: impact, characteristics, and detection of wikipedia hoaxes," in *Proceedings of the 25th International Conference On World Wide Web*, pp. 591–602, Montréal, Canada, April 2016.

[21] H. Cai, V. W. Zheng, and C. Chang, "A comprehensive survey of graph embedding: problems, techniques, and applications," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 9, pp. 1616–1637, 2018.

[22] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2021.

[23] S. Kirill, T. Denis, and Z. Andrey, "Make social networks clean again: graph embedding and stacking classifiers for bot detection," *CEUR Workshop Proceedings*, vol. 2482, 2019.

[24] A. Seyed Ali, N. Pejman, T. Raad Bin et al., "Detect me if you can: spam bot detection using inductive representation learning," in *Proceedings of the the Web Conference 2019-Companion of the World Wide Web Conference*, pp. 148–153, New York, NY, USA, May 2019.

[25] G. Wang, X. Zhang, S. Tang et al., "Unsupervised clickstream clustering for user behavior analysis," in *Proceedings of the Chi Conference. ACM, 2016*, San Jose, CA, USA, May 2016.

[26] D. Kim, T. Graham, Z. Wan, and M.-A. Rizoiu, "Analysing user identity via time-sensitive semantic edit distance (t-sed): a case study of Russian trolls on twitter," *Journal of Computational Social Science*, vol. 2, no. 2, pp. 331–351, 2019.

[27] R. Xin, Z. Wu, H. Wang et al., "Profiling online social behaviors for compromised account detection," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 176–187, 2016.

[28] S. Wu, Q. Liu, Y. Liu et al., "Information credibility evaluation on social media," in *Proceedings of the 30th AAAI Conference On Artificial Intelligence*, pp. 4403-4404, Phoenix, ARI, USA, February 2016.

[29] Z. Yamak, J. Saunier, and L. Vercouter, "Detection of multiple identity manipulation in collaborative projects," in *Proceedings of the 25th International Conference Companion on World Wide Web*, pp. 955–960, Montréal, Canada, April 2016.

[30] N. Chavoshi, H. Hamooni, and A. Mueen, "DeBot: Twitter Bot Detection via Warped Correlation," ICDM," *IEEE Computer Society*, vol. 1, 2016.

[31] Y. Liu, J. Wang, and Y. Jiang, "PT-LDA: a latent variable model to predict personality traits of social network users," *Neurocomputing*, vol. 210, 2016.

[32] P. Zhang, H. Gu, M. Gartrell et al., "Group-based latent dirichlet allocation (group-LDA): effective audience detection for books in online social media," *Knowledge-Based Systems*, vol. 105, 2016.

[33] P. Shinjee, K. Eunhui Kim, and K. Munchurl Kim, "LDA-based unified topic modeling for similar TV user grouping and TV program recommendation," *IEEE Transactions on Cybernetics*, vol. 45, no. 8, pp. 1476–1490, 2015.

[34] Z. Gao, Y. Fan, C. Wu et al., "SeCo-LDA: mining service Co-occurrence topics for composition recommendation," *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 446–459, 2019.

[35] R. Yan and S. J. Li, "Document retrieval algorithm based on query intent identification and topic modeling," *computer engineering*, vol. 44, no. 3, pp. 189–194, 2018.

[36] O. Varol, E. Ferrara, C. A. Davis et al., "Online human-bot interactions: detection estimation, and characterization," in *Proceedings of the Eleventh International AAAI Conference on Web and Social Media*, Montréal, Canada, May 2017.

[37] J. Roesslein, "Tweepy," http://www.tweepy.org.

[38] D. Trang, F. Johansson, and M. Rosell, "Evaluating algorithms for detection of compromised social media user accounts," in *Proceedings of the 2015 Second European Network Intelligence Conference*, pp. 75–82, IEEE, Karlskrona, Sweden, September 2015.

[39] N. V. Chawla, K. W. Bowyer, L. O. Hall et al., "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, no. 1, pp. 321–357, 2011.

[40] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Towards detecting compromised accounts on social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 447–460, 2017.

[41] H. Tang, X. Wang, K. Zheng et al., "Detection of compromised accounts in osns based on a supervised analytical hierarchy process," *IET Information Security*, vol. 14, 2020.

[42] R. Kaur, S. Singh, K. Harish, and "TB-CoAuth, "Text based continuous authentication for detecting compromised accounts in social networks," *Applied Soft Computing Journal*, vol. 97, 2020.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 5597592, 11 pages
https://doi.org/10.1155/2021/5597592

Research Article

Weighted Polynomial-Based Secret Image Sharing Scheme with Lossless Recovery

Yongjie Wang, Jia Chen, Qinghong Gong, Xuehu Yan, and Yuyuan Sun

National University of Defense Technology, Hefei 230037, China

Correspondence should be addressed to Jia Chen; chenjia9624@nudt.edu.cn and Xuehu Yan; publictiger@126.com

Received 3 March 2021; Revised 14 April 2021; Accepted 16 May 2021; Published 25 May 2021

Academic Editor: Jialiang Peng

In some particular scenes, the shadows need to be given different weights to represent the participants' status or importance. And during the reconstruction, participants with different weights obtain various quality reconstructed images. However, the existing schemes based on visual secret sharing (VSS) and the Chinese remainder theorem (CRT) have some disadvantages. In this paper, we propose a weighted polynomial-based SIS scheme in the field of GF (257). We use (k, k) threshold polynomial-based secret image sharing (SIS) to generate k shares and assign them corresponding weights. Then, the remaining $n - k$ shares are randomly filled with invalid value 0 or 255. When the threshold is satisfied, the number and weight of share can affect the reconstructed image's quality. Our proposed scheme has the property of lossless recovery. And the average light transmission of shares in our scheme is identical. Experiments and theoretical analysis show that the proposed scheme is practical and feasible. Besides, the quality of the reconstructed image is consistent with the theoretical derivation.

1. Introduction

With the development of Internet technology and digital multimedia technology, digital images are more and more widely used. Meanwhile, security is also threatened. In particular, personal privacy images, confidential commercial images, medical images, and military drawings are easy to be intercepted, tampered, and destroyed in the process of storage and transmission. Cryptography [1, 2] and steganography [3, 4] are commonly used to protect images. A normal image is converted into a noise-like image through encryption technology. We cannot understand the secret image, but we can tamper with or destroy it, because it is clear that the image has been encrypted. Steganography improves the security of images, making it difficult for attackers to detect the existence of secret information. But steganography is the single-channel transmission, and if part of the area of data hiding is lost in transmission, the secret message could not be recovered.

Secret sharing (SS) is another technology to protect data with the features of multichannel transmission and loss tolerance. In 1979, Shamir [5] and Blakley [6] independently proposed the (k, n)-threshold SS scheme. The extension of SS to images is called secret image sharing (SIS). The secret image can be distributed among n participants by dividing it into n shadow images (also called shares or shadows). The secret can be reconstructed from any k or more authorized shadow images, while any $k - 1$ or fewer shadow images could not recover the secret. At present, in the SIS research field, visual cryptography schemes (VCS), also called visual secret sharing (VSS), schemes based on the CRT, and polynomial-based SIS schemes are the primary branches.

In 1995, Noar and Shamir [7] first proposed the (k, n)-threshold VCS. In general VCS, a binary image is encrypted to n shadow images on transparencies. The secret image can be obtained by superposing any k or more shadow images. The recovery process relies on the human visual system (HVS) and does not require cryptographic computation or device [8, 9]. According to the implementation principle, the VCS can be divided into schemes based on the basis matrix [7] and the random grid [10]. In the VCS field, current researches focus on these areas, including improving the visual quality of reconstructed images [11, 12],

implementing general access structures [13, 14], share authentication [15], and meaningful shadow images [16–18].

Mignotte [19] first proposed the (k, n)-threshold SS scheme based on the CRT in 1982. Then, Asmuth and Bloom [20] proposed a threshold SS scheme based on the CRT with random factors A. In their scheme, a set of integers $\{p, m_1 < m_2 < \cdots < m_n\}$ is chosen subject to certain conditions. Then, $A \in [\lfloor N/p \rfloor, \lceil (M/p) - 1 \rceil]$, where p is a prime number, $M = \prod_{i=1}^{k} m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$. Yan et al. [21] first applied the CRT to SIS. But the scheme has slight information leakage, and the recovery is lossy. Yan et al. [22] proposed a (k, n)-threshold SIS based on CRT for grayscale images. The scheme is lossless recovery and without auxiliary encryption. After that, most of the SIS schemes [23, 24] based on the CRT were studied based on Asmuth and Mignotte's scheme.

Thien and Lin [25] applied SS proposed by Shamir to SIS and first proposed a (k, n)-threshold SIS scheme. For the polynomial-based SIS, the sharing and recovery processes are simple, efficient, and easy to implement and have fewer public parameters. Therefore, polynomial-based SIS schemes are widely used [26–28]. However, most polynomial-based SIS schemes are slightly lossy. To achieve lossless recovery, many polynomial-based SIS schemes have been studied. We can segment pixel values greater than 250, operate in the field of $\mathrm{GF}(2^8)$, or choose a prime number greater than 255. In this paper, we choose the prime number 257 and use the screening operation to achieve lossless recovery.

In the above SIS schemes, the participants have the same weight and importance. However, in some scenarios, to indicate the status or importance of the participants, the shadow images need to be given different weights. Hou et al. [29] proposed a privilege-based VSS model. The model implemented a $(2, n)$-threshold VSS without pixel expansion. The participants of their scheme have the same size and different privileges. In the recovery phase, the greater the shadows' weight, the better the quality of the reconstructed image. But the average light transmissions of shares are not equal. Yang et al. [30] extended Hou et al.'s scheme with a correct privilege level, achieving the consistency of the average light transmission and the sum of privilege levels. Both Hou and Yang's schemes require a codebook and are lossy in recovery. Liu et al. [31] proposed a weighted (k, n)-threshold random grid VSS(RG-VSS) with lossless recovery. Each share has a weight in their scheme, and the secret image can be recovered by OR and XOR operations. Especially, the recovered image is lossless when using XOR operations. The secret image format of the weighted VSS schemes is only binary image. Tan et al. [23] proposed a weighted (k, n)-threshold SIS scheme based on the CRT for sharing grayscale images. Tan et al.'s scheme requires a weight generation modulus. And the average light transmissions of shares of their scheme are also unequal. To sum up, the weighted schemes based on VSS are lossy and can only share the binary images, not grayscale images. For the weighted schemes based on the CRT, we need to set parameters according to requirements in advance, and the number of participants is limited. Compared with VSS and CRT, polynomial-based SIS has some advantages. Therefore, we consider combining polynomial-based SIS with different weights to overcome the above disadvantages.

In this paper, we propose a weighted polynomial-based SIS scheme with lossless recovery. Each share is assigned to a weight. We improve Thien and Lin's scheme, choosing the prime number 257 and using the screening operation to achieve lossless recovery. A polynomial generates the n share pixel values, and then k of them are selected according to their weights. The remaining $n - k$ shadows are randomly filled with invalid value 0 or 255. In the recovery phase, when the threshold is satisfied, the greater the weight of one of the shadows or the number of shadows, the better the quality of the recovery secret image.

The contributions of our work are summarized as follows:

(1) We propose a weighted polynomial-based SIS scheme in the field of $\mathrm{GF}(257)$.

(2) When the threshold is satisfied, the number and weight of share can affect the quality of the reconstructed image. And the reconstructed image is lossless when all shares are selected.

(3) The scheme overcomes the problem that the average light transmissions of shares are not identical.

The rest of this paper is organized as follows. In Section 2, we review Shamir's scheme and Thien and Lin's scheme and then introduce the definition of the correct recovery probability (CRP). The proposed scheme and the theoretical analyses are described in Section 3. Section 4 gives experimental results and comparisons. Finally, conclusions are drawn in Section 5.

2. Preliminaries

In this section, we review the polynomial-based SIS schemes proposed by Shamir and Thien and Lin. Then, the evaluation parameter CRP of the reconstructed secret images of our scheme is given.

2.1. Review of Shamir's Scheme. In 1997, Shamir [5] proposed the (k, n)-threshold SS scheme based on polynomial properties. If a plane has k points, there exists a unique $k - 1$ degree polynomial. Shamir shared a secret S into n different shares $S_1, S_2, \ldots, S_n$ based on this property. Then, n shares were distributed to n participants $P_1, P_2, \ldots, P_n$. The secret S was chosen from the field of $\mathrm{GF}(p)$, where p is a prime greater than S and n. The polynomial of Shamir's scheme was defined as shown in

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \pmod{p}, \quad (1)$$

where the coefficient a_0 was the secret S, and the other $k - 1$ coefficients are chosen from the field of $\mathrm{GF}(p)$. In the sharing phase, we set $x = x_i$ and then obtain $f(x_i)$, where $i = 1, 2, \ldots, n$. The n pair of points $(x_i, f(x_i))$ were generated according to the above polynomial.

After obtaining n pair of points, any k or more of which can recover the secret S, while any $k-1$ or fewer pairs cannot recover the secret. The secret S can be reconstructed by using Lagrange's interpolation as shown in equation (2). When $x=0$, the secret was reconstructed by calculating $\psi(x)$, i. e., $S=\psi(0)$.

$$\psi(x)=\sum_{i=1}^{k} f(x_i) \prod_{j=1, j\neq i}^{k} \frac{x-x_j}{x_i-x_j} \pmod p, \tag{2}$$

where $x_i \neq x_j$, and $i, j = 1, 2, \ldots, n$.

2.2. Review of Thien and Lin's Scheme. Thien and Lin [25] first applied the SS scheme to share a secret grayscale image in 2002. In their scheme, a secret image S was shared to n shadow images $\mathrm{SC}_1, \mathrm{SC}_2, \ldots, \mathrm{SC}_n$, and any k or more of which can recover the secret image. In Thien and Lin's scheme, all the coefficients were used to share the secret image's pixels. Then, the successive k pixels of the secret image were shared through a polynomial presents two problems. The first is that each shadow image size is $(1/k)$ of the original secret image. Second, there may be information leakage because of the correlation among pixels. Therefore, the secret image pixels should be encoded before the sharing phase to increase security. In Thien and Lin's scheme, the value of prime p was taken as 251. However, the range of the 8-bit grayscale image pixel value was $[0, 255]$. The pixels between 251 and 255 were truncated to 250, resulting in the fact that all the pixels were within $[0, 250]$. Therefore, the reconstructed secret images were lossy. At the same time, the method of lossless recovery was provided in their scheme. The secret pixel values of more than 250 required additional operations, and that led to the expansion of shadow images.

There are 256 pixels of the 8-bit grayscale image between 0 and 255. To achieve lossless recovery, all need to be included in the sharing phase. A prime number greater than 256 is 257, $[0, 255] \subset \mathrm{GF}(257)$. But 256 also belongs to $\mathrm{GF}(257)$, and the sharing process needs to be redone if a pixel value is shared to 256. Random numbers are generated to update the other $k-1$ coefficients in the polynomial except a_0 until all the share pixel values are within $[0, 255]$. Thus, the probability P of an invalid value occurring when sharing a pixel is $P = (257 - 256/257) \times 100\% \approx 0.389\%$. At the same time, in the weighted SIS scheme, we filled in 0 and 255 as invalid values. That is to say, there may be three invalid values, i.e., 0, 255, and 256, during the sharing of a pixel value. The probability P_w of an invalid value occurring per share operation is $P_w = (3/257) \times 100\% \approx 1.167\%$. This can achieve lossless recovery, and the efficiency of sharing is not greatly affected, which is within the acceptable range. Therefore, in our scheme, we choose the prime number 257 and use the screening operation.

2.3. Correct Recovery Probability (CRP). For the quality evaluation of the reconstructed image in the general SIS schemes, the most commonly used is mean squared error (MSE) and peak sign-to-noise value relation (PSNR). MSE is used to assess the distinction between the recovered image and the secret image. The lower MSE value indicates that the reconstructed image is close to the original image. PSNR represents the reconstructed image's quality. The higher the PSNR value is, the closer the reconstructed image is to the original image.

In our weighted SIS scheme, we adopt the correct recovery probability (CRP) [32] to evaluate the reconstructed image's quality. CRP is the ratio of the number of identical pixels in the same locations between the reconstructed image and the secret image to the image's total pixels. The higher the CRP value is, the more the number of pixel values is recovered correctly, that is, the closer the reconstructed image is to the secret image. The reconstructed image is lossless when $\mathrm{CRP} = 1$.

For a secret image S with the size of $A \times B$, the CRP of its reconstructed image S' is calculated by

$$\mathrm{CRP} = \frac{T}{A \times B}, \tag{3}$$

where T is the number of identical pixels in the same locations in both two images.

3. The Proposed Scheme

In this section, we propose a weighted polynomial-based SIS scheme based on Shamir's scheme. To achieve lossless recovery, we choose the prime number 257 and use the screening operation. Each participating shadow image is assigned a weight, and the sum of these weights is equal to 1. Each pixel of the secret image generates k share pixel values by a polynomial, and we assign them weights. The remaining $n-k$ shares are randomly filled with invalid value 0 or 255.

When recovering the secret image, we adopt Lagrangian interpolation to obtain the secret pixel values. The secret image cannot be recovered from less than k shares. When more than k shares are collected, the higher the weights of the shares are, the better the recovered secret image's quality is. At the same time, our scheme can achieve lossless recovery when all the shadow images are used to participate in the recovery. The design idea of the sharing phase of our scheme is shown in Figure 1.

3.1. The Sharing Phase. In the sharing phase of our scheme, for each pixel of the original secret image, k share pixels are generated by the polynomial-based SIS scheme with a (k, k)-threshold $(\mathrm{PSIS}(k, k))$. Then, k shares are distributed to k participants through a certain probability determined by the weights of the participants, and the shares of the other $n-k$ participants are filled with invalid values. The detailed steps are described in Algorithm 1.

In the sharing phase, each shadow image is assigned a certain weight. Suppose that the weights of shares are $w_1, w_2, \ldots, w_n$, where $w_1 + w_2 + \cdots + w_n = 1$. Then, we set corresponding weight interval for each shadow image in the interval of $[0, 1]$ as shown in Figure 2. The proportion of the $t-$th interval in the whole interval is w_t. We randomly generate any real numbers x in the interval of $[0, 1]$. If $x \in [w_1 + w_2 + \cdots + w_{t-1}, w_1 + w_2 + \cdots + w_{t-1} + w_t]$,

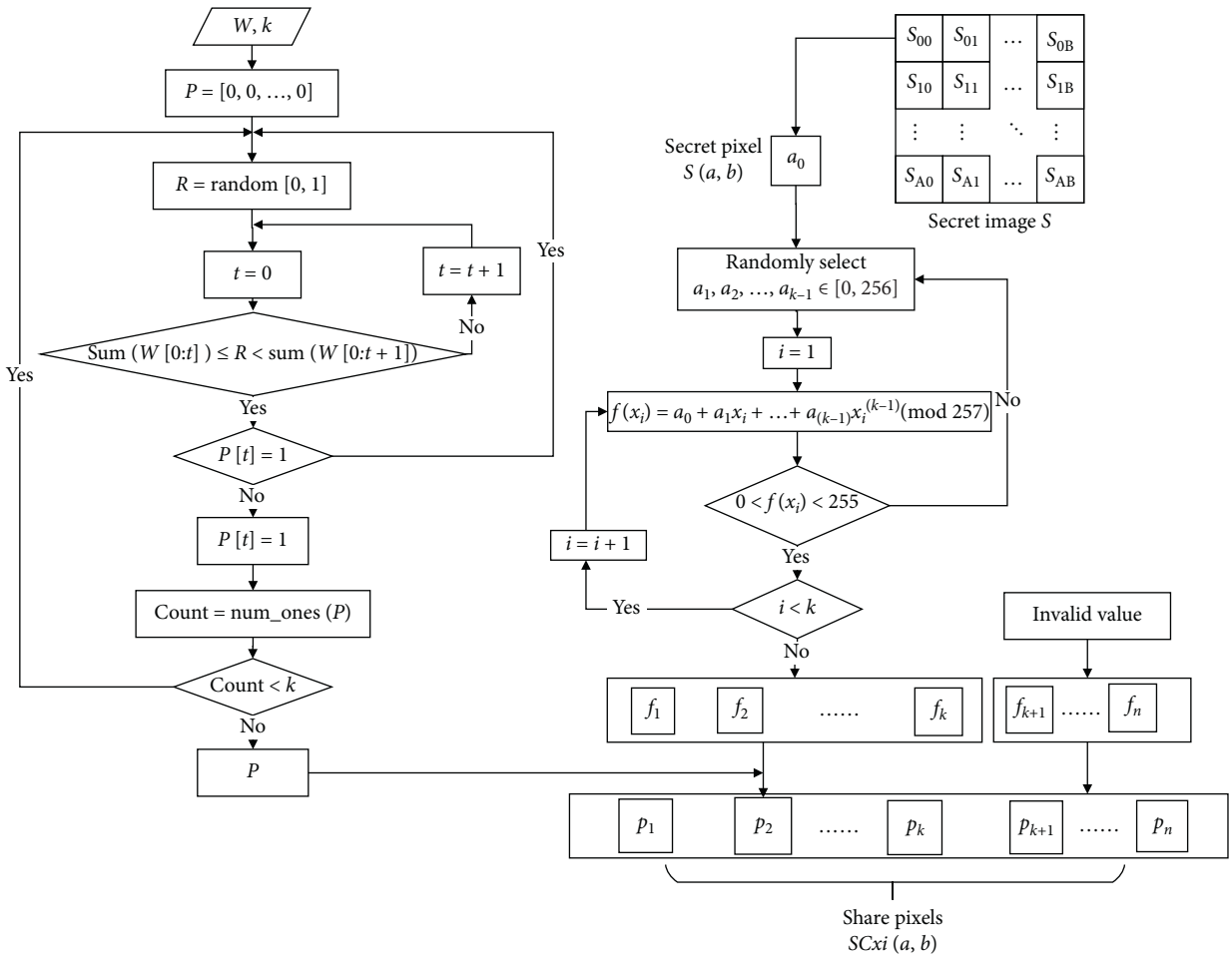


Figure 1: The flowchart for generating shares with different weights.

(1) Input: a secret image S with the size of $A \times B$; the threshold parameters (k, n); n participant serial numbers $x_1, x_2, \ldots, x_n$; the weights $W = [w_1, w_2, \ldots, w_n]$; initial share allocation list P.
(2) Output: n shadow images $\mathrm{SC}_1, \mathrm{SC}_2, \ldots, \mathrm{SC}_n$.
(3) Step 1. Repeat Steps 2–7 for each pixel of the secret image, where the pixel position is $(a, b) \in \{(a, b) | 1 \le a \le A, 1 \le b \le B\}$.
(4) Step 2. Randomly generate any real number R in the interval of [0, 1]. When $\mathrm{sum}(W[0{:}\ t]) < R < \mathrm{sum}(W[0{:}\ t+1])$, let $P[t] = 1$. If $P[t]$ has been set to 1, a random number will be generated again until the number of "1" in the share allocation list P is k.
(5) Step 3. Set polynomial coefficient, where $a_0 = s$, and $a_1, \ldots, a_{k-1}$ are assigned to a random value within the field of GF(257).
(6) Step 4. Repeat Steps 5–6 until k share values are calculated for each participant $P(x_i)(i \in [1, k])$.
(7) Step 5. Calculate the shared value $f(x_i)$ by the formula $f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \mathrm{mod} 257$.
(8) Step 6. If $0 < f(x_i) < 255$, continue or return to Step 3 and redo Steps 3–6.
(9) Step 7. Scan the share allocation list P; if $P[t] = 1$, valid values $f(x_i)$, $(i \in [1, k])$ are assigned to $\mathrm{SC}_t(a, b)$; if $P[t] = 0$, randomly fill in the invalid value.
(10) Step 8. Output n shadow images $\mathrm{SC}_1, \mathrm{SC}_2, \ldots, \mathrm{SC}_n$.

Algorithm 1: The sharing process of the weighted polynomial-based SIS scheme.

Figure 2: The weights interval partition.

participant P_t is selected, i.e., $P[t] = 1$. If the interval has been selected before that, i.e., $P[t]$ has been set to 1, then random real number will be generated to perform the above operation. This process is repeated until k different participants are selected. By performing this operation, k shares have been distributed to k of the n participants according to a certain probability, while the remaining $n-k$ participants have been distributed to invalid values.

3.2. The Recovery Phase. Our scheme is based on the polynomial-based SIS scheme and can be recovered by Lagrangian interpolation. The secret image cannot be recovered from less than k shares. When more than k shares are collected, the higher the weights of the shares are, the better the recovered secret image's quality is. If all the shares participate in the restoration of the secret image, the reconstructed image is lossless. The specific recovery steps are shown in Algorithm 2.

3.3. Theoretical Analyses. In this subsection, some theoretical analyses of our scheme are presented. First, our weighted polynomial-based SIS scheme is based on Shamir's scheme. The constant coefficient of the polynomial is replaced with the pixel value of the secret image. And all the operations are performed in the field of GF(257). There are 256 pixels of grayscale image, and $[0, 255] \subset \mathrm{GF}(257)$. Therefore, our scheme can be applied to grayscale images. According to the principle of polynomial and Lagrange interpolation algorithm, any less than k equations cannot obtain the polynomial coefficients. Thus, $k-1$ or fewer shares could not recover the pixel value of the secret image. Because we fill in invalid values to represent different weights of shares, when k shares are involved in reconstruction, some pixel values cannot be correctly recovered. When all shares are involved in reconstruction, we can exclude all invalid values and then use the remaining k valid values to recover the secret image's corresponding pixel value. Therefore, our scheme can achieve lossless recovery.

Then, we theoretically analyze the quality and the effect factors of the reconstructed secret image. Each share is assigned a weight w_i in the proposed scheme, and $\sum_{i=1}^{n} w_i = 1$. The reconstructed secret image's quality is related to the weights of the shares involved in the reconstruction. To evaluate the quality of the reconstructed secret image, we compared the pixels in the corresponding positions of the two images, counted the number of identical pixels in the same positions, and combined them with the weights. Then, we calculated the CRP of the reconstructed secret image in our scheme with (k, n)-threshold theoretically as $\mathrm{CRP}_t(S)$ according to

$$\mathrm{CRP}_t(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}, \tag{4}$$

where k, n are threshold parameters, and t denotes the number of shares involved in the reconstruction. i_j is the j th share in the i th combination, w_{i_j} denotes the weight of share i_j, and $\sum_{j=1}^{t} w_{i_j} = 1$. The number of combinations of arbitrary k of t shares is denoted by C_t^k $(k \le t \le n)$. $\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}$ denotes the probability sum that arbitrary k of t shares are selected. The probability sum that arbitrary k of t shares are selected is denoted by $\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}$.

Intuitively, we can guess that the number and weight of shadows can affect the reconstructed secret image's quality. Theoretically, if the threshold is satisfied, and the number of shadows is increased, the recovery quality of the secret image will be better. When all shadows participate in reconstruction, the secret image can be recovered in a lossless way. That is to say, our scheme is progressive in reconstruction. Second, if the threshold is satisfied, and the weight of one of the shadows in the set increases, the recovery quality of the secret image will be better.

Assuming that there are t shadows in the set, the secret image could be recovered when these shadows participate in the recovery. The CRP of the reconstructed image is shown in equation (4). If another shadow l is added in the set to participate in the recovery, and the weight of shadow l is w_l, then the CRP of the reconstructed image of $t+1$ shadows recovery as $\mathrm{CRP}_t(S)$ is calculated by

$$\mathrm{CRP}'_t(S) = \frac{\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}. \tag{5}$$

When comparing the two reconstructed images' quality, it can be determined by subtracting $\mathrm{CRP}_t(S)$ and $\mathrm{CRP}'_t(S)$. The result is shown in

$$\mathrm{CRP}'_t(S) - \mathrm{CRP}_t(S) = \frac{\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j} - \sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}. \tag{6}$$

According to the properties of combinatorial numbers, equation (7) holds.

$$\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j} = \sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_l \left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j} \right), \tag{7}$$

where $i'_j \neq l$.

Therefore, equation (6) can be rewritten as

$$\begin{aligned} \mathrm{CRP}'_t(S) - \mathrm{CRP}_t(S) &= \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_l \left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j} \right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \\ &\quad - \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \\ &= \frac{w_l \left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j} \right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k}} > 0, \end{aligned} \tag{8}$$

where $i'_j \neq l$.

(1) Input: k shadow images $SC_{i_1}, SC_{i_2}, \ldots, SC_{i_k}$ and the corresponding participant serial number x_{i_j}, $(i_1, i_2, \ldots, i_k) \subseteq \{1, 2, \ldots, n\}$
(2) Output: the original secret image S
(3) Step 1. Repeat Steps 2–4 for each pixel $SC_{i_j}(a, b)$ of the shadow image, where $(a, b) \in \{(a, b) | 1 \le a \le A, 1 \le b \le B\}$.
(4) Step 2. Judge whether the share pixel value is invalid value 0 or 255. Only if it is valid, it will participate in the recovery.
(5) Step 3. Calculate Lagrange interpolation $f(x)$ in the field of GF(257) by the formula $\psi(x) = \sum_{j=1}^{k} f(i_j) \prod_{\substack{l=1 \\ l \neq j}}^{k} ((x - i_l)/(i_j - i_l))$. Then, set $x = 0$ to obtain $f(0)$.
(6) Step 4. $S(a, b) = f(0)$.
(7) Step 5. Output the recovered image S.

Algorithm 2: The recover procedure of the weighted polynomial-based SIS scheme.

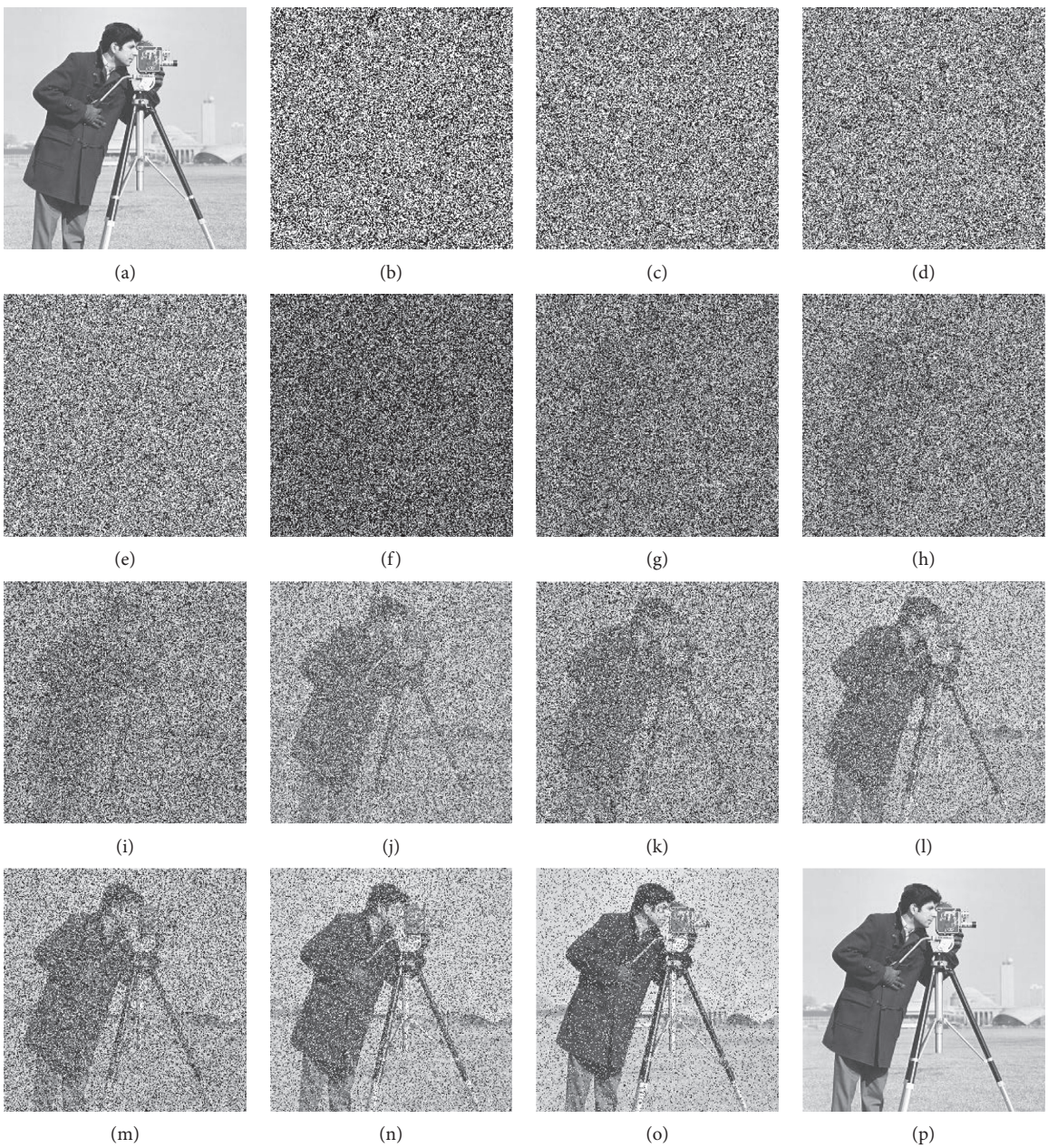
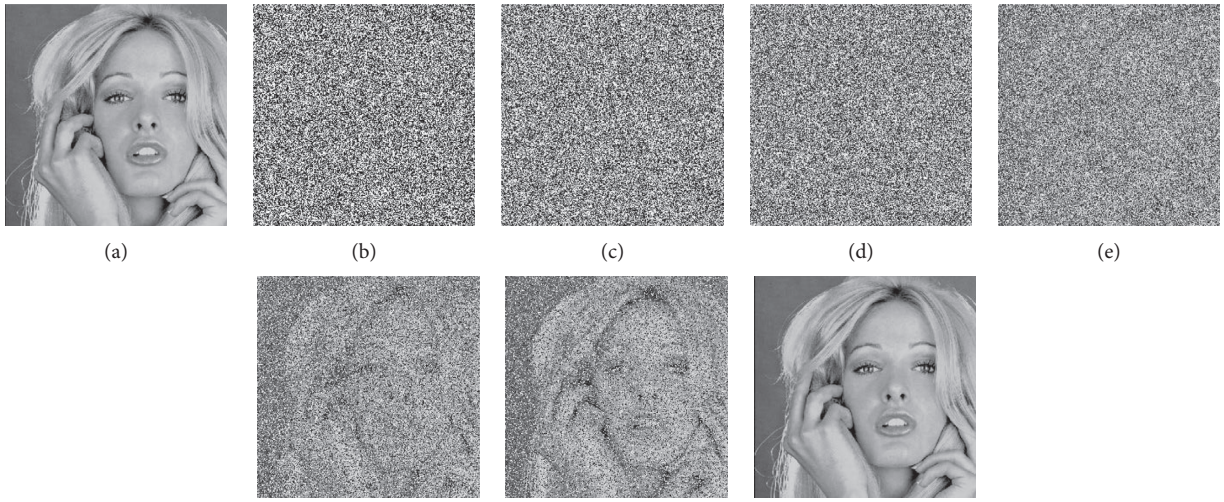


Figure 3: Our $(2, 4)$-threshold weighted SIS scheme. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) $SC_{1,2}$. (g) $SC_{1,3}$. (h) $SC_{1,4}$. (i) $SC_{2,3}$. (j) $SC_{1,2,3}$. (k) $SC_{2,4}$. (l) $SC_{1,2,4}$. (m) $SC_{3,4}$. (n) $SC_{1,3,4}$. (o) $SC_{2,3,4}$. (p) All. In $f - p$, the subscript indicates the number of shares involved in the reconstruction.



(a) (b) (c) (d) (e)

(f) (g) (h)

Figure 4: Our $(2,3)$-threshold weighted SIS scheme. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) $SC_{1,2}$. (f) $SC_{1,3}$. (g) $SC_{2,3}$. (h) $SC_{1,2,3}$. In $e-h$, the subscript indicates the number of shares involved in the reconstruction.

Table 1: Evaluating the quality of reconstructed images for $(2,4)$-threshold scheme.

Participants	Weights	Weights sum	Identical pixels in Tan's	Identical pixels in our	$CRP_{Our}(S)$	$CRP_{Tan}(S)$	$CRP_t(S)$
[1, 2]	[0.1, 0.2]	0.3	3258	3393	0.0497	0.0518	0.0571
[1, 3]	[0.1, 0.3]	0.4	5190	5119	0.0792	0.0781	0.0857
[1, 4]	[0.1, 0.4]	0.5	7475	7340	0.1141	0.1120	0.1143
[2, 3]	[0.2, 0.3]	0.5	10548	10703	0.1609	0.1633	0.1714
[2, 4]	[0.2, 0.4]	0.6	15392	15353	0.2349	0.2343	0.2286
[3, 4]	[0.3, 0.4]	0.7	24649	24439	0.3761	0.3729	0.3428
[1, 2, 3]	[0.1, 0.2, 0.3]	0.6	18684	18760	0.2851	0.2863	0.3143
[1, 2, 4]	[0.1, 0.2, 0.4]	0.7	25672	25781	0.3916	0.3917	0.4000
[1, 3, 4]	[0.1, 0.3, 0.4]	0.8	36937	36560	0.5636	0.5579	0.5429
[2, 3, 4]	[0.2, 0.3, 0.4]	0.9	50158	50240	0.7654	0.7666	0.7429
[1, 2, 3, 4]	[0.1, 0.2, 0.3, 0.4]	1.0	65536	65536	1.0	1.0	1.0

Table 2: Evaluating the quality of reconstructed images for $(2,3)$-threshold scheme.

Participants	Weights	Weights sum	Identical pixels	$CRP_{Our}(S)$	$CRP_t(S)$
[1, 2]	[0.2, 0.3]	0.5	10721	0.1636	0.1935
[1, 3]	[0.2, 0.5]	0.7	21326	0.3254	0.3226
[2, 3]	[0.3, 0.5]	0.8	34005	0.5189	0.4839
[1, 2, 3]	[0.2, 0.3, 0.5]	1.0	65536	1.0	1.0

In equation (8), $CRP'_t(S)$ is greater than $CRP_t(S)$. That is to say, the quality of the reconstructed secret image from $t+1$ shadows is better than that of t shadows. Therefore, if the threshold is satisfied, the reconstructed image's quality will improve with the increase in the number of shadows involved in the recovery.

Assuming that there are t shadows in the set, the secret image could be recovered when these shadows participate in the recovery. The shadow v is replaced by the more heavily weighted shadow u, where $w_v > w_u$. According to equations (8) and (7), we can get equations (9) and (10).

$$CRP_t^v(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_v\left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j}\right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}, \tag{9}$$

where $i'_j \neq v$;

$$CRP_t^u(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_u\left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j}\right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}, \tag{10}$$

where $i'_j \neq u$.

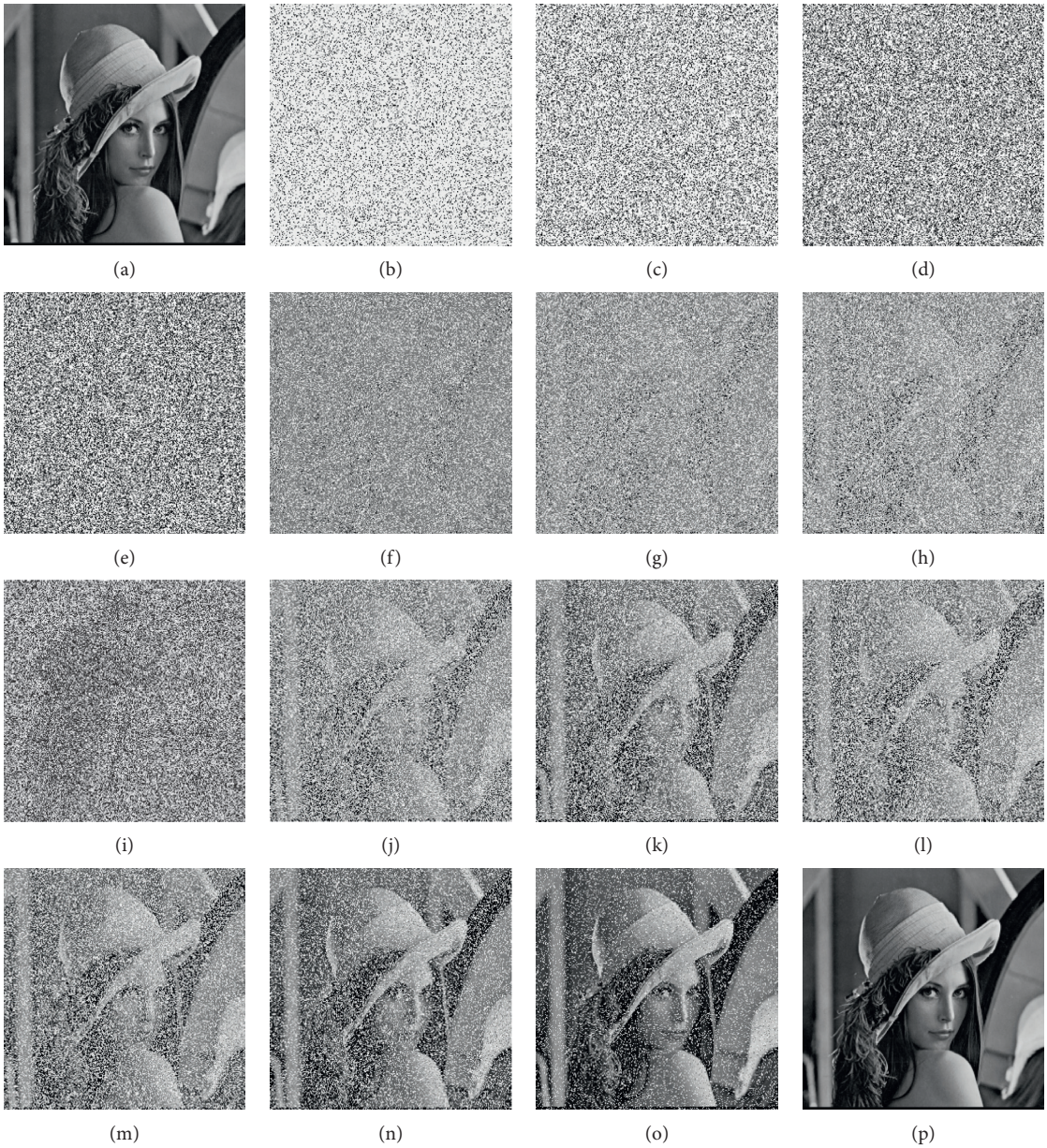


Figure 5: Tan's $(2,4)$-threshold weighted SIS scheme based on CRT. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) $SC_{1,2}$. (g) $SC_{1,3}$. (h) $SC_{1,4}$. (i) $SC_{2,3}$. (j) $SC_{2,4}$. (k) $SC_{3,4}$. (l) $SC_{1,2,3}$. (m) $SC_{1,2,4}$. (n) $SC_{1,3,4}$. (o) $SC_{2,3,4}$. (p) All. In $f-p$, the subscript indicates the number of shares involved in the reconstruction.

Then, the result of subtracting equations (9) from (10) is shown in

$$\mathrm{CRP}_t^u(S) - \mathrm{CRP}_t^v(S) = \frac{(w_u - w_v)\left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j}\right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j} > 0.} \quad (11)$$

As shown in equation (11), $\mathrm{CRP}_t^u(S)$ is greater than $\mathrm{CRP}_t^v(S)$. Therefore, if the threshold is satisfied, the reconstructed image's quality will improve with increasing the weight of one of the shadows.

4. Experiment and Evaluation

In this section, we give two examples to verify the feasibility of the scheme in the Subsection 4.1 and evaluate the reconstructed image's quality in the Subsection 4.2. Then, we compare other weighted SIS schemes in the Subsection 4.3.

4.1. Image Illustration. To verify the feasibility of our scheme, two examples with $(2,4)$ and $(2,3)$ thresholds are given using Python in a PC with Windows 10. Figure 3

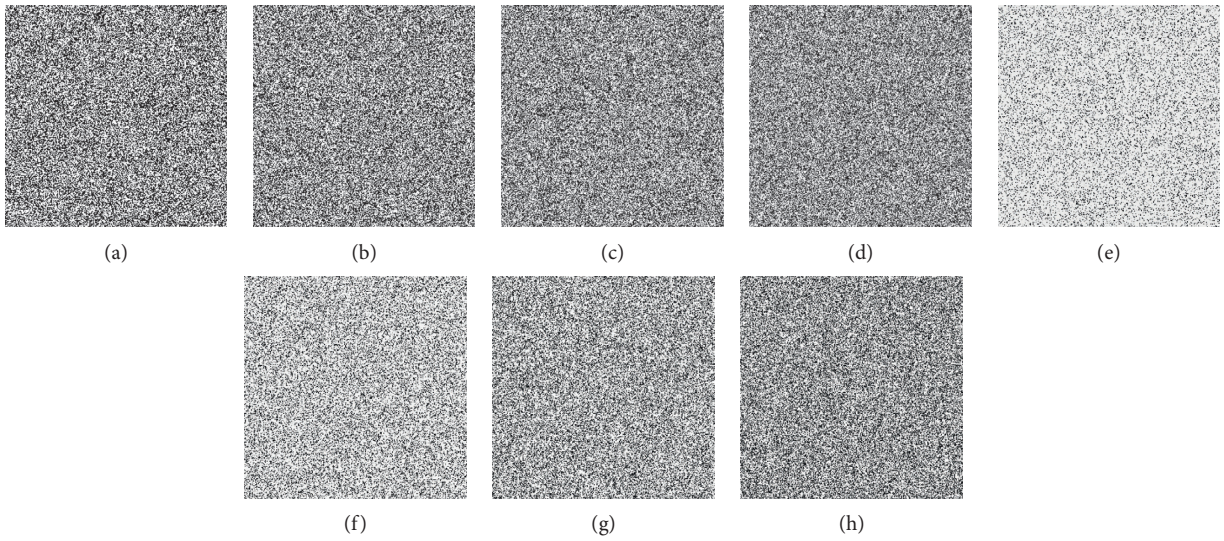


Figure 6: The average light transmission of shares in two schemes. $(a \sim d)$ are our scheme. $(e \sim j)$ are Tan's scheme.

Table 3: Comparisons with the characteristics of weighted schemes.

	Threshold	Image format	Based methods	Is lossless?	Identical average light transmission?	Additional information
Hou et al. [29]	$(2, n)$	Binary image	VSS	No	Yes	Codebook
Yang et al. [30]	$(2, n)$	Binary image	VSS	No	Yes	Codebook
Liu et al. [31]	(k, n)	Binary image	VSS	Yes	Yes	Weight generation and RG
Tan et al. [23]	(k, n)	Grayscale image	CRT	Yes	No	Weight generation and modulus
Our	(k, n)	Grayscale image	Polynomial	Yes	Yes	Weight generation

illustrates our $(2, 4)$-threshold SIS scheme. A Cameraman image with the size of 256×256 is tested as the secret image as shown in Figure 3(a). The weights of the shares are $W = [0.1, 0.2, 0.3, 0.4]$. Figures 3(b) ~ 3(e) show four shares generated by a polynomial. When two shares are collected, the secret image could be recovered. Figures 3(f) ~ 3(p) show the results of different weights of shares participating in recovery, and the sum of weights goes from low to high. When all shares participate in reconstruction, the secret image can be recovered in a lossless way as shown in Figure 3(p). The subscript of the name indicates the number of shadows involved in the reconstruction.

Figure 4 shows our $(2, 3)$-threshold SIS scheme. The secret image is the blonde woman image with the size of 256×256 as shown in Figure 4(a). The weights of the shares are $W = [0.2, 0.3, 0.5]$. The three shares are shown in Figures 4(b) ~ 4(d). Figures 4(e) ~ 4(g) display the reconstructed images recovered from two shares. Figure 4(h) presents the reconstructed lossless image recovered from all shares. The subscript of the name indicates the number of shadows involved in the reconstruction.

4.2. Quality of the Reconstructed Images. In our scheme, each share is assigned a weight in the sharing phase, and the recovery phase is progressive. Both the weight and the number of shadows affect the quality of the reconstructed image. The CRP is used to evaluate the quality of the reconstructed images. The greater the CRP value, the better the quality of the reconstructed image, and the more effective our scheme. Equations (4) and (5) are used to compute $\mathrm{CRP}(S)$ and $\mathrm{CRP}_t(S)$. $\mathrm{CRP}_{\mathrm{Our}}(S)$ represents the actual value of the experiment for our proposed scheme. $\mathrm{CRP}_t(S)$ denotes the theoretical value. The results of our $(2, 4)$ and $(2, 3)$ threshold weighted schemes are shown in Tables 1 and 2.

From Figure 3 and Table 1, we can draw the following conclusions:

(1) Our weighted polynomial-based SIS scheme is effective, and the shadows have weights that can affect the quality of the recovered secret image.

(2) The quality of the reconstructed image is consistent with theoretical estimates.

(3) When the numbers of shares involved in reconstruction are the same, the greater the sum of the weights is, the better the reconstructed image's quality is. When the sums of the weights of the shares are the same, the more shares involved in the reconstruction are, the better the quality of the

reconstructed image is. When the number and weights sum of shares involved in the reconstruction are the same, the reconstructed image's quality is judged according to the identical pixels in two images.

4.3. Comparison with Other Weighted SIS Schemes. In this subsection, we compare our scheme with other weighted SIS schemes from several relevant features. Figure 5 shows Tan's $(2,4)$-threshold scheme based on the CRT with $(p, m_1, m_2, m_3, m_4) = (131, 247, 249, 251, 253)$. The weights of shares are also $W = [0.1, 0.2, 0.3, 0.4]$. Figure 5(a) shows the secret image Lena with the size of 256×256. Figures 5(b) ~ 5(e) are four shares. Figures 5(f) ~ 5(p) are reconstructed secret images by collecting different shares, in which Figure 5(p) is lossless by collecting all shares. Each share has a weight in both our scheme and Tan's scheme, and the reconstructed secret image can be recovered in a lossless way.

From Table 1, we can find that the theoretical values are the same between our scheme and Tan's scheme. And our experimental values are similar to those of Tan's scheme, which are consistent with the theoretical values. This is because the same method is used to give weight to each share in our scheme and Tan's scheme. The obvious difference between the two schemes is the average light transmission of shares as shown in Figure 6. There is no obvious difference for the average light transmission of four shares in our scheme. For the remaining $n-k$ shares, we fill with invalid value 0 or 255 randomly. However, the average light transmissions of four shares in Tan's scheme are different. In their scheme, the remaining $n-k$ shares are filled with the corresponding privacy modulus. As the weight increases, the shadow image gets darker. Obviously, this phenomenon will leak out the importance of shadow images and reduce the security of the weighted scheme to some extent.

In general, SIS schemes have many features. Table 3 shows the main characteristics and comparisons of our scheme with related weighted schemes. All schemes listed are weighted schemes. Liu et al.'s, Tan et al.'s, and our schemes with (k,n)-threshold are more flexible than $(2,n)$-threshold of Hou et al. and Yang et al. Image format, lossless recovery, and additional information are related to the sharing method. Compared to the methods based on VSS and the CRT, our polynomial-based scheme has many advantages, such as less computation, less additional information, and lossless recovery. Meanwhile, compared with Tan's scheme, we overcome the problem that the average light transmissions of shares are not identical.

5. Conclusion

In this paper, a weighted SIS scheme with lossless recovery is proposed. Each share has a weight. The larger the weight is, the greater the influence on the reconstructed image's quality is, when it participates in the recovery. When the threshold of secret image recovery is satisfied, the number and weight of share can affect the reconstructed image's quality. When all shares are involved in the reconstruction, the reconstructed image can be lossless. And we overcome the problem that the average light transmissions of shares are not identical. Theoretical analysis and experimental results show the effectiveness of the scheme. In future work, we will extend our weighted SIS scheme for color images and study the polynomial-based SIS scheme in the field of $GF(2^8)$.

Data Availability

Some or all data, models, or code generated or used during the study are available from the corresponding (chenjia9624@nudt.edu.cn) author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is funded by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (number: 61602491). The authors are thankful to the reviewers for their valuable comments and suggestions to improve the manuscript.

References

[1] L. Li, A. A. A. El-Latif, Z. Shi, and X. Niu, "A new loss-tolerant image encryption scheme based on secret sharing and two chaotic systems," *Research Journal of Applied Ences, Engineering and Technology*, vol. 4, no. 8, pp. 877–883, 2012.

[2] A. A. A. El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on ISB matching revisited," *IEEE Trans Inform Forensics Secure*, vol. 5, no. 2, pp. 201–214, 2010.

[5] S. Adi, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[6] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the AFIPS National Computer Conference*, vol. 48, June 1979.

[7] M. Naor and A. Shamir, "Visual cryptography," *Lecture Notes in Computer Science*, vol. 950, no. 9, pp. 1–12, 1994.

[8] X. Yan, S. Wang, and X. Niu, "Threshold construction from specific cases in visual cryptography without the pixel expansion," *Signal Processing*, vol. 105, pp. 389–398, 2014.

[9] X. Yan, S. Wang, A. A. A. El-Latif, X. Niu, and Z. Wei, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," *Multimedia Tools and Applications*, vol. 74, no. 9, pp. 3231–3252, 2015.

[10] X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 61–73, 2018.

[11] X. Wu, T. Liu, and W. Sun, "Improving the visual quality of random grid-based visual secret sharing via error diffusion,"

Journal of Visual Communication and Image Representation, vol. 24, no. 5, pp. 552–566, 2013.

[12] X. Yan, S. Wang, A. A. A. El-Latif, X. Niu, and Z. Wei, "A new assessment measure of shadow image quality based on error diffusion techniques," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 118–126, 2013.

[13] S. Shyu Jian, "Visual cryptograms of random grids for general access structures," *Theoretical Computer Science*, vol. 565, pp. 30–49, 2015.

[14] X. Yan and Y. Lu, "Progressive visual secret sharing for general access structure with multiple decryptions," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 1–20, 2017.

[15] X. Yan, Y. Lu, C. N. Yang, X. Zhang, and S. Wang, "A common method of share authentication in image secret sharing," *IEEE Transactions on Circuits and Systems for Video Technology Early Access*, vol. 193, p. 1, 2020.

[16] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 307–322, 2011.

[17] X. Wu and W. Sun, "Extended capabilities for XOR-based visual cryptography," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1592–1605, 2017.

[18] A. A. A. El-Latif, X. Yan, L. Li, N. Wang, J. Peng, and X. Niu, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," *Optics Laser Technology*, vol. 54, pp. 389–400, 2013.

[19] M. Mignotte, "How to share a secret," *Eurocrypt*, vol. 149, no. 4, pp. 371–375, 1982.

[20] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.

[21] W. Yan and Q. Dongxu, "Image sharing based on Chinese remainder theorem," *Journal of North China University of Technology*, vol. 12, no. 1, pp. 6–9, 2000.

[22] X. Yan, Y. Lu, L. Liu, S. Wan, and H. Liu, "Chinese remainder theorem-based secret image sharing for (k, n) threshold," in *Proceedings of the International Conference on Cloud Computing and Security*, November 2017.

[23] L. Tan, Y. Lu, X. Yan, L. Liu, and L. Li, "Weighted secret image sharing for a (k, n) threshold based on the Chinese remainder theorem," *IEEE Access*, no. 99, p. 1, 2019.

[24] L. Li, Y. Lu, X. Yan, L. Liu, and L. Tan, "Lossless (k, n)-threshold image secret sharing based on the Chinese remainder theorem without auxiliary encryption," *IEEE Access*, vol. 7, pp. 75113–75121, 2019.

[25] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[26] P. Li, C.-N. Yang, and Q. Kong, "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 41–50, 2018.

[27] P. Li, Z. Liu, and C. N. Yang, "A construction method of (t, k, n) -essential secret image sharing scheme," *Signal Processing Image Communication*, vol. 65, pp. 210–220, 2018.

[28] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3848–3858, 2020.

[29] Y. C. Hou, Z. Y. Quan, and C. F. Tsai, *A Privilege-Based Visual Secret Sharing Model*, Academic Press, Inc., Cambridge, USA, 2015.

[30] C.-N. Yang, J.-K. Liao, and D.-S. Wang, "New privilege-based visual cryptography with arbitrary privilege levels," *Journal of Visual Communication and Image Representation*, vol. 42, pp. 121–131, 2017.

[31] F. Liu, X. Yan, X. Yan, L. Liu, Y. Lu, and L. Tan, "Weighted visual secret sharing with multiple decryptions and lossless recovery," *Mathematical Biosciences and Engineering*, vol. 16, no. 5, pp. 5750–5764, 2019.

[32] L. Liu, Y. Lu, X. Yan, and H. Wang, "Greyscale-images-oriented progressive secret sharing based on the linear congruence equation," *Multimedia Tools and Applications*, vol. 77, 2017.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 5531505, 16 pages
https://doi.org/10.1155/2021/5531505

Research Article

Generalized Proxy Oblivious Signature and Its Mobile Application

Shin-Yan Chiou [1,2] **and Yi-Xuan He** [1]

[1]*Department of Electrical Engineering, College of Engineering, Chang Gung University, Kwei-Shan, Taoyuan, Taiwan*
[2]*Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, Taoyuan, Taiwan*

Correspondence should be addressed to Shin-Yan Chiou; ansel@mail.cgu.edu.tw

Received 19 February 2021; Revised 17 April 2021; Accepted 3 May 2021; Published 25 May 2021

Academic Editor: Manjit Kaur

Oblivious signature ensures users select from the specified candidates. However, users can choose only one candidate. This paper proposes a generalized oblivious signature scheme with proxy function. The scheme can be applied to many applications such as multichoice e-voting or e-lottery. Since there have been many applied research studies on e-voting, in this paper, we decided to apply this scheme to e-lottery, which is fair, secure, efficient, multiselect, and agent-based. In the lottery system, the server cannot cheat after a user makes a choice, and no one even the proxy can get any benefits. The signature scheme along with the lottery system is proved secure in the random oracle model. The lottery system is also implemented on Android smartphones. To the best of our knowledge, this is the first work done on a generalized proxy oblivious signature along with a fair and secure multiple-choice e-lottery system.

1. Introduction

In recent years, network transactions for applications such as Internet auctions and banking have increased greatly. Network and mobile security technologies play important roles in protecting users' privacy [1–4]. In this regard, digital signatures have attracted considerable attention. By using public key cryptography, a signer can sign a message using his or her private key, which is owned only by the signer, to create a digital signature for the message. Then, any verifier can validate the correctness of this signature by using the signer's public key.

However, it is necessary to protect the privacy of signature receivers in some situations, such as the contents of signed message in a digital cash system or the choices from candidates in an e-voting situation. In 1982, Chaum [5] introduced a blind signature scheme to offer blindness which protects the signee's privacy. In 2013, Nayak et al. [6] proposed a blind signature scheme based on an elliptic curve discrete logarithm problem. In 1981, Rabin [7] introduced the concept of oblivious transfer. In 1994, Chen [8] proposed the concept of oblivious signatures and considered two types of oblivious signature schemes. In 2008, Tso et al. [9] provided formal definitions and security requirements for an oblivious signature scheme. In 2012, Chou [10] proposed a more efficient and secure k-out-of-n oblivious transfer scheme. In 2018, Zhang et al. [11] proposed a new post-quantum blind signature from lattice assumptions. In 2019, Wang et al. [12] introduced a new construction of blind signatures from braid groups.

In 1996, Mambo et al. [13] proposed the concept of proxy signature. Various proxy-based schemes have been proposed [14, 15]. In 2000, Lin et al. [16] proposed the first proxy blind signature scheme that combines the functionalities of both proxy signatures and blind signatures. In 2002, Tan et al. [17] proposed a proxy blind signature scheme; however, in 2003, Lal et al. [18] showed this scheme to be insecure and further proposed a new scheme that is secure and more efficient than Tan's scheme. In 2013, Yang et al. [19] proposed a new proxy blind signature scheme that allows revocation.

In 2017, Chiou et al. [20] proposed two novel 1-out-of-n blind (oblivious) and proxy signature schemes that combine the advantages of oblivious signatures and proxy signatures and satisfy the security properties of these two signature schemes. In 2018, Lin et al. [21] proposed a short linearly

homomorphic proxy signature scheme, and Li et al. [22] proposed a blind proxy resignature scheme based on isomorphisms of polynomials. In 2019, Tso [23] proposed a two-in-one oblivious signature that combines message oblivious and signer oblivious into one scheme.

For electronic voting systems, in 2001, Ray et al. [24] introduced an online anonymous e-voting protocol that allows a voter to cast his or her ballot anonymously by exchanging untraceable authentic messages. In 2013, Pan et al. [25] proposed an e-voting scheme that is based on the ring signature and is resistant to a clash attack. Several schemes with delegated voting functionality have been proposed. In 2013, Zwattendorfer et al. [26] proposed a proxy voting scheme that allows a voter to delegate his or her voting power to a proxy who actually casts the ballots for all represented voters. Norway has used an Internet-based voting protocol for some years, and the vote privacy and correctness of this scheme have been demonstrated [27]. In 2016, Kulyk et al. [28] proposed a new coercion-resistant proxy voting scheme by extending the coercion-resistant JCJ/Civitas theme, aiming to prevent direct voter coercion, delegation coercion, and proxy coercion. They also proposed a new proxy voting scheme [29] and extended the Helios voting system [30] with delegated voting functionality. In 2017, Cohensius et al. [31] considered a social choice problem and demonstrated that the mechanism using proxy voting better approximates the optimal outcome. In the end of 2017, Chiou et al. [20] proposed an anonymous e-voting system with proxy signer based on their proposed 1-out-of-n blind and proxy signature schemes.

For electronic lottery systems, many scholars have proposed protocols [32–37] in attempts to achieve true fairness and satisfy security requirements. However, these measures suffer from security issues including insufficient fairness or privacy concerns. For example, in some protocols (e.g., [32, 35, 36]), the trusted third party mechanism is required to maintain system fairness. In other methods (e.g., [34]), one side can decide key parameters for determining the winner. Moreover, some schemes (e.g., [33]) fail to account for player privacy concerns.

Paper Motivation. Compared with a blind signature scheme, an oblivious signature scheme used in e-voting or e-lottery provides one more property: ambiguity in selected messages. A signer cannot find out which message a voter or a player has selected while signing the messages, but the signer can be certain that the message the voter/player chooses is one or some of the predetermined messages; otherwise, the signature would not be accepted by a verifier. Therefore, in oblivious signature systems, which differ from blind signature schemes, the limited signed contents can prevent potential malicious users from obtaining valid signatures of some candidates for unauthorized purposes.

In addition, because each unit of a group (such as each state of a country, each county of a state, each campus of a school, or each approved bank of a group) may use different methods to authorize their members (using different keys), polling/betting booths with proxy ability are required. Additional benefits include reducing the load at voting centers or lottery owners and avoiding network jams. Moreover, the mobility of the voting/lottery functionality allows people to vote/play from anywhere using their mobile devices, thereby making the electronic voting/lottery system more convenient.

The goal in this research is a design of a generalized oblivious signature scheme with proxy function and extend the designed schemes to applications such as e-voting and e-lottery systems.

Paper Contribution. This paper proposes a generalized t-out-of-n proxy oblivious signature, which combines the advantages of proxy signature [13, 38] and 1-out-of-n oblivious signature [8, 9, 38, 39] and satisfies the security properties of the signature scheme. By using the concept proposed in [40], we conduct security analyses and proofs. The performance comparisons show that our scheme is efficient. Our scheme can be easily applied to an anonymous t-out-of-n e-voting system with proxy signer using Chiou's method [20]. Based on our scheme, we also design a proxy-based fair e-lottery system which provides a multiple-prize multiple-choice function and satisfies the fairness and security properties of a lottery. There security analyses and feature comparisons are conducted, and the results showed that our scheme has better performance. Finally, the system is implemented on a smart phone to provide the player with a more convenient digital experience while participating in game activities which take place in a truly fair environment. The user studies for college students indicate that most users think the e-lottery is convenient and more than half persons are willing to play the game again. To the best of our knowledge, this is the first work done on t-out-of-n proxy blind signature scheme and fair multiple-choice e-lottery system.

Paper Structure. The rest of this paper is organized as follows. Section 2 reviews the relevant literature, and Sections 3 and 4 provide definitions of security and system requirements of the proposed signature algorithm and lottery scheme along with descriptions of the protocol and the systems. Section 4 provides a comparison analysis in terms of system security and fairness for the proposed protocol and our system and demonstrates their security features. Section 5 describes the system implementation, and Section 6 provides conclusions.

2. Related Works

2.1. Proxy Signature Scheme. The proxy signature method was first proposed by Mambo in 1996 [13]. The method includes three roles: original signer, proxy signer, and verifier. The original signer can authorize the proxy signer to represent him/her in signing public-facing documents.

Delegation [35] can be categorized as full delegation, partial delegation, and delegation by warrant, as follows:

(1) *Full Delegation*. The proxy signer obtains a copy of the original signer's signature key to produce a proxy signature value identical to the signature of the original signer.

(2) *Partial Delegation*. The proxy signer's signature key is obtained through a calculation based on the original signer's private key. However, the proxy signature key cannot be used to obtain information related to the original signer's private key. Partial delegation can be categorized as one of two types: proxy-unprotected or proxy-protected. In the former, the original signer and proxy signer can both provide valid proxy signatures. In the latter, only the proxy signer can provide a valid proxy signature.

(3) *Delegation by Warrant*. A warrant based on the original signer's signature is used to validate the proxy signer's signing authority. The proxy signer's authorization message and proxy signature content are included in the proxy signature, and the verifier is used to determine the legitimacy of the authorization.

2.2. Oblivious Signature Scheme. Oblivious signature is a variation of digital signature and was first proposed by Chen [8]. The method includes three roles: the signer, recipient, and verifier. Oblivious signature seeks to ensure that the recipient can only receive plaintext values specified by the signer, selecting one or more of the plaintext values for signing. When the signer signs, he/she remains unaware of the selected plaintext content.

Tso et al.'s oblivious signature protocol [9] provided the first clear definition of oblivious signature security requirements as completeness, unforgeability, and ambiguity.

(1) *Completeness*. If the signer and recipient follow the protocol steps, the signature information received by the final recipient must be from the signer's valid signature

(2) *Unforgeability*. Given a public signature algorithm, attackers will still have difficulty forging a usable signature in a reasonable or acceptable amount of time

(3) *Ambiguity*. When the recipient requests the signer's signature, the signer is unable to determine the content of the signed plaintext message, thus maintaining the recipient's privacy

In 2017, Chiou et al. [38] proposed a novel oblivious signature which is integrated with proxy signature. Their protocol defines seven security requirements: completeness, unforgeability, unlinkability, undeniability, verifiability, distinguishability, and ambiguity. Except completeness, unforgeability, and ambiguity, the other four requirements are shown as follows:

(1) *Unlinkability*. The proxy signer can identify neither the message nor the proxy signature he or she generates associated with the scheme after the signature is revealed when necessary

(2) *Undeniability*. Neither the original signer nor the proxy signer can deny the signature they have created after signature generation

(3) *Verifiability*. The signature that the receiver receives should be able to convince the verifier of the agreement from the original signer and the proxy signer

(4) *Distinguishability*. The proxy signature is distinguishable from a normal one

In 2018, Chiou and Chen [39] presented a novel t-out-of-n oblivious signature, which is applied to multiple-choice e-voting scheme on the mobile system. Their scheme satisfies not only the security requirements but also t-out-of-n selection restriction and nonreduplication making such scheme well suited for multiple-choice e-voting applications. The added two requirements are shown as follows:

(1) *Selection Restriction*. The recipient is unable to get a valid signature of any message except the n messages

(2) *Nonreduplication*. The recipient cannot get more than one signature on the same message in a signing process

2.3. Fair Online Game System. In the virtual world of digital communications, a wide range of security requirements has driven the continuous development of new digital signature techniques [41–44]. The real-world equivalent of the game includes probability factors which impact winning conditions (e.g., luck) in competitive activities. With the rapid development of the Internet, electronic game environments [45–49] have gradually achieved mass market penetration, and the fairness of online games has received increased attention, prompting the development of many protocols since the 1990s.

Zhao et al. proposed a fair online game protocol [32] using the trusted third party (TTP) mechanism to maintain system fairness where the key parameters (banker vs. player) are entirely determined by the banker. In actual practice, however, this can potentially create an unfair situation for the Player.

Kushelevitz et al. proposed a fair lottery system [33] which does not require TTP, but the protocol does not take into account player privacy issues and only discusses factors impacting the generation of a winning random number in the context of one-on-one competitions, frequently raising fairness issues due to potential cheating on the part of the banker.

In 2004, Blundo et al. proposed a secure electronic game platform [34] featuring the comprehensive design of an online game system architecture including payment mechanisms between players, player anonymity, and player privacy options. However, the key parameters for determining the winner are decided exclusively by one side, thus again raising fairness issues in the practical application of the game.

2.4. Proxy Partially Blind Signature Scheme with Proxy Revocation. Yang and Liang [19] indicated that Liu et al.'s scheme [50] is unable to provide untraceability and is susceptible to the attacks of counterfeit signatures. They

proposed a new proxy blind signature scheme that improves Liu et al.'s scheme [50] and allows revocation. Their scheme combines the techniques of Schnorr signature [51], partially blind signature [52], and proxy signature [53] that can terminate proxy privileges and simultaneously provide untraceability, unforgeability, and the other security features required of proxy signatures. The scheme provides seven requirements: distinguishability, nonrepudiation, verifiability, unforgeability, identifiability, prevention of misuse, and unlinkability.

3. Proposed *t*-out-of-*n* Proxy Blind Signature Protocol

The proposed t-out-of-n proxy blind signature is based on the security requirement in Definition 1.

3.1. Attacker Model. The proposed signature schemes consist of four entities: an original signer **A**, a proxy signer **B**, a receiver **R**, and a verifier **V**. In our scheme, we assume the channels between **A** and **B** are secure. Any identity (i.e., **R** or **V**) communicates with **B** via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model [54, 55]:

(1) An adversary may eavesdrop on all communications between protocol actors over the public channel
(2) An attacker can modify, delete, resend, and reroute the eavesdropped message
(3) An attacker cannot intercept a message over a secure channel
(4) An attacker cannot be a legitimate original signer or proxy signer
(5) The attacker knows the protocol description, which means the protocol is public

3.2. Security Requirements. System requirements [13, 36, 56] of the proposed signature system are described as Definition 1.

Definition 1 (system requirements of t-out-of-n proxy blind signature protocol). Assume an original signer, a proxy signer, a recipient, and a verifier interact in t-out-of-n proxy blind signature protocol. The protocol is secure if it achieves the following conditions. (1) Completeness: recipient obtains a signer's signature to verify the message completeness. (2) Distinguishability: from the signature message, anyone can distinguish whether or not the signature is a proxy signature. (3) Identifiability: from the signature information, anyone can determine the identity of the signer. (4) Verifiability: once they receive the signature information, anyone can test the signature's validity. (5) Ambiguity: when the recipient requests the signature, the signer is unable to determine the content of the signed plaintext, thus ensuring the recipient's privacy. (6) Nonrepudiation: once the proxy signer signs the plaintext authorization specification, it becomes valid and the original signer is unable to repudiate the proxy signer's authorization, while the proxy signer is unable to repudiate that he/she signed the document. (7) Unforgeability: aside from the proxy signer specifically authorized by the original signer, no one can produce a verifiable signature, including the original signer him or herself. (8) Prevention of misuse: once the proxy signer secures the original signers proxy authorization, the proxy authority cannot be used outside the specified use, and misuse of authorization should be clearly demonstrable.

3.3. Proposed Protocol. The proposed t-out-of-n proxy blind signature protocol is based on RSA-FDH, RSA-based blind signatures, and certificate chains that follow the hash-and-sign paradigm. It includes four roles (original signer O, proxy signer P, recipient R, and verifier V) and is divided into four phases (initialization, proxy, signing, and verification) (Figures 1–3).

(1) *Initialization Phase.* O and P generate RSA cryptosystem public keys (e_O, N_O) and (e_P, N_P) and private keys (d_O, N_O) and (d_P, N_P) and then produce the warrant of delegation m_{wr} to demonstrate the proxy signer's signing authorization.
(2) *Proxy Phase.* As shown in Figure 1, O transfers signing authority to P as follows:
(1) O calculates $s_O \equiv H(m_{wr} \| e_P)^{d_O} \bmod N_O$ and transfers s_O and m_{wr} to P.
(2) P verifies whether $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ is held. If it does, it is believed O's authorization is obtained.
(3) *Signing Phase.* As shown in Figure 2, P transmits n plaintext documents $m_i\,(i = 1, 2, \ldots, n)$ allowing recipient R to determine t "selections" $(t < n)$. Then, R blinds the "selections" before transmitting them to P for signing. Finally, R resolves P's valid signature as follows:
(1) P selects a random number $SN \in Z_{N_P}$ as a protocol identifier and then calculates $s_{m_i} \equiv H(m_i \| m_{wr} \| SN)^{d_P} \bmod N_P$ before transmitting SN, $\{m_i, s_{mi}\}$, s_O, and m_{wr} to R.
(2) R verifies whether $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{m_i}^{e_P ?} \equiv H(m_i \| m_{wr} \| SN) \bmod N_P$. If both the equations hold, it is believed that m_i is a legitimate option. R selects t options $M_j = m_i$ $(j = 1, 2, \ldots, t)$, selecting a random number $b_j \in Z_{N_P}^*$ as a blinding factor, then calculates $\beta_j \equiv b_j^{e_P} \times M_j \bmod N_P$, and transmits $\{\beta_j\}$ to P.
(3) P selects a random number $r_j \in Z_{N_P}$, calculates $s_j \equiv (H(r_j \| SN) \times \beta_j)^{d_P} \bmod N_P$, and transmits s_j and r_j to R.
(4) R calculates $s_{c_j} \equiv b_j^{-1} s_j s_{M_j} \bmod N_P$ to obtain a valid signature for M_j: $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_P\}$.
(4) *Verification Phase.* As shown in Figure 3, R sends the M_j signature value to the verifier V for verification. V thus believes the plaintext has in fact been selected

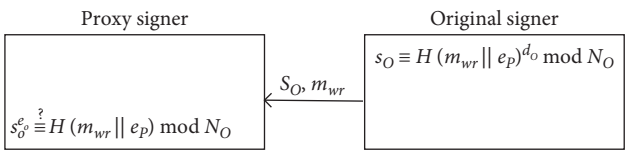


Figure 1: Proxy phase.

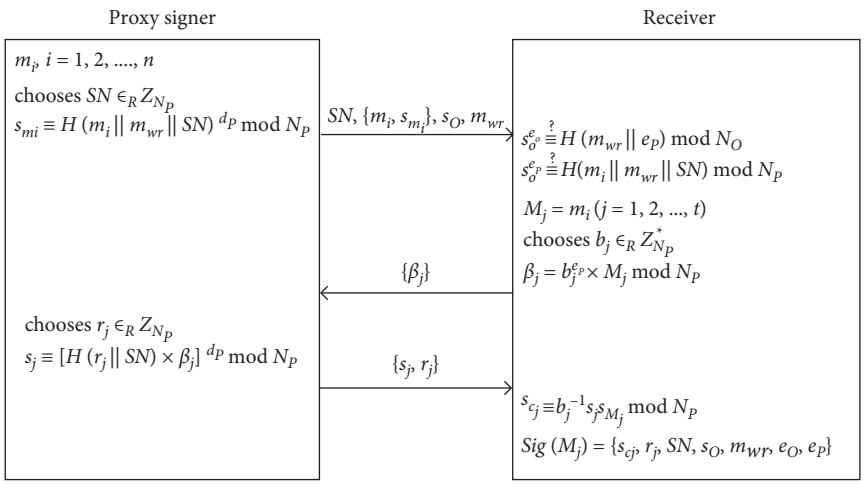


Figure 2: Signing phase.

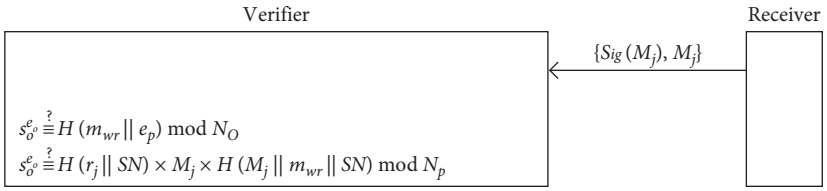


Figure 3: Verification phase.

by a legitimate signer, and this plaintext was in fact selected by R, as follows:

(1) R sends $\mathrm{Sig}(M_j)$ and M_j to V.

(2) V verifies $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$. If both the equations hold, the signature is valid.

4. Proposed Fair Lottery System

4.1. Security and System Requirements of the Proposed E-Lottery System. The proposed lottery system satisfies the game fairness principle, and its security and security requirements are described as Definitions 2 and 3.

Definition 2 (security requirement of fair e-lottery system). Assume owner, banker, and player interact in the fair e-lottery system. The system is secure if it achieves the following conditions. (1) Verifiability: After the lottery, player can verify the prize content announced by banker, thus protecting his own interests. Once the winning card is redeemed, anyone can verify its validity. (2) Privacy: Player's identifying information is never made available in the public lottery information, thus ensuring player's privacy. In the lottery process, player's selection must be kept secret to protect the privacy of the winning content. (3) Undeniability: After the lottery, banker is unable to repudiate the prize content or player's claim. (4) Unforgeability: Valid winning card information can only be produced through the valid protocol and cannot be forged. (5) Fairness for all players: In the lottery, no player (including owner and banker) should have an unfair advantage over other players.

Definition 3 (system requirement of our lottery system). Our lottery system is correct if it conforms the following characteristics: (1) no need for a trusted third party, (2) owner may not repudiate a legitimate lottery card, (3) the privacy of the player's selection content is protected, (4) the player is anonymous, (5) fairness for all players, and (6) multiple choices with multiple prizes.

4.2. Proposed System. The proposed lottery system design is an electronic adaptation of popular "scratch card" type lotteries. In the system, all messages are presented digitally. Hereinafter, the proposed e-lottery system is referred to as "the game" and traditional scratch cards are referred to as "(digital) lottery."

Each game session includes one lottery card and three roles: owner O, banker B, and player. O holds the money for the game and bears responsibility for profits and losses. Under the owner, there can be multiple bankers who are primarily responsible for verifying game wins or losses. B is the agent for O and serves as the host of the game, providing a link between player and O. B is responsible for issuing a lottery card with a valid signature and for signing player's selection. Player is in competition with O and makes a request to participate in the game.

B provides a lottery card containing a total of n blind prizes. Player can select t prizes. Once his selection is confirmed, player can know the content of his own selection. He can then present his card to O as proof to receive his prize. Each game session includes four phases (initialization, lottery card production, player drawing, and prize redemption) (Figures 4–7).

(1) *Initialization Phase.* As shown in Figure 4, owner O authorizes the agent to create banker B's game as follows:

(1) O calculates $s_O \equiv H(m_{wr}\|e_B)^{d_O} \bmod N_O$ and sends s_O and m_{wr} to B.

(2) B verifies $s_O^{e_O ?} \equiv H(m_{wr}\|e_B) \bmod N_O$ to check O's authorization.

(2) *Lottery Card Production Phase.* As shown in Figure 5, player requests a game from B, triggering the lottery production process as follows:

(1) B receives player's request and applies to O for a lottery card.

(2) O selects a random number $r_O \in Z_{N_O}^*$, calculates $h_k = \quad h_k = H(k\|m_k\|r_O\|e_B)$ to blind prize $m_k\,(k = 1, 2, \ldots, n)$, and calculates $SN \equiv r_O^{e_O} \bmod N_O$ and $s_{SN} \equiv H(SN\|h_1\|\ldots\|h_n)^{d_O} \bmod N_O$. O then transmits the lottery card information $\{h_k\}$, SN and s_{SN} to B, and stores (r_O, h_k, k, m_k) in the database.

(3) Once B has received the lottery card, he/she verifies $s_{SN}^{e_O ?} \equiv H(SN\|h_1\|\ldots\|h_n) \bmod N_O$ to establish the card as accepted. B then selects a random number $r_B \in Z_{N_B}$, extracts current time t_B, and calculates $\{p_i\} = \{H(h_k\|r_B\|t_B)\}$ and $s_{p_i} \equiv H(p_i\|m_{wr}\| \ SN)^{d_B} \bmod N_B$.

(3) *Player Drawing Phase.* As shown in Figure 6, player selects t p_i unseen by B and obtains B's valid signature for p_i as follows:

(1) B transmits SN, $\{p_i, s_{pi}\}$, s_O, and m_{wr} to player.

(2) Player verifies $s_O^{e_O ?} \equiv H(m_{wr}\|e_B) \bmod N_O$ and $s_{p_i}^{e_B ?} \equiv H(p_i\|m_{wr}\|SN) \bmod N_B$ to check whether p_i is a valid selection. Player selects t options $M_j = p_i$ and $j = 1, 2, \ldots, t$, selects a random number $b_j \in Z_{N_B}^*$ as the blinding factor, calculates $\beta_j \equiv b_j^{e_B} \times M_j \bmod N_B$, and sends β_j to B.

(3) B selects a random number $r_j \in Z_{N_B}$, calculates $s_j \equiv [H(r_j\|SN) \times \beta_j]^{d_B} \bmod N_B$, and sends $\{s_j, r_j\}$, r_B, t_B to player.

(4) Player calculates $s_{c_j} \equiv b_j^{-1} s_j s_{M_j} \bmod N_B$ and obtains the valid signature value for M_j: $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_B\}$.

(4) *Prize Redemption Phase.* As shown in Figure 7, player sends the signed content to O for verification, unlocking the prize content and obtaining the game prize as follows:

(1) Player sends $\{\mathrm{Sig}(M_j), M_j\}, r_B, t_B$ to O.

(2) O verifies $s_O^{e_O ?} \equiv H(m_{wr}\|e_B) \bmod N_O$ and $s_{c_j}^{e_B ?} \equiv H(r_j\|SN) \times M_j \times H(M_j\|m_{wr}\|SN) \bmod N_B$ to check whether the lottery card is valid. O calculates $r_O \equiv SN^{d_O} \bmod N_O$ and checks whether the value r_O exists in the database. If it does, (r_O, M_j, r_B, t_B) is used to find h_k from $M_j = p_j = H(h_k\|r_B\|t_B)$ and resolve k_j and m_{k_j} and then M_j data k_j, m_{k_j}, r_O are announced to player. Finally, the item about (r_O, h_k, k_j, m_{k_j}) is marked as "completed" in the database.

(3) Player verifies $M_j \stackrel{?}{=} H(H(k_j\|m_{k_j}\|r_O\|e_B)\|r_B\|t_B)$ to confirm and collect the prize content m_{k_j}.

5. Comparison and Security Analysis

5.1. Performance Comparison of the Proposed Signature Protocol. This section provides a comparison between the proposed signature protocol and the methods proposed by Yang et al. [19], Chen [8], Tso et al. [9], Chiou et al. [38], and Chiou and Chen [39], where Yang et al.'s [19] scheme is a blind signature scheme, Chiou and Chen's [39] scheme is a t-n (t-out-of-n) OT scheme, and the others are 1-n (one-out-of-n) OT schemes.

In Table 1, T_{ex} indicates modular exponentiation operation time unit, which is the most significant computational operation while the other operations in the schemes are ignored. The results in Table 1 show that the proposed method outperforms other protocol in terms of computational analysis.

Table 2 shows that the proposed method provides improvement or similar performance in terms of communication cost, where $q|p-1$ and $(l_N, l_p, l_q, l_m, l_H)$ indicates the length of N, p, q, a message, and a hash function.

Table 3 shows that the proposed method provides more features than other protocols. Therefore, compared with other related schemes, our scheme provides the most abilities with low computation cost. Furthermore, the communication cost is no higher than that of other oblivious signature schemes.

5.2. Functional Comparison of Lottery System. This section compares the proposed online lottery system with systems proposed by Zhao [32], Kushilevitz [33], and Blundo [34] in terms of the system requirements in Definition 2, and the results are summarized in Table 4. From Table 4, only our proposed lottery scheme provides "fairness for all players"

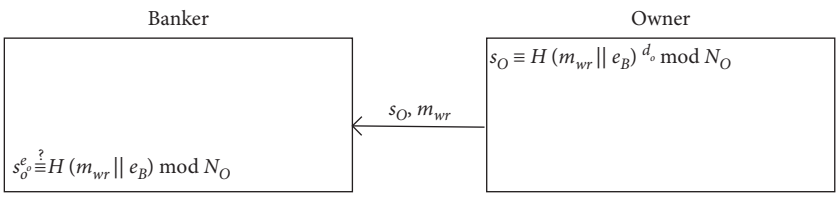


Figure 4: System initialization phase.

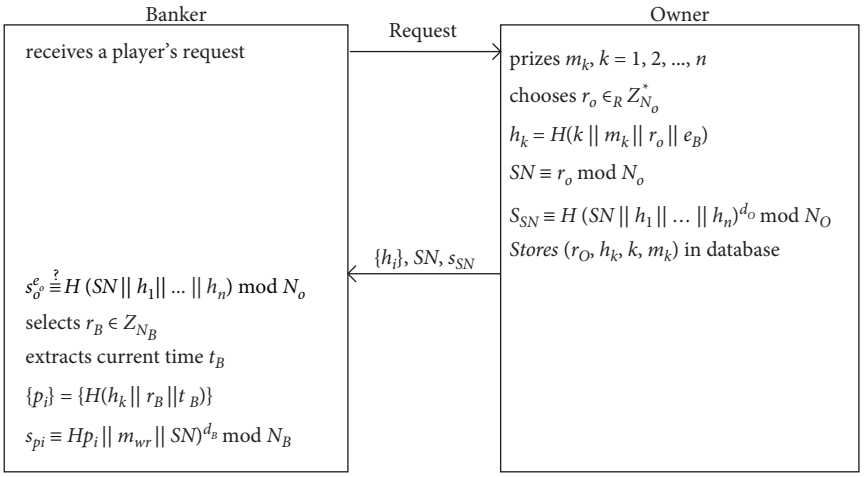


Figure 5: Lottery card production phase.

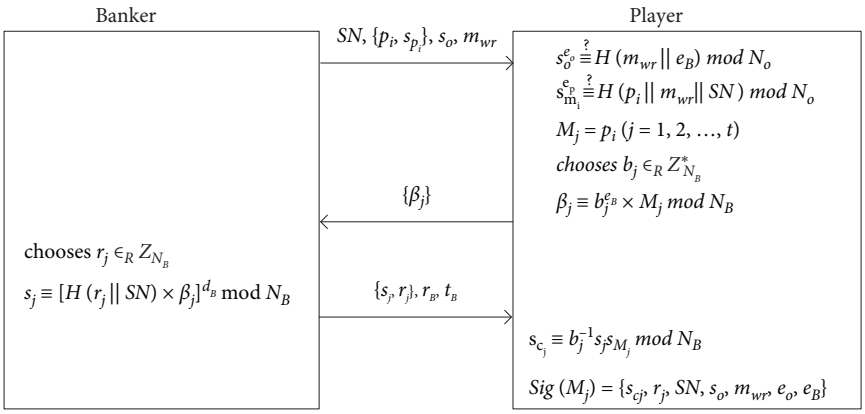


Figure 6: Player drawing phase.

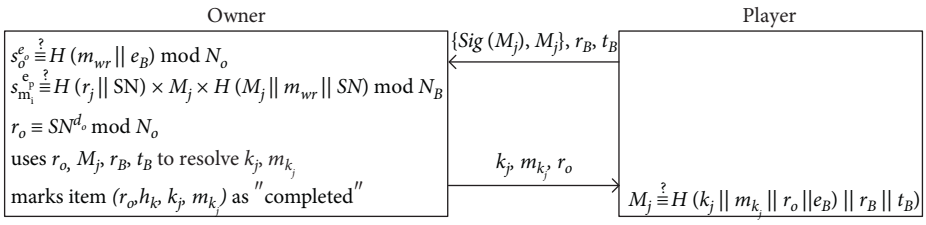


Figure 7: Prize redemption phase.

Table 1: Computation cost comparison.

Scheme	Original signer	(Proxy) signer	Receiver	Verifier
Yang (blind) [19]	T_{ex}	$4T_{ex}$	$2T_{ex}$	$3T_{ex}$
Chen (1-n) [8]	—	$3nT_{ex}$	$(2n+10)T_{ex}$	$8T_{ex}$
Tso (1-n) [9]	—	$2nT_{ex}$	$(2n+2)T_{ex}$	$2T_{ex}$
Chiou (1-n) [38]	$2T_{ex}$	$(n+2)T_{ex}$	$(2n+2)T_{ex}$	$2T_{ex}$
Chiou (1-n) [39]	—	$(n+1)T_{ex}$	$2nT_{ex}$	$2T_{ex}$
Chiou (t-n) [39]	—	$(n+t)T_{ex}$	$2nT_{ex}$	$2tT_{ex}$
Proposed (1-n)	T_{ex}	$(n+2)T_{ex}$	$(n+2)T_{ex}$	$2T_{ex}$
Proposed (t-n)	T_{ex}	$(n+t+1)T_{ex}$	$(n+t+1)T_{ex}$	$(t+1)T_{ex}$

Table 2: Communication cost comparison.

Scheme	OS $\longrightarrow$ PS	PS $\longrightarrow R$	$R \longrightarrow$ PS	$R \longrightarrow V$
Yang (blind) [19]	$l_q + l_H$	$l_p + l_q + l_H$	l_q	$l_q + 2l_H$
Chen (1-n) [8]	—	$3nl_p + nl_q$	l_q	$7l_p + l_q + l_H$
Tso (1-n) [9]	—	$n(l_q + l_H)$	l_p	$l_q + l_H$
Chiou (1-n) [38]	$l_p + l_q$	$n(l_q + l_H)$	l_p	$l_q + l_H$
Chiou (1-n) [39]	—	$(2n+1)l_N + nl_m$	l_N	$l\, l_N + l_m + l_H$
Chiou (t-n) [39]	—	$(2n+t)l_N + nl_m$	tl_N	$t(l_N + l_m + l_H)$
Proposed (1-n)	$l_N + l_m$	$(n+4)l_N + (n+1)l_m$	l_N	$4l_N + 2l_m + 2l_q$
Proposed (t-n)	$l_N + l_m$	$(n+2t+2)l_N + (n+1)l_m$	tl_N	$4tl_N + 2tl_m + 2tl_q$

Table 3: Ability comparison.

Scheme	Blindness	Ambiguity	Multichoice	Proxy ability
Chen [8]	✓	✓		
Mambo [13]				✓
Tso [9]	✓	✓		
Yang [19]	✓			✓
Chiou [38]	✓	✓		✓
Chiou [39]	✓	✓	✓	
Proposed	✓	✓	✓	✓

Table 4: System feature comparison.

Scheme	[A]	[B]	[C]	[D]	[E]	[F]
Zhao [32]		✓	✓	✓		
Kushilevitz [33]	✓	✓	✓			
Blundo [34]	✓	✓	✓	✓		
Proposed	✓	✓	✓	✓	✓	✓

[A]: no need for a trusted third party (TTP); [B]: owner may not repudiate a legitimate lottery card; [C]: the privacy of the player's selection content is protected; [D]:the player is anonymous; [E]: fairness for all players; [F]: multiple choices with multiple prizes.

and "multiple choices with multiple prizes." Zhao et al.'s method [32] requires a TTP to achieve fair online gambling, and Kushilevitz and Rabin's e-lottery and e-casino schemes [33] do not provide an anonymous-player function.

5.3. Security Analysis of the Proposed Signature Protocol. This proposed signature protocol provides eight security requirements defined in Definition 1.

(1) *Completeness*. From the signature initialization phase to the final verification phase, R can finally use the verification formula $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$ to determine whether P and O are valid signers in the protocol and can also use the verification formula to validate the signatures, thus ensuring the protocol's integrity. Theorems 1 and 2 prove the property of completeness from Definitions 4 and 5.

(2) *Distinguishability*. It is provided from $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_P\}$, where the authorization validation m_{wr} shows the proxy relationship between O and P, thus anyone can determine that the signature on this message is a proxy signature. Theorem 3 proves the property of distinguishability from Definition 6.

(3) *Identifiability*. The verification equations in the verification phase $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$ require the use of a valid signer's public key to conduct the necessary calculations for a successful verification, thus V can use the verification public keys e_P and e_O to determine the identity of the document signer. Theorem 4 proves the property of identifiability from Definition 7.

(4) *Verifiability*. Using public keys (e_P, N_P) and (e_O, N_O) can verify $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$ via the signature $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_P\}$. Moreover, the ownership of public keys can be verified using the public key of root CA from a PKI system. Theorem 5 proves the property of verifiability.

(5) *Ambiguity*. In the signing phase, R selects t blind factors b_j and calculates $\beta_j \equiv b_j^{e_P} \times M_j \bmod N_P$, thus

P is unable to determine the content of the signed message. Then, R sends s_j back to P, and P calculates $b_j^{-1}s_j s_{M_j}$ to obtain the valid signature for M_j, thus ensuring the privacy of R. This method implies another security feature in which each of the t signatures M_j can be independently verified. This means that, according to the requirements of the situation, R only wants to provide a proof of signature and does not require open verification of t signatures, thus the privacy of R's other selections. Theorem 6 proves the property of ambiguity from Definition 8.

(6) *Nonrepudiation*. During signing, this protocol requires the use of P and O's private keys along with a hash function. Given that others do not have access to these private keys, they are unable to create a signature which would pass verification. Likewise, a verifiable signature must have the public key's master signature at the time of verification, which the signer is unable to repudiate. Theorem 7 proves the property of nonrepudiation.

(7) *Unforgeability*. We analyze warrant and message unforgeability, and Theorem 8 proves the property of unforgeability.

(8) *Prevention of Misuse*. The signature of m_{wr} is verified, and m_{wr} is used to verify the authentication to clearly document the proxy signer's signing capability, time, and usage conditions. The authorization certificate cannot be forged, thus the proxy signer is unable to use its proxy signature for unauthorized purposes, thus preventing misuse of the proposed protocol. Theorem 9 proves the property of prevention of misuse.

5.4. Security Analysis of Proposed Lottery System. In practice, each banker hosts one or multiple servers. Assuming that multiple bankers represent a single owner, then multiple servers jointly use a single private key. For the overall system, this is equivalent to putting all of one's eggs in a single basket, and thus the security of the overall system relies on a single key. On the other hand, using a proxy system can significantly reduce the potential risk to system security even if the banker's key or even the owner's key is stolen. This additional layer of protection greatly increases overall system security.

If the prize redemption involves actual money, it could be realized through anonymous and secure mechanisms which are commonly applied in online transactions [57–60]. A user can register with a third party middleman (such as Paypal, Google Checkout, or Amazon Payment), providing required information, such as bank accounts and redemption certificates. The middleman presents the owner with a cash request based on these redemption certificates. Once the middleman receives the required payout and delivers a corresponding receipt to the owner, the middleman then transfers the money to the player's bank account. Thus, the identity of the prize winner is not revealed to the owner (thus achieving privacy). Moreover, this approach eliminates the possibility of the owner refusing to deliver the claimed prize.

To meet the game's fairness principle, this system satisfies the five security requirements as defined in Section 5.1: verifiability, privacy, undeniability, unforgeability, and fairness for all players.

(1) *Verifiability*. In the prize redemption phase, player uses the verification equation $M_j \stackrel{?}{=} H[H(k_j \| m_{k_j} \| r_O \| e_B) \| r_B \| t_B]$ to inspect the prize content. When redeeming prizes, anyone can substitute O and B's public key into the verification equations $s_O^{e_O ?} \equiv H(m_{wr} \| e_B) \bmod N_O$ and $s_{c_j}^{e_B ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_B$ to inspect the card validity. Theorem 10 proves the property of verifiability.

(2) *Privacy*. Each lottery session does not require the use of player's identifying information, thus the public lottery card information will not leak the player's identity. In the lottery process, player's selection uses the random number b_j plus blinding and thus B is unaware of the selection, ensuring the privacy of the prize content. Theorem 11 proves the property of privacy.

(3) *Undeniability*. Prizes are awarded through a one-way hash function algorithm. When the prizes are awarded, O is unable to change the prize content or otherwise deceives player. Player's selection is verified using O and B's public key, and thus O is unable to repudiate the lottery card's validity. Theorem 12 proves the property of undeniability.

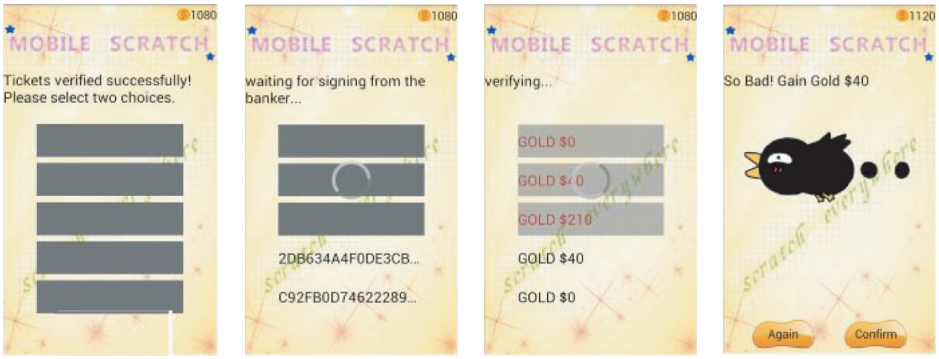
(4) *Unforgeability*. Player's prize must be legitimately signed using B's private key. Following the signing phase, it will be impossible to forge another valid winning lottery card. Theorem 13 proves the property of unforgeability.

(5) *Fairness for All Players*. At the outset, O uses a one-way hash function to blind the selected prize. Aside from O, no other parties know the prize content. Then, B double blinds the prize item, at which time no one including O and B is able to determine which card has the prize. Theorem 14 proves the property of fairness for all players.

6. Implementation

This section presents an implementation of the proposed e-lottery system on an Android platform, allowing the user to interact with the system through a mobile device to achieve a scratch game e-lottery. The implementation results are presented in two parts. First, we introduce the program flow chart and then show the user experience through the interface.

The program's related user interface is illustrated in Figure 8. The owner and banker roles operate on the server end, while the player role operates on the client-end mobile device, as shown in Figure 9. (please refer to http://youtu.be/9je3gtThnTY for the full demonstration.).



(a) (b) (c) (d)

Figure 8: (a) Player receives the successful lottery card verification from cloud banker; (b) after choosing an option, player waits for banker's signature; (c) player verifies the prize; (d) following the successful verification, the game is concluded.

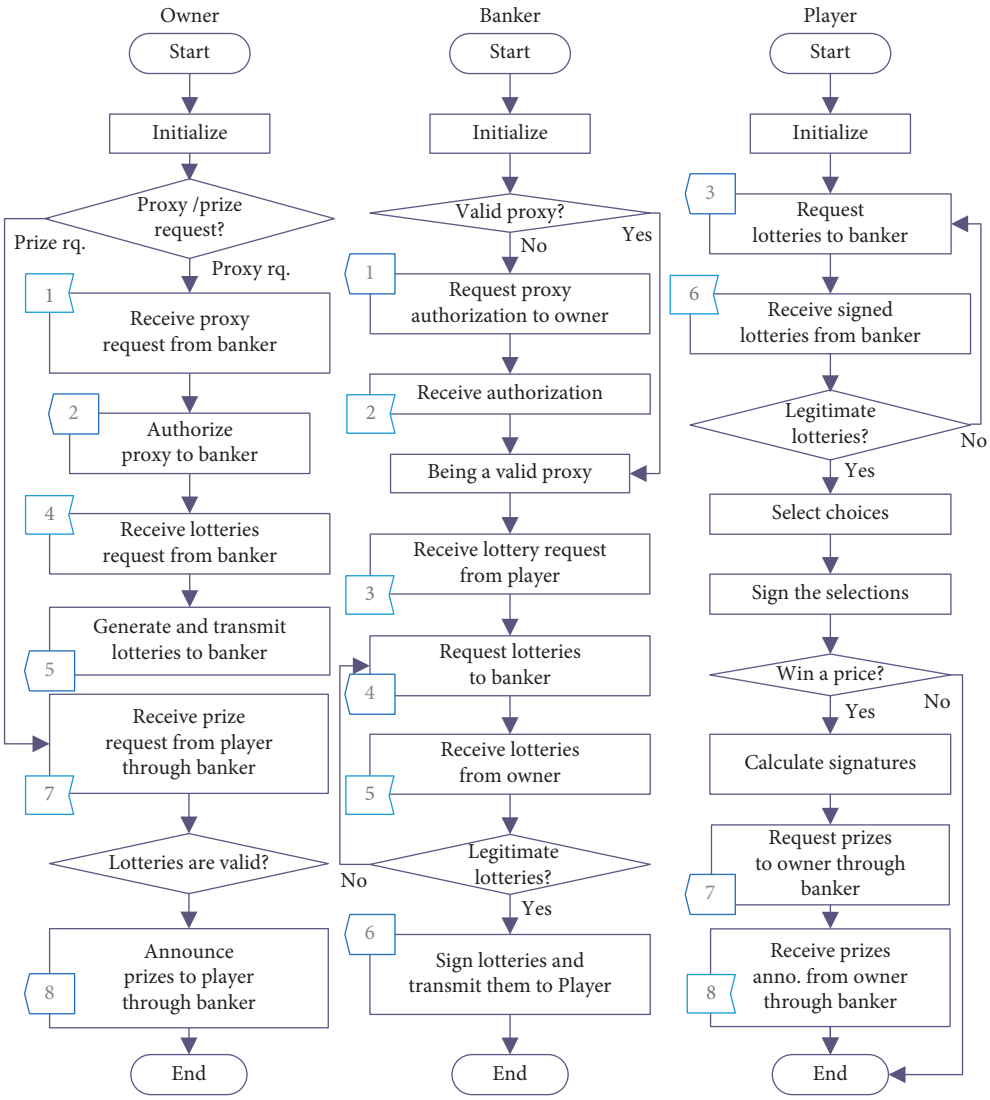


Figure 9: Application flow chart.

Table 5: Implementation time.

Phases	Banker	Owner	Player	Trans.	Time
Lottery card prod. phase	79.85	79.85	—	38.65	198.35
Player drawing phase	39.35	—	97.6	401.6	538.55
Prize redemption phase	—	39.6	21.15	261.55	322.3

Time unit: millisecond (ms).

Table 6: Ranking of user studies.

Item	Trust before expl.	Convenience	Willing to play	Trust after expl.
Average	5.67	7.79	5.36	6.83
Variable	5.47	3.70	6.13	5.17
≥5	73.74%	94.95%	70.71%	85.86%
≥6	54.55%	84.85%	52.53%	79.80%

We use one personal computer and one android phones to implement two servers (banker and owner) and a player, where the player communicates to each other through WiFi wireless networks and the owner and the banker communicate to each other through wired networks. The personal computer implementation used Windows 10 with an Intel (R) Xeon (R) CPU E3-1230 v3 @ 3.30 GHz (8 CPUs) and 8G RAM. Android phone implementation used HTC Desire 816 based on Android 5.0 and Qualcomm S400 1.6 G Hz.

The owner and banker (server) programs are written in JAVA and run under Windows 10. The RSA system parameters are generated through an official method with a module length of 1024 bits. The hash function used is SHA-256 [61]. In this scenario, we set $t = 2$ and $n = 5$. Each time the program needs only 1~3 seconds to finish all the processes (from initialization to prize redemption) excluding the user's operating time. Table 5 shows the average implementation time in each phase.

Table 6 shows the ranking result of user studies for 99 college students. The ranking score is from 1 (the lowest) to 10 (the highest), the ranking items include (1) trust before explanation, (2) convenience, (3) willing to play, and (4) trust after explanation, and the statistical information includes (1) average, (2) variable, (3) "≥5" (scores equal to or great than 5), and (4) "≥6."

In the first phase, we let users play the mobile lottery and rank the scores of the first three items (i.e., trust before explanation, convenience, and willing to play). In the second phase, we let users rank the final item (i.e., trust after explanation) after the one-minute explanation of the security design on our mobile lottery scheme. Normally, a "sense of security" is remarkably increased after a slight explanation. Most users think the mobile lottery is convenient, and more than half persons are willing to play the game again.

7. Conclusion

This paper proposes a generalized t-out-of-n oblivious signature scheme with proxy function. A new mobile lottery system is then proposed based on the proposed signature protocol with the aim of providing a more complete fairness and more convenient security. Compared with other schemes, only our system provides the system property: fairness for all players and multiple choices with multiple prizes. Moreover, most signature schemes do not supply both multichoice and proxy ability while preserving the security properties (along with security proves via a formal security proving model), including blindness and ambiguity. The proposed system is implemented on in Android smart phone, providing greater convenience for the user as compared with traditional game counter mechanisms. Based on the above analysis, the proposed signature protocol can also be used in applications outside lottery systems. Our future work will focus in this area, along with making further improvements to increase efficiency and security.

Appendix

The appendix provides 14 theorems along with definitions and proofs security analysis of the proposed signature protocol and e-lottery system using a formal proof method [40].

A. Security Proofs of the Proposed Signature Protocol

A.1. Completeness

Definition 4 (1st modified RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b, b' \in Z, s^e = H(b\|a) \bmod N$, and $s'^e = H(b'\|a) \bmod N$. If (s', b') can be evaluated from given (a, s, b), then we say the 1st modified RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', b'|, a, s, b) = \varepsilon_1$).

Theorem 1 (warrant completeness). *In our scheme, if an adversary can modify (s_O, m_{wr}) to a valid (s'_O, m'_{wr}), then the 1st modified RSA signature forgery problem can be solved.*

Proof. In our scheme, assume an adversary tries to calculate (s'_O, m'_{wr}) from eavesdropped (s_O, m_{wr}, e_p), where $s_O^{e_O} = H(m_{wr}\|e_p) \bmod N_O$ and $s_O'^{e_O} = H(m'_{wr}\|e_p) \bmod N_O$. Let RO_1 be a random oracle: input s_O, m_{wr}, and e_p to output

s'_O and m_{wr}' (i.e., $RO_1(m_{wr}, e_p, s_O) \longrightarrow (s'_O, m_{wr}')$). In Definition 4, let $e_p \leftarrow a$, $m_{wr} \leftarrow b$, and $s_O \leftarrow s$ be input parameters of RO_1 and obtain output s'_O and m'_{wr}. Let $s' \leftarrow s'_O$ and $b' \leftarrow m'_{wr}$, then (s', b') are evaluated. Therefore, $\Pr(s'_O, m'_{wr}|e_p, s_O, m_{wr}) \le \Pr(s', b'|a, s, b) = \varepsilon_1$, which means the 1st modified RSA signature forgery problem can be solved if RO_1 exists.

Definition 5 (2nd modified RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b, b' \in Z$, $a, b, b' \in Z$, $s^e \equiv H(r_1 \| r_2) \cdot m_1 \cdot H(m_1 \| m_2 \| r_2) \bmod N$, and $s'^e \equiv H(r_1' \| r_2') \cdot m_1' \cdot H(m_1' \| m_2 \| r_2') \bmod N$. If (s', m_1', r_1', r_2') can be evaluated from given (s, m_1, r_1, r_2, m_2), then we say the 2nd modified RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', m_1', r_1', r_2'|s, m_1, r_1, r_2, m_2) = \varepsilon_2$).

Theorem 2 (message completeness). *In our scheme, if an adversary can modify (s_c, M_j, r_j, SN) to valid (s_c', M_j', r_j', SN') from given m_{wr}, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. In our scheme, assume an adversary tries to calculate (s_c', M_j', r_j', SN') from $(s_c, M_j, r_j, SN, m_{wr})$, such that $s_c'^{e_p} \equiv H(r_j' \| SN') \times M_j' \times H(M_j' \| m_{wr} \| SN') \bmod N_P$. Let RO_2 be a random oracle: input $(s_c, M_j, r_j, SN, m_{wr})$ to output (s_c', M_j', r_j', SN'). In Definition 5, let $(s, m_1, r_1, r_2, m_2) \leftarrow (s_c, M_j, r_j, SN, m_{wr})$ be input parameters of RO_2 and obtain output (s', m_1', r_1', r'). Let $(s_c', M_j', r_j', SN') \leftarrow (s', m_1', r_1', r')$, then (s_c', M_j', r_j', SN') are evaluated. Therefore, $\Pr(s_c', M_j', r_j', SN'|s_c, M_j, r_j, SN, m_{wr}) \le \Pr(s', |m_1', r_1', r_2'|s, m_1, r_1, r_2, m_2) = \varepsilon_2$, which means the 2nd modified RSA signature forgery problem can be solved if RO_2 exists.

A.2. Distinguishability

Definition 6 (RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b, a', b' \in Z$, $s^e = H(b \| a) \bmod N$, and $s'^e = H(b' \| a') \bmod N$. If (s', b', a') can be evaluated from given (s, b, a, e, N), then we say the RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', b', a'|s, b, a) = \varepsilon_3$).

Theorem 3 (Distinguishability). *In our scheme, if an adversary can counterfeit a valid (s_O', m_{wr}', e_P') from $(s_O, m_{wr}, e_P, e_O, N_O)$, then the RSA signature forgery problem can be solved.*

Proof. In our scheme, assume an adversary tries to calculate (s_O', m_{wr}', e_P') from $(s_O, m_{wr}, e_P, e_O, N_O)$, where $s_O^{e_O} = H(m_{wr} \| e_p) \bmod N_O$ and $s_O'^{e_O} = H(m_{wr}' \| e_P') \bmod N_O$. Let RO_3 be a random oracle: input $(s_O, m_{wr}, e_P, e_O, N_O)$ to output (s_O', m_{wr}', e_P'). In Definition 6, let $(s_O, m_{wr}, e_P, e_O, N_O) \leftarrow (s, b, a, e, N)$ be input parameters of RO_3 and obtain output (s_O', m_{wr}', e_P'). Let $(s', b', a') \leftarrow (s_O', m_{wr}', e_P')$, then (s', b', a') are evaluated. Therefore, $\Pr(s_O', m_{wr}', e_P'|s_O, m_{wr}, e_P, e_O, N_O) \le \Pr(s', b', a'|s, b, a) = \varepsilon_3$, which means the RSA signature forgery problem can be solved if RO_3 exists. □

A.3. Identifiability

Definition 7 (2nd RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $m, m' \in Z$, $s^e = H(m) \bmod N$, and $s'^e = H(m') \bmod N$. If (s', m') can be evaluated from given (s, m, e, N), then we say the 2nd RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', m'|s, m, e, N) = \varepsilon_4$).

Theorem 4 (identifiability). *Given (e_{Root}, N_{Root}). In our scheme, if an adversary can counterfeit valid (s_{e_O}', e_O') from (s_{e_O}, e_O) or counterfeit valid (s_{e_p}', e_P') from (s_{e_p}, e_P), such that $s_i^e = H(e_i) \bmod N$, where $(s_i, e_i) = (s_{e_O}, e_O)$, (s_{e_p}, e_P), (s_{e_O}', e_O'), or (s_{e_p}', e_P'), then the 2nd RSA signature forgery problem can be solved.*

Proof. In a PKI system, a signature s_i on a public key e_i is signed by root such that $s_i^{e_{\text{root}}} = H(e_i) \bmod N_{\text{root}}$, where $(e_{\text{Root}}, N_{\text{Root}})$ are root public keys. Assume an adversary tries to counterfeit (s_{e_O}', e_O') from (s_{e_O}, e_O) or counterfeit (s_{e_p}', e_P') from (s_{e_p}, e_P). Let RO_4 be a random oracle: input (s_{e_O}, e_O) to output (s_{e_O}', e_O'). In Definition 7, let $(s, m, e, N) \leftarrow (s_{e_O}, e_O, e_{\text{Root}}, N_{\text{Root}})$ be input parameters of RO_4 and obtain output (s', m'). Let $(s_{e_O}', e_O') \leftarrow (s', m')$, then (s_{e_O}', e_O') are evaluated. Therefore, $\Pr(s_{e_O}', e_O'|s_{e_O}, e_O, e_{\text{Root}}, N_{\text{Root}}) \le \Pr(s', m'|s, m, e, N) = \varepsilon_4$, which means the 2nd RSA signature forgery problem can be solved if RO_4 exists. □

A.4. Verifiability

Theorem 5 (verifiability). *In our scheme, if an adversary can forge valid signatures (s_O', m_{wr}') and (s_c', M_j', r_j', SN') from (s_O, m_{wr}) and $(s_c, M_j, r_j, SN, m_{wr})$ and pass the verification equations using public keys (e_P, N_P, e_O, N_O), then both the 1st and 2nd modified RSA signature forgery problems can be solved.*

Proof. The proofs are the same as the content of the proof of Theorem 1 plus the proof of Theorem 2.

A.5. Ambiguity

Definition 8 (entropy problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b \in Z$, and $\alpha = b^e \times m \bmod N$. If m can be evaluated from given (α, e, N) without given b, then we say the entropy problem is solved. The probability of solving this problem is denoted as $\Pr(m|\alpha, e, N) = \varepsilon_5$.

Theorem 6 (ambiguity). *In our scheme, if the proxy signer or an adversary can calculate M_j from (β_j, e_P, N_P), then the entropy problem can be solved.*

Proof. In our scheme, assume the proxy signer or an adversary tries to calculate M_j from (β_j, e_P, N_P) where $\beta_j = b^{e_P} \times M_j \bmod N_P$. Let RO_5 be a random oracle: input (β_j, e_P, N_P) to output M_j. In Definition 8, let (β_j, e_P, N_P), $\leftarrow$, (α, e, N) be input parameters of RO_5 and obtain output M_j. Let m, $\leftarrow$, M_j, then m is evaluated. Therefore, $\Pr(M_j|\beta_j, e_P, N_P) \leq \Pr(m|\alpha, e, N) = \varepsilon_5$, which means the entropy problem can be solved if RO_5 exists.

A.6. Nonrepudiation

Theorem 7 (nonrepudiation). *In our scheme, if an adversary can calculate a valid signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_P, N_O)$ without given d_O, then the 1st modified RSA signature forgery problem can be solved. If an adversary can calculate a valid signature (s'_c, M'_j, r'_j, SN') from $(s_c, M_j, r_j, SN, e_P, N_P)$ without given d_P, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is the same as the content of the proof of Theorem 1 plus the proof of Theorem 2.

A.7. Unforgeability

Theorem 8 (unforgeability). *In our scheme, if an adversary can evaluate a forged warrant signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_P, N_O)$, then the 1st modified RSA signature forgery problem can be solved. If an adversary can evaluate a forged message signature (s'_c, M'_j, r'_j, SN') from $(s_c, M_j, r_j, SN, e_P, N_P)$, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is the same as the content of the proof of Theorem 1 plus the proof of Theorem 2.

A.8. Prevention of Misuse

Theorem 9 (prevention of misuse). *In our scheme, if an adversary can calculate valid signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_P, N_O)$ without given d_O, then the 1st modified RSA signature forgery problem can be solved. If an adversary can calculate valid signature (s'_c, M_j, r'_j, SN') from $(s_c, M_j, r_j, SN, e_P, N_P)$ without given d_P, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is the same as the content of the proof of Theorem 2.

B. Security Proofs of the Proposed Lottery System

B.1. Verifiability

Theorem 10 (verifiability). *In our scheme, if an adversary can forge valid (s'_O, m'_{wr}) and (s'_c, M'_j, r'_j, SN') from (s'_O, m'_{wr}) and (s_{c_j}, M_j, r_j, SN), then both the 1st and 2nd modified RSA signature forgery problems can be solved. If an adversary can counterfeit valid $(k'_j, m'_{k_j}, r'_O, e'_B, t'_B, r'_B)$ from $(k_j, m_{k_j}, r_O, e_B, t_B, r_B)$, then both the 2nd RSA signature forgery problem and the hash problems can be solved.*

Proof. (1) The proofs about (s'_O, m'_{wr}) and (s'_c, M'_j, r'_j, SN') forgery are the same as the content of the proof of Theorem 1 plus the proof of Theorem 2. (2) About $(k'_j, m'_{k_j}, r'_O, e'_B, t'_B, r'_B)$ counterfeit, the proof for uncounterfeiting e'_O is the same as the content of the proof of Theorem 4. (3) The value t'_B is the banker's current time and cannot be forged because it can be verified by the play's current time. (4) The value r'_O cannot be forged because it can be verified via $SN^? \equiv r'^{e_O}_O \bmod N_O$ and counterfeiting a r'_O faces to a RSA signature forgery problem. (4) Forging (k'_j, m'_{k_j}) directly faces hash problem because player verifies $M_j \stackrel{?}{=} H(H(k_j \| m_{k_j} \| r_O \| e_B) \| r_B \| t_B)$ to confirm (k'_j, m'_{k_j}).

B.2. Privacy

Theorem 11 (privacy). *In our scheme, if the banker or an adversary can calculate M_j from (β_j, e_B, N_B), then the entropy problem can be solved.*

Proof. The proof is similar to the content of the proof of Theorem 6.

B.3. Undeniability

Theorem 12 (undeniability). *In our scheme, if an adversary can calculate a valid signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_B, N_O)$ without given d_O, then the 1st modified RSA signature forgery problem can be solved. If an adversary can calculate a valid signature (s'_c, M'_j, r'_j, SN') from $(s_{c_j}, M_j, r_j, SN, e_B, N_B)$ without given d_B, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is similar to the content of the proof of Theorem 7.

B.4. Unforgeability

Theorem 13 (unforgeability). *In our scheme, if an adversary can evaluate a forged warrant signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_B, N_O)$, then the 1st modified RSA signature forgery problem can be solved. If an adversary can evaluate a forged message signature (s'_c, M'_j, r'_j, SN') from $(s_{c_j}, M_j, r_j, SN, e_B, N_B)$, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is similar to the content of the proof of Theorem 8.

B.5. Fairness for All Players

Theorem 14 (fairness for all players). *In our scheme, if any of players, bankers, or the owner can calculate m_k in player drawing phase, then the RSA decryption problem or entropy problem can be solved.*

Proof. In our scheme, assume a banker tries to calculate m_k from (h_k, e_B, SN, e_O, N_O), where $h_k = H(k\|m_k\|r_O\|e_B)$ and $SN \equiv r_O^{e_O} \bmod N_O$. It faces RSA decryption problem. If the owner tries to get the connection between h_k and p_i from $\{p_i\}$ and $\{h_k\}$ without known (r_B, t_B), where $p_i \equiv H(h_k||r_B||t_B)$, it faces entropy problem. If a player tries to calculate m_k from p_i without known (r_B, t_B), it also faces entropy problem.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the Ministry of Science and Technology under grant MOST 109-2221-E-182-020 and by the CGMH project under grant BMRPB46.

References

[1] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and privacy-preserving authentication scheme for wireless body area networks," *Journal of Information Security and Applications*, vol. 52, Article ID 102499, 2020.

[2] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[3] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 147, pp. 1–19, 2020.

[4] R. Rabaninejad, M. A. Attari, M. R. Asaar, and M. R. Aref, "A lightweight identity-based provable data possession supporting users' identity privacy and traceability," *Journal of Information Security and Applications*, vol. 51, Article ID 102454, 2020.

[5] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology*, vol. 82, pp. 199–203, 1982.

[6] S. K. Nayak, B. Majhi, and S. Mohanty, "An ECDLP based untraceable blind signature scheme," in *Proceedings of the 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, Kumaracoil, Nagercoil, India, March 2013.

[7] M. O. Rabin, "How to exchange secrets by oblivious transfer," Technical Report TR-81, Aiken Computation Laboratory, Harvard University, Cambridge, MA, USA, 1981.

[8] L. Chen, "Oblivious signatures," in *Proceedings of the Computer Security-ESORICS 94*, pp. 161–172, Brighton, UK, November 1994.

[9] R. Tso, T. Okamoto, and E. Okamoto, "1-out-of-*n* oblivious signatures," *Proceedings of ISPEC2008, Lectures Notes in Computer Science*, vol. 4991, pp. 45–55, 2008.

[10] J. S. Chou, "A novel *k*-out-of-*n* oblivious transfer protocol from bilinear pairing," *Advances in Multimedia*, vol. 2012, Article ID 630610, 3 pages, 2012.

[11] P. Zhang, H. Jiang, Z. Zheng, P. Hu, and Q. Xu, "A new post-quantum blind signature from lattice assumptions," *IEEE Access*, vol. 6, pp. 27251–27258, 2018.

[12] L. Wang, Y. Tian, Y. Pan, and Y. Yang, "New construction of blind signatures from braid groups," *IEEE Access*, vol. 7, pp. 36549–36557, 2019.

[13] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transaction on Fundamentals*, vol. E79-A, no. 9, pp. 1338–1354, 1996.

[14] B. T. Lau, "Proxy signature schemes," in *Proceedings of the 2006 1ST IEEE Conference on Industrial Electronics and Applications*, Singapore, March 2006.

[15] H. Wang and R. Yan, "A code-based multiple grade proxy signature scheme," in *Proceedings of the 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Compiegne, France, October 2013.

[16] W. D. Lin and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," in *Proceedings of the International Conference on Chinese Language Computing*, pp. 273–277, Chicago, IL, USA, November 2000.

[17] A. Z. Tan, Z. Liu, and C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," *MM Research Preprints*, vol. 21, no. 7, pp. 212–217, 2002.

[18] S. Lal and A. K. Awasthi, "Proxy blind signature scheme," *Journal of Information Science and Engineering*, vol. 72, 2003.

[19] F.-Y. Yang and L.-R. Liang, "A proxy partially blind signature scheme with proxy revocation," *Journal of Ambient Intelligence and Humanized Computing*, vol. 4, no. 2, pp. 255–263, 2013.

[20] S. Y. Chiou, T. J. Wang, and J. M. Chen, "Design and implementation of a mobile voting system using a novel oblivious and proxy signature," *Security and Communication Networks*, vol. 2017, Article ID 3075210, , 2017.

[21] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[22] H. Li, Z. Han, L. Wang, and L. Pang, "Blind proxy re-signature scheme based on isomorphisms of polynomials," *IEEE Access*, vol. 6, pp. 53869–53881, 2018.

[23] R. Tso, "Two-in-one oblivious signatures," *Future Generation Computer Systems*, vol. 101, pp. 467–475, 2019.

[24] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the internet," in *Proceedings of the Third International Workshop on IEEE Advanced Issues of E-Commerce and Web-Based Information Systems*, San Juan Capistrano, CA, USA, June 2001.

[25] H. Pan, E. Hou, and N. Ansari, "RE-NOTE: an e-voting scheme based on ring signature and clash attack protection," in *Proceedings of the Global Communications Conference (GLOBECOM)*, Atlanta, GA, USA, December 2013.

[26] B. Zwattendorfer, C. Hillebold, and P. Teufl, "Secure and privacy-preserving proxy voting system," in *Proceedings of the 2013 IEEE 10th International Conference on e-Business Engineering (ICEBE)*, pp. 472–477, Coventry, UK, September 2013.

[27] S. Kardaş, M. S. Kiraz, M. A. Bingöl, and F. Birinci, "Norwegian internet voting protocol revisited: ballot box and receipt generator are allowed to collude," *Security and Communication Network*, vol. 9, no. 18, pp. 5051–5063, 2016.

[28] O. Kulyk, S. Neumann, K. Marky, J. Budurushi, and M. Volkamer, "Coercion-resistant proxy voting," in

Proceedings of the 31st International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2016), pp. 3–16, Ghent, Belgium, June 2016.

[29] O. Kulyk, K. Marky, S. Neumann, and M. Volkamer, "Introducing Proxy Voting to Helios," in *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 98–106, Salzburg, Austria, September 2016.

[30] B. Adida, "Helios: web-based open-audit voting," *USENIX Security Symposium*, vol. 17, pp. 335–348, 2008.

[31] G. Cohensius, S. Mannor, R. Meir, E. Meirom, and A. Orda, "Voting for better outcomes," in *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*, pp. 858–866, Sao Paulo, Brazil, May 2017.

[32] W. Zhao, V. Varadharajan, and Y. Mu, "Fair on-line gambling," in *Proceedings of the 16th Annual Conference Computer Security Applications, 2000, ACSAC'00*, Washington, DC, USA, December 2000.

[33] E. Kushilevitz and T. Rabin, "Fair e-lotteries and e-casinos," *Topics in Cryptology—CT-RSA 2001*, Springer, Berlin, Heidelberg, Germany, 2001.

[34] C. Blundo and S. Cimato, "A platform for secure e-gambling," in *Proceedings of the ITCC 2004, International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, April 2004.

[35] Y. Han and T. Okamoto, "Information and communications security," in *Proceedings of theInternational Conference on Information and Communications Security*, pp. 223-224, Beijing, China, November 1997.

[36] B. Lee, H. Kim, and K. Kim, "Strong proxy signer and its applications," in *Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS' 01)*, pp. 603–608, Oiso, Japan, January 2001.

[37] H. Gao, Z. Ma, S. Luo, and Z. Wang, "BFR-MPC: a blockchain-based fair and robust multi-party computation scheme," *IEEE Access*, vol. 7, pp. 110439–110450, 2019.

[38] S. Y. Chiou, T. J. Wang, and J. M. Chen, "Design and implementation of a mobile proxy voting system using a novel oblivious and proxy signature," *Security and Communication Networks*, vol. 2017, Article ID 3075210, 16 pages, 2017.

[39] S. Y. Chiou and J. M. Chen, "Design and implementation of a multiple-choice e-voting scheme on mobile system using novel *t*-out-of-*n* oblivious signature," *Journal of Information Science and Engineering*, vol. 34, no. 1, pp. 135–154, 2018.

[40] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73, Fairfax, VA, USA, November 1993.

[41] H. Wang, "Identity-based distributed provable data possession in multicloud storage," *IEEE Transactions on Services Computing*, vol. 8, no. 2, pp. 328–340, 2015.

[42] V. Chang and M. Ramachandran, "Towards achieving data security with the cloud computing adoption framework," *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138–151, 2016.

[43] Y. A. Ridhawi and A. Karmouch, "Decentralized plan-free semantic-based service composition in mobile networks," *IEEE Transactions on Services Computing*, vol. 8, no. 1, pp. 17–31, 2015.

[44] B. Dong, R. Liu, and H. W. Wang, "Trust-but-verify: verifying result correctness of outsourced frequent itemset mining in data-mining-as-a-service paradigm," *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 18–32, 2016.

[45] N. Basilico, N. Gatti, M. Monga, and S. Sicari, "Security games for node localization through verifiable multilateration," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 72–85, 2014.

[46] J. Vaidya, B. Shafiq, W. Fan, D. Mehmood, and D. Lorenzi, "A random decision tree framework for privacy-preserving data mining," *IEEE Transactions on on Dependable and Secure Computing*, vol. 11, no. 5, pp. 399–411, 2014.

[47] X. Chen, I. Diakonikolas, A. Orfanou, D. Paparas, X. Sun, and M. Yannakakis, "On the complexity of optimal lottery pricing and randomized mechanisms," in *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 1464–1479, Berkeley, CA, USA, October 2015.

[48] J. Pak and L. Zhou, "Temporal patterns of structural deception behavior in a massively multiplayer online game," in *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 131–140, Kauai, HI, USA, January 2015.

[49] E. Arslan, M. Yuksel, and M. H. Gunes, "Training network administrators in a game-like environment," *Journal of Network and Computer Applications*, vol. 53, pp. 14–23, 2015.

[50] W. Y. Liu, F. Tong, B. W. Wang, and Y. D. Wang, "A new proxy blind signature scheme with proxy revocation," *Journal of Electornics and Information Technology*, vol. 30, no. 10, pp. 2468–2471, 2008.

[51] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[52] F. Y. Yang and J. K. Jan, "A secure scheme for restrictive partially blind signatures," in *Proceedings of the Sixth International Conference on Information Integration and Web-Based Applications & Services (IIWAS 2004)*, pp. 541–548, Jakarta, Indonesia, September 2004.

[53] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837–842, 2005.

[54] S. Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, vol. 40, no. 4, pp. 1–15, 2016.

[55] S. Y. Chiou, "Common friends discovery for multiple parties with friendship ownership and replay-attack resistance in mobile social networks," *Wireless Networks*, vol. 24, no. 3, pp. 1–15, 2018.

[56] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strongnon-designated proxy signature," in *Information Security and Privacy*, ACISP 2001, Lecture Notes in Computer Science, V. Varadharajan and Y. Mu (Eds.), vol. 2119, pp. 474–486, Springer, Berlin, Germany, 2001.

[57] W. Qian and C. Li, "The model of anonymous fair e-cash transactions protocol with off-line TTP," in *Proceedings of the Second International Conference on Innovative Computing, Information and Control (ICICIC'C7)*, Kumamoto, Japan, September 2007.

[58] V. V. Das, "Protocol for anonymous and secure e-cash transaction," in *Proceedings of the International Conference on Advances in Computing, Control, & Telecommunication Technologies (ACT'09)*, Bangalore, India, December 2009.

[59] D. Slamanig and S. Rass, "Anonymous but authorized transactions supporting selective traceability," in *Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT)*, Athens, Greece, July 2010.

[60] M. Zhang, "The online game secure transaction platform based on cooperation model," in *Proceedings of the 2010 International Conference on E-Product E-Service and E-Entertainment (ICEEE)*, Henan, China, November 2010.

[61] Elar: Java JS SHA-256, https://www.cnblogs.com/elaron/archive/2013/04/09/3010375.html.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 8340925, 9 pages
https://doi.org/10.1155/2021/8340925

Research Article

Collaborative Learning Based Straggler Prevention in Large-Scale Distributed Computing Framework

Shyam Deshmukh,[1] **Komati Thirupathi Rao**,[1] **and Mohammad Shabaz**[2]

[1]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522502, AP, India*
[2]*Arba Minch University, Arba Minch, Ethiopia*

Correspondence should be addressed to Mohammad Shabaz; mohammad.shabaz@amu.edu.et

Received 7 April 2021; Revised 9 May 2021; Accepted 13 May 2021; Published 24 May 2021

Academic Editor: Manjit Kaur

Modern big data applications tend to prefer a cluster computing approach as they are linked to the distributed computing framework that serves users jobs as per demand. It performs rapid processing of tasks by subdividing them into tasks that execute in parallel. Because of the complex environment, hardware and software issues, tasks might run slowly leading to delayed job completion, and such phenomena are also known as stragglers. The performance improvement of distributed computing framework is a bottleneck by straggling nodes due to various factors like shared resources, heavy system load, or hardware issues leading to the prolonged job execution time. Many state-of-the-art approaches use independent models per node and workload. With increased nodes and workloads, the number of models would increase, and even with large numbers of nodes. Not every node would be able to capture the stragglers as there might not be sufficient training data available of straggler patterns, yielding suboptimal straggler prediction. To alleviate such problems, we propose a novel collaborative learning-based approach for straggler prediction, the alternate direction method of multipliers (ADMM), which is resource-efficient and learns how to efficiently deal with mitigating stragglers without moving data to a centralized location. The proposed framework shares information among the various models, allowing us to use larger training data and bring training time down by avoiding data transfer. We rigorously evaluate the proposed method on various datasets with high accuracy results.

1. Introduction

Any organization that depends on a cloud computing environment majorly focuses on factors like CPU usage, memory, I/O and Network for performance optimization. However, all these parameters are susceptible to performance degradation and may result in suboptimal quality of service (QoS). The Google cluster's trace study is a milestone toward the analysis of workloads in a cloud environment with multiple servers as studied in Dean and Ghemawat [1]; Chen et al. [2]; Reiss et al. [3]. This provides the analysis of workload data recorded on Google cluster trace. The important contribution is the analysis of many tasks and jobs that offer an efficient allotment of the resources for new upcoming tasks to the cloud data center, thereby increasing a throughput of the data center. Owing to the inherent nature of a parallel execution in distributed computing systems, sometimes, it experiences the slow-running tasks known as stragglers, potentially resulting in a delayed job execution. Cloud computing and high-performance computing frameworks typically monitor task completion status and launch backup tasks for stragglers during job execution. Such redundant approaches incur huge operational and financial costs. Even with this, they do not provide postevent analyses to diagnose the causes of the stragglers and their proactive prevention. Typical straggler identification is performed in two modes: (1) reactive (online) and (2) proactive (offline). Reactive techniques typically use a criterion of comparing the task execution time with a threshold calculated based on the median value within all the tasks [4].

Monitoring data may not be always accessible from the user side since the monitoring tools are hard to install and tune. Hence, some studies focus on the offline strategy by analyzing logs instead of monitoring Lu et al.[5]. Cluster managers, e.g., YARN in Vavilapalli et al. [6], Isard et al. [7], Verma et al. [8], have different focuses. They provide resource isolation and allocation based on usages, job priorities, and fairness. They do not provide answers to which tasks are stragglers within a job or to why those tasks are slower.

On the other hand, proactive methods analyze dynamic features like resource utilization, node performance, and heterogeneity that change over time. Using ML, it is possible to build models for previously unknown values using training data that can predict the future and identify straggler [9]. Straggler detection and analysis using ML can be categorized under proactive approaches. Javadpour et al. [10] propose a dynamic method that applies neural networks for identifying straggler tasks to increase the efficiency. Another method of straggler-identification compares the task's execution time (or progress) with a threshold calculated based on the median value within all the tasks. Moreover, there are a breed of techniques of straggler identification based on CPU utilization. It has been identified that there is a strong correlation between high system CPU utilization and straggler occurrence as examined in Reiss et al. [3]; Shen and Li [11]. The reason for this occurrence is resource contention. This is further compounded due to Head-of-Line blocking (HOL blocking), task interference during execution, busy locks, queue issues, hazard rates of task execution, and launching additional speculative replicas, which requires additional time for execution.

The state-of-the-art proactive models as studied analyze the workload and compute nodes as a separate straggler estimation task with independent models. One of the motivations for pursuing a separate ML model for each workload and node independently is because there exists a wide variety of resources allocation ranging from node to node and workload to workload. Consequently, a wide variety of straggler patterns arise because of such heterogeneity. This was demonstrated by Yadwadkar et al. [4]. Thus, a separate ML model training deemed to be necessary. However, such models face a couple of major challenges: (1) independent node and workload that need a set of new training leading to increased time for data gathering, and (2) data scarcity that might arise for a given workload for respective node yielding suboptimal ML models. This set of challenges can be effectively addressed by the ML model that learns the straggler prediction task collaboratively. In such approaches, the node, where sufficient training data would not be available, would get the data, while it was executing other workloads, or from other nodes running the same workload. This can be achieved in practice using multitask learning (MTL) as demonstrated by Yadwadkar et al. [9]. Another approach mentioned in Deshmukh et al. [12] tried to avoid straggler occurrence through data parallelism techniques like MPI-libraries.

Developing a distributed machine learning approach, which distributes large scale data efficiently, is challenging. Standard ML techniques need the training data to be gathered at a centralized location, i.e., on one machine or in a data center. Such data collection and analysis might be difficult to conduct in practice because of resource constraints. In a distributed setting, multiple nodes collaboratively work toward a common optimization objective through an interactive process of local computation and communication, which ideally should result in all models converging to a global optimum.

To alleviate problems, in this paper, we propose a Collaborative Learning-based (CL) formulation for learning predictors that are highly accurate and generalize better than multiple independent models. This is based on the alternate direction method of multipliers- (ADMM-) based support vector machine (SVM), proposed by Boyd et al. [13]. The proposed model enables the nodes to collectively learn a shared prediction model while keeping all the training data on nodes, decoupling the ability to do ML from the need to store the data in the centralized manner. CL allows for smarter models, lower latency, and less power consumption, all while ensuring privacy. There exists a subtle difference between parallel variants of traditional ML models and the CL-based ones; traditional ones have single instruction multiple data (SIMD) architecture, while the latter have decentralized/distributed optimization of model parameters. The local models make predictions on the nodes by bringing the model training to the node as well.

In CL, there exist two types of nodes: (1) a common handler that shares the model updates with other nodes, and (2) independent nodes that are the members of the data center. Independent node downloads the current model, improves it by learning from data on node itself, and then performs the model parameter changes as an update. Only this update to the model is sent to the common node, where it is immediately processed with other node updates to improve the shared model. All the training data remains on the node, and no individual updates are stored in the common node. Consequently, no data transfer takes place among the nodes making it highly resource-efficient and quick. In case of straggler identification, each independent node would be trained on the local data, and thus, forming a local model (A) for straggler identification, and the parameters of all such nodes are aggregated (B) to form a consensus change. Note here that all data reside on local nodes, while only ML model parameters are shared. The consensus change form (B) is reflected on the global straggler identification model (C), owing to the decentralization property of collaborative filtering. Finally, a copy of (C) is made available on each of (A) for straggler prediction. To that end, our key contributions are as follows:

(1) A novel CL-based technique of the straggler identification problem that is resource-efficient and captures the heterogeneous resource contention patterns across workloads and nodes.

(2) A rigorous evaluation of the proposed system for predicting and avoiding stragglers in both generated data and real-world production cluster traces.

(3) The robust CL-based formulation for straggler detection even with a small number of stragglers, thus tackling class imbalance problems, a phenomenon that frequently occurs in ML problems because of lack of sufficient training examples.

In what follows, we first give some background on stragglers in Section 2. We then describe the proposed CL-based straggler detection framework in Section 3. In Section 4, we empirically evaluate our formulations on the various workloads. In Section 5, we describe the results substantiating claims proposed in this article. We conclude with an outlook of improvement and discussion of the proposed work.

2. Related Work

Considering the dynamic nature of the cloud environment including nonreliable resources, heterogeneous workload, and quality of service (QoS) requirements, a static resource management solution may not work. Therefore, a static resource manager is extended with a monitoring module, which collects the valuable information on the performance of the application along with the resource utilization of system components about the state of the system. On the other hand, advances in machine-learning-based (ML) methods offer all the behavioral patterns and interesting changes of monitored components. Obtained knowledge about nonconforming patterns, which is often referred to as an outlier induced for a variety of reasons, helps improve the system performance. Parallel computing frameworks that follow the MapReduce by Dean and Ghemawat [1] paradigm are widely used in real-world big data applications to handle batch and streaming data. Among these, Zaharia et al. [14] have recently gained wide adoption. Different from the Hadoop framework as in Manikandan and Ravi [15], Vavilapalli et al.[16], Spark supports a more general programming model, in which an in-memory technique, called Resilient Distributed Dataset (RDD), Zaharia et al. [17], is used to store the input and intermediate data generated during computation stages. Spark is an implementation of the MapReduce model that outperforms Hadoop by packing multiple operations into single tasks, and by utilizing the RAM memory for caching intermediate data. We target Apache Spark, because it is a widely used, efficient, state-of-the-art platform for data analytics, and it is currently the fastest-growing such open-source platform, Zaharia et al. [14].

Apache spark is an open-source cluster computing engine for large data processing. One of the most important factors in processing large datasets is the speed achieved through running computations in memory. At its core, Spark is a 'computational engine' that is responsible for scheduling, distributing, and monitoring applications consisting of many computational tasks across many worker machines, or a computing cluster. Spark is designed to efficiently scale up from one-to-many thousands of compute nodes. To achieve this while maximizing flexibility, Spark can run over a variety of cluster managers, including Hadoop YARN, and a simple cluster manager included in Spark itself called the Standalone Scheduler. The Spark context connects to the Spark cluster manager, which then allocates resources across the worker nodes for the application. The cluster manager allocates executors across the cluster worker nodes. It copies the application jar file to the workers, and finally it allocates tasks.

LATE by Zaharia et al. [18] uses progress score to enhance the performance as compared to speculative execution. But it exerts pressure on other running tasks by competing for the resources and presumes that tasks make development at a roughly constant rate, which is not always the case. Mantri proposed by Ananthanarayanan et al. [19] focuses more on saving computing resources of a cluster, i.e., task slots. If the backup job has an extremely large probability to finish early, Mantri will stop the initial task while the cluster is active (kill-restart method). However, the kill-restart method may not guarantee that the new task will be completed earlier than the original one. In all reactive techniques, the problem gets even worse when some tasks start straggling when they are well into their execution. Cloning mechanism like Dolly proposed by Ananthanarayanan et al. [20] is proactive but focuses only on interactive jobs and is replicative in nature, incurring additional resources.

A detailed survey of load balancing strategies using Hadoop queue scheduling and virtual machine migration was proposed by Dey and Gunasekhar [21]. A method was proposed by Sravanthi and Rao [22], which is a dynamic, processing aware job scheduler, a technique that performs load allotment work to nodes based on their prior performance. Similarly, a method was proposed by Naresh et al. [23] performing optimal resource discovery and dynamic resource allocation. It is based on improved particle swarm optimization and cuckoo search algorithms. Load balancing is the process of adapting to increase and decrease in the workload with associated resource consumption in data centers that enhance the overall performance of the system achieving client satisfaction. An effective measure was studied by Talasila et al. [24] for tackling the load balancing phenomenon for efficient traffic handling in the public cloud. Another method based on Ant colony swarm optimization based on performance analysis of load balancing techniques in cloud centers was studied by Reddy et al. [25], to prevent the latency in real-time stream processing engines like Apache Spark streaming, with an additional technique like dolly retreat mechanism to avoid stragglers and process data efficiently, as studied in Srikanth and Reddy [26]. Radha and Rao [27] offered a comprehensive review of techniques to increase MapReduce performance in heterogeneous cloud environments by partitioning data locality through intermediate data at the reducer side. By applying the delayed scheduling by enhancing the data locality in MapReduce, Radha and Rao [28] have shown the performance improvement in slot Utilization and Hadoop cluster. Praveen et al. [29] proposed an effective resource allocation using a social group optimization algorithm in conjunction with the scheduling of tasks by application of shortest-job-first scheduling technique for minimizing the makespan time and maximizing throughput.

Many researchers have attempted to avoid stragglers through machine learning approaches. The poor performing nodes are identified and blacklisted [30, 31] during the task scheduling phase. These techniques again lead to resource wastage, as they are not able to participate in the execution as stragglers are mainly nonpersistent. Mao et al. [32], Du et al. [33], and Zhang et al. [34] have applied a reinforcement learning approach for mitigating stragglers, which reduce job completion time, but the preciseness of identification of stragglers may not be optimum. Existing approaches used in decentralizing data consists of Alternating Direction Method of Multipliers (ADMM) based algorithms like [35–39].

3. Proposed Work

3.1. Framework. We introduce a novel framework to identify stragglers, as illustrated in Figure 1 which is based on two main stages. The first stage consists of two parts: (1) extraction of feature vectors from various job resources utilization metrics of nodes; (2) training a global classifier with the help of multiple independent local models as described in the current and next sections as depicted in Figure 2. The second stage consists of testing workloads from the validation or unseen environment by applying the learned model. The feature designing from the test data is the same as mentioned above. Testing at nodes is performed by copying the global model to a node.

The training of the proposed framework takes place in multiple stages as depicted in Figure 2. It shows learning phase of distributed SVM via ADMM, in which individual worker trains SVM model concurrently and separately. In the beginning, each worker's local SVM will be different, but after exchange of model parameters with global model, it becomes more similar in each iteration. The global model will aggregate the local model parameters and generate the consensus model.

3.2. ADMM-Based Collaborative Learning. We consider a set of n nodes and a central aggregator. Each node $i \in n$ has an independent training dataset. $D_i := (a_{i,j}, b_{i,j})$: $\forall j \in m_i$ where m_i is the number of training samples in the dataset D_i, $a_{i,j} \in R^d$ is the d – dimensional feature vector of the j-th training sample, and $b_{i,j} \in R^p$ is the corresponding p-dimensional data label. In this paper, we consider a star network topology, where each node can communicate with the central aggregator, and the aggregator is responsible for message passing and aggregation. The goal of straggler identification is to train a supervised learning model on the segregated dataset $D_i, i \in n$ from n nodes. This enables predicting a label for any new data feature vector of job utilization metrics. The learning objective can be formulated as

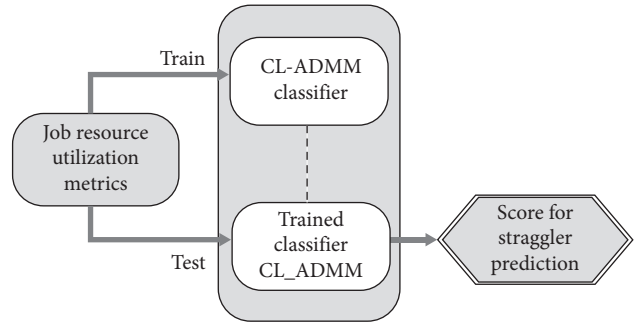


Figure 1: Workflow of proposed straggler detection framework.

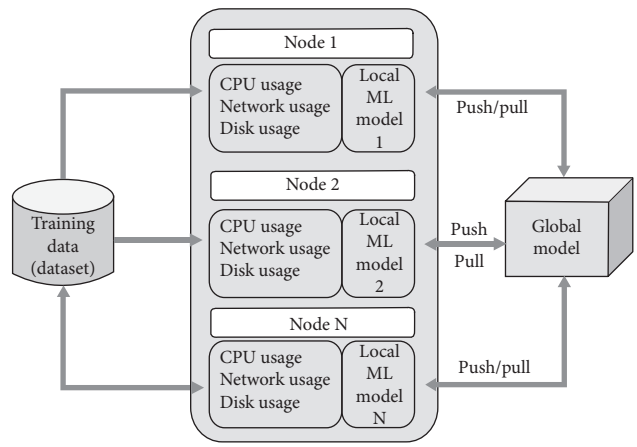


Figure 2: Training phase of the proposed architecture.

the following regularized empirical risk minimization problem:

$$\min_{w} \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{1}{m_i} l\left(a_{i,j}, b_{i,j}, w\right) + \lambda R(w), \tag{1}$$

$w \in R^{d\times p}$ is the trained global ML model. $l(\cdot)$: $R^d \times R^p \times R^{d\times p} \longrightarrow R$ is the loss function used to measure the quality of the trained model, $R(\cdot)$ refers to the regularizer function introduced to prevent overfitting, and $\lambda > 0$ is the regularizer parameter controlling the impact of regularization. Casting Equation (1) can be cast into the loss function of binary logistic regression classifier as follows:

$$l\left(a_{i,j}, b_{i,j}, w\right) = \ln\left(1 + \exp\left(-b_{i,j} w^T a_{i,j}\right)\right). \tag{2}$$

To apply ADMM, we reformulate Equation (1) as

$$\min_{\{w_i\}_{i\in n}} \sum_{i=1}^{n} \left(\sum_{j=1}^{m_i} \frac{1}{m_i} l\left(a_{i,j}, b_{i,j}, w_i\right) + \frac{\lambda}{n} R(w_i) \right), \tag{3}$$

$$\text{such that } w_i = w, \quad i = 1, \ldots, n.$$

In standard ADMM, the augmented Lagrangian function associated with the problem (3) is

$$L_\rho(w, \{w_i\}_{i\in n}, \{\gamma_i\}_{i\in n}) = \sum_{i=1}^{n} L_{\rho,i}(w_i, w, \gamma_i), \tag{4}$$

where

$$L_{\rho,i}(w_i, w, \gamma_i) = \sum_{j=1}^{m_i} \frac{1}{m_i} l\left(a_{i,j}, b_{i,j}, w_i\right) + \frac{\lambda}{n} R(w_i) - \gamma_i, w_i - w + \frac{\rho}{2}\|w_i - w\|^2, \tag{5}$$

$\{\gamma_i\}_{i\in n} \in R^{d\times p\times n}$ are the dual variables associated with the constraints, and $\rho > 0$ is the penalty parameter. The standard ADMM solves the problem in Equation (3) in a Gauss-Seidel manner by minimizing Equation (4) with respect to $\{w_i\}_{i\in n}$ and **w** alternatively followed by a dual update of $\{\gamma_i\}_{i\in n}$. The formulation is based on the work presented in [13].

3.3. Straggler Prediction Model Using Probabilistic Classification. The training dataset $D = \{(a_i, b_i)|a_i \in R^d, b_i \in (-1, +1)\}_{i=1}^{m}$ is either −1 or +1, indicating the class to which data point ai belongs. The objective of probabilistic classification using logistic regression as mentioned above is to learn the class-posterior probability $p(\mathbf{b} \mid \mathbf{a})$ of the training samples dataset D. Based on the class-posterior probability, classification of a new sample a_{test} can be carried out $b_{\text{test}} := \max_{b} \in \{-1, +1\} p(b|a)$ with confidence $p(b|a)$. Let $b \in \{-1, +1\}$ represent the nonstraggler and straggler class, respectively. The task of straggler detection is to assign the value of the estimate $\widehat{p}(a)$ for test data, given training data and model. The conditional probability of straggler is given by $\widehat{p}(a, \theta)$, where θ is the vector of parameters learned in Section 3.*2 - w, w_i, ρ and γ* respectively.

4. Experimental Study

4.1. Configurations. The various configuration parameters are mentioned in Table 1.

4.2. Cluster Setup. We have a network of nodes in a Hadoop Cluster as per the configurations as shown in Table 1. We have built the Hadoop Cluster of five nodes to estimate the proposed solution for discovering straggler nodes. One of the nodes is picked as a master node, and it runs the Hadoop Distributed File System (Name-node) and MapReduce run time (Resource manager). The remaining four nodes are slave nodes (Data-nodes and Node-managers). The regular block size in Hadoop is 128 MB. When a larger file is inserted into HDFS, it will be broken down into 128 MB pieces and divided between data nodes. All systems in the multinode setup use Ubuntu v16.04 operating system, JDK 1.7, and Hadoop 2.7.1 version for performance.

4.3. Workload. We executed two different types of jobs on intensive Hadoop memory and intensive CPU utilization. Memory intensive tasks such as machine learning-based K-Nearest neighbors and image-processing were performed. CPU intensive tasks were created by kernel Support vector machines and similar algorithms. Some network intensive tasks using heavy uploads and downloads were also created in conjunction with the first two types of load creation mechanism.

4.4. Dataset

4.4.1. Features. We have used 22 features, most of them related to CPU utilization (e.g., CPU idle time, user time, system, CPU wait, I/O and CPU speed, etc.), disk utilization (e.g., amount of free space, local read/write statistics from the data nodes, maximum percent used for all partitions, etc.), memory utilization (e.g., Amount of buffered, cached, shared, free and total amount of available memory, etc.), network utilization (e.g., packets in and out per second, etc.), and system-level features (e.g., total number of processes, total number of running processes, total amount of swap memory, amount of available swap memory, etc.). The job history server traces job execution time through start time, finish time, task execution time, read data in bytes, write data in bytes, and elapsed time that are also obtained. We have not used any feature reduction technique as the number of features is already lower in number, and performance demonstrated using the proposed method in section 5 does not seem to be affected by the number of features.

4.4.2. Dataset Generation. For constructing the prediction models, we require a labelled dataset consisting of {feature, label} pairs. We have used Ganglia-based node-monitor by Massie et al. [40] to capture resource utilization metrics of nodes. We get the features related to jobs from Hadoop. We select a subset consisting of five features, that is, execution time, average CPU utilization ratio, memory usage, disk I/O time, and cycles per instruction, empirically using the proposed ADMM. The metric used for deciding the straggler is normalized duration (execution) time suggested by Yadwadkar et al. [4]:

$$n\,d(t) = \left[\frac{\text{task execution time}}{(\text{amount of work bytes read/written by task } t)}\right]. \tag{6}$$

An ith task t of job J is called a straggler if $n\,d(t_i) > (\beta \times \text{median}\{n\,d(t_i)\})$, where β is the threshold

Table 1: Hardware and software configurations used.

Attributes	Values
Hadoop cluster installation mode	Fully distributed
Number of cluster nodes	5
RAM at nodes 1, 2, 3, and 4	4 GB
Network topology	Star with master-slave
Hard disk space	500 GB
Master node	Has a job follower
Slave node	Data node and task follower
File block size	128 MB
Clock frequency	2.7 GHz

coefficient, taken as 1.3, as a rule of thumb. However, we see the variation of performance metrics across various values of β.

4.5. Experimental Setup. With labelling the dataset, we evaluate the performance of straggler prediction on all the workloads using ADMM-based SVM. First, each node builds its local classification model by collecting data on that node. To get the features related to the straggler node, we have overloaded each node alternatively and then captured its features. This process of capturing the dataset for straggler and nonstraggler in the training phase requires little time, and we incrementally increased the number of stragglers in the system. The standard feature normalized data is fed to the ADMM SVM written in the Spark environment by Dhar et al. [41]. This reduces the model building time with a small amount of model parameter transfer. This completes the model training phase. This global model would reside on each node for the classification.

In this experiment, we have chosen a binary classification method, where +1 is the label for straggler and -1 for nonstraggler. For ADMM-SVM for logistic regression, logistic loss is used. The practical implementation of ADMM-LR is referred to in [34]. For ADMM-SVM with least square formulation, the loss function is least square for both methods, and the regularization parameter is elastic net. The parameters λ and ρ are set to 1. For MPI logistic regression from Scikit-learn by Pedregosa et al. [42], we use *L2* penalty, with regularization constant C being set to 1.

We consider a 5-fold cross validation method to determine the performance metrics. Here, we provide the results of ADMM-SVM with logistic regression and least-squares SVM and centralized parallel (message passing interface) SVM (LIBLINEAR) from Pedregosa et al. [42] and Fan et al. [43] and then evaluate them using the following scenarios:

(1) Classification accuracy when there is sufficient data

(2) Classification accuracy when sufficient data is not available We also provide the performance across various β. Overall, we have 724 stragglers and 21000 nonstraggler records.

5. Results and Discussions

5.1. Performance Evaluation Metrics. We use Precision, Recall, and $F1$-Score (denoted as $F1$) to evaluate the performance of all models: the true positives (TP) are the true straggler detected by the system. False positives (FP) are the nonstraggler data points detected as stragglers. True negatives (TN) are the correct nonstragglers detected by the system, and false negatives (FN) are stragglers detected as nonstragglers by the system. With this set of definitions,

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}},$$
$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{7}$$
$$F1\ \text{score} = \frac{2 \times \text{Precision Recall}}{\text{Precision} + \text{Recall}}.$$

5.2. Evaluation. We report the quantitative improvement for identification of stragglers: Figure 3 presents the F1 score (harmonic mean of precision and recall) of straggler detection averaged across the 5-fold with 80/20 ratio of train and test. All data points on the plot are a 5-fold quantity average. Figure 3 reports values of F1 score for various values of β. From the figures, our approaches outperform the MPI-based methods. We have an extremely high F1-score of more than 98% for beta values 1.6 to 1.8. The benchmark method has a lower performance. A potential reason for MPI-based SVM to perform slightly worse is because it is not easily scalable. Besides, the class imbalance between stragglers and nonstragglers is problematic for most supervised learning methods. Our framework alleviates these problems by including a training dataset estimating correct data distributions of each class. Figure 4 represents the classification accuracy when sufficient data is not available. It represents the accuracy of 5-fold straggler detection average with 80/20 ratio of train and test. All data points on the plot are a 5-fold quantity average. With the increase in the number of straggler class examples available for training, the straggler detection improves. Again, ADMM-LR-SVM performs best, while its variant ADMM-LS-SVM is not far from it. With just 183 sets of straggler examples, our framework achieves more than 94% accuracy. The performance of both of these methods remains constant with increased inclusion of straggler records.

MPI based SVM performs relatively poorly because of class imbalance examples. Similarly, Figure 5 represents the F1 score computed against various numbers of straggler records. With increasing the number of straggler examples, F1-score of straggler detection improves. Again, ADMM-LR-SVM performs best, while its variant ADMM-LS-SVM is not far from it. With just 183 sets of straggler examples, our framework achieves F1-score more than 98%. As seen in

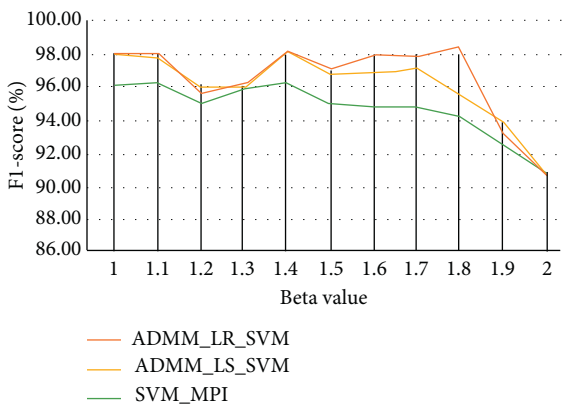


Figure 3: The F1-score variation across various values of β.

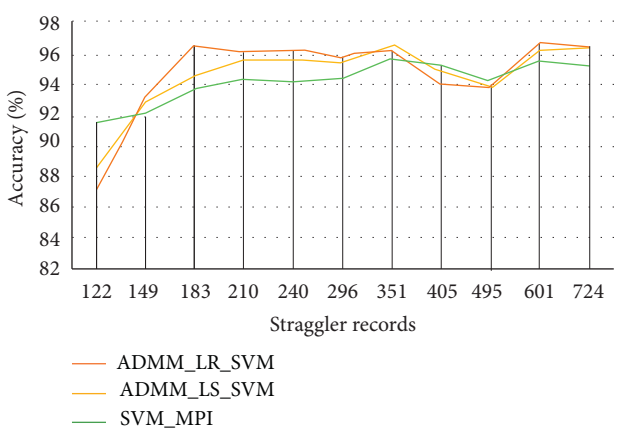


Figure 4: Variation of accuracy with increasing number of stragglers.

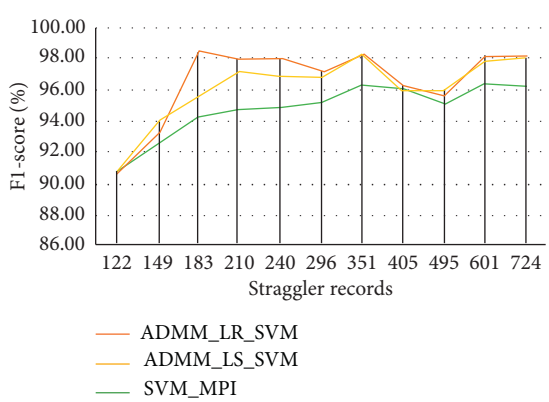


Figure 5: Variation of F1-score with increasing number of stragglers.

Figures 3–5, there is considerable improvement of lesion detection, thanks to the proposed framework.

6. Conclusion

We have introduced a novel method for straggler detection based on support vector machine variants of alternating directions of method of multipliers. The efficacy of our method was evaluated through rigorous evaluation on straggle data. We have demonstrated that our method achieves better performance compared to the benchmark method: MPI-based SVM. Our formulation can achieve better accuracy with only a third of the training data and can generalize better than other approaches for learning tasks with little or no data. Thus, the class imbalance problem is tackled naturally. Our methodology is more suitable for straggler analysis because of its ability to capture heterogeneous distribution of stragglers correctly. This performance suggests that it can provide valuable assistance in detecting the stragglers in production with high reliability. The proposed framework is generic in nature and can be extended to various types of workloads, e.g., workloads across various data centers, independent of big data computing frameworks. The framework described here allows for exploration of additional information with node and job utilization resources. For example, one can consider infusing distribution of node utilization metrics with task utilization metrics and thus can help in further management of scheduling of jobs. The adaptation of ADMM-SVM investigated for learning a comprehensive predictor with better accuracy and reduced job completion along with improved data privacy as no data movement from client site is required for sensitive applications.

Data Availability

The data are available upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Dean and S. Ghemawat, "MapReduce," *Communications of the ACM*, vol. 51, no. 1, pp. 107–113, 2008.

[2] Q. Chen, C. Liu, and Z. Xiao, "Improving mapreduce performance using smart speculative execution strategy," *Institute of Electrical and Electronics Engineers Transactions on Computers*, vol. 63, no. 4, pp. 954–967, 2013.

[3] C. Reiss, J. Wilkes, and J. L. Hellerstein, *Google Cluster-Usage Traces: Format Schema*, Google Inc, White Paper, , pp. 1–14, 2011.

[4] N. J. Yadwadkar, G. Ananthanarayanan, and R. Katz, "Wrangler: Predictable and faster jobs using fewer resources." in *Proceedings of the ACM Symposium on Cloud Computing*, pp. 1–14, Seattle WA USA, November 2014.

[5] S. Lu, X. Wei, B. Rao et al., "LADRA: log-based abnormal task detection and root-cause analysis in big data processing with Spark," *Future Generation Computer Systems*, vol. 95, pp. 392–403, 2019.

[6] V. K. Vavilapalli, A. C. Murthy, C. Douglas et al., "Apache hadoop yarn: yet another resource negotiator," in *Proceedings of the 4th Annual Symposium on Cloud Computing*, pp. 1–16, Santa Clara, CA, USA, October 2013.

[7] M. Isard, V. Prabhakaran, J. Currey, U. Wieder, K. Talwar, and A. Goldberg, "Quincy: fair scheduling for distributed computing clusters," in *Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles*, pp. 261–276, Big Sky, MT, USA, October 2009.

[8] A. Verma, L. Pedrosa, M. R. Korupolu, D. Oppenheimer, E. Tune, and J. Wilkes, "Large-scale cluster management at Google with borg," in *Proceedings of the European Conference on Computer Systems (EuroSys)*, Bordeaux, France, April 2015.

[9] N. J. Yadwadkar, B. Hariharan, J. E. Gonzalez, and R. Katz, "Multi-task learning for straggler avoiding predictive job scheduling," *The Journal of Machine Learning Research*, vol. 17, no. 1, pp. 3692–3728, 2016.

[10] A. Javadpour, G. Wang, S. Rezaei, and K. C. Li, "Detecting straggler mapreduce tasks in big data processing infrastructure by neural network," *The Journal of Supercomputing*, vol. 2020, 25 pages, 2020.

[11] H. Shen and Li C. Zeno, "A straggler diagnosis system for distributed computing using machine learning," in *Proceedings of the International Conference on High Performance Computing*, pp. 144–162, Springer, Pune, India, December 2020.

[12] S. Deshmukh, J. Aghav, K. T. Rao, and B. T. Rao, "Avoiding slow running nodes in distributed systems, Lecture Notes in Networks and Systems," in *Proceedings of the Computer Communication, Networking and Internet Security*, Springer, Berlin, Germany, pp. 411–420, 2017.

[13] S. Boyd, N. Parikh, and E. Chu, *Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers*, Now Publishers Inc., Delft, Netherlands, 2011.

[14] M. Zaharia, A. Konwinski, A. D. Joseph, R. H. Katz, and I. Stoica, "Improving mapreduce performance in heterogeneous environments," *Osdi*, vol. 8, no. 7, 2016.

[15] S. G. Manikandan and S. Ravi, "Big data analysis using Apache hadoop," in *Proceedings of the 2014 International Conference on IT Convergence and Security (ICITCS)*, pp. 1–4, IEEE, Beijing, China, October 2014.

[16] V. K. Vavilapalli, A. C. Murthy, C. Douglas et al., "Apache hadoop yarn: yet another resource negotiator," in *Proceedings of the 4th Annual Symposium on Cloud*, Santa Clara, CA, USA, October 2013.

[17] M. Zaharia, R. S. Xin, P. Wendell et al., "Apache spark: a unified engine for big data processing," *Communications of the ACM"*, vol. 59, no. 11, pp. 56–65, 2012.

[18] M. Zaharia, M. Chowdhury, T. Das, and A. Dave, "Resilient distributed datasets: a fault-tolerant abstraction for in-memory cluster computing," in *Proceedings of the Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation R12*, pp. 15–28, Renton, WA, USA, April 2008.

[19] G. Ananthanarayanan, S. Kandula, A. G. Greenberg et al., "Reining in the outliers in map-reduce clusters using mantri," *Osdi*, vol. 10, p. 24, 2010.

[20] G. Ananthanarayanan, A. Ghodsi, S. Shenker, and I. Stoica, "Effective straggler mitigation: attack of the clones," in *Proceedings of the Presented as part of the 10th USENIX Symposium on Networked Systems Design and Implementation*, vol. 13, pp. 185–198, Berkeley, CA, USA, April 2013.

[21] N. S. Dey and T. Gunasekhar, "A comprehensive survey of load balancing strategies using hadoop queue scheduling and virtual machine migration," *Institute of Electrical and Electronics Engineers Access*, vol. 7, pp. 92259–92284, 2019.

[22] S. Sravanthi and K. Rao, "Efficient big data analytics with optimized parallel processing," in *Proceedings of the 2014 IEEE 28th International Parallel and Distributed Processing Symposium*, vol. 11, pp. 312–318, Phoenix, AZ, USA, May 2016.

[23] T. Naresh, A. Lakshmi, and V. Reddy, "An efficient resource allocation strategy based on improved particle swarm optimization (ipso)," *Pakistan Journal of Biotechnology*, vol. 14, pp. 125–128, 2017.

[24] S. Talasila, V. Havisha, S. Koushik, M. Deep, and V. Reddy, "Load balancing techniques for efficient traffic management in cloud environment," *Inter- National Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, p. 963, 2016.

[25] V. Reddy, K. Surya, M. Praveen, B. Lokesh, A. Vishal, and K. Akhil, "Performance analysis of load balancing algorithms in cloud computing environment," *Indian Journal of Science and Technology*, vol. 9, 2016.

[26] B. V. S. Srikanth and V. Krishna Reddy, "Efficiency of stream processing engines for processing BIGDATA streams," *Indian Journal of Science and Technology*, vol. 9, no. 14, 2016.

[27] K. Radha and D. B. Rao, "A review on enhancing map reduce performance with data locality in heterogeneous environment," *International Journal of Control Theory and Applications*, vol. 9, pp. 8463–8472, 2016.

[28] K. Radha and B. T. Rao, "Slot utilization and performance improvement in hadoop cluster," *Advances in Intelligent Systems and Computing*, vol. 72, pp. 49–62, 2016.

[29] s Praveen, T. R. Komati, and B. Janakiramaiah, "Effective allocation of re- sources and task scheduling in cloud environment using social group optimization," *Arabian Journal for Science and Engineering*, vol. 43, 2017.

[30] N. J. Yadwadkar and W. Choi, *Proactive Straggler Avoidance Using Machine Learning*, Univ. California, Berkeley, CA, USA, White Paper, 2012.

[31] X. Ouyang, C. Wang, and J. Xu, "Mitigating stragglers to avoid QoS violation for time-critical applications through dynamic server blacklisting," *Future Generation Computer Systems*, vol. 101, Article ID 831842, 2019.

[32] H. Mao, M. Schwarzkopf, S. Bojja Venkatakrishnan, Z. Meng, and M. Alizadeh, "Learning scheduling algorithms for data processing clusters," 2018, http://arxiv.org/abs/1810.01963.

[33] P. Lubell-Doughtie and J. Sondag, "Practical distributed classification using the alternating direction method of multipliers algorithm," in *Proceedings of the 2013 IEEE International Conference on Big Data*, pp. 773–776, Silicon Valley, CA, USA, October 2013.

[34] H. Du, S. Zhang, P. Han, K. Zhang, and B. Xu, "Cheetah: A dynamic performance optimization approach on heterogeneous big data analytics cluster," in *Proceedings of the 5th International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 169–177, QingDao, China, August 2019.

[35] H. Du and S. Zhang, "Hawkeye: adaptive straggler identification on heterogeneous spark cluster with reinforcement learning," *Institute of Electrical and Electronics Engineers Access*, vol. 8, pp. 57822–57832, 2020.

[36] E. Wei and A. Ozdaglar, "Distributed alternating direction method of multipliers," in *Proceedings of the 2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, pp. 5445–5450, Wailea, HI, USA, December 2012.

[37] J. Bhola, S. Soni, and G. K. Cheema, "Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1281–1288, 2019.

[38] Q. Ling and A. Ribeiro, "Decentralized linearized alternating direction method of multipliers," in *Proceedings of the Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pp. 5447–5451, IEEE, Florence, Italy, May 2014.

[39] Q. Ling, Y. Liu, W. Shi, and Z. Tian, "Weighted admm for fast decentralized network optimization," *Institute of Electrical and Electronics Engineers Transactions on Signal Processing*, vol. 64, no. 22, pp. 5930–5942, 2016.

[40] M. L. Massie, B. N. Chun, and D. E. Culler, "The ganglia distributed monitoring system: design, implementation, and experience," *Parallel Computing*, vol. 30, no. 7, pp. 817–840, 2004.

[41] S. Dhar, C. Yi, N. Ramakrishnan, and M. Shah, "Admm based scalable machine learning on spark," in *Proceedings of the 2015 IEEE International Conference on Big Data (Big Data)*, pp. 1174–1182, IEEE, Santa Clara, CA, USA, November 2015.

[42] F. Pedregosa, G. Varoquaux, A. Gramfort et al., "Scikit- learn: machine learning in python," *The Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[43] R. E. Fan, K. W. Chang, C. J. Hsieh, X. R. Wang, and C. J. Lin, "Liblinear: A library for large linear classification," *Journal of Machine Learning Research*, vol. 9, pp. 1871–1874, 2008.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9940183, 15 pages
https://doi.org/10.1155/2021/9940183

Research Article

Lightweight Technical Implementation of Single Sign-On Authentication and Key Agreement Mechanism for Multiserver Architecture-Based Systems

Darpan Anand,[1] **Vineeta Khemchandani**,[2] **Munish Sabharawal**,[3] **Omar Cheikhrouhou**,[4] **and Ouissem Ben Fredj**[5]

[1]*Chandigarh University, Punjab 140301, India*
[2]*J.S.S. Academy of Technical Education, Noida, India*
[3]*Galgotias University, Noida, India*
[4]*College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[5]*University of Kairouan, Route Périphérique Dar El Amen 3100, Kairouan, Tunisia*

Correspondence should be addressed to Ouissem Ben Fredj; ouissem.benfredj@gmail.com

Received 21 March 2021; Revised 29 April 2021; Accepted 4 May 2021; Published 17 May 2021

Academic Editor: Vijay Kumar

Authentication is the primary and mandatory process for any Information and Communication Technology (ICT) application to prove the legitimacy of the genuine user. It becomes more important and crucial for public platforms like e-governance platforms. The Government of India is transforming the country into Digital India through various e-governance initiatives based on ICT. For authentication, National e-Authentication Framework (NeAF) was proposed by the Indian government which is a policy framework for authentication. This framework does not provide any technical and unified solution for authentication systems while it is based on centralized verification data. In this paper, we proposed a solution for the authentication which provides the unified authentication solution for the Indian e-governance system with existing infrastructure. This solution also provides the features such as scalability, security, and transparency based on distributed computing and working on multiserver architecture. This solution also fulfills the need of the current Indian government to provide multiple e-governance services through a single smart card.

1. Introduction

Authentication is the primary and mandatory process for any application to prove the legitimacy of the user [1]. It becomes more important and crucial for public platforms. There are many ways to prove the authenticity of the user for any application, software, or service and authentication where ICT has been used. It can be done using various techniques such as password and biometrics [2] and is used in various sectors such a banking [2, 3]. But, due to the increase in Internet coverage, various organizations, groups, companies, and firms started the delivery of their services through Information Communication Technology (ICT). One of the popular examples of this type of service is e-governance. Similar to the other applications, authentication is also required it. The Government of India also took serious steps towards transforming the country to Digital India through various e-governance initiatives based on Information Communication Technology (ICT). In the pace of development, National e-Authentication Framework (NeAF) was proposed by the Indian government. NeAF has been prepared by the National e-Governance Division (NeGD) within the Department of Information Technology (DIT).

NeAF is a policy framework for authentication for the Indian e-governance system. This paper is analyzing the requirements of an authentication protocol for the Indian e-governance system under the boundaries of NeAF.

Further, the paper extends up to the implementation, its concepts, and architecture to overcome the authentication issues and provides an integrated and unified view to the whole Indian e-governance system. The problem arises that individual registration and authentication process is required for each e-governance service. Therefore, a unified single sign-on authentication technique is required for the Indian e-governance system to integrate all e-governance services. The same problem is reflected in the survey conducted by us [4, 5].

Due to the increase in Internet coverage, various organizations, groups, companies, and firms started the delivery of their services through Information Communication Technology (ICT); therefore, authentication is becoming the most important process to provide accessibility of the services only for a legitimate user [6]. The same concept is applying by the government to serve its citizens through various services, which is called e-governance [7–9].

Since the 1970s, the Government of India took serious steps towards transforming the country to Digital India through various e-governance initiatives based on Information Communication Technology (ICT) [5, 10]. The journey of e-governance development in India started in 1970 with the establishment of the Department of Electronics, which is related to ICT development [11]. Then, National Information Center (NIC) was established in 1977, NICNET which is a satellite-based computer network was established in 1987, and District Information System of the National Information Center (DISNIC) was launched in 1990 [12]. Ministry of Information Technology was established to monitor Information Technology-related issues in 2000, the government formally launched its National e-Governance Plan (NeGP) [13], a guideline for all types of governments under the federal structure to implement e-governance in 2000 [14], e-Authentication framework was launched for user authentication for e-governance under NeGP in 2012 [15], next version of National e-Governance Plan e-Kranti is launched to improve and strengthen the existing NeGP in 2013, and finally, Digital India was established in the year 2014. In the pace of development, National e-Authentication Framework (NeAF) was proposed by the Indian government. NeAF has been prepared by the National e-Governance Division (NeGD) within the Department of Information Technology (DIT). NeAF is a policy framework for authentication to prove the legitimacy of the citizens to access various services of/from the Indian e-governance system [16].

There is no provision to access various services through single sign-on. User needs to register at every portal of government service, and the architecture of these services is different. There are various authentication techniques adopted by the respective department on their own, such as biometric, Q&A, OATH, OTP authentication, and LDAP. It creates a problem for integration and intercommunication. The second issue is the scale of the users. How can the government offer to access huge services at every point for billions of people? This paper found a solution to install the thin service over the ATM and other kiosks to access government services along with the existing financial services. Later, the architecture to implement thin service is also explained in this manuscript. Therefore, the UIAP is secure, multiserver architecture-oriented, based on distributed computing, using smart card, and able to integrate the existing system and fulfill the need of billions of people to access the government services to provide a unified view to the Indian e-governance system.

The available authentication framework and developments are explained at the outset of this paper which includes the National e-Authentication Framework and then e-Pramaan. Then, the working of these projects is explained, and in the next section, the proposed protocol has explained its implementation process. The performance parameters are explained along with the conclusion of the work [17]. In Section 3, related work has been discussed. The existing Indian e-governance authentication system has been discussed in Section 4. The UIAP protocol proposed to integrate the Indian e-governance system has been proposed in Section 5. Section 6 explains the process to implement the UIAP for the existing Indian e-governance system. Finally, Section 7 concludes the paper.

The Government of India expressed its interest to provide a smart card for authentication for various e-governance services. The e-governance environment is working on a multiserver architecture-based environment and using distributed computing. Many researchers presented different authentication protocols both for two-layer and for multilayer architecture-based systems. The authentication schemes for multiserver architecture are available in the literature [18–23]. It has been observed that the hash-based authentication schemes are the most efficient techniques [18, 22, 24–26]. In 2014, Hu [27] proposed a technique [19], which claims anonymity and traceability with all necessary security properties as in Li. et al.'s protocol [19]. Gaharana and Anand presented a security analysis of various multiserver authentication techniques [28]. These techniques are based on two-way and three-way factor-based authentication [29–34]. Generally, authentication schemes are dependent on a central server that stores the verification data. Because of centrally stored verification data, these schemes are vulnerable. Therefore, a new authentication scheme is required to overcome the vulnerabilities due to centrally stored verification data such as reflection attack, insider attack, and smart card loss attack, and Anand D. and Khemchandani V. proposed a technique to overcome this weakness [35, 36].

2. Motivation of This Work

The available authentication solutions are not capable of giving a unified authentication view for the e-governance services in India. Citizens need to register themselves for each service and then the services are integrated using the ADHAAR number which is a unique identification number for citizen which is centralized. Therefore, there is a requirement for an authentication technique that can give a unified view to the authentication process to access e-governance services at geographically distributed servers and departments. Along with this unified view, there is also a

requirement for this authentication process that it should not depend on any centralized storage and should be able to store the related information at distributed storage.

The novel authentication mechanism is the requirement of the time for the Indian e-governance system and this is the motivation for this work. Motivated by this, the paper proposes a robust and efficient user authentication scheme. The major contributions of this paper are smart card-based authentication scheme for a multiserver environment with the following selected features:

Secure: all the major security threats and goals are tested

Light-weighted: distributed parameters are used in place of centralized storage

Single sign-on: single registration may work for all the departments as per the existing e-governance architecture

Efficient: light-weighted and secure protocol which is capable of handling big amount of requests for a huge population through existing resources

3. Related Work

Various authentication schemes have been proposed to handle the security threats specifically for e-governance projects. Roy and Karforma proposed a secure and smart system for e-governance which is using ECDSA (Elliptic Curve Digital Signature Algorithm) based on UML [79]. In this technique, they proposed the e-governance system model dependent on Multipurpose Electronic Card (MEC). In other work, Roy et al. proposed another approach in which ECDSA was replaced with the RSA approach for object-oriented modeling of RSA digital signature. Mutual authentication is the basic security requirement that needs to incorporate in the e-governance system as in 2006. Liao et al. proposed a mutual authentication scheme. Yoon and Yoo [38] analyzed the scheme of Liao et al. and proved that it is unable to resist playback threats and offline password guessing. Other techniques have been proposed by Ku and Chen [39] and Yoon et al. [40]. Wang et al. [41] analyzed these schemes in 2007 and found the security threats such as forgery and DoS threats. To overcome these threats, Wang et al. proposed another scheme with all the security functionalities available in Ku and Chen [39] and Yoon found during the analysis such as insider attack, reflection attack, and parallel session attack [42–44].

Chung et al. [45] analyzed the scheme of Wang et al. [41] in 2009 and observed that the scheme is unable to resist impersonation and password guessing attack. The further author proposed a technique providing security services such as offline password guessing attack, impersonation attack, insider attack, the stolen smart card attack, and the modification of account-database attack. Additionally, the scheme was able to achieve the perfect forward secrecy [46, 47]. Xu et al. [47] analyzed the Lee et al. [46] and Lee and Chiu [48] schemes and proved that these techniques are not able to resist forgery attack. Then, Xu et al. [47] promulgated an improvised scheme to remove security weakness. Song [49] proposed a better scheme in which the drawback of the scheme of Xu et al. [47] has been improvised to overcome the existing impersonation attack. Chen et al. [50] analyzed the scheme of Wang et al. [41]. It has been observed Wang's technique is not able to resist the security attacks such as parallel sessions and forgery attacks. Further, Chen et al. proposed a better technique. Chen et al. [50] analyzed the techniques of Sood et al. [51] and Song [49] in 2012. According to Chen et al. [50], the improvements recommended by Song [49] and Sood et al. [51] are very sensitive to many known attacks. In this method, Chen et al. recognized security defects in the enhanced smart card-based password authentication and key agreement schemes of Sood et al. [51] and Song [49]. The technique of Sood et al. does not support an important security requirement of mutual authentication, and Song's technique was susceptible to offline guessing attacks and stolen card and thus enhanced the technique of Chen et al., which eradicated these security weaknesses, and the technique achieved mutual authentication, withstands various attacks, and is efficient. He also exposed that the technique of Sood et al. [51] has two drawbacks. Firstly, the technique is in a one-way authentication mechanism as the server verifies the authenticity of the entity and has no reciprocal mechanism of authentication. The second is erroneous input detection. Chen et al. [50] also determined the offline password guessing attack concerning Song's scheme, which led to the lack of security. Additionally, Chen et al. [50] presented an authentication mechanism to overcome the security flaws. In 2013, Li et al. [52] found that Chen et al. failed to satisfy forward secrecy and proposed an improved scheme. Jiang et al. [30] analyzed the scheme of Chen et al. [50] and found that the scheme is insecure to password guessing attack.

4. Authentication System for Indian e-Governance System

The journey towards authentication system for the Indian e-governance system started in 1970 with the establishment of the Department of Electronics since then many milestones have been achieved. In 1977, NIC was established. In the year 2006, the government launched NeGP (National e-Governance Plan), a guideline for all types of governments under the federal structure to implement e-governance.

4.1. National e-Authentication Framework. This project has an objective to develop an online service delivery mechanism to authenticate the user's identity electronically to prove their legitimacy to access each government service securely. Therefore, the Department of Information Technology, Government of India, has proposed the National e-Authentication Framework (NeAF).

The objective of NeAF is to provide a guiding framework to all central ministries, state departments, and other government agencies for the implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy. The overall objective is to

provide a trusted electronic environment where the users can transact easily and securely with the government. The framework first defines the principles of e-Authentication along with its various components such as Identity Management, Authentication, Authorization, Credential Registration, Permission Assignment, Deregistration, and Single Sign-on. The framework then defines a layered approach towards e-Authentication along with a six-step methodology to determine the business and assurance requirements of government applications, the user registration process, the implementation model, and the assessment of the chosen authentication model. It is also recommending the procedure to define the sensitivity level of the respective application for National Service Delivery Gateway (NSDG), State Service Delivery Gateway (SSDG), and Mobile Service Delivery Gateway (MSDG). Further, the framework is followed by the technical architecture of "e-Authentication" as well as the roles and responsibilities of stakeholders towards acceptance and execution of this framework [5, 53–55].

Implementation of the authentication is depended on the available technologies, mechanisms, and interfaces. These are incorporated in NeAF as illustrated in Figure 1. The following sections are describing these components.

4.2. Authentication Protocols. The organizations build Information and Communication Technology- (ICT-) based systems to provide quality services to their end-users. Several interconnected servers are required for the efficient and effective use of these services. The user legitimacy test is very important for ICT-enabled services. Different authentication protocols to test are adopted by the various departments for their projects. For authentication, identification is important because, ultimately, the identity of the user will be proved in the authentication [37, 56].

The proposed protocols and methods identified in NeAF are as follows:

(1) Biometric: biometric authentication is simply the process of verifying the user's identity using measurements or other unique characteristics of his/her body and then logging in to the system, an app, a device, and so on [57]. For these body measurements (such as iris, fingerprints, palm design, face detection, and voice), specific hardware is used to extract the features and match them with already recorded features [58, 59].

This technique has some disadvantages as follows:

Unable to update or change because biometrics is last a lifetime
"Master fingerprints" can trick many phones and scanners
Vulnerabilities in biometric authentication software
Creating a fake identification such as finger (spoofing the fingerprint)
Hacking the biometric sensor and stealing the data

(2) QnA: in this mechanism, the user can either set their own set of questions and answers during the QnA creation stage, or the application can choose to ask predefined questions to the user. It can be used as a secondary, second factor of two-factor authentication or in the password change process. It cannot be used as a primary authentication process because the vulnerability is very high and the probability to break it is also very high [60, 61].

(3) OATH: this mechanism is the initiative of industrial collaboration and combined efforts to develop a strong and secure authentication scheme that is open to use. It uses open standards to endorse the implementation of strong authentication [62, 63]. The objective of this scheme is to make the authentication process independent from the vendor or development platform. In this way, the development cost of the product will decrease and the use of the product will become simple [64]. There are various levels of the OATH standard. For the basic level, OATH is using the following credentials for authentication:

One-time password- (OTP-) based authentication
Public key infrastructure- (PKI-) based authentication (using X.509.v3 certificate)
Subscriber identity module- (SIM-) based authentication (using GSM/GPRS SIM)

However, OATH is very useful, but some disadvantages are also identified as phishing, centralized, anonymity issue, etc.

(4) OTP authentication: automatically generated, an alphanumeric, fixed-length string of characters used to authenticate the legitimacy of the user for a single transaction or a specific session is called a one-time password (OTP). OTP is more secure in comparison with the static or user-created password due to its randomness and single-time use. The OTPs may use as authentication login information, but generally, it is used as a second-factor authentication credential for the multifactor authentication mechanism [65, 66].

(5) Kerberos, X.509 certificates: the X.509 is a type of digital certificate that uses a widely accepted public key infrastructure (PKI) standard for the verification of the identity of the user/computer/service claimed at the remote location. The X.509 certificate was firstly issued as a part of the International Telecommunications Union's Telecommunication Standardization Sector (ITU-T) and X.500 Directory Services Standard in 1988. Later, it has been identified that it is not secure against attacks and also requires a huge hierarchy. The maintenance of Kerberos is also costly as it required maintaining various lists and status of the certificates such as Certificate Revocation List (OCR) and Online Certificate Status through Online Certificate Status Protocol (OCSP) [67].

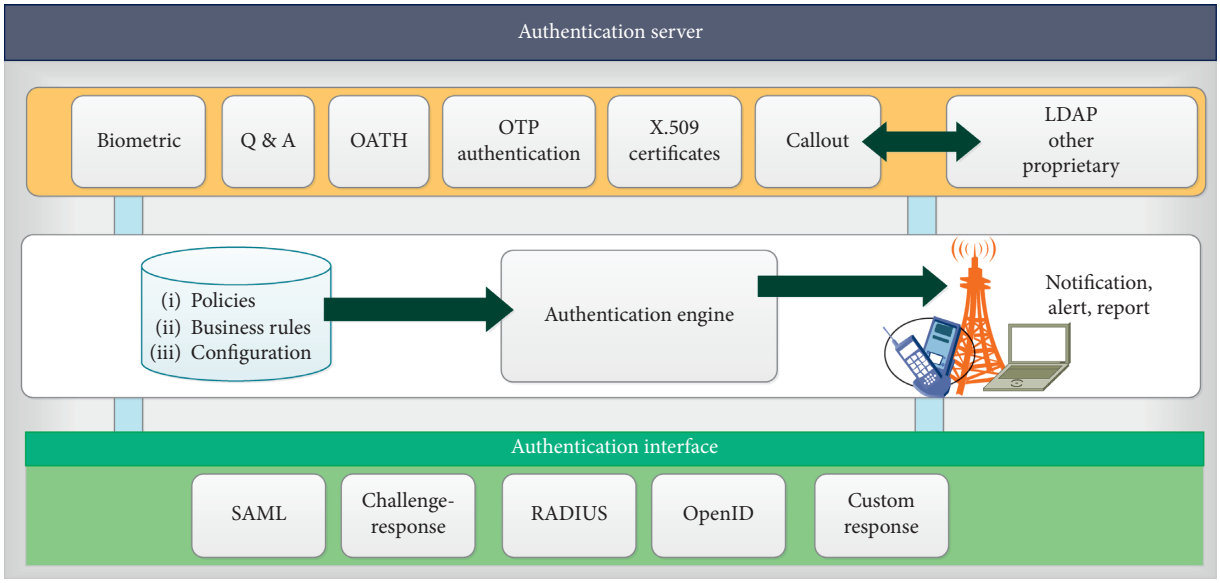


Figure 1: Block diagram for NeAF system.

(6) The Lightweight Directory Access Protocol (LDAP): the protocol was developed for directory services in which distributed lists of information are systematized into a tree of directory information, which are stored within an LDAP database. If the user wants to access the information from an LDAP database, then he/she has to prove his/her identity. In this way, it is quite consuming. The problem with LDAP and its type of solution is the integration of the active directory at the cloud [68]. Additionally, the support for Mac and Linux platforms can be extremely burdensome. Due to these problems, drawbacks, challenges, and cons, there is a serious need for innovation within the directory realm [69, 70].

4.3. Authentication Interface. An authentication interface is one of the most core interfaces to provide a platform for the user to connect with the security framework. NeAF has announced the following authentication interfaces.

4.3.1. Security Assertion Markup Language (SAML). Current software and services are working on the distributed environment in which there is a need to pass on the identification credentials from one node to another node. In this regard, SAML is very useful to open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). The major benefit of the SAML is that a set of credentials is sufficient to access various websites/services as one site pass on the credentials to another node.

4.3.2. Challenge-Response. Two friends are only the persons known the secrets of each other. The same concept is applied for challenge-response authentication. It is an interface for authentication where one entity provides a challenge (a secrete question, etc.) and at the other end, the second entity provides the corresponding response to complete the authentication process successfully. If a second entity fails to provide a valid response, then the authentication process fails with fail status and denies the second entity to access services, computer, network, or another network resource at the first entity [71].

4.3.3. Remote Authentication Dial-In User Service (RADIUS). This protocol is developed for the Network Access Servers (NAS) which requires authenticating its links and a shared authentication server along with authorization, and configuration. Therefore, this protocol is working as AAA protocol, i.e., authentication and authorization protocol for specific applications such as Network Access or IP Mobility. To authenticate the user, this protocol uses Password Authentication Protocol (PAP), Extensible Authentication Protocol (EAP), or Challenge Handshake Authentication Protocol (CHAP) and accesses text file, Database, and LDAP servers for authentication [1]. The authentication credentials are accessed from the above-said storage entities, and after completion of the authentication process, the credentials are returned back to the respective NAS [72].

4.3.4. OpenID. Nowadays, every user is required to access various services available on the Internet using a computer or using mobile. It is very tough to manage the authentication credentials for all the services as all the services are deployed on different platforms and the authentication of each service is different. Therefore, it is a requirement to sign in at one website and access any service without creating new passwords. This objective is achieved by the OpenID which allows the user to use an existing account to sign in to multiple websites. For OpenID authentication, the associate information with OpenID is passing to the other websites like name or email address. This information can be controlled and configured for the amount which can be shared

with other websites. The password or authentication credentials are taking care of by the primary website which is responsible to prove the legitimacy of the user and confirm the authentication of the user and the rest websites are not able to access these authentication credentials. Hence, a user does not need to worry about an unscrupulous or insecure website compromising your identity.

4.4. e-Pramaan. It is a framework standard for authentication of the users and also provides security for various government services on the Internet or mobile platform. It is based on the National e-Authentication framework. The e-Pramaan authentication framework is providing the exclusive unified login service for national and state-level e-governance applications. The services of e-Pramaan are implanted through SAML 2.0-based single sign-on (SSO) and provide multifactor authentication using various authentication parameters such as OTP, password, biometrics, and a digital certificate. e-Pramaan is also providing chaining of user's authentication through various government legitimate verification methods such as Aadhaar-based user identity verification and PAN-based identity verification. The details and analysis of the e-Pramaan have been provided in the next section [5].

The e-Pramaan has been proposed in 2012 and deployed in India in 2015. It is implemented on the web for the citizens. The citizen has to get registered for this service. After successful registration and authentication, the user can access the services through the given links.

4.4.1. Workflow of e-Pramaan. The workflow of e-Pramaan is shown in Figure 2. To access selected e-governance services, the Government of India provides a platform through a web portal, i.e., https://epramaan.gov.in. Before accessing any authorized e-governance service, the user needs to get registered on this site. This registration process requires the user's Aadhaar information. Figure 2 illustrates the e-Pramaan workflow which requires registration followed by the login process. After successful login, the e-Pramaan website redirects the users to the specific departmental server.

4.4.2. Information Flow of e-Pramaan. The information flow is illustrated in Figure 3. The process is started with two options, either the user is already registered or he/she is a new user to register. If the user is already registered, then he/she is redirected to the login page and provides authentication credentials. These credentials are used for the purposes of authentication at the central repository. If the user's legitimacy is proved through the mentioned process, then the system redirects the request to a user's specific page. User can then access the e-governance services for which he/she is authorized. Once, the work is completed he/she can log out from the system.

However, in the case of registration, the user has three options as follows:

(i) Registration using base number/voter ID

(ii) Registration using driving license

(iii) Registration without identity verification

The registration process is successful once the information provided by the user is verified. After registration, the user can log in and access the desired services.

4.4.3. Sequence Flow of e-Pramaan. To understand the sequence of intercommunication of various processes/servers of the e-Pramaan, a sequence diagram is illustrated in Figure 3. The e-Pramaan layer is intermediate between user and department's services, i.e., e-governance services. To access the information, a user requests for authentication to the e-Pramaan layer. Based on the user's credentials, the authentication process verifies the user's legitimacy through the stored information. If the user proves its legitimacy, then the e-Pramaan website redirects the request to the requested server.

The flow of information of the e-Pramaan is illustrated in Figure 4. This flow diagram explained the flow of information for "already registered user" and also for "new user".

4.4.4. Analysis of NeAF and e-Pramaan. To make the system better, it is necessary to analyze the existing authentic system of India. The observations are as follows:

(i) There is a centralized data store for authentication credentials.

(ii) The whole authentication process depends on the single and centralized authentication credentials.

(iii) The e-governance services are individually accessed through their authentication system.

(iv) The registration process for each e-governance service is existing along with e-Pramaan registration. User is to get registered for each e-governance service individually.

(v) The multiple registrations for the services of a single organization (i.e., the registration process for various e-governance services) are a redundant process. These repetitions of the same process make citizens uncomfortable. The same results were highlighted by us in other works where government officials are also agreed on it [4, 5, 53, 73].

(vi) Through e-Pramaan, all the suitable e-governance services are made available at a single window. But it is not the integration of all the services as claimed. It infers that there are two ways to access the system, either to access a particular e-governance service directly from the department's server or through the e-Pramaan. It means there are two authentication processes for the same service, and therefore, redundant data have to be stored for authentication of a citizen for a service.

The unified and integrated authentication system means all the e-governance services are accessible only through a single authentication system. Whether users may access through the portal of service or from the platform

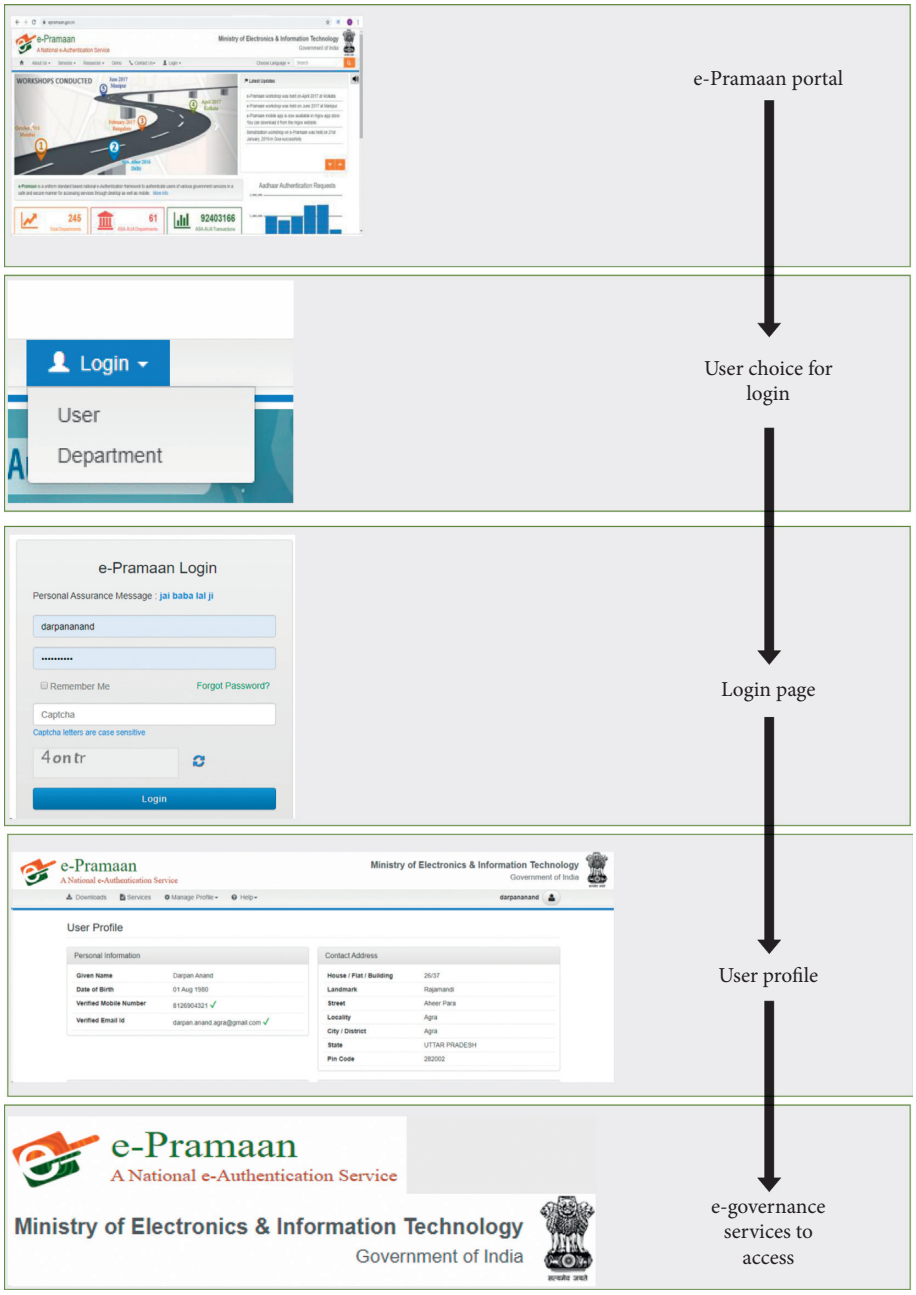


Figure 2: e-Pramaan live working flow.

government provides to access their services (as in the case of e-Pramaan). To make the system more secure and safe, the authentication should not be dependent on the central authentication store; therefore, the process should be distributed and not storing data on the central data store [35]. To solve these issues, Anand and Khemchandani propose a UIAP which is explained in the next section.

5. Unified Integrated Authentication Protocol (UIAP)

This section explains the proposed Unified and Integrated Authentication Protocol (UIAP), which is developed not only for authentication on multiserver architecture but also provides the facility of secrecy for communication among various involved servers and layers. Because of this, the protocol can integrate the existing isolated system in a unified manner. In UIAP, once a user gets registered for any service, he/she can be authenticated to access a particular service provided by a server other than the server on which registration has been done. If the user wants to access the services from service-providing server (other than service providing server, where a user got registered), the session key will be shared between all the involved servers including service providing server where users got registered. In this way, the data required for registration are stored at the service providing server and central authentication server in a distributed manner during the registration process. This

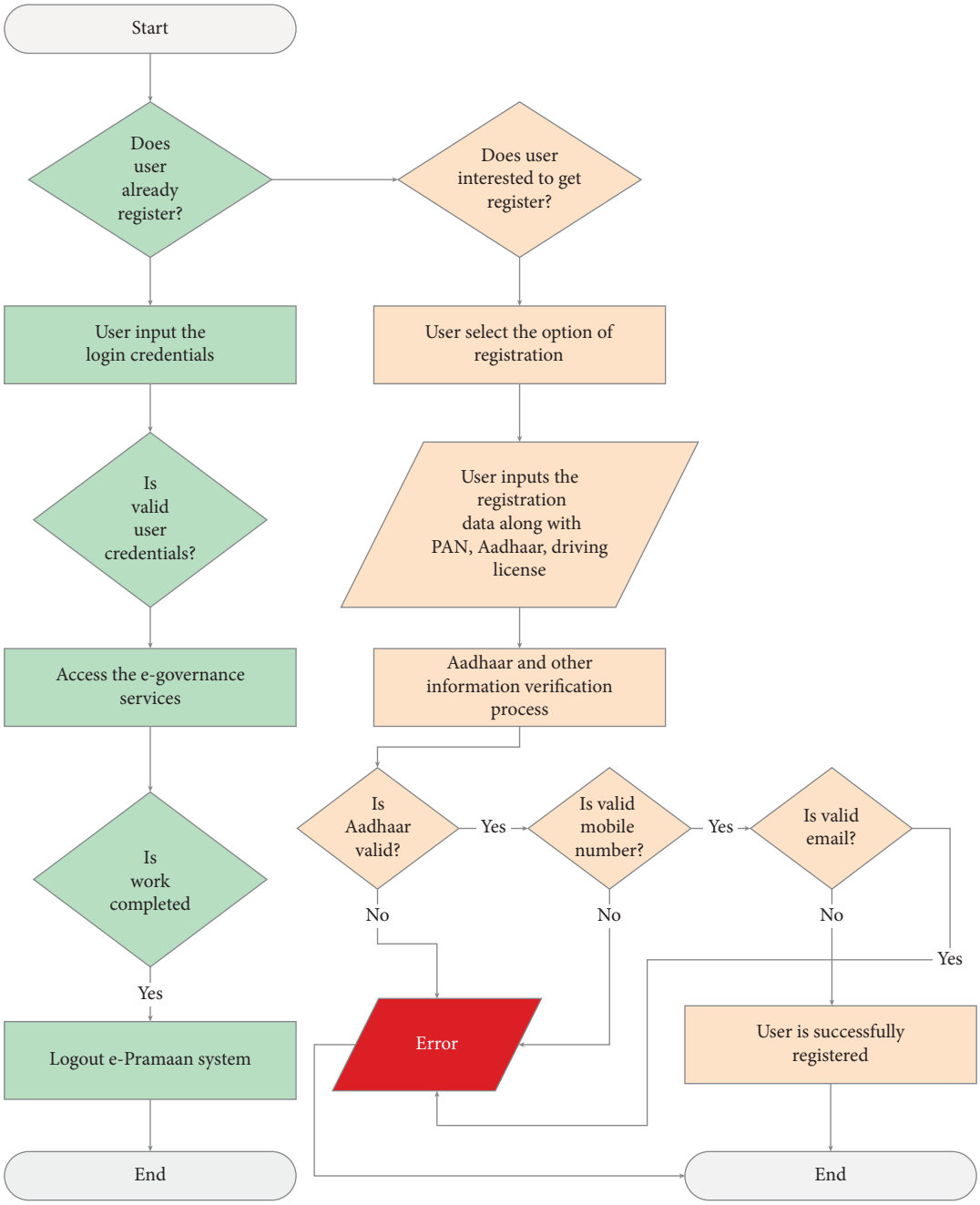


Figure 3: Process flow for e-Pramaan.

proposed protocol contains three kinds of layers for the authentication process as a Common Service Center (CSC), the Department Service Providing Server (DS)/Department Service Used for Registration Server (DSO), and the Central Authentication Server (CAS).

U_i is ith user from a set of users U, $h(.)$ is expressing a hash function, E is expressing the ciphering/encryption algorithm, k is denoting the concatenation (bitwise), $\oplus$ is expressing XOR operation for bit values, UID_i is users U_i identity, $r1$, $r2$, and $r3$ are denoting the random numbers at CSC, DSO, and CAS, respectively, key1 is symmetric key for encryption between CSC and DSO, key2 is symmetric key for encryption between DSO and CAS, $\mathrm{ID}_{\mathrm{DSO}}$ is used to express the ID of DSO, $\mathrm{ID}_{\mathrm{DS}}$ is used to express the ID of DS, TS_1, TS_2, and TS_3 and N_1, N_2, and N_3 are denoting the timestamps and nuances generated at CSC, DS, and CAS, respectively, PIN is used to encrypt the data read from smart card for further processing, $\Delta\mathrm{TS}_{\mathrm{DSTV}}$, $\Delta\mathrm{TS}_{\mathrm{CASTV}}$, and $\Delta\mathrm{TS}_{\mathrm{DSOTV}}$ are acceptable time duration between the timestamp values generated at DS with TS_1, CAS with TS_1, and DSO with TS_1, respectively, and SessKey is the final session key deduced at each layer which is used for communication after authentication.

The detailed working of the UIAP is illustrated in Figure 5. The responsibilities of each layer are as follows. This section explains the proposed Unified and Integrated

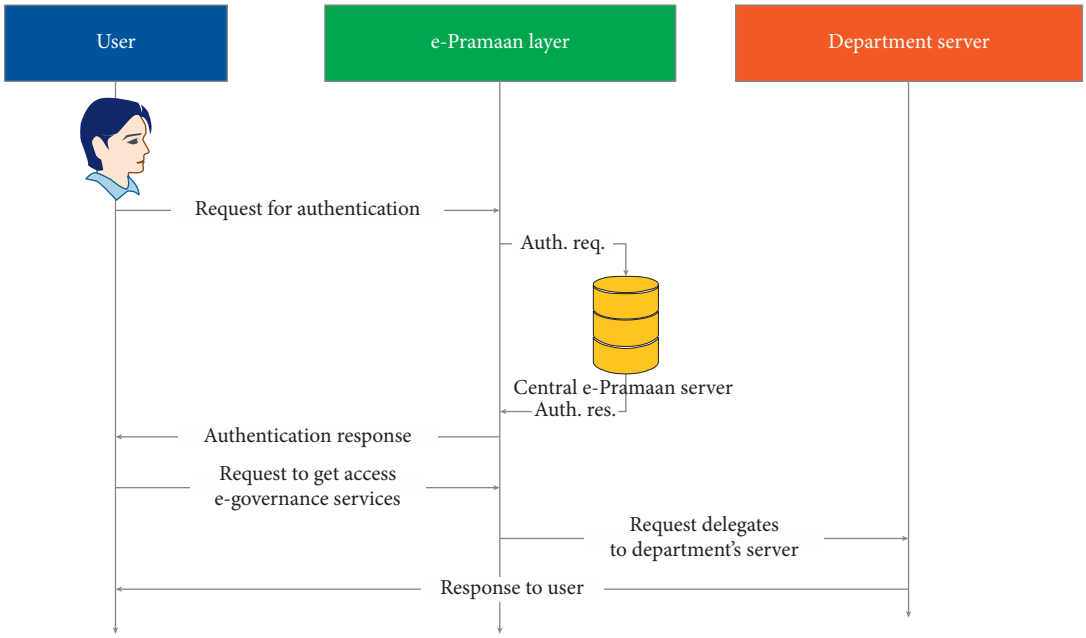


Figure 4: Sequence diagram of e-Pramaan.

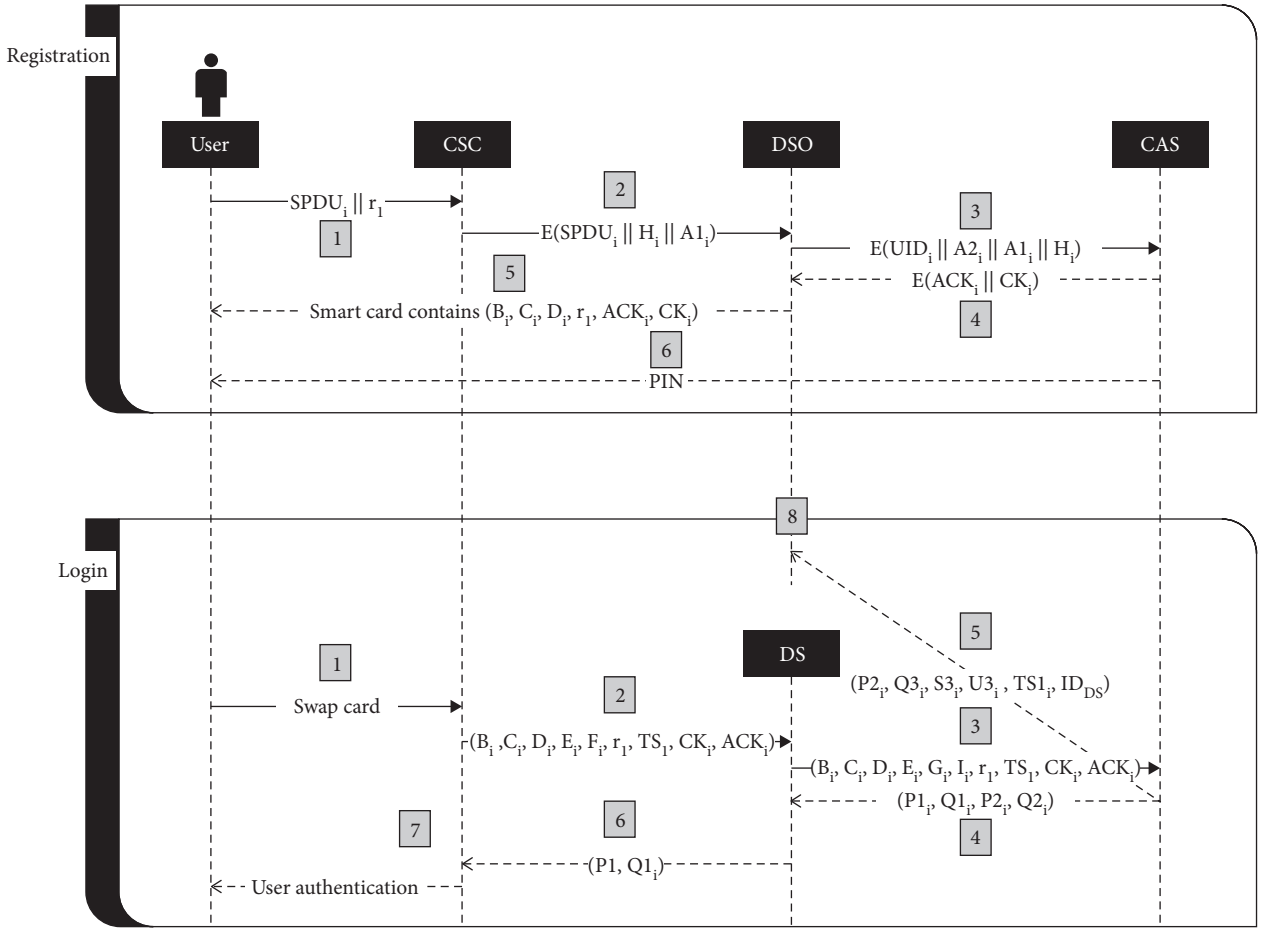


Figure 5: Communication phases of UIAP.

Authentication Protocol (UIAP), which is developed not only for authentication on multiserver architecture but also provides the facility of secrecy for communication among various involved servers and layers. Because of this, the protocol can integrate the existing isolated system in a unified manner. In UIAP, once a user gets registered for any service, he/she can be authenticated to access a particular service provided by a server other than the server on which registration has been done. If the user wants to access the services from service providing server (other than service providing server, where a user got registered), the session key will be shared between all the involved servers including service providing server where users got registered. In this way, the data required for registration are stored at the service providing server and central authentication server in a distributed manner during the registration process. This proposed protocol contains three kinds of layers for the authentication process as a Common Service Center (CSC), the Department Service Providing Server (DS)/Department Service Used for Registration Server (DSO), and the Central Authentication Server (CAS). The detailed working of the UIAP is illustrated in Figure 5. The responsibilities of each layer are as follows:

(1) Common Service Center (CSC): the user interacts with the whole system through this layer. Generally, organizations installed various ICT kiosks, i.e., CSC to access the services. These kiosks will be enabled with all the required resources such as computer systems, Internet, scanner, power backup, and installed nearby the residences of remote users. These centers are useful for remote residents and also for busy persons who are unable to reach the office physically for any service. The registration can be done only from a legitimate CSC or from any legitimate office of the organization. The request for login goes from the CSC layer. CSC layer validates the registration, standardizes and formats the information, and then forwards to the next layer for further processing.

(2) Department Service Providing Server (DS): there are various departments to handle a specific type of service. These services (such as road transportation office, passport office, banks, and income tax office in case of e-governance) are only accessible by the legitimate and registered users. This layer is the set of servers, which are collectivity called as Department Service Providing Layer or DS. This layer is responsible to provide the services after validating the legitimacy of the users through CSC.

(3) Department Service Used for Registration Server (DSO): this type of servers is the members of the set of DS layer, but the primary responsibility of it is to register user and store the registration data. The stored data will be used for authentication to prove the legitimacy of the user by passing messages among CSC, DS, and CAS. This layer is also responsible to serve the users by providing services as by the DS layer.

(4) Central Authentication Server (CAS): this layer has a responsibility to authenticate the users. At the time of login, this layer will identify the user's DSO server where detailed information is stored at the time of registration. Therefore, there is no need to store the whole data on a central server or central cloud.

There are three processes to implement UIAP for authentication:

(i) Initialization and registration phase: this phase is responsible to register the citizens who approach to access any e-governance service. In this phase, various parameters are shared between the various communication entities and some of them are stored on these layers for the further authentication process in a distributed manner.

(ii) Login phase: this main process is used to prove the legitimacy of the genuine user. If the user is unable to prove its legitimacy, then the user cannot allow accessing the system.

(iii) Authentication and key agreement phase: after successful login, through the same parameters which are shared in the login phase, a session key is deduced and used for secure communication.

6. Lightweight Technical Implementation of UIAP

There are several existing projects which are running on various servers to provide various services to citizens. For these services and servers, citizens have registered for individual services at a specific server. To implement the UIAP, the following components of the system are required:

(i) UIAP implementation architecture: this is a framework that comprised of the relationships and interactions between application components, such as middleware systems, user interfaces, and databases.

(ii) Data structure: How do we represent, organize, manage, and store the information that enables efficient access and modification for UIAP communication.

(iii) Communication services: there are various standardized ways or media to propagate communication between the various layers engaged in UIAP.

(iv) Integration with other e-governance services: the most challenging task to integrate the existing services with UIAP.

6.1. UIAP Implementation Architecture. The average Internet user gets to see a specific page on his/her system, through a series of interactions between various components of

applications, user interfaces, middleware systems, databases, servers, and the browser. The framework which ties up this relation and interaction together is the project implementation architecture. The project implementation architecture for UIAP is illustrated in Figure 6.

The user can access the e-governance services through three mediums as follows:

Government kiosks (Common Service Center): under the NeGP, the government began a venture CSC to encourage the citizens for e-governance by a stand adjacent to his/her home in farther regions of anywhere in the region of the country [74]. The CSC guidelines conceive a wide variety of substances and services that could be offered as training and education, health, insurance, banking (rural and urban), entertainment, agriculture, business, skill development, etc.

Web applications (HTTP-based application for laptop, desktop, or smartphone): the Government of India initiated the facility to access the various e-government services through web portals. As technology grows, the services are also provided for smartphones through Android or iOS apps. These services are responsive and based on web application architecture [75, 76]. This is also very useful as a major population is using smartphones and the Internet. Therefore, it is very much mandatory to facilitate citizens with an open platform to access e-governance services.

Through existing infrastructure like bank ATMs: there is a big challenge to deploy CSC to provide the reach to the citizens to access the e-governance services. To make it available to the citizens, apart from CSC and web application platforms, the bank ATMs can be another option. There are about 2.2 million ATMs including 15,626 WLAs working in India to serve the citizens and it is expected to 4 million in the next couple of years. The primary objective of these machines is related to money, basic bank operations, etc. Some of the ATMs are also working for income tax filing and other government-related tasks. The working of these ATMs can be extended to serve various existing e-governance services. This idea, to provide e-governance to all the citizens through exiting the ATM network, is useful to enhance the reach [77, 78].

6.2. UIAP Data Format. To exchange data among different servers involved during the authentication process, the lightweight data-interchange format JavaScript Object Notation (JSON) can be used to reduce communication overhead. It can be considered as of the best solutions to represent the data because the JSON objects are an open-standard file format that uses human-readable text to transmit data objects consisting of attribute-value pairs and array data types or any other sterilizable value. It is a very common data format, with a diverse range of applications. So, it is useful to integrate the existing e-governance services, whether they are working on any platform and technology [79, 80].

6.3. UIAP Deployment. Scalability is important for keys (used for authentication and establishment of keys) and services. To scale the authentication service for a billion people, there are two general technical options:

(i) Multiple servers with proper integration and synchronization

(ii) Cloud-based e-governance services can be implemented

The first option is not considered efficient as it is required to develop and deploy multiple services for an effective and efficient outcome like load balancing, security, backup services, and integration synchronization. The second option is suitable to deploy the proposed authentication service for e-governance services. The Government of India deployed its cloud platform for various e-governance services, i.e., MeghRaj (https://cloud.gov.in/). This cloud service is open for all e-governance services. The security concern can be addressed by efficiently implementing the following services:

(i) PaaS (Platform as a Service)

(ii) IaaS (Infrastructure as a Service)

(iii) SaaS (Software as a Service)

(iv) Storage (Storage as a Service)

(v) Load Balancer (Load Balancer as a Service)

(vi) Antivirus (Antivirus Service)

(vii) IP (Public IP Service)

(viii) RM (Resource Monitoring as a Service)

(ix) VA (Vulnerability Assessment Service)

(x) WAF (Web Application Firewall (WAF) Service)

(xi) Backup (Backup Service)

(xii) APM (Application Performance Management)

(xiii) DA (Data Analytics (DA) as a Service)

Many of these services are already deployed on the MeghRaj platform. The NIC National Cloud (MeghRaj) is presently hosting several critical applications on over 16,000 virtual servers supporting 480+ e-governance projects and 900+ user departments under Digital India. Therefore, MeghRaj is the prominent, efficient, secure, and effective option to deploy the proposed authentication service UIAP.

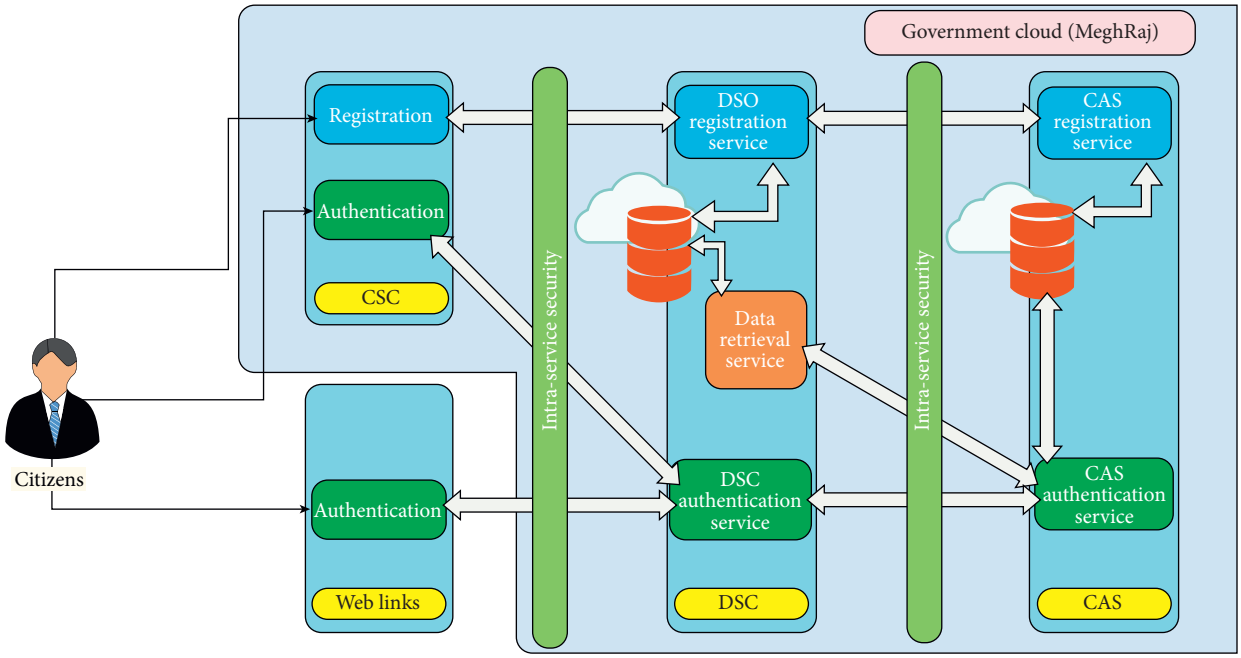


Figure 6: Proposed implementation architecture for UIAP.

7. Conclusion

The authentication process is very crucial and important for the highly scalable system providing multiple services through different servers. The same will apply to the e-governance system. The Government of India is also taken it seriously e-governance services, and therefore, NeAF and e-Pramaan projects are proposed. e-Pramaan just redirects the user to a specific departmental server to access the corresponding server after authentication. In this setup, the user has to authenticate himself/herself separately to access a specific service. Therefore, to access any service (which is not read-only), he/she has to execute two authentication processes with separate credentials. To provide a single authentication service to access all services, we propose the lightweight technical implementation of single sign-on authentication and key agreement mechanism based on UIAP. This paper also explains the implementation of the authentication mechanism using lightweight SOAP services deployed over a cloud-based platform. Further, the work will be extended to make the technique able for authorization of the e-governance services.

Data Availability

The data used to support the findings of the manuscript are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Dr. Omar Cheikhrouhou thanks Taif University for its support under the project Taif University Researchers supporting project number TURSP-2020/55, Taif University, Taif, Saudi Arabia.

References

[1] O. Cheikhrouhou, M. Laurent, A. B. Abdallah, and M. B. Jemaa, "An EAP-EHash authentication method adapted to resource constrained terminals," *Annals of Telecommunications - Annales des Télécommunications*, vol. 65, no. 5-6, pp. 271–284, 2010.

[2] M. Sabharwal, "The assessment of concerns, opinions and perceptions of Customers to find the significant metrics for deployment of Biometrics in E-banking," *International Journal of Computer Applications (IJCA)*, vol. 138, no. 14, pp. 28–41, 2016.

[3] M. Sabharwal, "Multi-modal biometric authentication and secure transaction operation framework for E-banking," *International Journal of Business Data Communications and Networking*, vol. 13, no. 1, pp. 102–116, 2017.

[4] D. Anand and V. Khemchandani, "An analytical method to audit indian e-governance system," *International Journal of Electronic Government Research*, vol. 13, no. 3, pp. 18–37, 2017.

[5] D. Anand and V. Khemchandani, "Study of e-governance in India: a survey," *International Journal of Electronic Security and Digital Forensics*, vol. 11, no. 2, pp. 119–144, 2019.

[6] S. Lauriks, A. Reinersmann, H. G. Van der Roest et al., "of ict-based services for identified unmet needs in people with dementia," *Ageing Research Reviews*, vol. 6, no. 3, pp. 223–246.

[7] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.

[8] B. Gupta, M. Tiwari, and S. Singh Lamba, "Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.

[9] R. Heeks, "Understanding e-governance for development," *I-Government Working Paper Series*, vol. 11, 2001.
[10] N. Yadav and V. Singh, "E-governance: past, present and future in India," 2013, https://arxiv.org/abs/1308.3323.
[11] L. Kant and S. K. Krishnan, "Information and communication technology in disease surveillance, India: a case study," *BMC Public Health*, vol. 10, no. 1, p. S11, 2010.
[12] S. Bhatnagar, "Information technology and development: foundation and key issues," 2000.
[13] R. Chauhan, *National E-Governance Plan in india*, United Nations University–International Institute for Software Technology, Macau, China, 2009.
[14] D. G. Chandra and R. S. Bhadoria, "Cloud computing model for national e-governance plan (negp)," in *Proceedings of the International Conference on Computational Intelligence and Communication Networks*, pp. 520–524, Mathura, Uttar Pradesh, India, November 2012.
[15] D. Mathur, P. Gupta, and A. Sridevi, "e-governance approach in India the national e-governance plan (negp)," *Transforming Government*, vol. 3, 2009.
[16] H. Goswami, "Opportunities and challenges of digital India programme," *International Education and Research Journal*, vol. 2, no. 11, pp. 78-79, 2016.
[17] A. Dubey, Z. Saquib, and S. Dwivedi, "Electronic authentication for egovernment services-a survey," in *Proceedings of the 10th IET System Safety and Cyber-Security Conference*, IET, Bristol, UK, October 2015.
[18] T. Hwang, Y. Chen, and C. J. Laih, "Non-interactive password authentications without password tables," in *Proceedings of theIEEE TENCON'90: 1990 IEEE Region 10 Conference on Computer and Communication Systems*, pp. 429–431, Hong Kong, China, June 1990.
[19] C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-I. Fan, "A secure dynamic identity based authentication protocol with smart cards for multi-server architecture," *Journal of Information Science and Engineering*, vol. 31, no. 6, pp. 1975–1992, 2015.
[20] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, "A novel smart card and dynamic id based remote user authentication] scheme for multiserver environments," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 85–5, 2013.
[21] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.
[22] Y.-P. Liao and S.-S. Wang, "A secure dynamic id based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.
[23] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609–618, 2011.
[24] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.
[25] C.-C. Nugent, T.-H. Lin, and R.-X. Chang, "A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13863–13870, 2011.
[26] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key greement using smart cards," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 2, pp. 793–800, 2009.
[27] W. Hu, K. Xue, P. Hong, and C. Wu, "Atcs: a novel anonymous and traceable communication scheme for vehicular ad hoc networks," *IJ Network Security*, vol. 13, no. 2, pp. 71–78, 2011.
[28] S. Gaharana and D. Anand, "Dynamic id based remote user authentication in multi server environment using smart cards: a review," in *Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks*, pp. 1081–1084, Jabalpur, India, December 2015.
[29] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390–1397, 2010.
[30] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383–393, 2015.
[31] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: a comparative evaluation of two-factor Authentication schemes," in *Proceedings of the 11th ACM on Asia Conference on Computerand Communications Security*, New York, NY, USA, September 2016.
[32] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2014.
[33] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity," *Information Sciences*, vol. 321, pp. 162–178, 2015.
[34] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Networks*, vol. 20, pp. 1–15, 2014.
[35] D. Anand and V. Khemchandani, "Unified and integrated authentication and key agreement scheme for e-governance system without verification table," *Sadhana*, vol. 44, no. 9, p. 192, 2019b.
[36] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.
[37] A. Roy and S. Karforma, "Authentication of user in e-governance: a digital certificate based approach," *International Journal of Scientific Research and Management (IJSRM)*, vol. 2, no. 8, pp. 1212–1221, 2014.
[38] E.-J. Yoon and K.-Y. Yoo, "Drawbacks of liao et al's password authentication scheme," in *Proceedings of the International Conference on Next Generation Web Services Practices*, pp. 101–108, Seoul, South Korea, June 2006.
[39] W.-C. Ku and S.-M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204–207, 2004.
[40] E.-J. Yoon, E.-K. Ryu, and K.-Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 612–614, 2004.
[41] X.-M. Wang, W.-F. Zhang, J.-S. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 29, no. 5, pp. 507–512, 2007.
[42] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "CyberSecurity attack prediction: a deep learning

approach," in *Proceedings of the 13th International Conference on Security of Information and Networks*, pp. 1–6, Merkez, Turkey, November 2020.

[43] I. Jemal, O. Cheikhrouhou, H. Hamam, and A. Mahfoudhi, "Sql injection attack detection and prevention techniques using machine learning," *International Journal of Applied Engineering Research*, vol. 15, pp. 569–580, 2020a.

[44] I. Jemal, M. A. Haddar, O. Cheikhrouhou, and A. Mahfoudhi, "ASCII embedding: an efficient deep learning method for web attacks detection," *Pattern Recognition and Artificial Intelligence*, vol. 1322, pp. 286–297, 2021.

[45] H.-R. Chung, W.-C. Ku, and M.-J. Tsaur, "Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 863–868, 2009.

[46] S.-W. Lee, H.-S. Kim, and K.-Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 27, no. 2, pp. 181–183, 2005.

[47] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[48] N.-Y. Lee and Y.-C. Chiu, "Improved remote authentication scheme with smart card," *Computer Standards & Interfaces*, vol. 27, no. 2, pp. 177–180, 2005.

[49] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, vol. 32, no. 5-6, pp. 321–325, 2010.

[50] T.-H. Chen, H.-C. Hsiang, and W.-K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," *Future Generation Computer Systems*, vol. 27, no. 4, pp. 377–380, 2011.

[51] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of wang et al. sauthentication scheme using smart cards," in *Proceedings of the 2010 National Cnference on Communications (NCC)*, Mumbai, India, May 2010.

[52] X. Li, J. Niu, M. Khurram Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[53] D. Anand and V. Khemchandani, "The challenges for authentication in indian e-governance system (a survey on indian administrative staff)," *International Journal of Control Theory and Applications*, vol. 40, no. 9, pp. 335–346, 2016.

[54] A. Jøsang, K. A. Varmedal, C. Rosenberger, and R. Kumar, "Service provider authentication assurance," in *Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust*, pp. 203–210, Paris, France, July 2012.

[55] M. Kumar and K. S. Vaisla, "Comparative study of e- Authentication framework for e-governance," in *Proceedings of the International Conference on Advances in Computing and Communication*, pp. 140–147, Mumbai, India, January 2014.

[56] V. Jain, R. Kumar, and Z. Saquib, "An approach towards digital signaturesfor e-governance in India," in *Proceedings of the 2015 2nd international Conference on Electronic Governance and Open Society: Challenges in Eurasia*, pp. 82–88, St. Petersburg, Russia, July 2015.

[57] T. Wiens, "Engine speed reduction for hydraulic machinery using predictive algorithms," *International Journal of Hydromechatronics*, vol. 2, no. 1, pp. 16–31, 2019.

[58] A. K. Jain and K. Nandakumar, "Biometric authentication: system security and user privacy," *Computer*, vol. 45, no. 11, pp. 87–92, 2012.

[59] R. K. Rowe, U. Uludag, M. Demirkus, S. Parthasaradhi, and A. K. Jain, "A multispectral whole-hand biometric authentication system," in *Proceedings of the 2007 Biometrics Symposium*, Baltimore, Maryland, September 2007.

[60] B. Bazelli, A. Hindle, and E. Stroulia, "On the personality traits of stackoverflow users," in *Proceedings of the 2013 IEEE.International Conference on Software Maintenance*, pp. 460–463, Eindhoven, Netherlands, September 2013.

[61] M. Yousuf and K. Khan, "A novel cost effective authentication framework for wireless lans in small medium enterprises (smes)," in *Proceedings of the 2011 IEEE 3rd International Conference on Communication Sofware and Networks*, pp. 158–162, Xi'an, China, August 2011.

[62] S. Osterland and J. Weber, "Analytical analysis of single-stage pressure relief valves," *International Journal of Hydromechatronics*, vol. 2, no. 1, pp. 32–53, 2019.

[63] W. Jerbi, A. Guermazi, O. Cheikhrouhou, and H. Trabelsi, "CoopECC: a collaborative cryptographic mechanism for the internet of things," *Journal of Sensors*, vol. 2021, Article ID 8878513, 8 pages, 2021.

[64] R. Wang, H. Yu, G. Wang, G. Zhang, and W. Wang, "Study on the dynamic and static characteristics of gas static thrust bearing with micro-hole restrictors," *International Journal of Hydromechatronics*, vol. 2, no. 3, pp. 189–202, 2019.

[65] Z. Sui, Y. Fang, M. Li, and L.-c. Liu, "Design improvement and implementation of authentication technology based on," *Information and Electronic Engineering*, vol. 4, 2005.

[66] Y. Xijun, W. Gouxin, X. Yong, and S. Kun, "Realization and improvement of otp authentication," *Computer Engineering*, vol. 9, 2000.

[67] M. A. Sirbu and J.-I. Chuang, "Distributed authentication in kerberos using public key cryptography," in *Proceedings of SNDSS'97: Internet Society 1997 Symposium on Network and Distributed System Security*, pp. 134–141, San Diego, CA, USA, March 1997.

[68] R. Chaari, O. Cheikhrouhou, A. Koubâa, H. Youssef, and H. Hmam, "Towards a distributed computation offloading architecture for cloud robotics," in *Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 434–441, IEEE, Tangier, Morocco, June 2019.

[69] T. Howes and M. Smith, "LDAP," in *Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*, M. S. Tim Howes, Ed., Macmillan Technical Publishing, New York, NY, USA, 1997.

[70] W. Yeong, T. Howes, and S. Kille, "Lightweight directory access protocol," *Network Working Group - Request for Comments*, vol. 1, p. 1777, 1995.

[71] M. Boujelben, O. Cheikhrouhou, M. Abid, and H. Youssef, "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks," in *Proceedings of the 2009 Third International Conference on Sensor Technologies and Applications*, pp. 442–448, IEEE, Bejing, China, June 2009.

[72] O. Cheikhrouhou, A. Koubaa, M. Boujelben, and M. Abid, "A lightweight user authentication scheme for wireless sensor networks," in *Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010*, pp. 1–7, IEEE, Hammamet, Tunisia, May 2010a.

[73] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.

[74] K. Datta and A. Saxena, "Developing entrepreneurship and e-government in India: role of common service centers," *Journal of E-Governance*, vol. 36, no. 2, pp. 92–100, 2013.

[75] O. B. Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam, and A. Derhab, "An OWASP top ten driven survey on web application protection methods," in *Risks and Security of Internet and Systems*, J. Garcia-Alfaro, J. Leneutre, N. Cuppens, and R. Yaich, Eds., Springer International Publishing, Cham, Switzerland, pp. 235–252, 2021.

[76] I. Jemal, M. A. Haddar, O. Cheikhrouhou, and A. Mahfoudhi, "M-CNN: a new hybrid deep learning model for web security," in *Proceedings of the 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–7, IEEE, Antalya, Turkey, November 2020b.

[77] O. Cheikhrouhou, A. Koubâa, G. Dini, and M. Abid, "RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 15, no. 8, pp. 783–797, 2011.

[78] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "PetroBlock: a blockchain-based payment mechanism for fueling smart vehicles," *Applied Sciences*, vol. 11, no. 7, p. 3055, 2021.

[79] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "UTM-chain: blockchain-based secure unmanned traffic management for internet of drones," *Sensors*, vol. 21, no. 9, p. 3049, 2021.

[80] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "BMC-SDN: blockchain-based multi-controller architecture for secure software-defined networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9984666, 12 pages, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9971705, 7 pages
https://doi.org/10.1155/2021/9971705

Research Article

Software-Defined Networking: An Evolving Network Architecture—Programmability and Security Perspective

Nitheesh Murugan Kaliyamurthy,[1] Swapnesh Taterh,[1] Suresh Shanmugasundaram,[2] Ankit Saxena,[3] Omar Cheikhrouhou,[4] and Hadda Ben Elhadj[5,6]

[1]*Amity Institute of Information Technology, Amity University, Jaipur, India*
[2]*Faculty of Engineering and Applied Sciences, Botho University, Gaborone, Botswana*
[3]*Department of CSE, Invertis University, Bareilly, India*
[4]*College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[5]*Higher Institute of Computer Science of Mahdia, Hiboun, Tunisia*
[6]*Laboratory of Signals, Systems, Artificial Intelligence and Networks, Sfax, Tunisia*

Correspondence should be addressed to Hadda Ben Elhadj; hadda.ibnelhadj@esti.rnu.tn

Received 24 March 2021; Revised 14 April 2021; Accepted 4 May 2021; Published 12 May 2021

Academic Editor: Manjit Kaur

Software-defined networking is an evolving network architecture beheading the traditional network architecture focusing its disadvantages in a limited perspective. A couple of decades before, programming and networking were viewed as different domains which today with the lights of SDN bridging themselves together. This is to overcome the existing challenges faced by the networking domain and an attempt to propose cost-efficient effective and feasible solutions. Changes to the existing network architecture are inevitable considering the volume of connected devices and the data being held together. SDN introduces a decoupled architecture and brings customization within the network making it easy to configure, manage, and troubleshoot. This paper focuses on the evolving network architecture, the software-defined networking. Unlike a generic view on the evolving network, which makes work as a review, this work addresses various perspectives of the architecture leaving it an intermediate work in between the review of the literature and implementation, contributing towards factors like the design, programmability, security, security behaviors, and security lapses. This paper also analyses various weak points of the architecture and evolves the attack vectors in each plane leaving a conclusion to further progress towards identifying the impacts of the attacks and proposing mitigation strategies.

1. Introduction

With the increased requirements, the connected devices over a period of time suffocates in executing its operations as intended. Being many reasons stated for this condition, listing a few proven causes as such the volume of data, the exponential increase in connected devices, and the need for high-speed processing of data. In addition to all these operational factors, security is being one of the highlighted reasons throughout this scenario as it voids any mitigation proposals in the recent past [1].

This paper addresses the existing architecture of the connected devices and the recent developments held over the past decade to mitigate the suffocation. Focusing on the recent developments, there are various exciting proposals, in which this paper addresses one of the proposals which is software-defined networking (SDN). In the domain of networks, the SDN approach is considered as another trending endeavor to address the existing challenges faced in the traditional connected devices [2].

As it is one of the evolving architectures, various flaws were identified in the due course and were made open to the research forums to come up with mitigation methods. These flaws again focus on various operations within the network models. To be more precise in achieving both quantitative and qualitative progress in the work, this work funnels down

after its discussion on traditional network architecture and SDN architecture into the security aspects. As there is already adequate proven research on the security aspects of traditional network architecture, this paper limits itself to focusing on the security aspects of SDN architecture. Further funneling down, within the security aspects of SDN architecture, this work concentrates on identifying and addressing the security problems on the grounds of the application layer in the architecture [3].

Thus, this work concludes by bringing in a spotlight on one of the key security issues in the trending SDN architecture over the past decade leaving scope for further research on mitigating the issue. This key security issue is unique to the SDN architecture as it is a possibility because of the architecture's decoupled approach in dealing with the systems and its feasibility to support programmability features. The flow of this paper is structured as stated in Figure 1. It starts from introducing the evolving network architecture and its efficiency towards network programmability followed by its various security issues and factors within the SDN architecture and diving towards the vital part of this work and analyzing the security issues, its types, and impact. This paper in its final part concludes by leaving progressive pathway for other researchers to move forward and propose various solutions to mitigate the addressed security issue effectively.

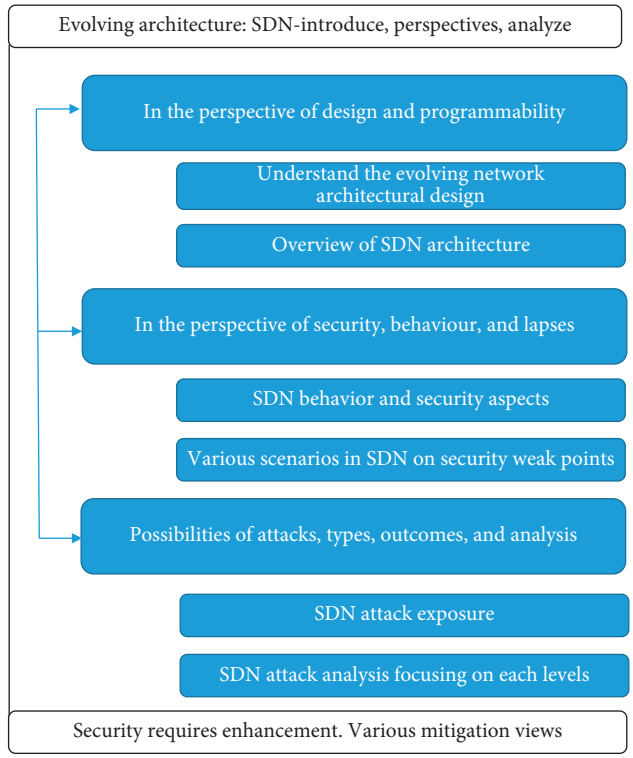


Figure 1: Diagrammatic representation of the work.

2. Evolving Architecture: In the Perspective of Design and Programmability

There are two deviant points that have to be made clearer while discussing and understanding the evolving network architecture. This section will walk through and help to gain crystal clear insights on the two aspects of evolving network architectural design. While thinking out of the box from the existing traditional network architectural (Banjar et al. [4]) design, the main focus could be to overcome the problems which are currently experienced such as exponential growth of the connected devices, the volume of data it generates, and the capacity of the devices to manage the overwhelming data which successively could be categorized within quality of service, load balancing, resource management, and Ssecurity. There are various international standards, proprietary protocols, and algorithms implemented in the existing network architecture to overcome the above-stated issues [5]. They, at one point, execute or function as anticipated overcoming the problems. However, in another dimension or perspective, they further make the network architecture more complex.

The networking domain, a couple of decades ago, was in a similar situation but for a different problem. The depletion of IPv4 addresses leads to the design of IPv6 protocol. Even though the problem was well mitigated by proposing the most secured and scalable IPv6 addressing scheme, it stills raises challenges in completely adopting IPv6 and aborting IPv4 [6]. It took over the next decade after the solution being proposed on a problem to effectively implement in the real-time operations not completely but at least to a wide level. This experience is kept in consideration while new scopes were defined to the current problems or issues being faced in the network architecture.

To overcome the complexity of the existing network architecture, a new approach is proposed, which is the network programmability. This is a feature that allows or supports programmability within a network helping to overcome resource management issues, security, and so on by programming and virtualizing [7] the network. So far before this concept, programmability and virtualization are supported within the network architecture at a limited scale. If they are already available, the difference is it was already available but not customizable. This statement helps to clarify a common myth that programming and virtualization are new concepts. Network programmability comes with a combination of various entities like the architectures, the protocols, support towards multiple programming languages and scripts, web coding tools, and the application programming interfaces. These entities help in a different order at different levels within the network to establish communication within the network devices in a comparatively simple way to the existing traditional network architecture [8].

The protocols like OpenFlow are used in network programming where it places itself as an intermediate between the programs and the forwarding devices to establish communication. Similar to the protocols, network programming also supports multiple programming languages and scripts like C, C++, Java, and Python. Along with these supportable resources, the network programming is also enriched with the web interface called REST application programming interface and with a collection of library

resources, the JAVA API (ARC). These entities add a strong core to network programming leveraging it to subdue the existing legacy traditional network architecture.

On addressing the capacity of overpowered network programming ability which exhibits a completely different face of a network domain, the other deviant is also equally placed amongst the interest of an infinite research community, which is software-defined networking. The history of software-defined networking leaves traces and tracks of various attempts which were made in over 30 years since now in overcoming the issues and complexity of traditional network architecture design. Various projects like GeoPlex [9] an initiative of ATandT and Supranet Transaction Server [10] from Ericson in the early 2000's are evidences of the traces and tracks.

Software-defined networking could be reckoned as a further enhancement of the network programming, which is intended to facilitate the network with software programs more efficiently. The statement "efficiently" is deliberately stated here because of the approach of software-defined networking's decoupled architecture. Software-defined networking architecture decouples the root of traditional network architecture [11], the control, and the data plane.

Even though various attempts were made in the past, the term software-defined networking was coined in the late 2000s and supported by open network foundation [12] since 2011. ONF is an international consortium led by a group of over 200 companies as members to formulate standards and make the new approach more viable. Similar to ONF is the Open Day Light which also focuses on ensuring various common industry standards [13]. Talking about the standards, OpenFlow is a standard proposed by ONF which helps in establishing communication between the data and the control plane. Open Stack is another software platform that focuses on cloud computing to facilitate infrastructure services as and when required [14, 15].

Figure 2 clearly states the decoupled architecture. The forwarding devices are separated from the controlling devices in the architecture facilitating an eagle-eye view and control over the network. The software-defined networking architecture works with the physical devices disassociated from the controller [16]. The physical devices, like switches in the network, are only forwarding devices that would predominantly reduce the complexity of resource utilization and controllability of the network.

The controller, as its name states, would control the network by sending instructions to all the forwarding devices based on the updated topology view and the commands executed by the applications which are customized as per the network sitting over the controller. The main purpose of the controller would be to initially configure the network, manage the network, and monitor and troubleshoot the network if required [17]. The API's help in communicating between the controller and the data plane, in this case, is OpenFlow and marked as Southbound API.

These intended operations of the controller like configuring, managing, and monitoring would be automated using customized programming features by the applications sitting above the controller in the application plane. The

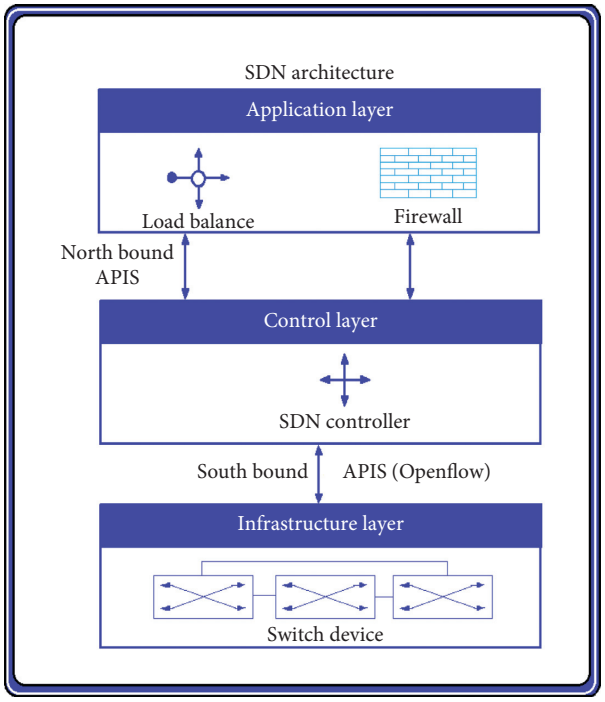


Figure 2: SDN architecture.

communication between the application and the controller is marked as northbound API. However, compared with the standards established within the Southbound API's, the Northbound APIs still lag behind and are more vendor-specific APIs.

By stating the architecture of software-defined networking and the capabilities of network programming marking with the existing traditional networking architecture, this paper has clarified the two deviant points categorizing the evolving network architecture. In the upcoming sections, the security aspects are discussed with adequate merits [18].

3. Evolving Architecture: In the Perspective of Security, Behavior, and Lapses

Being in the position of evolving network architecture, the SDN architecture brings in various advantages compared with the traditional networking architecture. As discussed in the previous section, the decoupled design itself is an added advantage in the aspect of security [19]. Because of its decoupled design, the controller places itself in a dominant position having an eagles-eye view over the network and able to control the flow of data. Controlling the data flow includes various factors of operating a network including inspecting the packets entering the network and balancing the load within the forwarding devices.

This centralized control point of SDN architecture allows to effectively respond to security flaws within the network comparing to the traditional network architecture. Focusing on security becomes a very important point irrespective of the size of the network, the volume of data being handled within the network, and so on. In a generic perspective, a

network's capabilities would be measured based on its resilience, redundancy, availability, scalability, resource utilization, and so on. However, all these metrics will be void if the network is vulnerable to attacks [20]. This brings the importance to analyze the behavior and lapses with respect to security measures within the SDN architecture.

This evolving architecture has centralized control, which could be an advantage in responding to any vulnerabilities. In the same way, the network as a whole is controlled in a central architecture, and an attack on the centralized controllers would in no time bring out the network. In this case, the advantage of SDN architecture on all aspects compared with the traditional networking architecture itself becomes a weak point in the perspective of security [21]. To understand the infrastructure more precisely in the aspect of security, the behavior of the architecture in the view of handling data within the networks needs in-depth view [22].

In SDN architecture, the packet when ingresses towards the interface matches with the forwarding device's flow table. When a successful match is found in the flow table, based on the information related to the path of the destination, the packets will flow through the network. When there is no match in the flow table with the ingress packets, they will be tagged with a "packet-in" message and will be forwarded to the control plane. The controller, based on its information received through the customized applications and the protocols, will forward the packets to the network by updating the forwarding devices' flow tables in the data plane. This behavior of SDN architecture is the advantage that overcomes the traditional network architecture by its efficient data flow within the forwarding planes.

This brings in the valid point deliberately showing multiple points within the SDN architecture where the decision of data movement depends on [23]. These are classified as different scenarios so that the lapse of the architecture in the aspect of security or, in other words, the weak points and vulnerabilities could be identified. To further address the security vulnerabilities within the architecture and to pave the way for future scope of this work entropy-based algorithms [24], machine-learning approaches and genetic algorithms [25] could be considered within the architecture.

SDN security scenario classified in Table 1 helps to understand the lapses within the SDN architectures all hierarchical levels in a briefer overview. In the study by Casado et al. [26], looking in-depth within each plane could pave a path to discuss and analyze various weak points which could be distinguished as subweak points within the different planes. Not only the weak points but also the attacks could be analyzed and determined if the lapses are identified. As this paper purposes to address the SDN architecture's security aspects and paves a pathway to address the security issues, this part skips the in-depth analysis of the weak points within each plane [27, 28].

Based on the above analysis relating to the architecture of the evolving SDN architecture, its design, programmability, behavior, and lapses, it is clearly visible that each hierarchical planes are vulnerable and are exposed to attacks which in-turn potentially reduces the overall efficiency of the architecture [29]. In the next section, the above-briefed scenario is taken, and the possibilities of attacks and its types are discussed concluding the work opening to future research contributions in mitigating the attacks and enhancing the evolving network architecture.

4. Evolving Architecture: Possibilities of Attacks, Types, Outcomes, and Analysis

The views from various existing literatures depict the current situation of the evolving network architecture. After considering the facts from the various research literatures, continuous assessments are done thoroughly in this work reckoning the architecture of software-defined networking architecture, and weak points were identified in all the hierarchical levels of the architecture. Continuously addressing the weak points does not constitute that SDN architecture is inefficient. [30]. The weak points and other discussions are majorly focused on the security aspects of the network and not the potential network operations and functions. Comparing to the traditional network architecture, the evolving SDN architecture overcomes the existing problems more efficiently. The need here is to enhance the security flaws to make the network more productive and secured [31].

In the earlier section, the identified weak points are further analyzed to look out for the possibilities of attacks, their type, and the impact that they could cause on the efficient functioning of the network. As stated during the beginning of this work, this part of the work remains the vital part discussing precisely the attacks, their types, and the impact they could cause to the entire network paving a path to further analyze each and every type of attack stated and work further to propose mitigation strategies to each type of attacks [32, 33].

In today's scenario, where attacks are peeking in a sky rate, the pandemic situations around the globe [34] also provide more flexible endurance for the attackers to succeed. A couple of years ago, today's situations like working from home and accessing cloud storage were not considered as an aspect within the infrastructure. [35]. This obviously forces the organizations to increase their budgets in infrastructures and its security. This proportionally increases the chances of the existing network architectures to move towards evolving network architecture irrespective of its size, being an enterprise, data centers, SoHo networks, and so on.

Keeping this current situation in mind, this work progresses in categorizing various types of attacks focused on this evolving network architecture. The categorization is done based on the reviews of the existing literature that addressing the types of attacks [36]. Based on the reviews, all the possible attacks in the evolving architecture are matched with the above-stated identified weak points in the architecture, and the following types or branches are arranged. They are arranged into six categories such as (1) Access Problems, (2) Data Outflow, (3) Denial of Service Attacks and Distributed Denial of Service attacks, (4) Data Alterations, (5) Misconfigurations, and (6) Malicious Applications which are the overall categories [37].

Table 1: SDN security scenario.

Possible security weak points	Reason to classify weak points
Flow table—data plane	The flow table in the forwarding devices, if compromised, will mislead the ingress and egress data flow in the network and could cause vital damage irrespective of how scalable, resilient, redundant, and efficient a network is.
Controller—control plane	The controller, as addressed earlier, being the central authority could cause a high impact over the flow of the network if compromised (in this case, we are discussing more focused on a single controller scenario; however, an SDN architecture could support distributed controllers within a network).
Applications—application plane	The applications which are customized for the network could lead to a devastating result if compromised.

Table 2: SDN attack analysis focusing on each level.

SDN architecture	Attacks vectors on each level of the SDN architecture
Data plane	- The data flow within the network could be forged and redirected - Manipulating session maintenance between the devices
Control plane	- SDN services could be denied to the network causing a denial of service/distributed denial of service - Compromised network topology information - The network could be manipulated because of its centralized and distributed controller attributes
Application plane	- Legitimate applications could be compromised and manipulated - Misconfigurations within the legitimate applications
Combination of all planes	- Majority of the attacks could be initiated using compromised trusted networks causing distributed denial of service - Sniffing the packets to gain network information
Interfaces	- Exploiting the application programming interface

These above categorized attacks are specific and could potentially make software-defined networking architecture vulnerable; however, the vulnerabilities are not limited to the above-stated attacks alone. Further adding values and contributing towards the work, few more possible attacks are listed here including compromising admin credentials, network manipulation, and man-in-the-middle attacks which might lead to activities like capturing the packets and analyzing the packets for enhanced attacks, session-related attacks, compromised applications, and the APIs. An optimized design [38] is vital to mitigate these categorized and noncategorized attacks.

If and in case the evolving network architecture fails to take appropriate security mitigation methods focusing on the above-stated attacks [39], the networks are very viable and easy to get exposed to these attack vectors. Based on the categorized and discussed attack types, to further analyze the outcome of these attacks, they are further placed over the architectures' weak points identified in the earlier section.

The SDN attack analysis described in Table 2 gives a detailed view on the overall analysis of the types of attacks, their impact, and the outcome within the SDN architecture. With a clear view of the weak points placed at different positions within an SDN architecture, it would now be a comparatively convenient approach to further classify and move out to proceed with various methods of mitigation. Various algorithms [40] at different levels for different purposes could be considered in enhancing the security within the architecture. Considering the intensity of these diversified attack methods and their scopes, more automated and advanced technologies like artificial neural network [41] approach could also be considered in effectively mitigating the weak points. This paper with above classifications made would help diverse technology researchers to showcase their skillset [42] in mitigation approach.

5. Conclusion

This work concludes after the analysis of various types of attacks, classifying them based on the architectural levels of SDN gives a broader view to understand and move forward in mitigating the attacks, thus making a unique representation. This work also underlines the attacks and their impact on the evolving network architecture that the SDN architecture is exposed to various attacks and those attacks are similar to the legacy networking architecture. This again places the research at the starting point of the problem where the evolving SDN architecture is also vulnerable to the attack vectors to which the traditional network architecture is exposed too. As a fact of analysis and thorough literature studies, it is an unfortunate yes until the first point making the statement "exposed to similar threats" true. However, that does not mean that the whole research towards the evolving network architecture is forced to come back to a point where it started because, even though both these architectures are exposed to similar kinds of attack vectors, and the evolving architecture, SDN always has an upper hand advantage in mitigating these attacks. The decoupled architecture of SDN is its advantage adding along with the programmability and interoperability features. The disadvantage of this evolving network architecture will exist if it fails to take appropriate security mitigation methods focusing on the above-stated and discussed attacks. To conclude the work, furthermore research works should focus on

identifying the operation of attacks in each attack vector focusing on the various planes and proposing an effective mitigation solution.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Omar Cheikhrouhou thanks Taif University for their support under the Taif University Researchers Supporting Project (TURSP-2020/55), Taif University, Taif, Saudi Arabia.

References

[1] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "CyberSecurity attack prediction: a deep learning approach," in *Proceedings of the 13th International Conference on Security of Information and Networks*, pp. 1–6, Turkey, November 2020.

[2] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "BMC-SDN: blockchain-based multi-controller architecture for secure software-defined networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9984666, , 2021.

[3] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.

[4] A. Banjar, P. Pupatwibul, and R. Braun, "Comparison of TCP/IP routing versus openflow table and implementation of intelligent computational model to provide autonomous behavior," *Computational Intelligence and Efficiency in Engineering Systems, Part II*, Springer International Publishing, vol. 595, pp. 121–142, , NY, USA, 2015.

[5] S. M. AlShehri, "Software defined networking: research issues, challenges and opportunities," *Indian Journal of Science and Technology*, vol. 10, no. 29, pp. 1–9, 2017.

[6] R. Perlman, D. Eastlake, D. G. Dutt, S. Gai, and A. Ghanwani, "Routing bridges (rbridges): base protocol specification," *Technical Reports*, 2011.

[7] K. Giotis, G. Androulidakis, and V. Maglaris, "Leveraging SDN for efficient anomaly detection and mitigation on legacy networks," in *Proceedings of the 2014 Third European Workshop on Software Defined Networks*, p. 6, Budapest, Hungary, September 2014.

[8] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: past, present, and future of pro- grammable networks,," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.

[9] P. Dutta, "Internet object caching," in *Proceedings of the 7th IEEE Intelligent Network Workshop*, Bordeaux, France, May 1998.

[10] "Network Security," Network Security: http://www.networxsecurity.org/members-area/glossary/s/sdn.html.

[11] A. Doria, J. H. Salim, R. Hass et al., *Forwarding and Control Element Separation (ForCES) Protocol Specification*, Internet Engineering Task Force, Fremont, CA, USA, 2010, http://www.ietf.org/r/fc/rfc5810.txt.

[12] Open Networking Foundation, *Open Networking Foundation*, Open Networking Foundation, Menlo Park, CA, USA, 2011, https://www.opennetworking.org/about/onf-overview.

[13] "Linux foundation collaborative project," 2013, http://www.opendaylight.org.

[14] G. Yao, J. Bi, and P. Xiao, "Source address validation solution with OpenFlow/NOX architecture," in *Proceedings of the 19th annual IEEE International Conference on Network Protocols, ICNP 2011*, pp. 7–12, Vancouver, BC, Canada, October 2011.

[15] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks," in *CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, pp. 413–424, Berlin, Germany, November 2013.

[16] S. Shin and G. Gu, "CloudWatcher: network security monitoring using OpenFlow in dynamic cloud networks (or: how to provide security monitoring as a service in clouds?)," in *Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP)*, Austin, TX, USA, October 2012.

[17] M. Casado, T. Garfinkel, A. Akella et al., "SANE: a protection architecture for enterprise networks," in *Proceedings of the 15th USENIX Security Symposium*, vol. 15, Vancouver, B. C., Canada, July 2006.

[18] B. Nordquist, *An-Introduction-to-Software-Defined-Networking*, Storagecraft, Draper, UT, USA, 2019, https://blog.storagecraft.com/an-introduction-to-software-defined-networking/.

[19] Y. Jarraya, T. Madi, and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1955–1980, 2014.

[20] P. Göransson and C. Black, *Software Defined Network, A comprehensive approach*, Morgan Kaufmann Publishers, Burlington, MA, USA, 1 edition, 2014.

[21] Open Networking Foundation, *Principles and Practices for Securing Software-Defined Networks Version No. 1.0 ONF Document Type: TR (Technical Recommendation)*, Open Networking Foundation, Menlo Park, CA, USA, 2015, https://opennetworking.org/.

[22] M. Boujelben, O. Cheikhrouhou, M. Abid, and H. Youssef, "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks," in *Proceedings of the 2009 Third International Conference on Sensor Technologies and Applications*, pp. 442–448, Athens, Greece, June 2009.

[23] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, "Software-defined network (SDN) data plane security: issues, solutions, and future directions," in *Handbook of Computer Networks and Cyber Security*, B. Gupta, G. Perez, D. Agrawal, and D. Gupta, Eds., Springer, Cham, Switzerland, 2020.

[24] T. A. Sangeetha and G. M. Amalanathan, "Outlier detection in neutrosophic sets by using rough entropy based weighted density method," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 2, pp. 121–127, 2020.

[25] B. R. Murlidhar, R. K. Sinha, E. T. Mohamad, R. Sonkar, and M. Khorami, "The effects of particle swarm optimisation and genetic algorithm on ANN results in predicting pile bearing capacity," *International Journal of Hydromechatronics*, vol. 3, no. 1, p. 69, 2020.

[26] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: taking control of the enterprise," *ACM*

SIGCOMM Computer Communication Review, vol. 37, no. 4, pp. 1–12, 2007.

[27] P. Porras, S. Shen, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, A security enforcement kernel for OpenFlow networks," in *HotSDN'12: Proceedings of the First Workshop on Hot Topics In Software Defined Networks*, pp. 121–126, Helsinki, Finland, August 2012.

[28] M. Kaur, D. Singh, and R. Singh Uppal, "Parallel strength pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2020.

[29] S. Shin, L. Xu, S. Hong, and G. Gu, Enhancing network security through software defined networking (SDN)," in *Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–9, Waikoloa, HI, USA, August 2016.

[30] G. Kannan, K. C. Meng, A literature review on Software-Defined Networking (SDN) research topics, challenges and solutions," in *Proceedings of the Fifth International Conference on Advanced Computing (ICoAC)*, pp. 293–299, Chennai, India, December 2013.

[31] A. S. Alshra'a and J. Seitz, "External device to protect the software-defined network performance in case of a malicious attack," in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pp. 1–6, Orsay, France, July 2019.

[32] O. B. Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam, and A. Derhab, "An OWASP top ten driven survey on web application protection methods," in *Risks and Security of Internet and Systems*, J. Garcia-Alfaro, J. Leneutre, N. Cuppens, and R. Yaich, Eds., Springer International Publishing, Cham, Switzerland, pp. 235–252, 2021.

[33] I. Jemal, O. Cheikhrouhou, H. Hamam, and A. Mahfoudhi, "Sql injection attack detection and prevention techniques using machine learning," *International Journal of Applied Engineering Research*, vol. 15, pp. 569–580, 2020.

[34] Hiscox, *Hiscox Cyber Readiness Report*, Hiscox, NY, USA, 2020.

[35] N. M. Kaliyamurthy, S. Taterh, and S. Suresh, "Vulnerability of SDN network architecture and proposed countermeasures on enhancing security," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4, pp. 2277–3878, 2019.

[36] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proceedings of the 2010 IEEE 35th Conference on Local Computer Network Conference*, pp. 408–415, Denver, CO, USA, October 2010.

[37] K. M. Modieginyane, B. B. Letswamotse, R. Malekiana, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportuni- ties for efficient network management: a survey," *Computers and Electrical Engineering*, vol. 66, pp. 274–287, 2018.

[38] C. Kandilli and B. Mertoglu, "Optimisation design and operation parameters of a photovoltaic thermal system integrated with natural zeolite," *International Journal of Hydromechatronics*, vol. 3, no. 2, p. 128, 2020.

[39] X. Huang, X. Du and B. Song, An effective DDoS defense scheme for SDN," in *Proceedings of the 2017 IEEE International Conference on Communications (ICC); 2017*, Paris, France, May 2017.

[40] C. Zhu, W. Yan, X. Cai, S. Liu, T. H. Li, and G. Li, "Neural saliency algorithm guide bi-directional visual perception style transfer," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 1–8, 2020.

[41] M. Safa, M. Ahmadi, J. Mehrmashadi et al., "Selection of the most influential parameters on vectorial crystal growth of highly oriented vertically aligned carbon nanotubes by adaptive," *International Journal of Hydromechatronics (IJHM)*, vol. 3, no. 3, pp. 238–251, 2020.

[42] Z. Ali and T. Mahmood, "Complex neutrosophic generalised dice similarity measures and their application to decision making," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 2, pp. 78–87, 2020.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9924478, 17 pages
https://doi.org/10.1155/2021/9924478

Research Article

An Efficient Three-Phase Fuzzy Logic Clone Node Detection Model

Sachin Lalar,[1] **Shashi Bhushan**,[2] **Surender Jangra**,[3] **Mehedi Masud**,[4] **and Jehad F. Al-Amri**[5]

[1]*Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India*
[2]*Department of Computer Science and Engineering, Amity University, Patna, India*
[3]*Department of Computer Application, Guru Tegh Bahadur College, Bhawanigarh, Punjab, India*
[4]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[5]*Department of Information Technology, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Mehedi Masud; mmasud@tu.edu.sa

Received 18 March 2021; Revised 7 April 2021; Accepted 16 April 2021; Published 26 April 2021

Academic Editor: Vijay Kumar

Wireless sensor networks have been deployed in the open and unattended environment where the attacker can capture the sensors and create the replica of captured nodes. As the clone nodes have been considered legitimate nodes, clone nodes can initiate different network attacks. We have designed a three-phase clone node detection method named fuzzy logic clone node detection (FLCND). The first phase of FLCND checks whether any node is missing from the network or not. In the next phase, FLCND finds out whether any missing node has arisen in the network in a stipulated time. If any missing node is alive, there is a possibility the node may be cloned. The information of suspected nodes is entered into the Hot-List, which has been maintained in the network. Phase III uses the suspected list and finds out the possibility of clone node using fuzzy logic. Two different scenarios have been simulated in NS2 to evaluate FLCND. The simulation result shows that the proposed method increases the packet delivery ratio (PDR) and reduces packet loss, end-to-end delay, and energy consumption. The simulation results illustrate that the FLCND method reduces the average power consumption by 27% and increases the detection rate by 46% compared to the existing techniques.

1. Introduction

Wireless sensor networks (WSNs) have small, low-cost, and resource-limited sensor nodes that have frequently been used in numerous surveillance functions. The sensor node is an active device that has a processor, memory, low-power supply, radio link, and actuators [1]. WSNs are susceptible to many types of attacks due to the network's open nature [2]. These attacks are classified into two types: application-based attacks and application-independent attacks. Application-based attacks target any network functions, such as data aggregation, localization, and routing [3]. This paper focuses on a clone node (replication) attack, which is recognized as an independent application attack. In some applications, sensor networks are deployed in an open and unattended environment where an attacker can access and capture the sensors. The attacker creates the replica of captured nodes by collecting the information, such as key and encrypted content, and places the clone nodes inside the network [4]. Adversaries insert these duplicate nodes into the tactical network position and commence more internal attacks. The clone node attack can happen either in a static wireless sensor network (SWSN) or in a mobile wireless sensor network (MWSN). In the former type of WSN, the sensor position is fixed in the network, whereas in MWSN, a sensor can change its position. Sensor nodes can move and exchange information with other sensor nodes in mobile sensor networks [5]. If any network communication channel is weak, the mobile node can be connected to the lost communication channel and improve channel efficiency. Mobility performs an essential factor in the sensor network [6].

An example of a mobile sensor network for wildfire tracking is shown in Figure 1. The motion sensor will preserve a certain distance from the fire and provide updated information to the firefighters. Similarly, if the flame spreads, the motion sensor can track and send the information to the base station. In this example, the sensor node has been replicated and inserted into various positions in the network. These clone nodes may produce false information regarding the fire. Mobile WSNs are vulnerable to clone node attacks. Clones can affect network performance if they cannot remove/detect from the network [7]. Some techniques have been proposed to detect clone node attacks in SWSN [8–21], but these methods do not apply to mobile WSNs. In this paper, we will propose a new clone node detection method for MWSN.

The clone node can also change its position in MWSN, so node replication attacks in MWSNs are more challenging to resolve. Attackers can use these mobile replicated nodes to initiate more covert attacks [22]. The discovery strategy may be used to check whether sensor nodes are found in their original position. However, sensor nodes appear at different locations at different times. Node replication attacks are dangerous in MWSN if it has not been eliminated from the network. It will prompt us to find the solution to detect a replicated node in MWSN. The attacker launches the clone node attack in three steps. In the first step, the attackers steal the sensor node from the network. The next step will generate the clone of the stolen node and then place it in the network. After that, the clone nodes can produce a different type of attack in the network. If we maintain the missing node information in the network, when replicated nodes are inserted back into the network, it will be detected.

A new method, FLCND, is proposed. It works in three phases with the step of generating the clone nodes. Initially, the proposed algorithm finds the node which is missing from the network. After that, the proposed algorithm finds out whether any missing node is to come alive in the network. If any missing node is alive, there is a possibility the node may be cloned. The suspected node's information is entered into the suspected list, which is maintained within the network. Phase III uses the suspected list and finds out the clone node by applying fuzzy logic. In the fuzzy method, the parameters are speed, packet delivery ratio (PDR), false input value, residual power, and delay, which are processed as fuzzy logic input and depend on the outcome module; the clone node is detected from the network.

There are the following contributions that are as follows:

(i) The paper proposes an FLCND-based distributed clone node detection method

(ii) The proposed method can increase the packet delivery ratio and reduce packet loss, energy consumption, and end-to-end delay

(iii) The proposed method does not increase the additional communication cost while increasing the detection rate compared to EDD, XED, HO, and CBCD methods

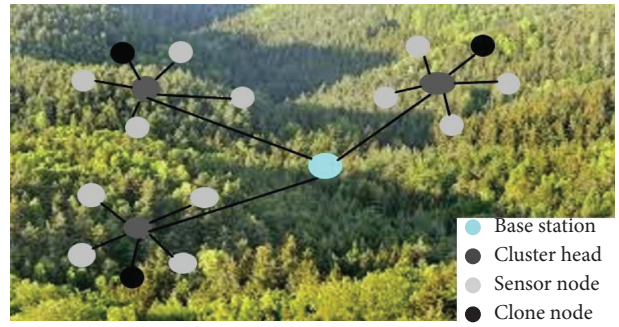


Figure 1: Clone node attack example.

The remainder of the paper is organized as follows. Section 2 reviews existing detection schemes for identifying mobile network cloned nodes. Section 3 describes the system and the attacking model. Section 4 explains the proposed method, fuzzy logic clone node detection (FLCND). Section 5 describes the simulation of the proposed method and the comparison of FLCND with the existing methods. Finally, the paper is concluded in Section 6.

2. Related Work

Different techniques have been invented to detect clone nodes in MWSN, which can be divided into two parts: centralized and distributed. In the centralized MWSN system, all mobile nodes receive information about the clone nodes and transmit the information to the base station, which makes the final decision about the detection of the clone node. On the other hand, the distribution system for identifying a clone node is locally identified by the node [23, 24].

Chia [25] designed the clone node detection method using location information. In this method, each sensor will interchange log lists with neighboring nodes to avoid unauthorized operations. Each node sustains a table that stores information about the nodes used to detect the clone nodes. When monitored nodes meet with each other and exchange recorded information about their IDs, they may find the clone node's conflicting information. Each node acts as a normal node as well as a monitoring node. However, for this method, each node must store a message of each monitored node. The storage overhead of the sensor nodes is high.

Ho et al. [26] proposed a detection scheme based on a probability ratio test. This method's idea is based on the speed of movement not exceeding the maximum speed set in the network for a mobile node. In contrast, clone nodes move much faster than normal nodes as the new clone node's measurement speed appears high to the node's configured maximum speed. When the node speed exceeds the configured speed value, the node's probability value as the clone node is increased. When using SPRT, if the speed is equal to or lower than the maximum speed of the configured system, the null hypothesis is used. If the alternative hypothesis is accepted, then the duplicate node is removed from the network. However, SPRT relies on the base station,

which has limitations such as rapid power loss of nodes near the base station and a single point of failure.

Chia et al. [27] proposed a new method, XED, to detect clone node attacks in MWSNs. The idea behind XED is that, in a nonreplicating network, sensor node, A, encountered another sensor node, B, and A sends a random number, r, to B. When node A meets Bnode again, A will ask for a random number, r, to determine if it is already a matching node. Based on these observations, a "strategy for learning and challenge" has been proposed. The sensor node generates a random number. When sensor nodes want to communicate, they will exchange the generated random number. Each node maintains a table containing the generated received random number and node ID. For a pair of nodes that have already been matched, perform the above steps to replace the random number with the new one.

Yu et al. [28] projected two methods, i.e., EDD and SEDD, to identify replication attacks. It works on an approach that node T that encounters node B must be limited to a number for a given time interval. Each node has the potential to detect duplicates. In EDD, the first phase has calculated the parameters and threshold, which is used to distinguish the actual nodes from the duplicates. In an online phase, each meeting of the node is computed by the node. In EDD, we can see that each node must maintain the list S, resulting in $O(n)$ storage overhead. The basic idea of SEDD is to monitor the subset of nodes instead of all nodes. The number of monitored nodes will be equal to the SEDD program's storage, so the storage overhead is diminished in it.

Deng et al. [29] proposed two schemes, ULTSE and MDLSD, to identify mobile WSN node replication vulnerabilities. As with any agreement, the witness will communicate over the network after receiving the time location statement. The basic idea is to use motion properties. When a node communicates with others, it will track time and location requirements. In other words, if the request for time location is tracked, the witnesses receive and reflect the communication, if they are outside, immediately when the status request witnesses are not sent, but the witness finds the status request for UTLSE multiple locations requiring each of the location claims. The data observed by the node described in the position claim extension are introduced by the method of saving only in the position of the MTLSD claim.

Deng and Xiong [30] projected a new protocol for detecting mobile replicated nodes. Bloom filter and polynomial-based key predelivery schemes are used to find the clone node. The base station finds how many time keys are used. This method runs in four steps: node initialization, pairing, side creation, and discovery. Before setting up the network, symmetric polynomial keys are formed for each node generated by the key server. Each node generates a statement periodically, which contains the ID and the number of keys used. The report was forwarded to the base station. The base station calculates each node's Bloom filter and collects the number of pairs of keys used. Nodes that exceed the limit of the key count are considered clone nodes.

Wang and Shi [31] used the mobile node as a patrol to find distributed clones in various areas of the network. Two detection mechanisms for fixed and mobile systems have been proposed, which include patrol methods. The proposed method identifies duplicates using fixed sensors; if more than two sensors in the same location have equal node ID, then sensors of the same ID will be considered clones. When using a patrol sensor, when the mobile sensor moves at a momentum that exceeds the specified maximum speed, it is considered an attacker node.

Lou et al. [32] proposed a node cloning attack detection protocol for mobile WSN, called single-hop detection (SHD). The node's neighborhood is distinguished by a list of one-hop neighbors available in the regular WSN. Neighboring nodes will be known when the sensor node communicates with other nodes. Each node must sign its neighbor list. When getting a fingerprint complaint from a nearby claim sensor, the receiving node determines that the monitoring node is a clone node.

Shaukat et al. [33] proposed a hybrid method to detect clones in MWSN-based danger theory in the human immune system. The fundamental strategy is to determine the cloned node by the observed abnormal behavior of mobile nodes in the MWSN.

Cheng et al. [34] proposed the NI-LEACH protocol, an improved version of the LEACH protocol. The authors influenced the power consumption of the data transmission and improved the clone node's detection efficiency.

Dong et al. [35] presented a new distributed clone detection protocol known as LSCD. The protocol projects the discovered path of the witness node in which the distance between any two detection paths should be less than the length of the tracking path. The clone detection is also performed in non-hot spot areas and maintains high energy levels that improve energy efficiency and network lifetime.

Anthoniraj and Razak [36] proposed a cluster-based clone detection method, CBCD. In this method, the network is divided into clusters, and each cluster has a cluster head. When the cloned node moves from one cluster to the other, it is identified by the cluster head. Rajesh and Shanmugam [37] proposed the RE-GSASA method in which the authors investigate the simulated model based on GSA to identify clone attack nodes in the network.

Sankar and Roy [38] proposed a CND algorithm based on a Cuckoo filter. The algorithm considers the maximum similarity statements of collaboration spectrum realization decision. The authors enhanced QoS using SDN-based algorithms and located the clones domestically and geographically with a low-cost authentication system.

Conti et al. [39] proposed two clone node detection methods known as HIP and HOP to identify the cloned node in MWNs, which uses the local information and node mobility. The nodes maintain the neighbor information and update the location claim after r number of rounds. The nodes compare their location claims with location claims received from the neighbor. In the HIP, the node compares its location claim only with its neighbor whereas in the HOP, the node compares the received location claim with the other

neighbors. The limitation of this algorithm is that it has high communication, computing, and storage cost.

Manickavasagam and Padmanabhan [40] proposed a new algorithm in mobile WSN to detect the clone nodes. The algorithm is based on the concept that different physical resources are proliferating when multiple clone nodes transmit data with the same source node ID. The algorithm uses the source number in each transmission of the message. If the intermediate node encounters any out-of-order message, it will check whether the source ID is cloned or not. The algorithm's limitation is that it has high communication and memory overload.

Jamshidi et al. proposed a new algorithm in [41] to detect the cloned nodes in a mobile WSN in which watchdog nodes use the learning agent. The watchdog nodes monitor the movement of nodes as well as network traffic. The watchdog changes the status of the learning agent after each monitoring round. The algorithm detects the cloned node by checking the status of the learning agent. The algorithm suffers from low detection and high communication rate when the network consists of a large number of sensor nodes. Jamshidi et al. proposed another watchdog-based algorithm in [42], which uses the node speed to determine the clone nodes in MWSN. If the watchdog node determines that a node is moving faster than a certain limit, the node is considered a replica node. The disadvantages of the algorithm are slow speed, high memory, and computing cost in a dense network.

Jamshidi et al. suggested one more clone node detection algorithm in [43], which uses the mobility model. The sensor node will meet with the same node in each monitoring round. If the node number is higher than a probability value, the node is considered a clone node. The algorithm works in three steps, and in the first step configuration of the watchdog, nodes are there. In the second step, each watchdog monitors the network traffic and records the observation process to estimate the probability value. Watchdog finds the replication node using the probability value calculated in the second step. The proposed method's limitation is that the cloned node cannot be detected if some calculation error is on the probability value. The communication cost is also high.

Anitha et al. [44] proposed three methods, i.e., exponential moving average-based replica detection (EMABRD), SACOP, and FZKA methods, to detect the cloned nodes in MWSN. The main work of the EMARBD algorithm is to compare the actual energy consumption and estimated energy consumption of the sensor node to identify the replication node. A SACOP-based algorithm calculates the trust value of a sensor node from the recommendations of its neighbors. FZKA algorithm relies on fingerprints to identify the clone nodes. The first level is used to verify each node's unique fingerprint, and the second level is used to verify each node's authenticity without sending a personal value. SACOP has a higher clone detection rate as compared to EMABRD and FZKA.

Many of the mobile network's early detection algorithms rely on node mobility and node-to-node communication, which reduces detection if the node moves slowly. This paper is a distributed replica detection program inspired by Ho et al. [26]. Related research of clone node detection in MWSN can be found in [45, 46].

3. System Model

This section explains the network and attack model for the proposed method.

3.1. Network Model. Each mobile sensor node has assigned a unique node ID. We have assumed that the network has a node replica, replicating with the same ID of a node [47, 48]. Each sensor communicates symmetrically and has an information radius. The network is deployed and used the random way motion model. We have assumed that the network is divided into different clusters, and each cluster has a cluster head. The sensor node belongs to anyone cluster. Cluster heads maintain various parameters, i.e., speed, residual energy, delay, packet delivery ratio, and the suspected node's false input value. It has been assumed that all nodes in the MWSN have the same initial energy and the same transmission power. $V_{\max}$ is the upper limit of the speed of node movement. During the simulation, each node begins to move from the starting point to the selected random object point in the simulation area. Table 1 mentions the notations used in the paper [49].

3.2. Attack Model. It has been assumed that the attacker can compromise sensors in the network, and the attacker can execute only a clone node attack. Clone nodes can be set up anywhere in the hostile network [50]. We can only copy legitimate node. It has been assumed that no node with a new node ID cannot insert into the network. Besides, we can use an identity-based public key to allow such nodes to be recognized.

4. Fuzzy Logic-Based Clone Node Detection (FLCND) Scheme

This section explains the new node replication detection method in MWSN. As we know, the clone node attack consists of three main steps as follows:

(a) Attacker first captures the legitimate node from the network

(b) Attacker creates the clone by extracting the information from the captured node and then deploying the network's clones

(c) Then, clone nodes can launch the different attacks inside the network

FLCND method works in three phases, and in each phase, the FLCND method works towards detecting the cloned node in WSN. The FLCND method is divided into three phases, which is explained as follows:

Phase I: find the missing node from the network

The base station initiates the detection phase after deployment of the sensor network. When an attacker

Table 1: Notations and their meanings.

Notations	Meaning
n	Total number of sensor nodes
k	Total number of cluster heads in the network
r_0	Threshold
E_{tp}	Transmitter energy
R	Distance between transmitter and receiver
E_{Ele}	The energy required to operate the transceiver
E_f	Transmitter energy for free space
E_m	Multipath transmitter energy
CH	Cluster head
E_{msg}	The energy required to transmit hello message
H	Number of cluster heads in the node transmitter range
$E_{\mathrm{msg\_CH}}$	The energy required by the cluster head to transmit hello message
CH_t	Relay node
CH_r	Receiver cluster head
$E_{\mathrm{Clone\_Detect}}$	Energy required to detect clone node
E_{SE}	The initial energy of the sensor node
N_F	Number of packets received by a sensor node
N_R	Number of packets received by neighbor nodes
$V_{\max}$	Maximum speed of sensor node

steals any node from the network and creates the replica of legitimate nodes, the complete process of replication will take time, which will be greater than the node's sleeping time. In WSN, the sensor node uses the sleeping time to save the energy/battery. In this phase, each node will check the presence of its neighbor. If any node is not missing from its position or does not give a response after sleeping time, the node will store the suspected node's information and send the information of that node to the cluster head. We will use that information in the second phase for further processing.

Phase II: create the Hot-List

In phase II, the node will check whether any missing node is coming alive or not. If any missing node is alive, that node may be a clone node [51, 52]. The sensor broadcasts the message containing the node ID in the network. The receiving sensors will determine whether the same ID exists in their neighbors or not. If any node ID is presented in the network, then the clone node has been detected from WSN. The information of clone nodes has been sent to the base station for further processing. If the same ID is not in the network, then the information of suspected nodes is entered into the network's Hot-List. There may be a possibility to add the cloned node later in the network. We will use the information entered in the Hot-List in the next phase.

Phase III: fuzzy-based clone node detection

Phase III of the proposed method finds the cloned node using fuzzy logic (Algorithm 1). The identification of clone nodes is predicted based on five parameters such as speed (SP), residual energy (RE), delay (DL), packet delivery rate (PDR), and false input value (FIV). The proposed method FLCND based on the fuzzy system will determine whether the node is a clone or not [53, 54]. The proposed method assumes that each node in MWSN has the same initial energy and transmission range. The four basic components are required to implement the FLCND method are shown in Figure 2 and explained below.

(1) Information: the sensor node sends all the information of suspected nodes from Hot-List in the form of a hello message. This communication occurs between nodes within the framework containing the parameters SP, RE, DL, PDR, and FIV.
(2) Data collection: the cluster head identifies and generates a list based on the hello message. The Hot-Lists, along with parameters, are stored in the database, as is the information for other nodes.
(3) Fuzzy interference system: while collecting data, the information of each suspected node is analyzed using the state of the parameter set. These parameters determine if a clone node exists on the network.
(4) Intra- and intercluster communication: after detecting the cloned node, the clone node's information has been sent to other cluster heads and base stations for further processing. After sending the information, the cloned node will be removed from the sink node's sensor network.

The flowchart of the fuzzy logic-based clone node detection scheme is shown in Figure 3.

4.1. Estimation of Metrics. This section calculates the fuzzification value of each input parameter. First, we will calculate the energy consumption of the sensor node.

4.1.1. Energy Model Analysis. The first step of the analysis is to find the sensor node's energy consumption during the transmission of data. Then, the residual energy is calculated by subtracting the energy consumption from the node's initial energy. Different methods have been proposed to

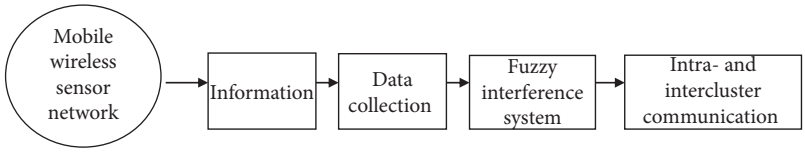


Figure 2: Information flow of the proposed method FLCND.

```
Algorithm: proposed clone node detection algorithm for FLCND
Phase I and II
(1) Begin
(2)   for each node n of the network
(3)     n = Encrypt (ID_i, L_i)//initialize each node with ID and Location
(4)   for each node n of the network
(5)     n[neighbor] = {id_j, L_j, Time_j }//each node finds its neighbor
(6)   For each node x
(7)     Check the response from its neighbor
(8)     if any node x does not respond
(9)       Wait for sleep time
(10)        If response does not come
(11)          Wait for Xn time
(12)          If response comes
(13)            Check the clone of x
(14)            if clone present
(15)              Send information to BS and initiate the trigger revocation procedure
(16)            else
(17)              Add x in the suspected list
(18)          else
(19)            Node x will be dead and send information to BS and go to step 6
(20)      else
(21)            go to step 6
Phase III
(22)  N = total suspected nodes
(23)  W = alive sensor node in the current round
(24)  for each node [N]
(25)      Cluster head receives message from neighbor of N
(26)    node[N].Info and calculate input parameter: node[N].RE, node[N].PDR node[N].SP, node[N].DL, node[N].FIV
//analysis through fuzzy inference system (FIS)
(27)    node[N].probability = FIS (node[N].RE, node[N].PDR node[N].SP, node[N].DL, node[N].FIV)
(28)    If node[N].probability == High
(29)            node[N].state = Clone
(30)            Advertise Clone_Message and initiate the trigger revocation procedure
(31)    else
(32)            go to step 24
(33) End
```

Algorithm 1: Phase III of the proposed method FLCND.

reduce the energy consumption in WSN [55, 56]. The energy consumption is found out by using a first-order radio model, as mentioned in [57, 58]. When the distance between the transmitter and receiver is less than the threshold r_0, then the data directly communicate between nodes. Otherwise, it will use the multipath fading channel. Equation (1) expresses the transmitter energy (E_{tp}) required for sending an l-bit packet at a distance r between transmitter and receiver. E_{Ele} needs the energy to operate the transceiver, which depends on factors, i.e., digital encoding and modulation, ε_f is the transmitter energy for free space, and ε_m stands for multipath transmitter energy.

$$Etp(l,r) = lE_{\text{Ele}} + l\varepsilon r^{\beta}, \tag{1}$$

$$Etp(l,r) = \left\{lE_{\text{Ele}} + l\varepsilon_f r^2, r < r_0 lE_{\text{Ele}} + l\varepsilon_m r^4, r \geq r_0\right. . \tag{2}$$

The threshold r_0 is calculated according to the following formula:

$$r_0 = \sqrt{\frac{\varepsilon_f}{\varepsilon_m}}. \tag{3}$$

The energy consumed by a node after receiving the message is given by

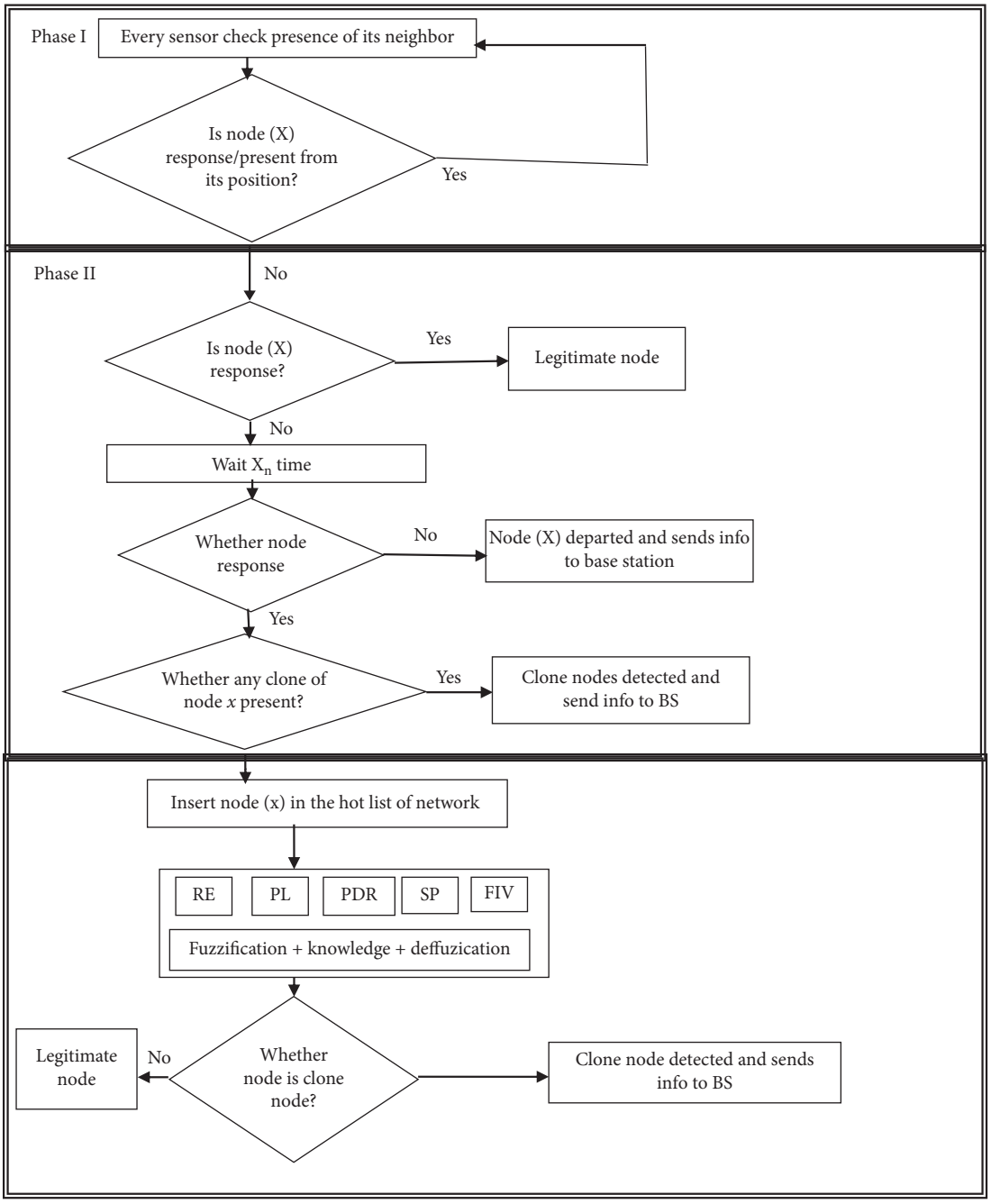


Figure 3: Flowchart of the proposed method FLCND.

$$Erp(l,r) = lE_{\text{Ele}}. \tag{4}$$

Furthermore, the detection process's energy consumption is divided into two phases: clone detection phase and data transmission phase. First, we will compute the energy required to detect the cloned node. When any node is suspected on any node, it will send the information to the cluster head (CH). The nodes will select the CH by sending the hello message among neighbor nodes. The energy required to transmit the hello message by CH is provided by equation (5). The first part calculates the energy required for transmitting the message. The next part represents the energy required to receive a message from other nodes (h):

$$E_{\text{msg}} = ml\left(E_{\text{Ele}} + l\varepsilon_f D_t^2\right) + \frac{h\pi D_t^2}{A^2} lE_{\text{Ele}}. \tag{5}$$

In equation (5), h indicates the number of CH in the range of CH_r, where A is the network region and it also refers to the energy consumed by the CH to transmit the hello message to the other cluster head.

$$E_{\text{msg\_CH}} = kl\left(E_{\text{Ele}} + l\varepsilon_f D_t^2\right) + \frac{n\pi D_t^2}{A^2} klE_{\text{Ele}}. \quad (6)$$

Similarly, equations (5)–(7) state the non-CH energy consumption where n is total nodes and k is cluster heads.

$$E_{\text{msg\_mem}} = (n-k)\left(E_{\text{Ele}} + l\varepsilon_f D_t^2\right) + \frac{k\pi D_t{}^2}{A^2} lE_{\text{Ele}}. \quad (7)$$

When data have been received from the non-CH node, the cluster head (CH) is aggregated, compressed, and sent to the BS or another cluster head. The data are forwarded to the next cluster head or BS that depends on the threshold. For example, if a data packet is transmitted to the CH and its distance from the BS is smaller than TH-BS, the data packet is directly transmitted to the BS. Otherwise, CH forwards to a chosen/relay node from its neighbor. Suppose CH_t as relay/forwarding node. As the free space propagation model has been using, CH_t will directly interact with the BS. The energy consumed by CH_r and CH_t can be given by

$$\begin{aligned} E_{\text{IM}} &= E_{tp}\left[l, r\left(\text{CH}_r, \text{CH}_t\right)\right] + E_{rp}\left[l, r\left(\text{CH}_t, \text{BS}\right)\right] + E_{rp} \\ &= l\left[E_{\text{Ele}} + \varepsilon_f r^2\left(CH_r, CH_t\right)\right] + l\left[E_{\text{Ele}} + \varepsilon_f r^2\left(\text{CH}_r, \text{BS}\right)\right] + lE_{\text{Ele}} \\ &= l\varepsilon_f\left(r^2\left(\text{CH}_r, \text{CH}_t\right) + r^2\left(\text{CH}_r, \text{BS}\right)\right) + 3lE_{\text{Ele}}. \end{aligned} \quad (8)$$

Obviously,$r^2\left(\text{CH}_r, \text{CH}_t\right) + r^2\left(\text{CH}_r, \text{BS}\right)$ plays a huge role in the total energy consumed during data transmission. Therefore, energy requires more for transmission when the distance is large. Thus, the entire detection phase of total energy consumption is given by

$$E_{\text{Clone\_Detect}} = E_{\text{msg}} + 2E_{\text{msg\_ch}} + E_{\text{msg\_mem}}. \quad (9)$$

Each node transmits the data to its CH during the data transfer phase, which is given by

$$E_{\text{msg\_data}} = l(n-k)\left(E_{\text{Ele}} + \varepsilon_f D^2\right). \quad (10)$$

Therefore, the estimation of the remaining energy of each node (n) using data communication is given by

$$E_{\text{res}} = E_{\text{SE}} - E_{\text{clone\_Detect}} - E_{\text{msg\_data}}, \quad (11)$$

where E_{SE} = initial energy node, $E_{\text{Clone\_Detect}}$ = energy consumed during detection, and $E_{\text{msg\_data}}$ = energy required for transmission of data.

4.1.2. Packet Delivery Ratio (PDR). PDR is the ratio packet forwarded by a node to receive from the neighboring nodes.

$$\text{PDR} = \frac{N_F}{N_R}, \quad (12)$$

where N_F is the number of packets sent by the node and N_R is the total packets received from its neighbor nodes. The fuzzification of N is based on the following equation:

$$\text{PDR}_f = \left\{ \text{PDR}\, N_R < N_F 1 - \text{PDR}\, N_R = N_F - \frac{1}{\text{PDR}} N_R > N_F \right. . \quad (13)$$

4.1.3. Delay (DL). It is the delay by a suspected node to the delay by its neighboring nodes.

$$\text{DL} = \frac{D_F}{D_R}, \quad (14)$$

where D_F is a delay caused by the node and D_R is the delay by the neighboring nodes. The fuzzification of DL is given by

$$\text{DL}_f = \left\{ \text{DL}\, D_R < D_F 1 - \text{DL}\, D_R = D_F - \frac{1}{\text{DL}} D_R > D_F. \right. \quad (15)$$

4.1.4. False Input Data (FIP). It is the ratio of the number of invalid inputs forwarded by a node to the number of packets forwarded by the neighbor nodes. The fuzzification of FIP is given by

$$\text{FIP}_f = \text{FIP}. \quad (16)$$

4.1.5. Speed (SP). This parameter is used to measure the speed of the node. The following equation gives the fuzzification of SP:

$$\text{SP}_f = \text{SP}. \quad (17)$$

4.2. Fuzzy Inference System. The fuzzy interference system's first step consists of fuzzifications that determine the appropriate uncertainty for the input parameters. Figures 4(a)–4(f) show the input and output variables' members, respectively.

The knowledge base consists of the evaluation of rules and the integration of rule results. In the rule evaluation, fuzzy rules were applied to the inputs and obtained the output. Then result aggregation is performed, as shown in Table 2. We have considered the five parameters to find the cloned node. When any clone node is inserted into the network, the node's speed and residual energy will be higher than with the existing node in the network. When any node wants to launch an attack in the network, the PDR of that node will be low, and the delay will be high. The attacker node will give the false sensing value in the network. If more than two states meet the above condition, then a node's probability as a clone node is high. When any two conditions satisfy, then the probability of clone node is medium. Otherwise, the node will consider as a normal node.

The ideal conditions of the node to become a clone node will be the following:

(1) Speed (SP) of the node will be higher than that of the normal node
(2) Delay (DL) will be high
(3) Packet delivery ratio (PDR) will be low
(4) Residual energy (RE) will be high
(5) False input value (FIV) will be high

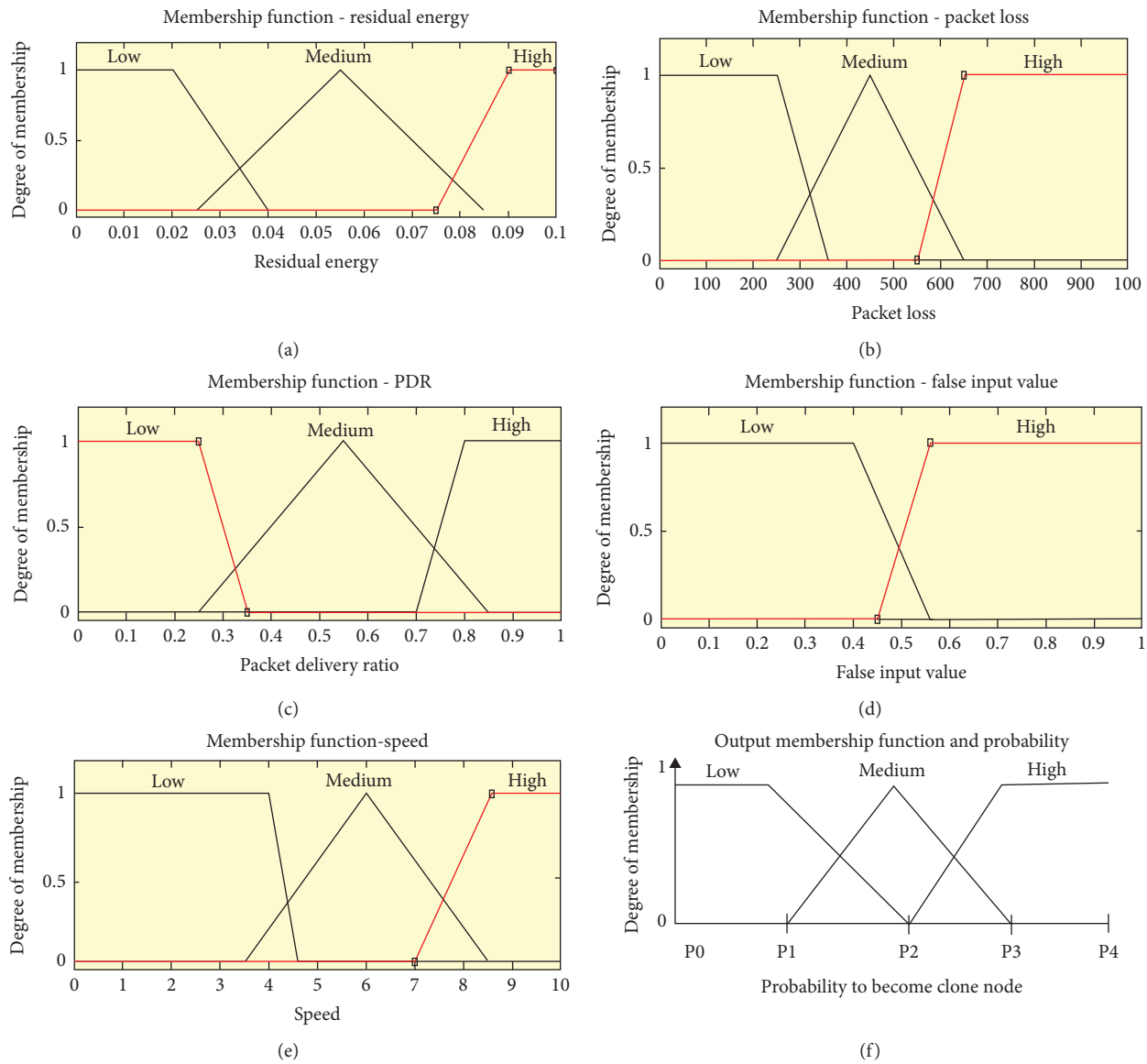


Figure 4: Proposed method input variable for membership function (MF). (a) MF and residual energy. (b) MF and delay. (c) MF and packet delivery ratio. (d) MF versus false input value. (e) MF versus speed. (f) Output variables, membership function, and probability.

The value of P_0, P_1, P_2, P_3, and P_4 is taken as 0, 0.3, 0.6, 0.8, and 1 in Figure 4(f). There are three output values, i.e., low, medium, and high, obtained from the output membership function and probability as symbolized in Figure 4(f). The probability of cloned nodes considers the medium value as best because the false detection will be low. If the proposed method considers the high probability value, the chance of false-positive detection will be high, which decreases the effectiveness of the proposed method.

5. Experiment Result and Performance Evaluation

The suggested FLCND method has been analyzed using Network Simulator (NS2). The simulation network consists of 100 mobile sensor nodes that have been propagated in a 750×750-meter area with a simulation time of 10 seconds. Table 3 summarizes the simulation parameters. Two different simulation cases have been implemented to verify the efficiency of the proposed method. In the first case, the standard network without the proposed method has been simulated, in which the attacker node exists in the network that will lodge different types of attacks inside the network. The second case consists of the same network, but the proposed method has been used in it. The network also has a clone node inside the network.

We evaluate the performance of the network in both cases using four performance parameters: PDR, packet loss, end-to-end (E-E) delay, and residual power .

(a) PDR: the second parameter is PDR, which measures the packet's ratio arriving at the receiver node to the number of packets sent. The comparison of the PDR

Table 2: Aggregation of fuzzy rules.

	Inputs					Output
	False input data	Speed	PDR	Delay	Residual energy	Probability to become clone node
1	Low	High	Low	High	Low	Medium
2	High	High	Low	High	Low	High
3	Low	High	Low	Low	Low	Low
4	High	High	Low	Low	Low	Medium
5	Low	Low	High	Low	Low	Low
6	High	Low	High	Low	Low	Medium
7	Low	High	High	Low	Low	Medium
8	High	High	High	Low	Low	High
9	Low	Low	Low	High	Low	Low
10	High	Low	Low	High	Low	Medium
11	Low	High	Low	High	Low	Medium
12	High	High	Low	High	Low	High
13	Low	Low	High	High	Low	Medium
14	High	Low	High	High	Low	High
15	Low	High	High	High	Low	High
16	High	High	High	High	Low	High
17	Low	Low	Low	Low	High	Low
18	High	Low	Low	Low	High	Medium
19	Low	High	Low	Low	High	Medium
20	High	High	Low	Low	High	High
21	Low	Low	High	Low	High	Medium
22	High	Low	High	Low	High	High
23	Low	High	High	Low	High	High
24	High	High	High	Low	High	High
25	Low	Low	Low	High	High	Medium
26	High	Low	Low	High	High	High
27	Low	High	Low	High	High	High
28	High	High	Low	High	High	High
29	Low	Low	High	High	High	High
30	High	Low	High	High	High	High
31	Low	High	High	High	High	High
32	High	High	High	High	High	High

Table 3: Simulation parameters.

Parameters	Values
Packet size	512 bytes
Simulation time	10 s
Traffic	CBR
Number of nodes	100
Mobility module	Random waypoint
Transmission range	150 meters
Speed	10–40 m/s

of both scenarios is shown in Figure 5. The green line in the figure represents the PDR of the 1st scenario where the proposed method has not been used in the network and replicate nodes are present. The red line in the figure represents the PDR of the 2nd scenario where the proposed method has been implemented in a sensor network when the attacker node is in the network, and the packet delivery rate is low compared to the 2nd scenario where the proposed method has been implemented. The 2nd scenario using the FLCND method delivers 57% more packets compared to the 1st scenario.

(b) End-to-end delay: the average time of a packet sent to the destination node from the source node. The comparison of the end-to-end delay for both scenarios is shown in Figure 6. The first scenario consists of the network containing the cloned nodes without the proposed method, and the 2nd scenario is the network having the clone nodes with the proposed method. The green line in the figure indicates the end-to-end delay in the first scenario. The E-E delay is high in this case at the attacker node. The red line in the figure shows the E2E delay for the second scenario. The E-E delay is low compared to the first scenario as clone nodes are detected by the proposed method and cannot affect the network's performance. Therefore, we can say that the clone node attack does not affect the second scenario of the network by using the proposed method.

(c) Packet loss: it is represented by the packet which does not reach the target node. Figure 7 shows a comparison of the packet loss in both situations. In the first case, the packet loss is higher due to clone nodes, while in the second scenario, the packet loss rate is lower due to the detection of clone nodes.

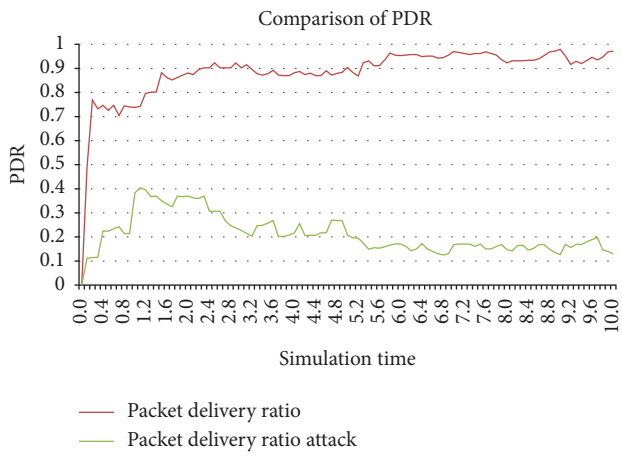


Figure 5: Comparison of packet delivery ratio.

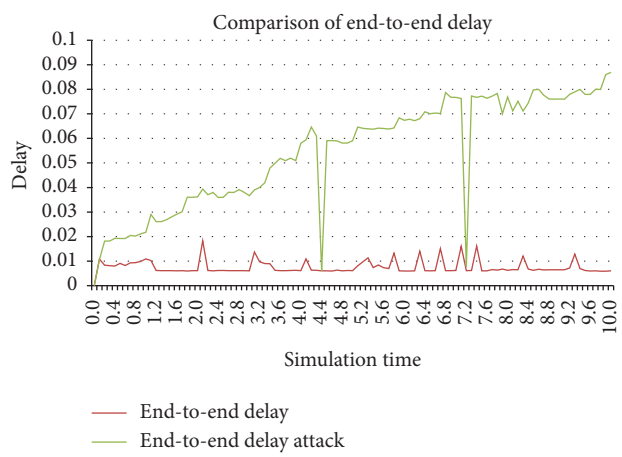


Figure 6: Comparison of end-to-end delay.

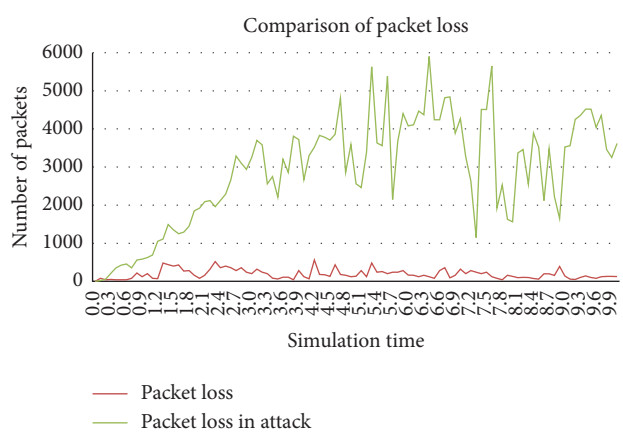


Figure 7: Comparison of packet loss.

Based on this result, we can conclude that the cloned node does not affect the network using the FLCND method.

(d) Residual energy: the next parameter is the residual energy [51, 56, 58], which is calculated as the total energy minus the power consumed by the node during data transmission. When the proposed method is not implemented in the network containing replicated nodes, the green line in the figure represents the residual energy in Figure 8. The red line in the figure shows the residual energy of the proposed method. However, the scenario using the FLCND method consumes 37% less energy than the 1st scenario. Therefore, the proposed method is also optimal in energy consumption.

5.1. Comparison of FLCND with Existing Methods. To calculate the proposed solution's effectiveness, we compared the work of FLCND with existing methods HO, XED, CBCD, and EDD. All five methods have been simulated by using an NS2 simulator by varying the speed and number of sensors from 20 to 200 and 10 m/s to 40 m/s. We have compared the FLCND method with HO, XED, CBCD, and EDD methods in total energy consumption, detection rate, and false-negative rate. Figures 9–11 demonstrate the result of the comparison of the proposed method with existing methods.

5.1.1. Energy Consumption. First, we have compared the total energy consumption of the detection methods by varying the total sensor from 20 to 200. We know that when any sensor transfers or processes the data using any detection method, the node will consume some energy. The lower energy cost indicates the higher efficiency of the detection method. Figures 9(a)–9(d) show the energy consumption of five clone node detection methods, where the number of nodes varies from 20 to 200, and the speed has changed from 10 to 40 m/s. The figures conclude that the total energy consumed of the proposed FLCND method has less among HO, XED, CBCD, and EDD methods. We calculate the total energy consumed for each case and determine the FLCND consumes 41% lower energy to the HO method, 27% lower than the XED method, 46% lower than the CBCD method, and 54% lower than to EDD method. The less energy consumption in FLCND may be due to its approach for the detection of clone nodes. The detection method of the FLCND method focuses only on those nodes which are suspected, whereas that of the HO, XED, CBCD, and EDD methods focuses on the complete network.

5.1.2. Clone Detection Rate. The second parameter is the detection rate of clone nodes. The detection rate of a clone node is calculated as the number of clone nodes detected from the total number of clone nodes existing in the network and then multiply it by 100. Figures 10(a)–10(d) show the detection rate of HO, XED, CBCD, EDD, and FLCND methods by varying the number of nodes and the speed of nodes. The figure shows that the proposed method, FLCND, has a 67% higher detection rate than the HO method, 65% higher detection rate than the XED method, 46% higher detection rate than the CBCD method, and 53% higher detection rate than the EDD method. For generating the

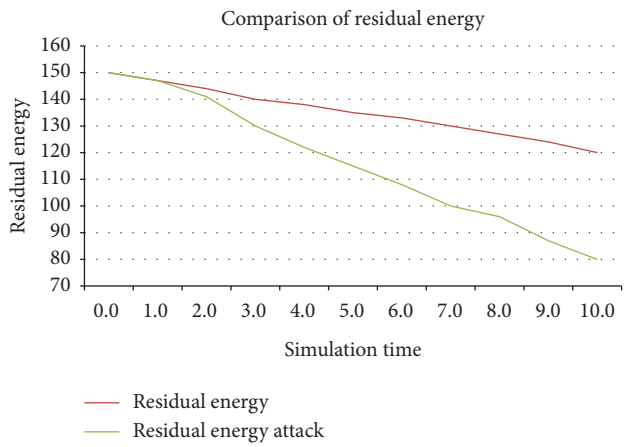


Figure 8: Comparison of residual energy.

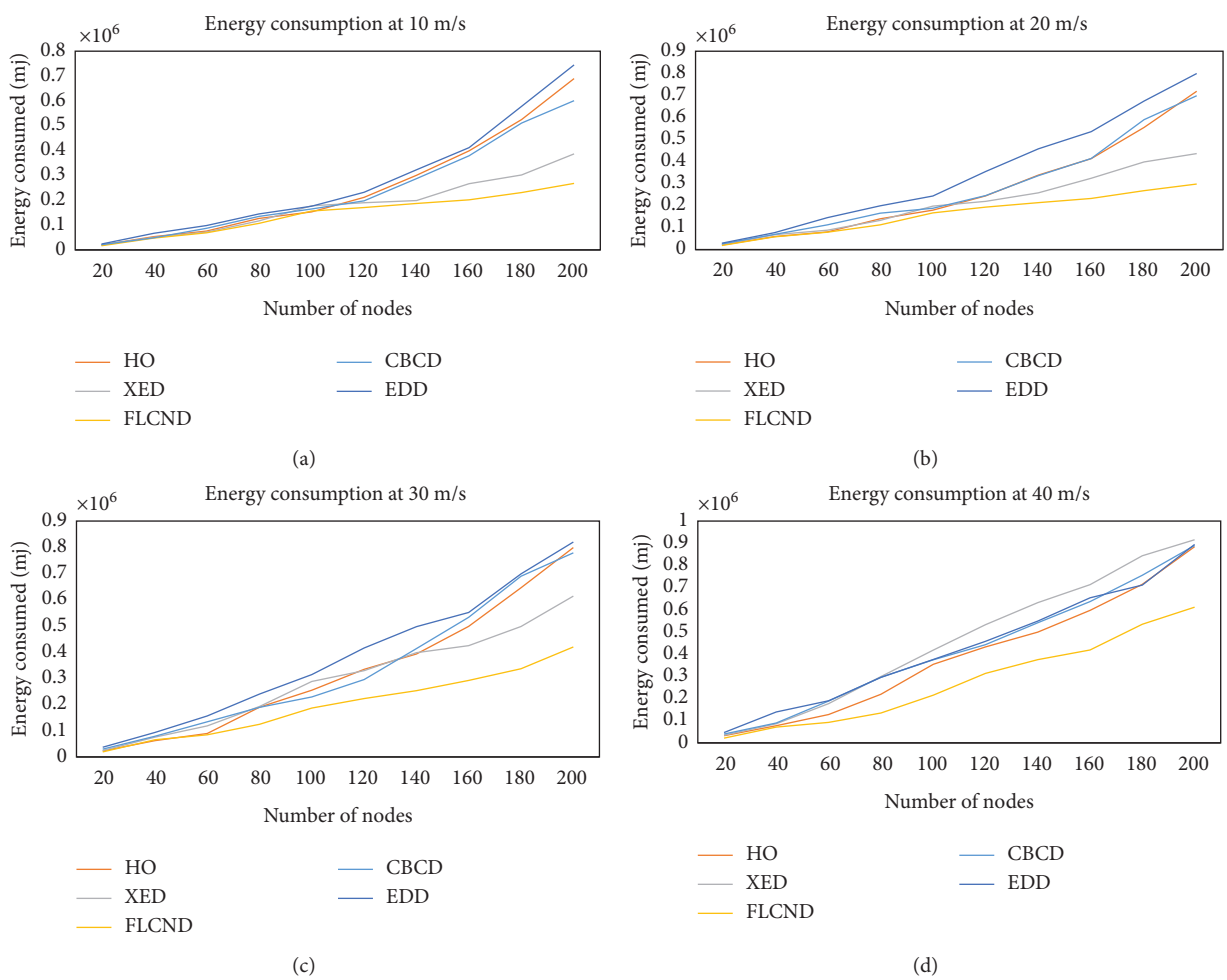


Figure 9: Comparison of total energy consumed at a speed of (a) 10 m/s, (b) 20 m/s, (c) 30 m/s, and (d) 40 m/s.

cloned node, the legitimate node must be stolen from the network. FLCND method finds the missing node from the network so that it may be the reason for the higher detection rate in FLCND.

5.1.3. False-Positive Rate. The next parameter is the wrongly detected clones known as false positive. Figures 11(a)–11(d) show the false-positive detection rate of XED, FLCND, HO, CBCD, and EDD methods

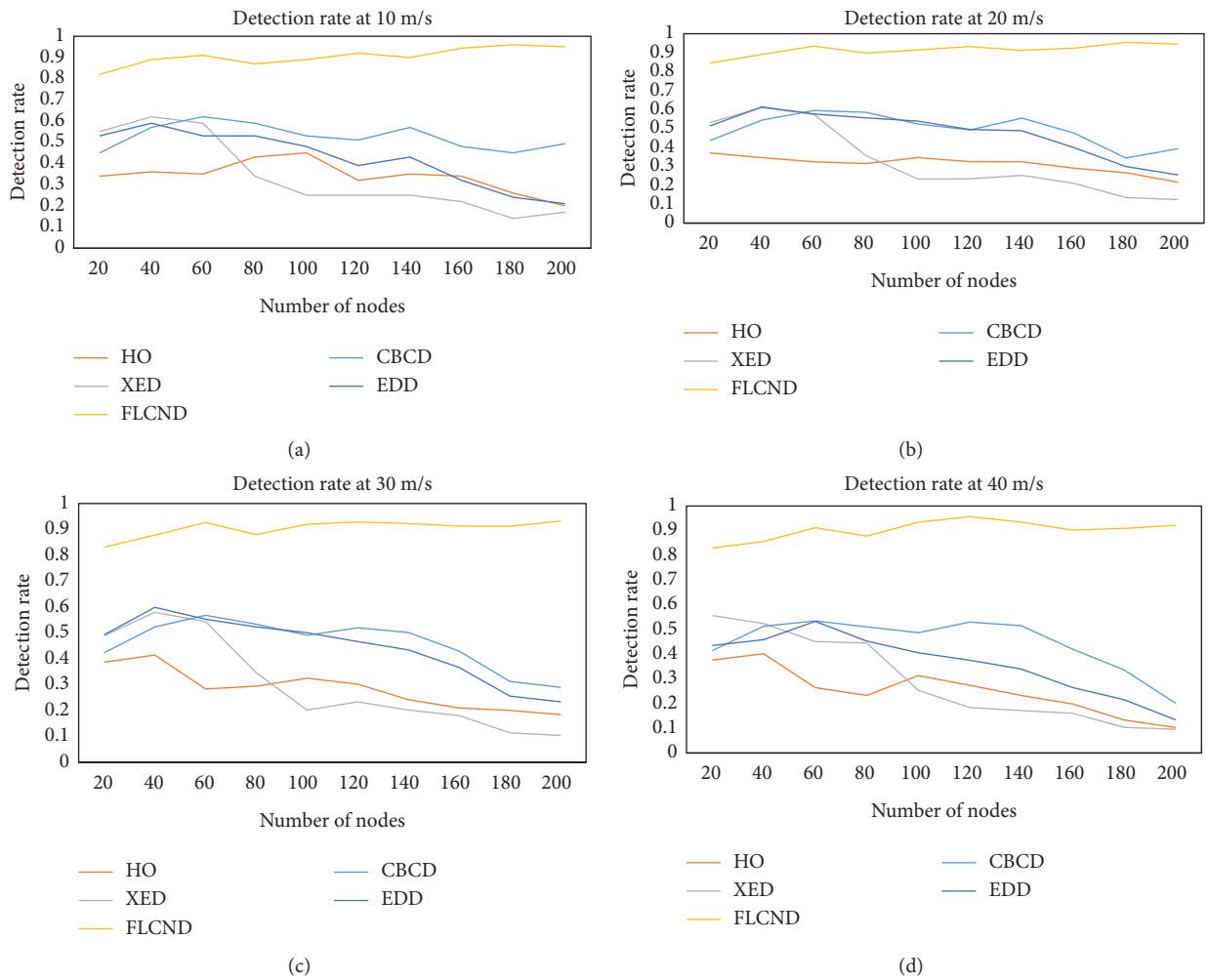


Figure 10: Comparison of detection rate at a speed of (a) 10 m/s, (b) 20 m/s, (c) 30 m/s, and (d) 40 m/s.

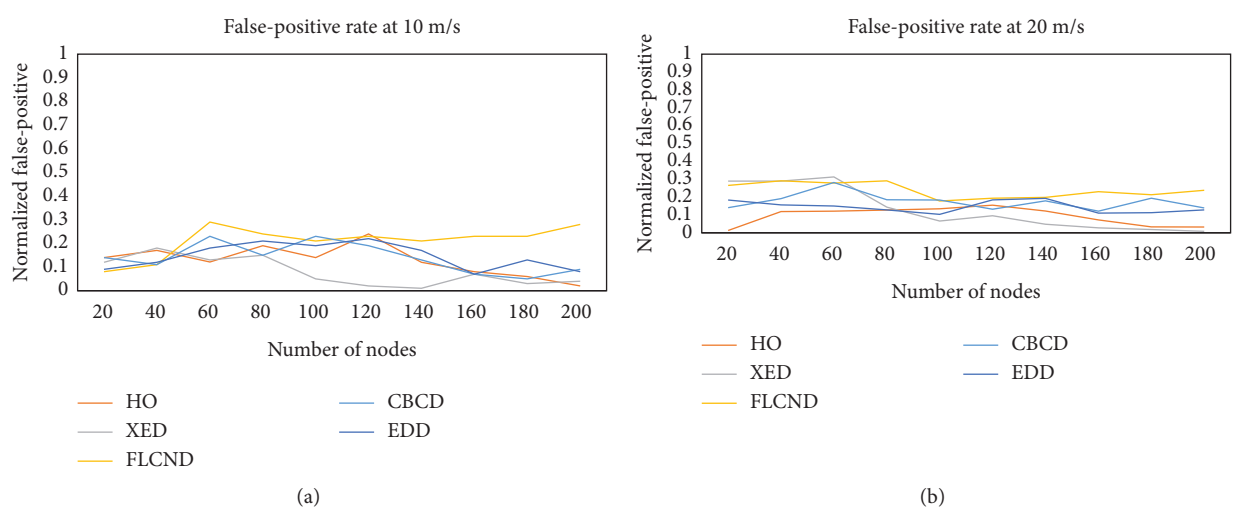


Figure 11: Continued.

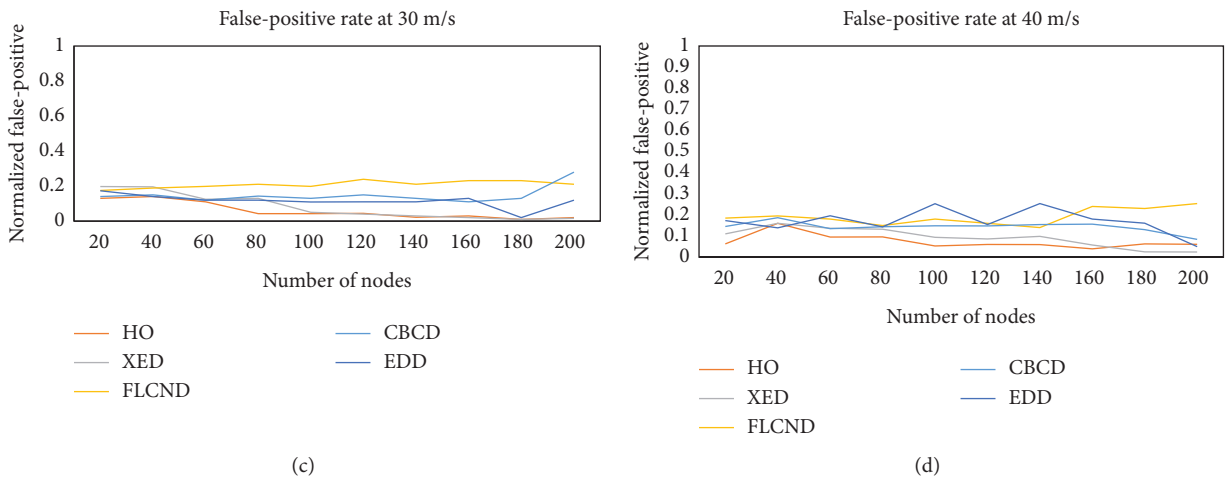


Figure 11: Comparative analysis of false-positive rate at a speed of (a) 10 m/s, (b) 20 m/s, (c) 30 m/s, and (d) 40 m/s.

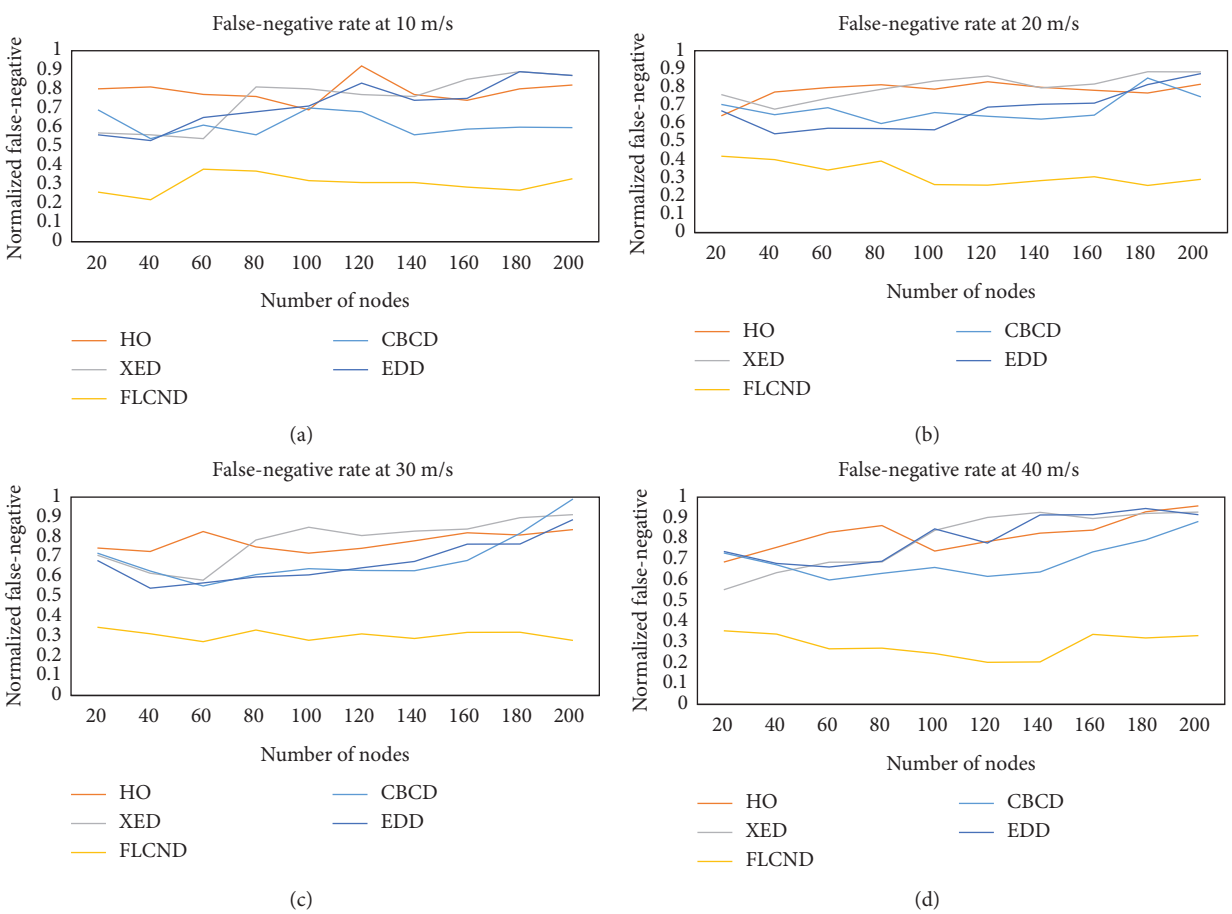


Figure 12: Comparative analysis of false-negative rate at a speed of (a) 10 m/s, (b) 20 m/s, (c) 30 m/s, and (d) 40 m/s.

concerning the number of sensor nodes and speed. In all cases, the false detection rate of the proposed FLCND approach is 21% greater than the XED approach, 19% greater than the HO approach, 16% greater than the CBCD approach, and 15% of the EDD method. As the detection rate of FLCND is higher than other existing methods, the false-positive rate of FLCND is also higher.

5.1.4. False-Negative Rate. The next parameter is the false-negative detection rate in which the clone mobile node is not identified as a clone. Figures 12(a)–12(d) show the false detection rate of XED, FLCND, HO, CBCD, and EDD methods concerning the number of sensor nodes and speed. In all cases, the false detection rate of the proposed FLCND approach is 31% less than the XED

approach, 28% less than the HO approach, 29% less than the CBCD approach, and 29% of the EDD method.

6. Conclusion

An FLCND method to detect the cloned node is designed. The parameters of FLCND are falsely input value, speed, PDR, delay, and residual power, which are processed as fuzzy logic inputs, and based on the outcome, a clone node is detected in WSN. The FLCND method's performance was evaluated using PDR, packet loss, E-E delay, and residual energy parameters in the NS2 simulator. Two different scenarios have been implemented in NS2, where the first scenario is a normal network which is having clone nodes, and the second case consists of the proposed method and the cloned nodes in the network. After comparing the results, the FLCND method consumes less energy and high packet delivery rate. We can conclude that the cloned node does not affect the network due to the FLCND method. We have also compared the proposed method with EDD, HO, CBCD, and XED in terms of total energy consumed, false-negative rate, and detection rate. FLCNDS consumes less than 27% energy with each method. FLCND has a 67% higher detection rate than the HO method, 65% higher detection rate than the XED method, 46% higher detection rate than the CBCD method, and 53% higher detection rate than the EDD method. The false-negative detection rate of the proposed FLCND approach is less than 28% of each method. We have found that the FLCND has less energy consummation and a better detection rate compared to XED, HO, CBCD, and EDD methods. In the future, we will simulate the proposed algorithm by changing the number of nodes from 1000 to 10000. We will evaluate the FLCND method's performance with other parameters and compare it with other existing methods.

In the near future, we will utilize various metaheuristic techniques to enhance the results further. Also, the proposed model will be tested on other kinds of wireless technologies.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors would like to acknowledge the support of Taif University Researchers Supporting Project number (TURSP-2020/211), Taif University, Taif, Saudi Arabia.

References

[1] A. Rajput and V. B. Kumaravelu, "Scalable and sustainable wireless sensor networks for agricultural application of Internet of things using fuzzy c-means algorithm," *Sustainable Computing: Informatics and Systems*, vol. 22, pp. 62–74, 2019.

[2] M. Naghibi and H. Barati, "EGRPM: energy efficient geographic routing protocol based on mobile sink in wireless sensor network," *Sustainable Computing: Informatics and Systems*, vol. 25, Article ID 100377, 2020.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[5] X. Du and Y. Xiao, "Chapter 17: a survey on sensor network security," in *Wireless Sensor Networks and Applications. Signals and Communication Technology*, Y. Li, M. T. Thai, and W. Wu, Eds., Springer, Boston, MA, USA, 2008.

[6] K. Chao, M. Jo, T. Kwon, H. H. Chen, and D. H. Lee, "Classification and experimental analysis for clone detection approaches in wireless sensor networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 26–35, 2012.

[7] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: the need for secure systems," Technical Report CU-CS-990-05, Department of Computer Science, University of Colorado at Boulder, Boulder, Colorado, 2005.

[8] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 49–63, Oakland, CA, USA, May 2005.

[9] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1246–1258, 2007.

[10] H. Choi, S. Zhu, and T. F. Porta, "SET: detecting node clones in sensor networks," in *Proceedings of the Third International Conference on Security and Privacy in Communications Networks*, pp. 17–21, Washington, WA, USA, October 2007.

[11] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc'07*, pp. 80–89, Montréal, Canada, September 2007.

[12] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in *Proceedings of the Twenty-Third Annual Conference in Computer Security Applications*, pp. 257–267, Miami Beach, FL, USA, December 2007.

[13] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Emergent properties: detection of the node-capture attack in mobile wireless sensor networks," in *Proceedings of the 1st ACM Conference on Wireless Network Security, WiSec'08*, Alexandria, VA, USA, January 2008.

[14] S. Lalar, S. Bhushan, and N. A. Surender, "Clone detection using fuzzy logic in static wireless sensor network," *International Journal of Vehicle Information and Communication Systems*, vol. 5, no. 3, pp. 334–353, 2020.

[15] Z. Zhang, S. Luo, H. Zhu, and Y. Xin, "A clone detection algorithm with low resource expenditure for wireless sensor networks," *Journal of Sensors*, vol. 2018, Article ID 4396381, 16 pages, 2018.

[16] M. Conti, R. Di Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE*

Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, 2011.

[17] C. M. Yu, C. S. Lu, and S. Y. Kuo, "CSI: compressed sensing-based clone identification in sensor networks," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications*, pp. 290–295, Lugano, Switzerland, March 2012.

[18] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 677–691, 2010.

[19] W. B. Jaballaha, M. Conti, G. File, M. Mosbah, and A. Zemmari, "Whac-a-mole: smart node positioning in clone attack in wireless sensor networks," *Computer Communications*, vol. 119, pp. 66–82, 2018.

[20] S. Lalar, S. Bhushan, and Surender, "An efficient tree-based clone detection scheme in wireless sensor network," *Journal of Information and Optimization Sciences*, vol. 40, no. 5, pp. 1003–1023, 2019.

[21] N. Muhammad, S. Fazli, Z. Khan et al., "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[22] J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *Proceedings - IEEE INFOCOM*, pp. 1773–1781, Rio de Janeiro, Brazil, April 2009.

[23] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in mobile sensor networks: theory and approaches," *Security and Communication Networks*, vol. 5, no. 5, pp. 496–507, 2011.

[24] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: a survey," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1022–1034, 2012.

[25] M. C. Chia, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in *Proceedings of the 70th IEEE Vehicular Technology Conference VTC. Fall 2009*, Anchorage, AK, USA, September 2009.

[26] J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," *IEEE Transactions on Mobile Computing*, vol. 10, no. 6, pp. 767–782, 2011.

[27] M. Y. Chia, S. L. Chun, and Y. K. Sy, "Mobile sensor network resilient against node replication attacks," in *Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'08)*, pp. 597–599, San Francisco, CA, USA, June 2008.

[28] C. M. Yu, C. Lu, and S. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in *Proceedings of the 70th IEEE Vehicular Technology Conference Fall (VTC '09-Fall)*, pp. 1–5, Anchorage, AK, USA, September 2009.

[29] X. Deng, Y. Xiong, and D. Chen, "Mobility-assisted detection of the replication attacks in mobile wireless sensor networks," in *Proceedings of the IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 225–232, Niagara Falls, Canada, October 2010.

[30] X.-M. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks," *Journal of Computer Science and Technology*, vol. 26, no. 4, pp. 732–743, 2011.

[31] L.-M. Wang and Y. Shi, "Patrol detection for replica attacks on wireless sensor networks," *Sensors*, vol. 11, no. 3, pp. 2496–2504, 2011.

[32] Y. Lou, Y. Zhang, and S. Liu, "Single hop detection of node clone attacks in mobile wireless sensor networks," *Procedia Engineering*, vol. 29, pp. 2798–2803, 2012.

[33] H. R. Shaukat, F. Hashim, and A. Sali, "Danger theory based node replication attacks detection in mobile wireless sensor network," in *Proceedings of the IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, April 2014.

[34] G. Cheng, S. Guo, Y. Yang, and F. Wang, "Replication attack detection with monitor nodes in clustered wireless sensor networks," in *Proceedings of the 34th IEEE International Performance Computing and Computing Conference*, pp. 1–8, Nanjing, China, December 2015.

[35] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, "LSCD: a low-storage clone detection protocol for cyber-physical systems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 5, pp. 712–723, 2016.

[36] J. Anthoniraj and A. Razak, "CBCD: cluster based clone detection in mobile wireless sensor networks," *Indian Journal of Science and Technology*, vol. 9, no. 31, pp. 1–10, 2016.

[37] D. Rajesh and A. Shanmugam, "A hyper heuristic localization based cloned node detection technique using GSA based simulated annealing in sensor networks," *Cognitive Computing for Big Data Systems Over IoT*, vol. 14, pp. 307–335, 2018.

[38] P. C. Sankar and M. Roy, "Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs," *IET Wireless Sensor Systems*, vol. 8, no. 3, pp. 121–128, 2018.

[39] M. Conti, R. Di Pietro, and A. Spognardi, "Clone wars: distributed detection of clone attacks in mobile WSNs," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 654–669, 2014.

[40] V. Manickavasagam and J. Padmanabhan, "A mobility optimized SPRT based distributed security solution for replica node detection in mobile sensor networks," *Ad Hoc Networks*, vol. 37, pp. 140–152, 2016.

[41] M. Jamshidi, S. Sheikh Abooli Poor, N. Nasih Qader, M. Esnaashari, and R. M. Mohammad, "A lightweight algorithm against replica node attack in mobile wireless sensor networks using learning agents," *IEIE Transactions on Smart Processing & Computing*, vol. 8, no. 1, pp. 58–70, 2019.

[42] M. Jamshidi, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, "Using time-location tags and watchdog nodes to defend against node replication attack in mobile wireless sensor networks," *International Journal of Wireless Information Networks*, vol. 27, no. 1, pp. 102–115, 2020.

[43] M. Jamshidi, S. Abooli, A. Arghavani, M. Esnaashari, A. A. Shaltooki, and M. R. Meybodi, "A simple, lightweight, and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information," *Ad Hoc Networks*, vol. 100, 2020.

[44] S. Anitha, P. Jayanthi, and V. Chandrasekaran, "An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks," *Measurement*, vol. 167, 2021.

[45] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang, and Y. Lu, "Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2041–2051, 2021.

[46] T. Dimitriou, E. A. Alrashed, M. H. Karaata, and A. Hamdan, "Imposter detection for replication attacks in mobile sensor networks," *Computer Networks*, vol. 108, pp. 210–222, 2016.
[47] T. Wiens, "Engine speed reduction for hydraulic machinery using predictive algorithms," *International Journal of Hydromechatronics*, vol. 2, no. 1, pp. 16–31, 2019.
[48] M. Kaur, D. Singh, and R. Singh Uppal, "Parallel strength pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2019.
[49] M. Khurana, R. Thalore, V. Raina, and M. K. Jha, "Improved time synchronization in ML-MAC for WSN using relay nodes," *AEU-International Journal of Electronics and Communications*, vol. 69, no. 11, pp. 1622–1626, 2015.
[50] R. Thalore, J. Sharma, M. Khurana, and M. K. Jha, "QoS evaluation of energy-efficient ML-MAC protocol for wireless sensor networks," *AEU-Journal of Electronics and Communications*, vol. 67, no. 12, pp. 1048–1053, 2013.
[51] S. Osterland and J. Weber, "Analytical analysis of single-stage pressure relief valves," *International Journal of Hydromechatronics*, vol. 2, no. 1, pp. 32–53, 2019.
[52] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.
[53] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.
[54] B. Gupta, M. Tiwari, and S. Singh Lamba, "Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.
[55] P. P. Devi and B. Jaison, "Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms," *Computer Communications*, vol. 152, pp. 316–322, 2020.
[56] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.
[57] SD. Gandham, S. Dawande, M. Prakash, and S. Venkatesan, "Energy efficient schemes for wireless sensor networks with multiple mobile base stations," in *Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM*, pp. 377–381, San Francisco, CA, USA, December 2003.
[58] R. Wang, H. Yu, G. Wang, G. Zhang, and W. Wang, "Study on the dynamic and static characteristics of gas static thrust bearing with micro-hole restrictors," *International Journal of Hydromechatronics*, vol. 2, no. 3, pp. 189–202, 2019.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9923389, 9 pages
https://doi.org/10.1155/2021/9923389

Research Article

Artificial Intelligence-Based Digital Image Steganalysis

Ahmed I. Iskanderani,[1] Ibrahim M. Mehedi,[1,2] Abdulah Jeza Aljohani,[1,2] Mohammad Shorfuzzaman,[3] Farzana Akther,[4] Thangam Palaniswamy,[1] Shaikh Abdul Latif,[5] and Abdul Latif[6]

[1]*Department of Electrical and Computer Engineering (ECE), King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[2]*Center of Excellence in Intelligent Engineering Systems (CEIES), King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[3]*Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia*
[4]*Aarhus BSS, Aarhus University, Aarhus, Denmark*
[5]*Department of Nuclear Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[6]*Department of Mathematics, King Abdulaziz University, Jeddah 21589, Saudi Arabia*

Correspondence should be addressed to Ibrahim M. Mehedi; imehedi@kau.edu.sa

Received 30 March 2021; Revised 5 April 2021; Accepted 9 April 2021; Published 21 April 2021

Academic Editor: Manjit Kaur

Recently, deep learning-based models are being extensively utilized for steganalysis. However, deep learning models suffer from overfitting and hyperparameter tuning issues. Therefore, in this paper, an efficient θ-nondominated sorting genetic algorithm- (θ NSGA-) III based densely connected convolutional neural network (DCNN) model is proposed for image steganalysis. θ NSGA-III is utilized to tune the initial parameters of DCNN model. It can control the accuracy and f-measure of the DCNN model by utilizing them as the multiobjective fitness function. Extensive experiments are drawn on STEGRT1 dataset. Comparison of the proposed model is also drawn with the competitive steganalysis model. Performance analyses reveal that the proposed model outperforms the existing steganalysis models in terms of various performance metrics.

1. Introduction

With the advancement in Internet technology and communication, a substantial amount of images are transferred over public networks. Recently, it has been found that many criminal groups utilize images to transfer their dangerous data. These groups hide their dangerous data in the images. Generally, they utilize steganography approaches to hide their harmful contents in the images [1]. Therefore, researchers have started utilizing steganalysis models to recognize the images which contain embedded data. Thus, image steganalysis is an approach for recognizing data embedded in images. Consequently, steganalysis classifies the given image as a stego-embedded image or normal image [2].

Zhou et al. [3] designed an ensemble learning model- (ELM-) based image steganalysis. SRNet and RESDET were utilized as base models. Fusion of the base models was then achieved to classify the embedded images. Zhang et al. [4] designed a CNN model by using 3×3 kernels, and the optimization of convolution kernels was achieved during the preprocessing layer. The minimal convolution kernels were utilized to minimize the initial parameters. Spatial pyramid pooling was also used to integrate the local features. Gowda et al. [5] designed an ensemble color space model (ECSM) to evaluate a weighted activation map. It can extract various features explicit to each color space. Levy-flight grey wolf optimization was utilized to minimize the number of features selected in the map.

Boroumand et al. [6] proposed a deep residual model (DRM) to reduce the heuristics and externally enforced elements. This model computes the noise residuals by disabling the pooling to overcome the suppression of the stego signal. Yedroudj et al. [7] designed a truncation activation-

based ensemble model (TREM) trained with Rich features. It utilizes a truncation activation function and batch normalization on a scale layer. Ye et al. [8] utilized high-pass filter-based CNN (HCNN) to achieve steganalysis. The weights of the initial layer were computed using a high-pass filter for evaluation of residual maps in a spatial rich model. It was utilized as a regularizer to suppress the image content efficiently. A truncated linear unit was also utilized. Wu et al. [9] utilized CNN and deep residual network for steganalysis. It contains a substantial number of network layers, which are significant for evaluating the complex statistics of images.

Yang et al. [10] designed thirty-two-layer CNNs to enhance the performance of features by integrating all features to enhance the gradient. The bottleneck layers enhance the feature propagation and minimize CNN parameters dramatically. Li et al. [11] designed a novel CNN model to evaluate embedded artifacts in an efficient manner. Information diversely was also achieved. A parallel subnet module was also designed utilizing numerous filters. Subnets were trained independently to improve computational speed. Zhang et al. [12] designed a novel CNN model to enhance the classification accuracy of spatial-domain steganography. A spatial pyramid pooling was utilized to integrate the local features. Sharma et al. [13] designed an aggregated residual transformation-based CNN model to obtain significant features for steganalysis. This model has limited initial parameters for enhancing the classification rate. The residual skip connections were also utilized.

Liu et al. [14] have shown the similarity and dissimilarity between SRM-EC and CNN models. An ensemble model was designed to integrate SRM-EC with CNN by averaging their resultant probabilities. Zeng et al. [15] utilized CNN for a Rich model feature set. The bottom to up strategy was utilized for training the output of each subnetwork to the actual output. Yang et al. [16] designed a max CNN for steganalysis. It allocates significant weights to features learned from the complex texture regions. Yang et al. [17] proposed image steganalysis using a transfer learning model with structure preservation. The discriminant projection matrix was utilized for building the model. Frobenius-norm-based regularization was also utilized to achieve better results. Ren et al. [18] designed an efficient selection channel network and steganalysis model. The steganalysis model combined with the trained selection channels estimates the final steganalysis outcomes.

From the extensive review, it has been observed that deep learning-based models can be utilized for steganalysis [19]. However, deep learning models suffer from overfitting and hyperparameter tuning issues. Therefore, in this paper, an efficient θ NSGA-III-based densely connected convolutional neural network (DCNN) model is proposed for image steganalysis. This is the principle difference from the existing model available in the literature.

The main contributions of this paper are as follows:

(1) An efficient θ NSGA-III-based DCNN model is proposed for image steganalysis.

(2) θ NSGA-III is utilized to tune the initial parameters of the DCNN model.

(3) Accuracy and f-measure performance metrics are used as a multiobjective fitness function.

(4) Extensive experiments are drawn on STEGRT1 dataset. Comparison of the proposed model is also drawn with the competitive steganalysis model.

The remaining paper is organized as follows: Section 2 presents the proposed θ NSGA-III-based DCNN model for steganalysis. Experimental results and comparative analysis are presented in Section 3. Section 4 concludes the paper.

2. Proposed Model

In this paper, an efficient θ NSGA-III-based DCNN model is proposed for image steganalysis. The following section discusses the working of DCNN and θ NSGA-III.

2.1. Densely Connected Convolutional Neural Network The diagrammatic flow of the DCNN is shown in Figure 1.

Assume a stego/normal image a_0, which is assigned to CNN. The model has N layers which utilize nonlinear transformation $I_n(\cdot)$ such that n shows the layer's indexes [20]. $I_n(\cdot)$ shows a set of operators like pooling, rectified linear units (ReLU), convolution (Conv), and batch normalization (BN). a_ℓ shows the outcome of the nth layer. However, the existing CNN joins the outcome of the nth layer as an input of $(n+1)^{\text{th}}$ layer. It achieves the layer transition as $a_n = I_n(a_{n-1})$. ResNets utilize a skip join which avoids the nonlinear transformations utilizing an identity operator such as

$$a_n = I_n(a_{n-1}) + a_{n-1}. \tag{1}$$

ResNets achieve better gradient flow compared to CNN. However, the summation of the identity operator with an output of I_n may hinder the data flow in the model.

Therefore, to enhance the data flow, a DenseNet was designed. It contains direct links from a given layer to every other layer. The nth layer takes the feature maps of all previous layers, $a_0, \ldots, a_{n-1}$, as input:

$$a_n = I_n([a_0, a_1, \ldots, a_{n-1}]), \tag{2}$$

Here, $[a_0, a_1, \ldots, a_{n-1}]$ shows the integration of feature maps obtained from layer $0, \ldots, n-1$.

$I_n(\cdot)$ is defined as a group operator. It contains BN, ReLU, and a 3×3 Conv.

The integration operator utilized in equation (2) is not sustainable if there are some variations in the size of the feature maps. The downsampling layers of CNN vary with the size of the feature maps. To achieve downsampling, the model is divided into various densely connected dense blocks. Layers among the blocks are represented as transition layers. In this paper, the transition layer utilizes BN and 1×1 Conv followed by a 2×2 average pooling layer. There are no links across dense blocks except the transition layer.

If every I_n generates k feature maps, it considers n^{th} layer with $J_0 + J \times (n-1)$ input feature maps. J_0 defines the channels of the input layer. The main significance of DenseNet over CNN is that it has confined layers, e.g.,

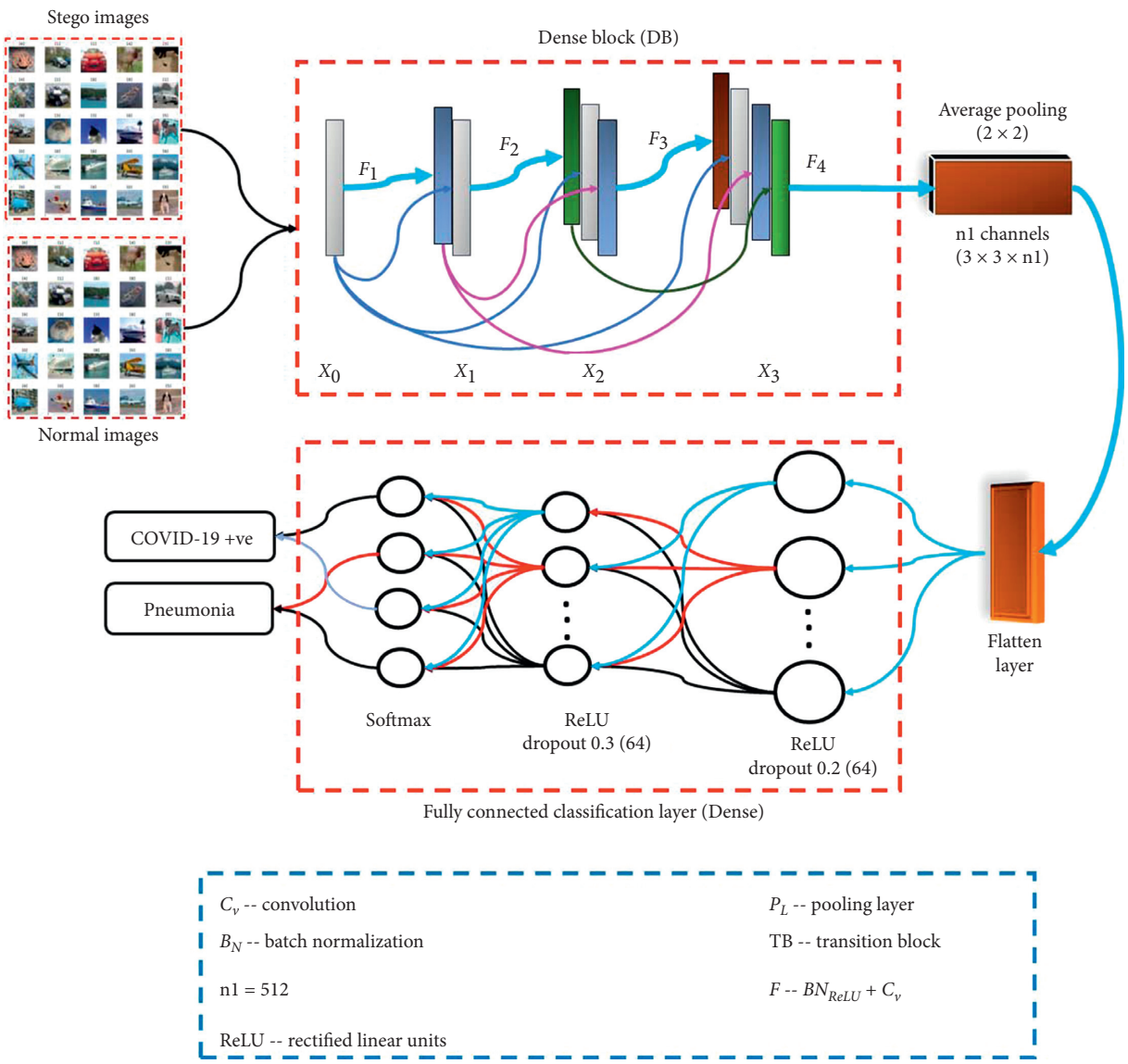


Figure 1: Diagrammatic flow of the DCNN model.

$J = 12$. J represents the growth rate of the DenseNet. Every layer merges with the J feature maps. The growth rate regulates the details of every layer's contribution to the global state. The global state is globally defined; therefore, it is not required to redefine in every layer.

Every layer will compute J feature maps, but it may have more inputs. 1×1 Conv is utilized as the bottleneck layer prior to every 3×3 Conv to minimize the size of feature maps and enhance the computational speed. This model is efficient for DenseNet, and DenseNet with bottleneck layer can be defined as BN-ReLU-Conv (1×1)-BN-ReLU-Conv (3×3) version of I_n, as DenseNet-B. In this paper, 1×1 Conv provides $4J$ feature maps.

To enhance the model density, the feature maps are minimized at the transition layers. If a dense block has c feature maps, then the transition layer computes $\lfloor \theta c \rfloor$ output feature maps. $0 < \theta \leq 1$ is represented as a compression factor. If $\theta = 1$, then the size of feature maps through the transition layer stays constant.

DenseNet contains four dense blocks. Each dense block contains an equal number of layers. Initially, Conv with 16 output channels is implemented on the input images. For Conv layers having kernel size as 3×3, every side of the inputs is zero-padded to maintain the fixed-size feature map. 1×1 Conv is followed by 2×2 average pooling between two connecting dense blocks. Finally, a global average pooling is implemented, and a softmax activation function is used. The sizes of feature map sizes in dense blocks are 32×32, 16×16, and 8×8, respectively. The DenseNet with configurations $\{N = 40, J = 12\}$, $\{N = 100, J = 12\}$, and $\{N = 100, J = 24\}$ are computed. The size of the input image is 256×256. Conv layer has $2J$ convolution having a size 5×5 and stride as 2.

The exact network configurations and other hyper-parameters of the DenseNet are tuned using $\theta - \text{NSGA} - \text{III}$.

2.2. θ-Nondominated Sorting Genetic Algorithm-III θ NSGA-III [21] has been extensively utilized to optimize many engineering applications. It has achieved good convergence speed, and it does not suffer from the premature convergence issue [22–24].

Table 1 represents the nomenclature of θ NSGA-III. Algorithm 1 illustrates the generation of an initial population of θ NSGA-III-based DCNN. Initially, a random population is computed by utilizing the normal distribution. The computed solutions are then mapped to the group of initial parameters of DCNN.

Algorithm 2 demonstrates the proposed θ NSGA-III-based DCNN model. Initially, we will test the DCNN by using the random population to train and test the model on the chunk of steganography dataset. The fitness of each solution is then obtained. Dominated and nondominated groups are then evaluated. Thereafter, mutation and crossover operations are used to compute the child solutions. Nondominated sorting is used to sort the obtained nondominated solutions. If the number of fitness evaluations exceeds the max allowed, then we return the tuned parameters of DCNN. Finally, θ NSGA-III-based DCNN is trained on the steganalysis dataset.

Table 1: Nomenclature of θ NSGA-III.

Symbol	Definition
κ	Optimal DCNN
E_t	Elite population
τ	Optimal layers
κ	Binary decision vector
τ	Permutation vector
α	Random variable $\in\in[0,1]$
$\mathscr{R}$	Group of τ', κ''
$\mathscr{K}$	Randomly group of solutions
ζ	Decompose random solutions to hyperparameters of DCNN

3. Performance Analysis

3.1. Dataset. Rezaei et al. [25] designed a reference dataset for image steganalysis. It is the so-called Real version 1 (STEGRT1), and it contains both JPEG and BITMAP images. It has 8000 cover and stego images with different sizes and characteristics. These images were obtained using various steganographic approaches such as payload and quality factors.

3.2. Experimental Set-Up. The experiments of the proposed and the existing models are drawn on MATLAB online server with the help of a deep learning toolbox. Additionally, to increase the size of the dataset, the BitMix data augmentation [26] is also implemented. The performance of the proposed model is compared with the HCNN [8], TREM [7], CNN [4], ELM [3], ECSM [5], and DRM [6].

3.3. Comparative Analysis. In this section, the comparison between the proposed and the existing CNN-based steganalysis models are presented.

Figure 2 shows the performance analysis of the proposed model. It is found that the best performance is found at epoch 8 and 47th iteration. Therefore, the proposed model converges efficiently with good convergence speed.

Figures 3 and 4 represent the confusion matrices obtained by using the proposed model with and without θ NSGA-III. It has been found that the majority of the obtained results lie in the true classes (i.e., in diagonal matrices). Therefore, it will lead to good performance results such as accuracy, f-measure, precision, recall, and area under the curve (AUC). In Figure 4, every diagonal value shows whether the corresponding class is true or false. It helps in evaluating the various performance metrics. Assume that stego-embedded image is our true class; it means the normal image belongs to the negative class. Overall, the analysis indicates that the proposed model with θ NSGA-III achieves better performance than without the use of θ NSGA-III.

Figures 5 to 9 show the comparative analysis between the existing and the proposed models. In these figures, the notched boxplots are shown. The box shows the interquartile range (IQR). Red line shows the median of the computed performance. Notch indicates a confidence interval around the median which is dependent upon the median $\pm$ interquartile range/sqrt of a number of experiments (n). Here, we have considered $n = 30$. If the size of a notch is smaller, then the steganalysis model achieves better results. To evaluate the significant improvement or reduction, we have selected the average computed values of the proposed model and one from the existing steganalysis models (i.e., showing a better average value among existing models). Thereafter, we evaluate their absolute difference. It computes the average mean improvement or reduction; to make it in percentage form, we divide the absolute difference by the maximum possible value and multiply the computed value by 100.

Figure 5 represents the comparison between the existing and proposed steganalysis models in terms of accuracy. It reveals that the proposed model achieves better accuracy than the existing steganalysis models. The proposed model outperforms the existing steganalysis models in terms of accuracy by 1.2643%.

Figure 6 represents the precision analysis among the proposed model and the existing steganalysis models. It is evaluated that the proposed model achieves consistent values of precision than the existing models. The proposed model outperforms the existing models by 1.1438%.

Figure 7 demonstrates the recall analysis of the proposed steganalysis model. It is observed that the proposed model outperforms the competitive models in terms of recall values compared to the existing models. The proposed model has shown an average enhancement in recall values by 1.2832%.

Figure 8 represents the f-measure analysis among the proposed model and the existing steganalysis models. It is

$\tau' \leftarrow$ Optimal number of layers.
$\tau'' \leftarrow \{\pi_1, \pi_s, \pi_{s-1}, \ldots, \pi_2\}$
$\kappa' \leftarrow$ Implement an optimal number of layers based on the DCNN model.
$\kappa'' \leftarrow \varnothing \mathscr{R} \leftarrow \{\zeta(\tau', \kappa''), \zeta(\tau'', \kappa'')\}$
while $z' = \varnothing$ do
$l \leftarrow$ Consider DCNN $l \in z'$ with maximum b_l/ω_l performance
$\kappa'' \leftarrow \kappa'' \cup \{l\}$
$\kappa' \leftarrow \kappa' \setminus \{l\}$
if (τ', κ'') is not dominated by (τ'', κ'') then
$\mathscr{R} \leftarrow \mathscr{R} \cup \{\zeta(\tau', \kappa'')\}$
else
$\mathscr{R} \leftarrow \mathscr{R} \cup \{\zeta(\tau'', \kappa'')\}$
end if
end while
$\mathscr{K} \leftarrow$ select a random group of $\alpha \times M$ solutions from $\mathscr{R}$ using a normal distribution
$\mathscr{L} \leftarrow$ compute a set of $(1-\alpha) \times M$ random solutions
$\mathscr{E}^{(0)} \leftarrow \mathscr{K} \cup \mathscr{L}$
return $\mathscr{E}^{(0)}$

Algorithm 1: Generate initial population.

$\widehat{E}_t \leftarrow$ elect randomly $0.2M_t$ solutions from the elite E_t
for all $b \in \widehat{E}_t$ do
$(\pi, z) \leftarrow$ decode b as initial parameters of DCNN
for $l \leftarrow 1$ to NR_π do
$\pi' \leftarrow$ compute DCNN with random initial parameters in π
if (π', z) is not dominated by (π, z) then
$(\pi, z) \leftarrow (\pi', z)$
end if
end for
if (π, z) is not dominated by any set in E_t then
$E_t \leftarrow E_t \cup \{\zeta(\pi, z)\}$
end if
for $i \leftarrow 1$ to NR_z do
$item \leftarrow$ select randomly an $item \in \{1, 2, \ldots, h\}$
if $item \in z$ then
$z' \leftarrow z \setminus \{item\}$
else
$z' \leftarrow z \cup \{item\}$
end if
if (π, z') is not dominated by any solution in E_t then
$E_t \leftarrow E_t \cup \{\zeta(\pi, z')\}$
end if
end for
end for
if $|E_t| > M_t$ then
$E_t \leftarrow$ select M_t solutions computed using θ NSGA-III
end if

Algorithm 2: θ-nondominated sorting genetic algorithm III-based DCNN model.

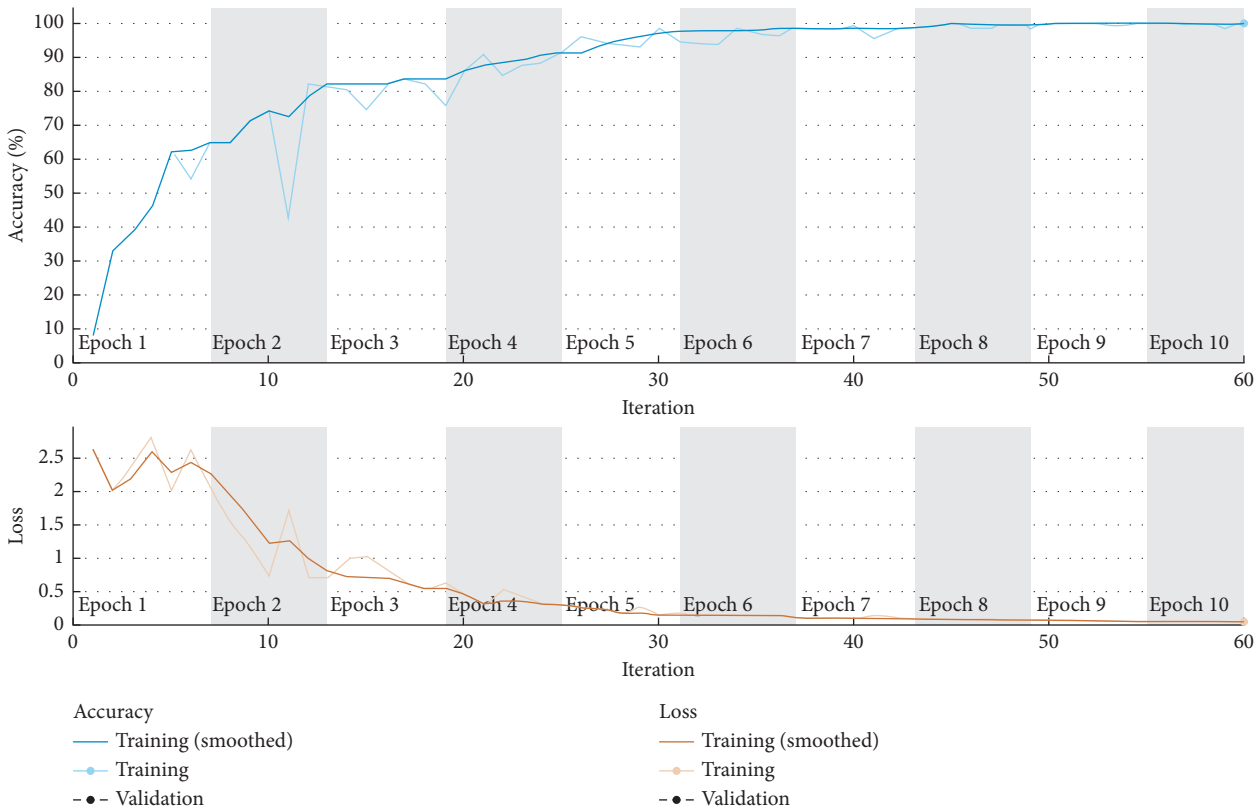


Figure 2: Performance analysis of the proposed model.

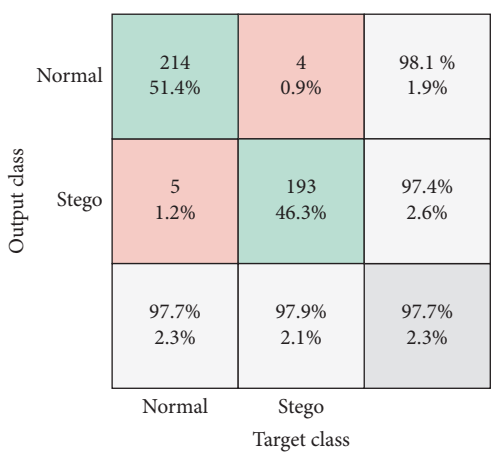


Figure 3: Confusion matrix of the proposed model without θ NSGA-III on steganalysis dataset.

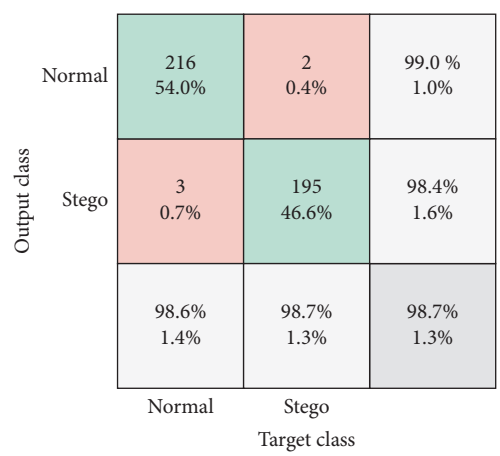


Figure 4: Confusion matrix of the proposed θ NSGA-III-based DCNN model on steganalysis dataset.

evaluated that the proposed model achieves consistent values of f-measure than the existing models. The proposed model outperforms the existing models by 1.0245%.

Figure 9 demonstrates the AUC analysis of the proposed steganalysis model. It is observed that the proposed model outperforms the competitive models in terms of AUC values compared to the existing models. The proposed model has shown an average enhancement in AUC values by 1.2913%.

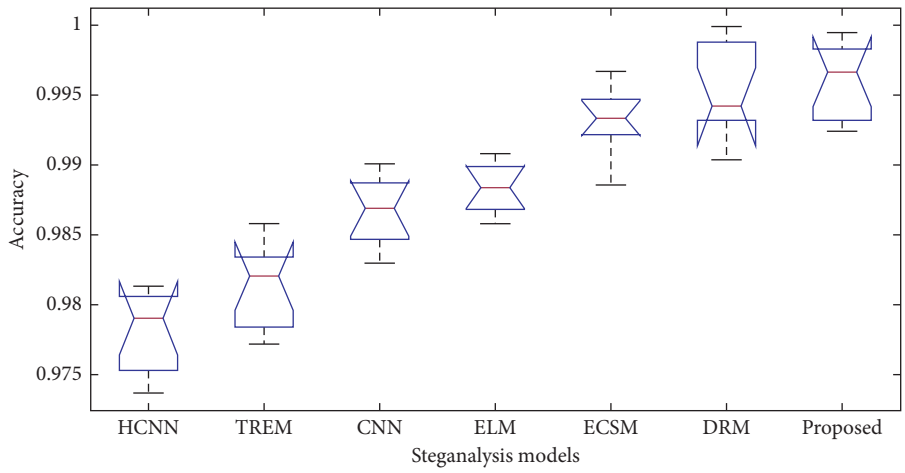


Figure 5: Analysis of accuracy.

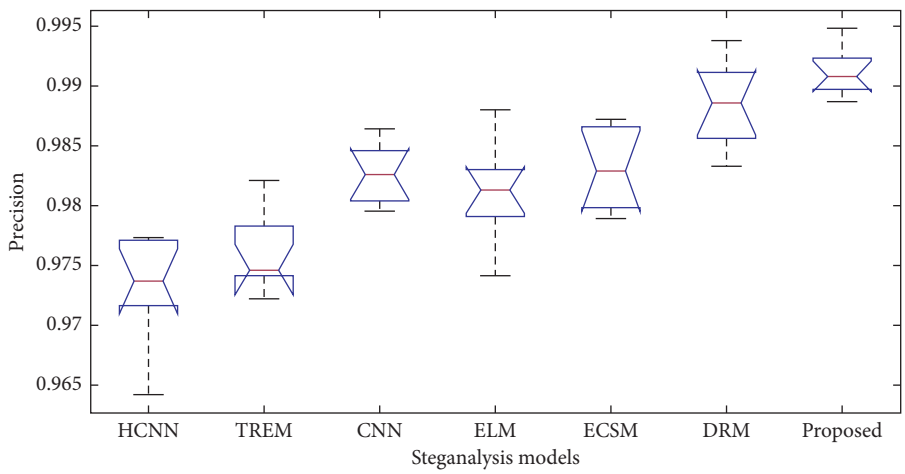


Figure 6: Analysis of precision.

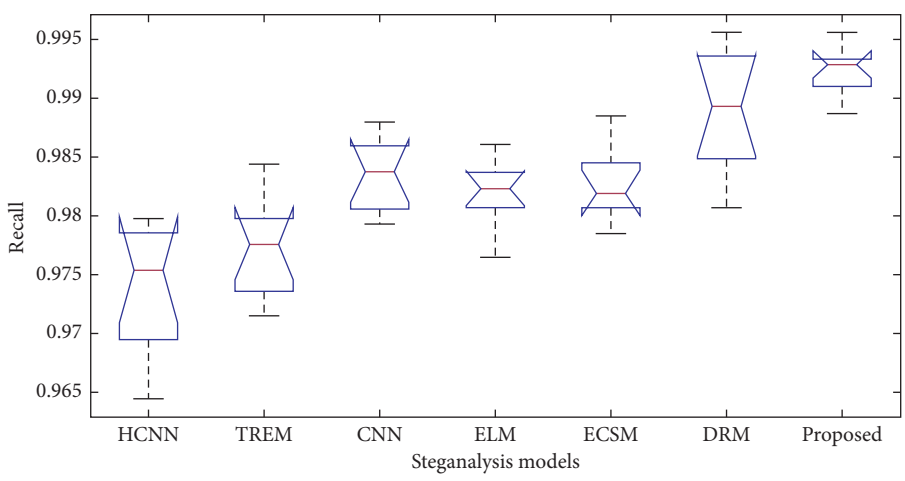


Figure 7: Analysis of recall.

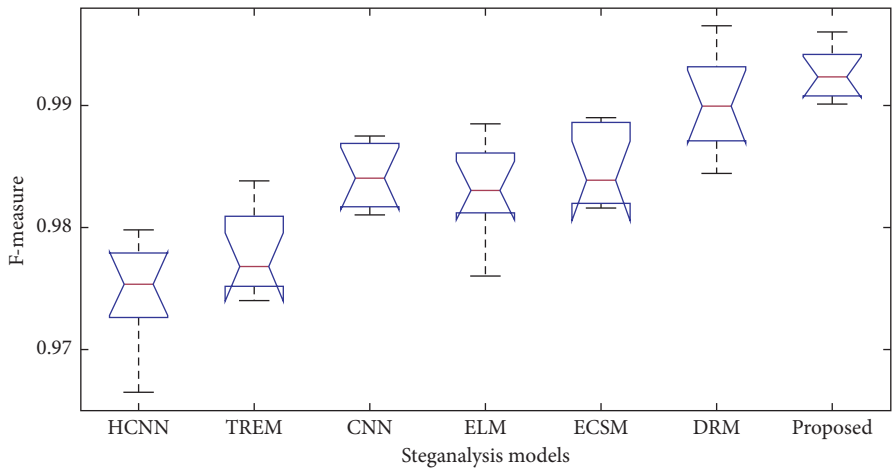


Figure 8: Analysis of f-measure.

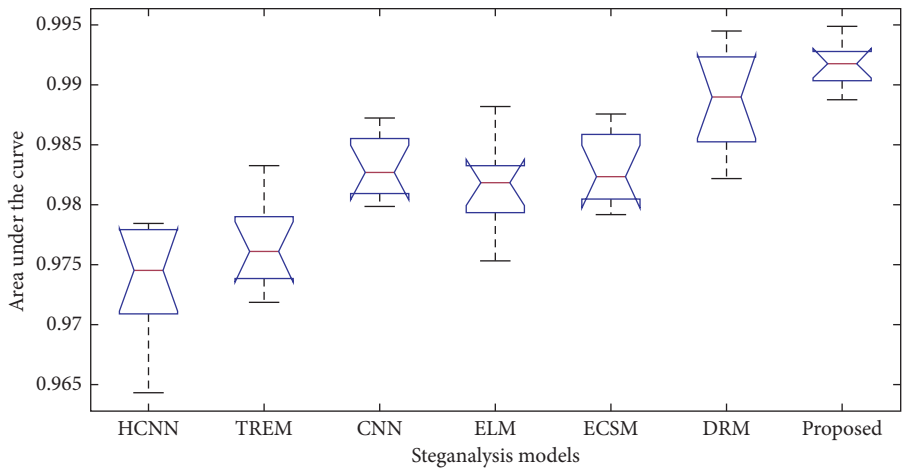


Figure 9: Analysis of area under the curve.

4. Conclusion

From the extensive review, it has been found that deep learning-based models have been extensively utilized for steganalysis. However, these models suffer from overfitting and hyperparameter tuning issues. Therefore, θ NSGA-III based DCNN model was proposed for image steganalysis. θ NSGA-III was utilized to optimize the initial parameters of DCNN model. The accuracy and f-measure were utilized to design a multiobjective fitness function. Extensive experiments were drawn on STEGRT1 dataset. Comparison of the proposed model was also drawn with the competitive steganalysis model. Performance analyses have shown that the proposed model outperforms the existing steganalysis models in terms of accuracy, f-measure, precision, recall, and AUC by 1.2643%, 1.0245%, 1.1438%, 1.2832%, and 1.2913%, respectively. The results show that the proposed model can record even little changes in image features.

In the near future, one may extend the proposed work by designing a novel deep learning model to enhance the results further. Additionally, one may test the proposed model on other steganography datasets.

Data Availability

No data were used to support this study

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research work was funded by Institutional Fund Projects under grant no (IFPRC-027-135–2020). Therefore, authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, Jeddah, Saudi Arabia.

References

[1] S. Tan, W. Wu, Z. Shao, Q. Li, B. Li, and J. Huang, "Calpa-net: channel-pruning-assisted deep residual network for steganalysis of digital images," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 16, no. 131–146, 2021.

[2] S. Ozcan and A. F. Mustacoglu, "Transfer learning effects on image steganalysis with pre-trained deep residual neural network model," in *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data)*, pp. 2280–2287, Seattle, WA, USA, December 2018.

[3] Z. Zhou, S. Tan, J. Zeng, C. Han, and S. Hong, "Ensemble deep learning features for real-world image steganalysis," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, no. 11, pp. 4557–4572, 2020.

[4] R. Zhang, F. Zhu, J. Liu, and G. Liu, "Efficient feature learning and multi-size image steganalysis based on cnn," 2018, https://arxiv.org/pdf/1807.11428.pdf.

[5] S. N Gowda and C. Yuan, *Stegcolnet: steganalysis based on an ensemble colorspace approach*, https://arxiv.org/abs/2002.02413, 2020.

[6] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1181–1193, 2018.

[7] M. Yedroudj, F. Comby, and M. Chaumont, "Yedroudj-net: an efficient cnn for spatial steganalysis," in *Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2092–2096, IEEE, Calgary, AB, Canada, April 2018.

[8] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017.

[9] S. Wu, S. Zhong, and Y. Liu, "Steganalysis via deep residual network," in *Proceedings of the 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 1233–1236, Wuhan, China, December 2016.

[10] J. Yang, Y.-Q. Shi, E. K. Wong, and X. Kang, "Jpeg steganalysis based on densenet," 2017, https://arxiv.org/pdf/1711.09335.pdf.

[11] B. Li, W. Wei, A. Ferreira, and S. Tan, "Rest-net: diverse activation modules and parallel subnets-based cnn for spatial image steganalysis," *Institute of Electrical and Electronics Engineers Signal Processing Letters*, vol. 25, no. 5, pp. 650–654, 2018.

[12] R. Zhang, F. Zhu, J. Liu, and G. Liu, "Depth-wise separable convolutions and multi-level pooling for an efficient spatial cnn-based steganalysis," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 15, pp. 1138–1150, 2019.

[13] A. Sharma and S. K. Muttoo, "Spatial image steganalysis based on resnext," in *Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT)*, pp. 1213–1216, IEEE, Chengdu, China, June 2018.

[14] K. Liu, J. Yang, and X. Kang, "Ensemble of cnn and rich model for steganalysis," in *Proceedings of the 2017 International Conference on Systems, Signals and Image Processing (IWSSIP)*, pp. 1–5, IEEE, London, UK, March 2017.

[15] J. Zeng, S. Tan, B. Li, and J. Huang, "Pre-training via fitting deep neural network to rich-model features extraction procedure and its effect on deep learning for steganalysis," *Electronic Imaging*, vol. 2017, no. 7, pp. 44–49, 2017.

[16] J. Yang, K. Liu, X. Kang, E. Wong, and Y. Shi, "Steganalysis based on awareness of selection-channel and deep learning, digital forensics and watermarking," in *Proceedings of the International Workshop on Digital Watermarking*, pp. 263–272, Springer, Jeju Island, Korea, October 2017.

[17] L. Yang, M. Men, Y. Xue, J. Wen, and P. Zhong, "Transfer subspace learning based on structure preservation for jpeg image mismatched steganalysis," *Signal Processing: Image Communication*, vol. 90, Article ID 116052, 2021.

[18] W. Ren, L. Zhai, J. Jia, L. Wang, and L. Zhang, "Learning selection channels for image steganalysis in spatial domain," *Neurocomputing*, vol. 401, pp. 78–90, 2020.

[19] A. Cohen, A. Cohen, and N. Nissim, "Assaf: advanced and slim steganalysis detection framework for jpeg images based on deep convolutional denoising autoencoder and siamese networks," *Neural Networks: The Official Journal of the International Neural Network Society*, vol. 131, pp. 64–77, 2020.

[20] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4700–4708, Honolulu, HI, USA, July 2017.

[21] Y. Yuan, H. Xu, B. Wang, and X. Yao, "A new dominance relation-based evolutionary algorithm for many-objective optimization," *Institute of Electrical and Electronics Engineers Transactions on Evolutionary Computation*, vol. 20, no. 1, pp. 16–37, 2015.

[22] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-iii based 4-d chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[23] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7d hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.

[24] M. Kaur, D. Singh, V. Kumar, and K. Sun, "Color image dehazing using gradient channel prior and guided l0 filter," *Information Sciences*, vol. 521, pp. 326–342, 2020.

[25] M. Rezaei, M. Riahi, and H. Hayati, "Stegrt1: a dataset for evaluating steganalysis systems in real-world scenarios," in *Proceedings of the 2020 28th Iranian Conference on Electrical Engineering (ICEE)*, pp. 1–5, IEEE, Tabriz, Iran, August 2020.

[26] M. Yedroudj, M. Chaumont, and F. Comby, "How to augment a small learning set for improving the performances of a cnn-based steganalyzer?" *Electronic Imaging*, vol. 2018, no. 7, pp. 317–321, 2018.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 6664426, 19 pages
https://doi.org/10.1155/2021/6664426

Research Article

Next-Generation Digital Forensic Readiness BYOD Framework

Md Iman Ali [1] **and Sukhkirandeep Kaur** [2]

[1]*Department of Computer Application, Lovely Professional University, Phagwara, Punjab, India*
[2]*Department of CSE, Lovely Professional University, Phagwara, Punjab, India*

Correspondence should be addressed to Md Iman Ali; mdiman@rediffmail.com

Received 31 December 2020; Revised 21 January 2021; Accepted 4 February 2021; Published 22 March 2021

Academic Editor: Manjit Kaur

Intel's "Bring Your Own Device" (BYOD) adoption quickly became popular as an alternative workplace solution strategy. It enables employees to use their personally owned devices to perform business activities, leading to increased productivity and employee satisfaction. However, BYOD also brought associated risks because of exponential growth in the number of cybersecurity incidents due to which business ecosystem gets disrupted and fragmented. Although several methods and mechanisms have been developed and adopted to mitigate the risk associated with BYOD, they still represent a challenge as corporate network gets exposed to inherent threats caused by the BYOD threat landscape. This work demonstrates especially two key aspects: The first focuses on how to detect and protect BYOD environment from an advanced level attack which cannot be detected by traditional tools and techniques even though available tools are quite effective. Before the attack and damage to the critical infrastructure due to BYOD threat, a strategy was indeed the key requirement for detecting attacks and protecting the environment. The second part of the research focuses on conducting forensic investigation model and developing a new approach by providing a reliable forensic investigation infrastructure to find digital evidence and detect the source of attack. This research work concluded with two different novel strategic ideas. The first part contributes to a new method of detecting and protecting against malicious activities which cannot be otherwise detected and protected by traditional security technology like IPS, IDS, AntiBot, or AntiVirus. The proposed technique compared to the existing methods led to a significant contribution to the identification of threats before an attack takes place. The second part of the research contributes to the defining of a new approach of the next-generation digital forensic readiness (NG-DFR) model in order to build a cyber forensic ecosystem so that cyber secured BYOD environment can be enabled safely.

1. Introduction

Bring Your Own Device (BYOD) is basically the consumerization of information technology (IT) where employees use their personal devices in the corporate networks. It helps the organization to save the cost and increases employee productivity and engagement. Adopting BYOD technology in enterprise leads to an increase in business productivity and enhances collaboration and business agility.

Bring Your Own Device (BYOD) becomes a rule rather than an exception. Technology transformation is the key role of every CIO and IT leader of any organization. As per the study of Gartner, BYOD users will get increased by 75% by 2022 [1] from 35% in 2018. By 2021 [2], maximum organizations are expected to use IoT; approximately 94% of the organizations will adopt IoT as per Microsoft report. During the COVID-19 global pandemic situation, demand for BYOD has even increased exponentially.

The BYOD infrastructure provides Internet access to the employees, while employees being trusted users access the enterprise infrastructure, which is intended to be secured. Guest user access is also one of the features of BYOD to provide access to the visited partner/guest using the self-registration portal or sponsored portal. During the initial stage of the BYOD solution adoption, most of the organizations did not give access through corporate network due to involved security risks. However, in the later stage, organizations started moving towards a positive direction

realizing that personal mobile devices are an integral part of employees' daily life. As BYOD connects untrusted external devices in the corporate wireless network infrastructure, increase in cybersecurity risks and data leakage incidents are observed. Malicious activities can be performed using BYOD. Unmanaged devices might not be following the standard security practice and may not follow the line of defense against malicious content [3]. A study concluded that 62% of digital incidents are triggered by inside users either intentionally or unknowingly [4]. Using BYOD services, users can try to get access to internal network and cloud network, and perform malicious activities, and damage the potential data which can cause the reputation loss of the organization. Data theft, shadow IT, and cybersecurity constitute a major concern in BYOD. Installing malware in BYOD and connecting to the Internet can also lead to serious damage and are a major security risk. While implementing the BYOD legal approach of the mitigation cannot be overlooked [5], every stage of the BYOD security policy should be always in line with protecting the internal network, data, and application. BYOD system has become a huge security risk [6]. Accessing corporate infrastructure using BYOD devices which may be owned by employees, suppliers, or partners makes corporate data protection a major concern for the organization; at the same time, isolating personal data is a need for employee privacy. In a study, the BYOD security impact assessment conducted for the airport smart system stated that compromised BYOD devices can have an impact on airport system integrity and availability [7]. Security breaches are more in terms of the network infrastructure where BYOD service is offered to employees, partners, and staff.

Cyberattack and security risk in airport security is a major risk of the country [8] due to BYOD. BYOD might become "bring your own danger" [9] if proper security control is not implemented and if the solutions do not include forensic investigation after crime.

Due to vulnerability, cyber-attacks have grown periodically. According to CVE [10], Figure 1 represents the growth of vulnerabilities in years. Increase in vulnerability has also increased the attacks.

DFR (digital forensic readiness) in BYOD infrastructure is one of the models that detect attackers' activities and behavior using honeypot, a deception technology. Extensive research has been conducted to improve the approach of DFR and CTI (cyber threat intelligence) to conduct a digital forensic investigation and to reduce the time and cost. Up to 90.73% [11] accuracy level was achieved in analyzing the root cause after an incident.

According to Juniper Survey, 80% of BYOD devices will be unprotected. There is a need for digital forensic infrastructure in BYOD technology to provide security. Lack of a proactive security model in BYOD architecture can cause digital forensic investigation. A large-scale clustering deployment of BYOD infrastructure needs an advanced model of digital forensic readiness infrastructure for the practice of detection and investigation [12].

Internet users are increasing exponentially by using IoT/BYOD in every organization, public environment, and smart city environment. Cyberterrorism is defined as the intentional use of a computer or network communication device using public networks to destruct the critical public and private infrastructure for personal objectives which may be political or ideological. The government and public/private sector must gear up to fight against this major crime. Cybercrime rates are also exponentially growing, and this is a challenging area to handle and investigate after an incident. Government of India has taken an initiative to enhance the infrastructure of the National Cybercrime Forensic Laboratory (NCFL) and started a new project called Cyber Prevention, Awareness & Detection Centre (CyPAD) as stated by Union Home Minister on the 18th of Feb 2019 [13]. Union Home Minister has pointed out that cybercrime has become a big challenge to handle. Different questions arise: How governments or private organizations will handle such big cyber forensic investigation and cyber fraud management in smart city environment where IoT users are in large numbers or BYOD users are increasing every day? Who will do this investigation? How those crimes will be handled? How to get the crime activity logs of BYOD/IoT users?

These questions can be addressed by developing and implementing a cyber secured BYOD infrastructure. After an attack, there is a need for forensic investigation in BYOD. Major components in digital forensic investigation are [14]

Computer forensic

Network forensic

Database forensic

Mobile forensic

Digital forensic or cyber forensic will ideally include the components [15] (a) humans, (b) digital evidence, and (c) process, which act as a reference point. After a cyber-attack analysis, event reconstruction, with reproducible and verifiable results, is an inline requirement for legal action in digital forensic investigation [16]. BYOD has all those components to be covered in forensic investigation. Threat finding after an incident and source of attack [8] finding are requirements in forensics; for example, a novel study was conducted for identifying human behavior in an automated way based on handwriting [17].

On the other hand, the cloud adoption rate is expected to be 83% by 2020 [18]. This increased rate of cloud adoption has increased the demand for BYOD at a much larger rate. All organizations are adopting cloud services for different applications and roaming user services, since the increased demand for working anywhere by any device has increased the BYOD demand. At the same time, BYOD security and cyber forensic investigation from enterprise network and cloud network are important concerns that need to be taken care of.

There is a serious need for BYOD forensics as BYOD devices are the most critical component in forensics and the source of evidence [19]. Due to the increased cyber incident

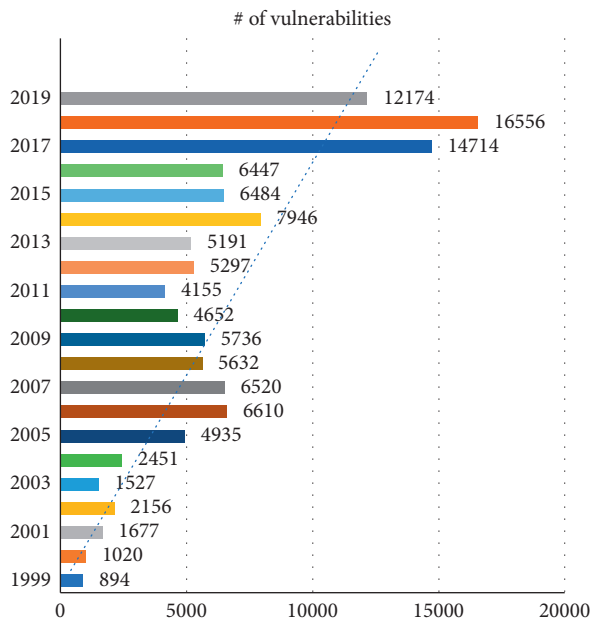


Figure 1: Vulnerabilities by year (CVE).

landscape, collecting, preserving, and analyzing digital evidence after an incident and presenting the analysis with integrity are required.

This paper is organized as follows: Section 2 discusses the related work, followed by design and methodologies in Section 3 and then results in Section 4. Comparison and analysis are provided in Section 5. The proposed new model of NG-DFR is explained in Section 6. Section 7 concerns NG-DFR model ecosystem. The discussion is covered in Section 8, contributions of the research in Section 9, future research areas in Section 10, and conclusion in Section 11.

2. Related Work

Most of the research in this area is conducted from the Golden Age of digital forensics (1997–2007) till today, which is not sufficient to complete the analysis as there was a need for a standard, modular [20] approach to digital forensic. Since new technologies are adopted, the deployment approach is also changing and there is no single mitigation technique [21] as methods of attacks keep on changing. Therefore, continuous evolvement in forensic technology is required as stated in a study by Deloitte [22]. There is no single agreed upon digital forensic process that has been developed [23]. Some of the existing methods and techniques are listed below.

2.1. Honeypot Technology. Deception technology honeypot has been explored to detect threats in BYOD infrastructure in 2016. This opens the way for doing root cause analysis after an incident [12]. An improved extended study of a generic digital forensic readiness model for BYOD using honeypot technology [12] was again conducted in 2019 where a Threat Intelligence Platform is used to detect the incident, and accuracy has been analyzed [11]. Using audit logs of malicious activities collected from the Threat Intelligence Collector, accuracy has been analyzed and found to be 90.73%, 96.16%, and 93.71% [11]. Subsequently, honeypot was integrated with cyber risk management process of five preparedness mission areas of FEMA (Federal Emergency Management Agency) [24].

2.2. Cryptographic Blockchain Method of Forensics. The cryptographic blockchain authentication process has been studied where the record-keeping system has been used for secure authentication of BYOD users. Evidence collection for forensic investigations has also been covered using records [25]. Furthermore, the digital method of record-keeping systems has been used for the multifactor authentication process [25]. This ledger makes an easier way to conduct digital evidence investigation after the crime/malicious activity, for example, image haze removal technique [26], forward mechanism, or reverse mechanism in dual-tree complex wavelet transform (DTCWT) [27]. Using advanced intrusion detection and distributed ledger technology in the IoT environment by identifying malicious activity and finding the source of the attack, storing the digital evidence is explored so that digital evidence can be collected to conduct a digital investigation [28].

2.3. STRIDE Based Threat Model. STRIDE [29] based BYOD threat model is proposed and analyzed threat interaction in BYOD. BYOD internal and external threat interaction with the corporate network are analyzed so that security and forensic threats in BYOD can be understood. Reverse adoption of encryption using the Group Encrypted Transport VPN (GETVPN) method of BYOD traffic was a novel approach to detecting malicious activities and to reducing threats. Therefore, the forensic analysis mechanism was analyzed for internal and external traffic threats [30].

2.4. Smart City IoT Cloud Data Security Forensics. Data security on the cloud is also an important aspect to be considered as stored data in the cloud does not have enough control. Since cloud data is not an enterprise control data center, so data accessed by unauthorized entities is a risk. Data integrity is an important parameter for postincident forensic analysis. Forensic analysis and finding out the root cause constitute the important view that has been highlighted. Artificial intelligence is also one of the major areas that have been pointed out in this study. The identification of security threats is studied in [31].

2.5. IoT Mobile Forensics. Smartphone IoT devices traces were used to find the logs of the incident for forensic investigation. Extracting the logs from IoT devices and analyzing logs captured with Wireshark for finding out digital evidence constituted one of the approaches [32]. Using smartphone devices, collecting the stored logs from the smartphones, and reconstructing the event of crime are very useful case studies done in DFRSW (Digital Forensic Research Workshop). Retrieving the information from digital

IoT devices and analysis of using multiple tools like Wireshark [33] were important findings of digital evidence of the crime [34].

2.6. Integration of Digital Forensics and Forensic Science. The task of collecting digital evidence from a dynamic IoT environment is very complex. Due to a lack of proper tools and techniques, the process becomes very challenging [35]. An important study was conducted regarding the integration of different forensic sciences to build a smart ecosystem of forensic science [36]. While various mechanisms are implemented to reduce security attacks, in some cases image processing reduces the computation speed which has also been addressed in the nondominated genetic algorithm [37]. A powerful digital forensic ecosystem can be created in case of a collaborative effort of different tools, technologies, and cyber laws, and forensic experts can integrate all together.

As per an IBM study in 2018, 77% of organizations do not have a consistent cybersecurity incident response plan (CSIRP) [38], even after the General Data Protection Regulatory (GDPR) has been in effect since May 2018 [39]. On average, it takes 23.6 hours [40] to address cybercrime aftermath. This indicates that there is a serious need for advanced level cybersecurity response systems, cyber defense mechanisms, and cyber forensic mechanisms.

If BYOD cyber forensic mechanism can be developed in such a way that the incident can be analyzed to detect the crime with sufficient evidence, then BYOD cyber forensic ecosystem can be a more reliable environment for the organization.

This study has shown a flagrant result of BYOD malicious activity forensic analysis which can be helpful for organizations to implement cyber defense and cyber forensic ecosystem in the BYOD environment.

2.7. Wireless Drone Forensic Readiness Model. The wireless forensic readiness model was explored with a dedicated forensic server with drone architecture in the year 2011. Packet decryption and Wireshark analysis were done to identify the attack [41], and the collection of digital evidence was explored. After collection of logs, analysis of wireless LAN traffic using NetWitness [23] was another approach explored to conduct a digital forensic investigation.

As discussed above, a different BYOD cyber forensic model has been explored in various tangents, but due to exponential increase of cyber-attack tools and technology, there is a definite need for further development in this area. Hence, the objective of this research is to first secure the BYOD infrastructure using traffic encryption and second develop BYOD forensic investigation using Check Point SandBlast.

3. Cyber Forensic Model: NG-DFR

3.1. High-Level Digital Forensic Readiness BYOD Model. This section presents a high-level digital forensic readiness model. An advanced level of the next-generation digital forensic readiness model is projected. This study has been conducted to detect the cyber-attack, protect infrastructure from threat, and develop a postincident forensic investigation process. As honeypot technology for digital forensic readiness (DFR) [12] is not sufficient and large-scale evidence finding technique was required, the deception technology has been used for digital forensic readiness. As the components of digital forensic or cyber forensic investigation include [15] (a) humans, (b) digital evidence, and (c) process, the model of the advanced digital forensic model needs to include all these parameters. After an incident, finding the threats and tracing the source of attack [8] become a major requirement, and prediction of future attacks based on the current attack is also important, for example, in an engine where future flow demands are based on the current flow [42]. Major components included in this study are represented in Figure 2.

DFR model includes people, process, technology, digital forensic infrastructure, and law enforcement.

3.2. Detailed DFR Model Architecture. The architecture for BYOD in this study was done as per standard design. Multiple OEM products are used. Initially, the BYOD setup was implemented for normal Internet access using the corporate wireless infrastructure.

The same wireless infrastructure is used for corporate wireless and BYOD services. Identity Service Engine [43] was used for authentication and back-to-back user identity was used as Microsoft Active Directory. Table 1 shows the components used during the research.

Components used for testing authentication traffic between branch locations and a central location are represented in Table 2, followed by additional forensic/investigation components used during the research for threat hunting and analysis in Table 3.

3.2.1. Implementation of BYOD Architecture. BYOD architecture was established to initiate the traffic from 2 different sources.

The first category of the BYOD traffic is mentioned in Table 4.

In this research, we conducted 2 different scenarios of BYOD forensic traffic analysis.

(a) Scenario 1. Analysis with Check Point SandBlast: Figures 3 and 4 show BYOD architecture and overall traffic flow with sandblasting as a forensic analysis mechanism.

The index used in Figure 3 for the demonstration is mentioned in Table 5.

(b) Scenario 2. Analysis with Palo Alto Forensic Cortex and cloud instance for BYOD forensic analysis: In this scenario, we conducted an analysis of BYOD forensic traffic with Palo Alto Cortex.

Figure 4 shows additional components used in the test.

The additional components used in the second scenario are presented in Table 6.

During the research in the second scenario, additional components used for BYOD traffic forensic analysis are Cortex of Palo Alto network and Palo Alto 820 as threat prevention, and also Palo Alto Cloud for threat management was used.

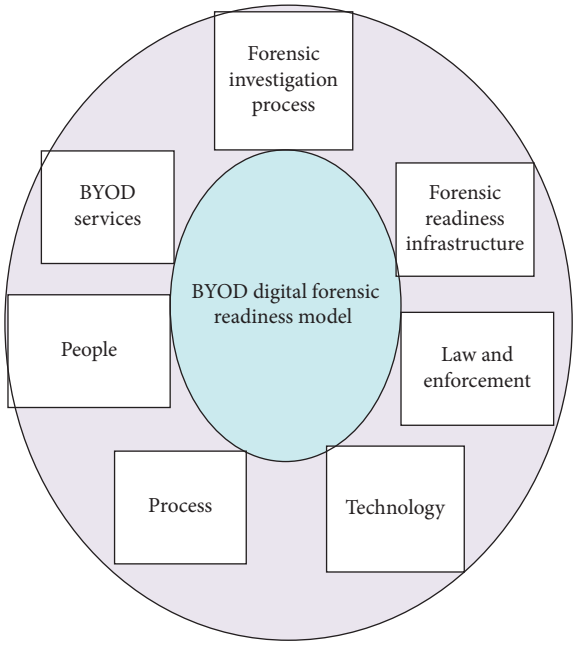


Figure 2: Digital forensic readiness (DFR) model components.

Table 1: Components used to set up the BYOD infrastructure.

Seq#	Product name	Make	Model	Usage
1	ISE (Identity Service Engine)	Cisco	SNS-3495-K9	AAA server
2	Internal firewall	Cisco	ASA5516-FPWR-K9	DMZ firewall
3	Access point	Cisco	AIR-AP4800-D-K9	Access point
4	External firewall	Check Point	CPAP-SG4400-NGFW	External firewall
5	Anchor controller	Cisco	AIR-CT5520-K9	BYOD guest controller
6	Foreign controller/mobility controller	Cisco	C9800-40-K9	Master wireless controller
7	Active Directory	Microsoft		For user database
8	Router	Cisco	ISR 4431	Routing
9	BYOD devices	Different mobile, laptop	Android/iPhone	Testing BYOD devices
10	Internal network endpoint	Lenovo	Laptop	For trusted zone device
11	Log management	Check Point	CPAP-SM225	For traffic log management

Table 2: Components for BYOD traffic.

Sl. no.	Components	Purpose
1	MPLS connectivity	Traffic flow from branch to central location
2	Internet link	BYOD Internet traffic exit

Table 3: Components used for forensic traffic analysis.

Sl. no.	Forensic components	Use
1	ISE	For authentication logs
2	Check Point Forensic Blade	For forensic traffic analysis
3	Check Point SandBlast	For threat hunting
4	Wireshark	Logs analysis

3.2.2. Authentication Mechanism and Onboarding Process of BYOD Users. Authentication and onboarding secured mechanism is used with certificate-based authentication [43]. During the study, for authentication procedures and traffic flow for authentication, ports are allowed on the DMZ firewall.

Table 4: BYOD traffic source/destination.

Sl. no.	Source	Destination	Description
1	Local BYOD users	Internet	Without MPLS network
2	Remote branch BYOD traffic	ISE for authentication	Across MPLS network

The ports opened on the DMZ firewall during the study index 6 (Figures 3 and 4) for communication purposes of BYOD management traffic are listed in Table 7.

3.2.3. Cyber Defense Ready BYOD Infrastructure. The proactive approach of implementing BYOD was followed so that malicious activities can be detected and protected against to reduce the threat and risk. Implementing

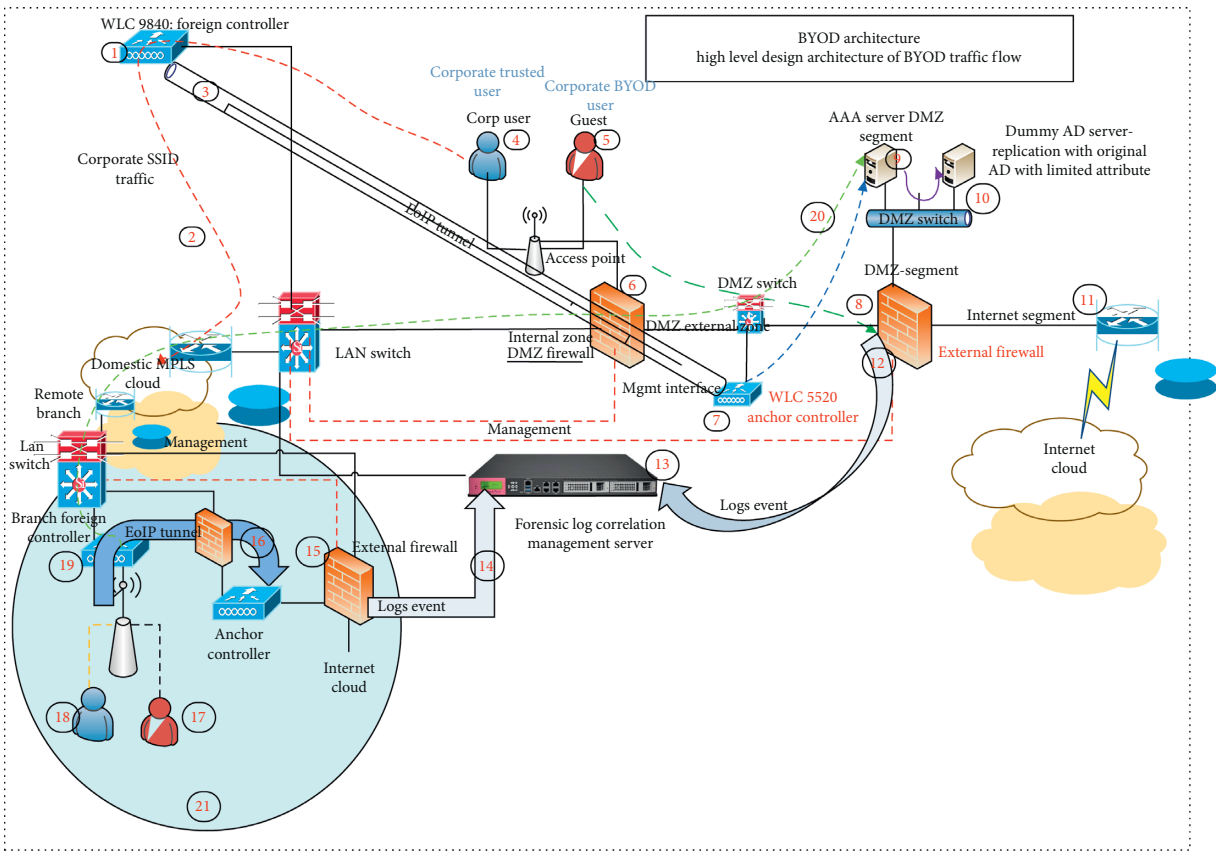


Figure 3: High-level BYOD traffic flow architecture.

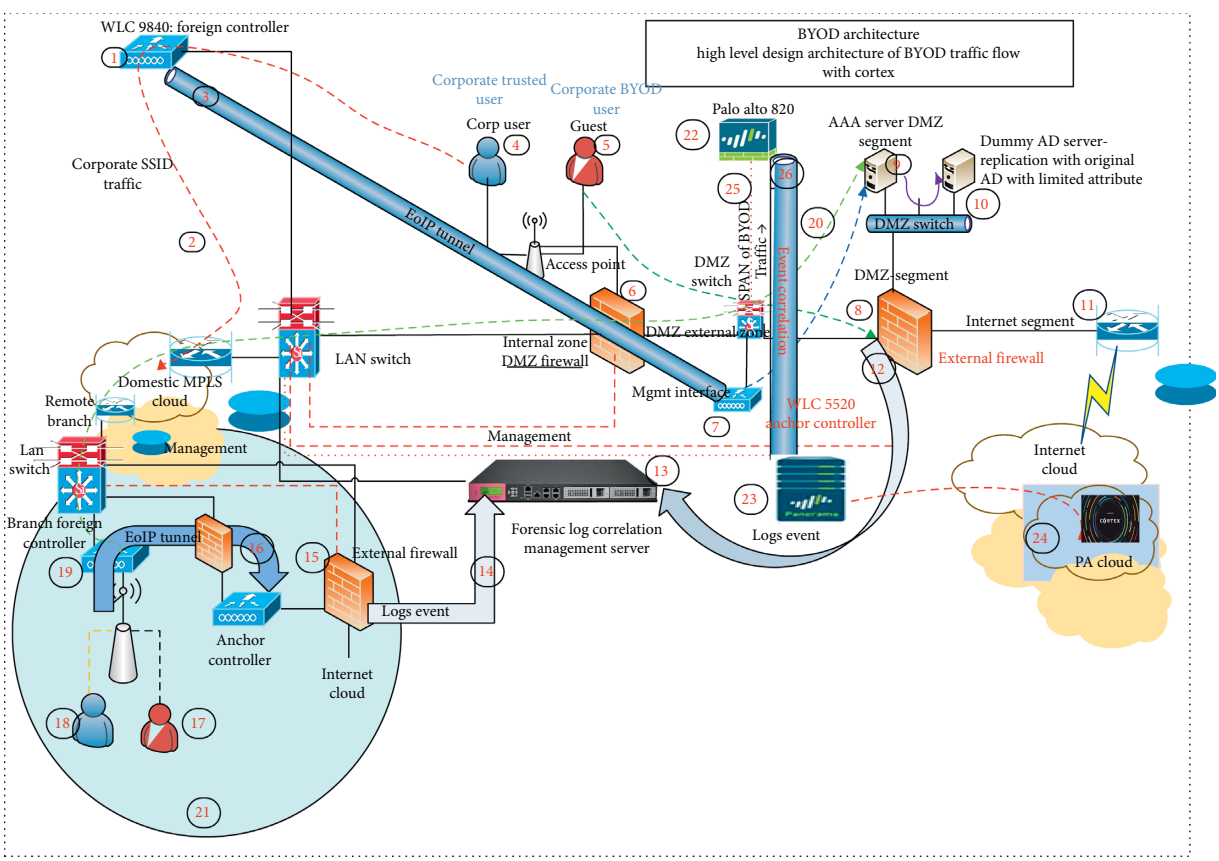


Figure 4: BYOD architecture with Palo Alto Cortex.

Table 5: The index used in Figure 3.

Index	Description
1	Wireless LAN controller
2	Authentication traffic from branch to AAA server
3	Ethernet over IP (EoIP) tunnel between foreign controller and anchor controller
4	Corporate users (non-BYOD)
5	BYOD untrusted users
6	DMZ segregation firewall
7	Anchor controller (guest controller)
8	External firewall
9	AAA (authorization, authentication, accounting) server for BYOD authentication
10	Active Directory for user identity
11	External Internet router
12	Traffic logs from gateway to management server for activity logs
13	Management server (log management)
14	Traffic logs from branch to central management server
15	Branch external firewall
16	EoIP tunnel
17	Branch BYOD users
18	Branch trusted users
19	Branch foreign controller
20	Authentication traffic from branch to central site AAA server
21	Branch/remote location

GETVPN for segregation and encryption of authentication traffic reduced the number of threats over MPLS [44]. Traffic was encrypted and segregated using GETVPN over MPLS which reduced the initial risk of the infrastructure and protected internal infrastructure.

3.2.4. Forensic Readiness BYOD Implementation. We have conducted a two-phase study and, during the first phase of the study, we have used Check Point SandBlast for threat hunting mechanism, threat emulation, and forensic investigation [45]. SandBlast is implemented on the Check Point management server. For the forensic investigation, we have also used a forensic module of Check Point to find the source of attack and logs of malicious activity. Clustering of multiple gateways was used to conduct crime analysis for large-scale deployment for correlated view [12].

During the second phase of the study, we have used Palo Alto Cortex which is an AI-based security platform for cyber defense mechanisms and Palo Alto Firewall for capturing BYOD threat traffic and analysis as well as Panorama for management and reporting.

4. Results

After implementation of the BYOD digital forensic infrastructure, we have captured and analyzed the results. The results have been also compared, and significant advancement of cyber defense mechanisms in BYOD forensic has been observed. The clustering approach implementation shows multiple incidents and malicious activities. The malicious activity was also captured using Wireshark logs, and it was analyzed [33]. The malware was created to test the malicious activity, a postincident forensic investigation was conducted, and the result was captured.

4.1. Detection of Critical Attack in BYOD and Forensic Analysis

4.1.1. Critical Attack View. Based on the analysis and detection of malicious activity conducted in a BYOD environment, Figure 5 represents the resultant forensic analysis of a critical attack. This was captured on the endpoint using Check Point SandBlast tool. The attack happened and was captured as Process ID 9232 was an attack in nature, and after entry of the malware, file was renamed and deleted in the BYOD environment.

The malicious activity was performed intentionally, the result was captured, and it was observed that Trojan which tried to damage the system in the BYOD environment was detected. It tried to damage the critical infrastructure.

4.1.2. Critical Attack View from Forensic Analysis View of Cortex. Similarly, from Palo Alto Cortex, attack information was captured and analyzed. After attack in the BYOD infrastructure, the investigation was conducted to complete the analysis as per Figure 6.

The result from Cortex is clearly reflected in Figure 6.

4.1.3. Critical Attack Logs from Cortex. During the investigation, critical attack information was further analyzed with raw logs to track the source of the attack. Source IP address and destination are presented in Table 8.

The attack was from IP addresses 172.28.15.14, 172.28.3.220, and 172.28.1.164, which were used in the BYOD devices as internal IP addresses. During the investigation process, we clearly detected the user and malicious activities performed by the users. Sensitive and robust analysis was done so that manual conventional result can be compared with the simulated analytical result as to how analysis is done in a study of pressure relief [46].

Table 6: Index used in Figure 4.

Index	Description
22	Palo Alto 3020 as firewall for capturing BYOD traffic
23	PA event log management M-200
24	Palo Alto Cloud Cortex
25	The span of BYOD traffic going towards the Internet
26	Event log traffic towards Panorama

Table 7: DMZ firewall open ports for the testing.

Sl. no.	Firewall	Source	Destination	TCT/UDP port
1	DM firewall	Foreign controller	Anchor controller	EoIP tunnel port
2	DMZ firewall	Foreign controller	ISE	1812
3	DMZ firewall	BYOD user	DNS	53
4	DMZ firewall	BYOD user	ISE	8443
5	DMZ firewall	BYOD	AAA server	8907

Figure 5: Critical attacks in the BYOD environment captured.

This traffic was captured from the architecture of Figure 4 and index 23. The malicious traffic observed in Cortex and cyber defense system was built to prevent those attacks as well, which is shown in Table 5.

4.1.4. Forensic Analysis from BYOD Endpoint. After analysis of malicious activities from gateway level, the next level investigation was conducted from the endpoint after identifying the attack source from sandblasting. Threat emulation shows the absolute result of malicious activities by endpoint BYOD devices as illustrated in Figure 7.

The result shows that malicious activity was detected during the preauthentication of the BYOD users, with a preauthentication segment IP address (192.168.1.x). One of the phishing attack packets was captured after an attack, and the details of the attack are represented in Figure 8(a).

This packet has the source IP address 172.28.1.164, attack type was phishing attack, and also user identity was traced from the Cisco Identity Service Engine during the test as per Figure 3, index 9. User identity was identified after the attack. This result was captured after detection of the endpoint performing reverse analysis from SandBlast from gateway level. Logs were captured for forensic analysis case event type from BYOD gateway as per Table 9.

The logs of this attack were captured after an incident, and we conducted the analysis of the threat. The attack ID is a4640108-ce8b-af06-5dd7-9aa500050000. Traffic from 172.28.1.164 was an attack, and traffic was decrypted in the gateway level. Besides, as seen in the result, the system was "Windows 10.0 Enterprise Edition" and the "Gen.SB.exe" was detected in the system which accessed c:\\users\\imanali\\desktop\\340s.exe. Finally, Trojan was detected.

The mentioned threat landscape detail was captured.

Table 8: Attack traffic captured from index 23, Figure 4.

Alert Id	Timestamp	Host	Host IP	User name	Severity	Alert
Source	Action	Category	Alert Name		Description	
	Initiated By		Initiator CMD		Initiator	
signature	Initiator signer		Event Type		CGO name	
	CGO CMD		CGO signature		CGO signer	
	CID	Target process name		Target process CMD		
	Process execution signature			Process execution signer		
	Target process SHA256			File path	File MD5	File
SHA256	Registry data		Registry full key		Local IP	
	Local port	Remote IP	Remote port		Remote Host	
	App -ID	Excluded	Starred	External Id		
32	Dec 21st 2019 10:30:20			172.28.15.14		
	172.28.15.14			High	PAN NGFW	
	Detected (Raised An Alert)			Spyware Detected via Anti-		
Spyware profile		Threat ID #109000001			None	
(S u spicious DNS Query (vltwox7zl7h1wv.com))						
	N/A	N/A	Netw ork Event			
	N/A	N/A				N/A
	N/A					
		172.28.15.14		39830	4.2.2.2	53
		dns	False	False	4662551	
14	Dec 18th 2019 14:25:15			INDELTEST		
	172.28.1.164		imanali	High	XDR Agent	
	Prevented (Blocked)		Malware	Behavioral Threat		
	Behavioral threat detected			mcpatcher.exe		
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "					
	N/A	Solimba Aplicaciones S.L.			Process	
Execution			N/A	N/A		
		N/A	N/A			
				False	False	
	1c1392bc217411eab7a1507b9d62f9c8					
12	Dec 18th 2019 14:25:08			INDELTEST		
	172.28.1.164		imanali	High	XDR Agent	
	Prevented (Bloc ked)		Malware	Behavioral Threat		
	Behavioral threat detected			mcpatcher.exe		
	"""C:\Users \imanali \Downloads \mcpatcher.exe"" "					N/A
	Solimba Aplicaciones S.L.			Process Execution		
		N/A	N/A			
	N/A	N/A				
			False	False		
	1789333c217411ea8e44507b9d62f9c8					
9	Dec 18th 2019 14:18:39			INDELTEST		
	172.28.1.164		imanali	High	XDR Agent	
	Prevented (Blocked)		Malware	Behavioral Threat		
	Behavioral threat detected			mcpatcher.exe		
	"""C: \Users \imanali \Downloads \mcpatcher.exe"" "					N/A
	Solimba Aplicaciones S.L.			Process Execution		
		N/A	N/A			
	N/A	N/A				
			False	False		
	3007c51e217311ea9fad507b9d62f9c8					
1	Dec 18th 2019 12:46:58			172.28.3.220		
	172.28.3.220			High	PAN NGFW	
	Detected (Raised An Alert)			Spyware Detected via Anti-		
Spyware profile		Threat ID #109000001			None	
(Suspicious DNS Query (7cfr5a9yjm3p.n9aupi94u3yt.com))						
		N/A	N/A	Network Event		
		N/A	N/A			
	N/A	N/A				
			172.28.3.220		58380	
	4.2.2.2	53		dns	False	False
	3401539					

This was an artifact after BYOD threat analysis with different risk, attack, and forensic information.

4.1.5. BYOD Environment Cyberattack Category Analysis. During the research, the different types of attacks in BYOD environment were reviewed and categorized by risk and criticality. The attack categorization framework was analyzed. Different attack event was framed.

We have captured a total of 966 packets from Check Point for analysis with different risk severity. Based on risk, the categorization of the traffic analysis result is shown in Figure 9.

The attack categorization framework was captured as per MITRE ATT&CK as shown in Figure 10.

5. Comparison and Analysis of Existing Technology

After conducting the research comparison and analysis, our prime focus was to find out the uniqueness of this simulation. Results and outcomes were compared with the existing available model of the threat detection process. While existing methods and techniques are quite effective in detecting known threats and protecting known threats, DNS layer security mechanism is not enough to protect. As per Cisco research, 91% of the malware attacks are in DNS layer [47] while the majority of the organizations do not have a mechanism for detection and protection. For unknown threat portfolio, available solutions of sandboxing are effective, but since the threat landscape is increasing day by day with new behavior, even an effective solution is not mitigating the new advanced threats. For better understanding, a graphical representation is used in Figure 11 for available solutions and limitations.

Figure 12 shows the limitations to the mitigation of a new zero-day malware attack.

An attack that is brand new or zero-day cannot be detected, and this might disrupt the business system such as the attack shown in the simulation.

In order to mitigate this situation, an advanced level of detection and protection mechanism is an upcoming requirement.

This research has a potential mechanism to detect attacks targeting system memory or CPU level attacks. As shown in Table 8, a system-level attack which executes commands at the process level was observed.

Dec 18th 2019 14:25 :08			INDELTEST	172.28.1.164
	imanali	High	XDR Agent	Prevented
(Blocked)	Malware	Behavioral Threat		Behavioral threat detected
	mcpatcher.exe			
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "			N/A
	Solimba Aplicaciones S.L.		Process Execution	

This was a zero-day attack that has not been identified by AntiVirus, AntiBot, or IPS as this was a brand new malicious

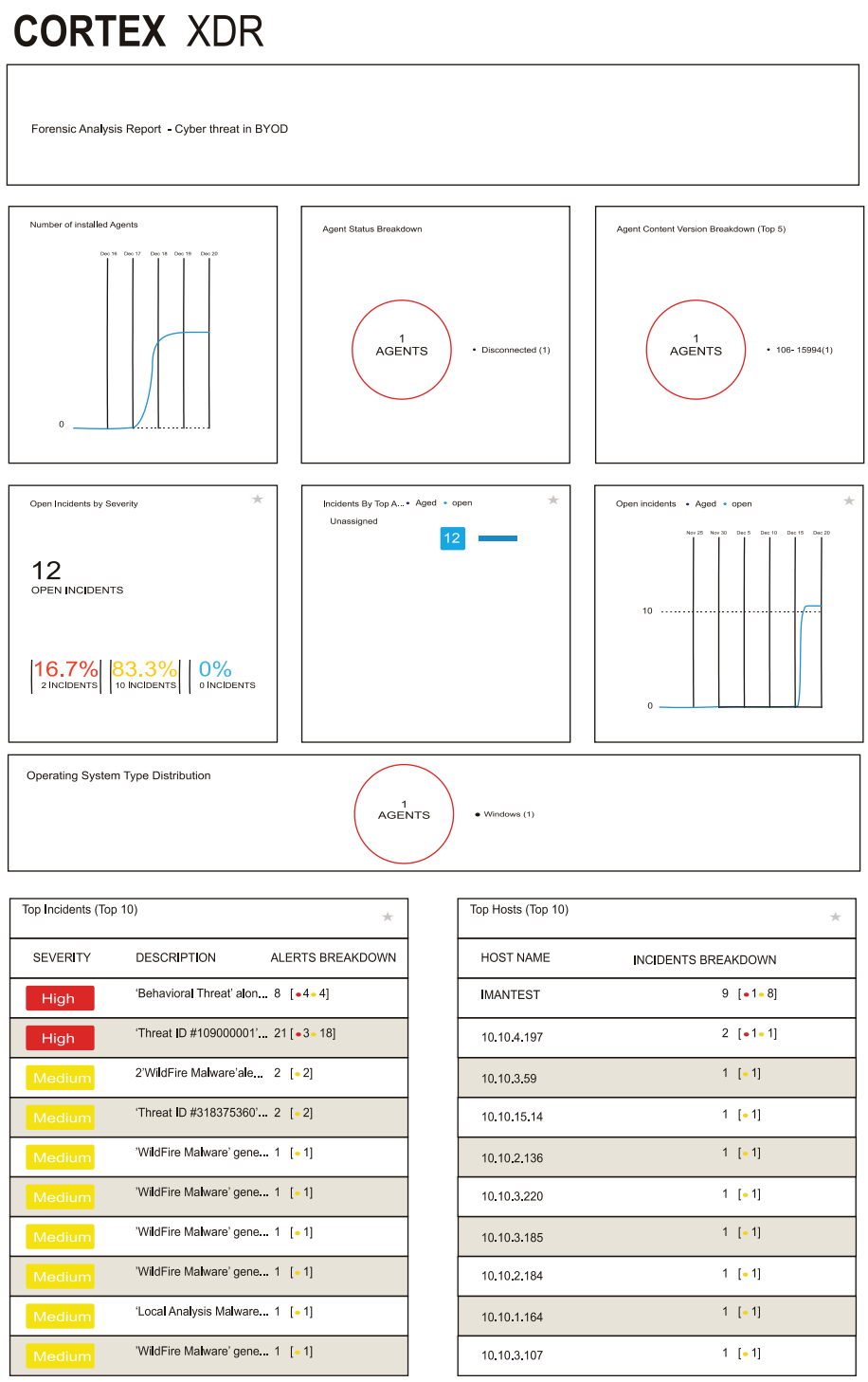


Figure 6: Malicious traffic captured from architecture of Figure 4, index 23 from Palo Alto as per design.

code that attacked the BYOD environment. Even regular sandboxing mechanism did not work to quarantine or to block it.

The architecture of the advanced threat detection model proposed in this research is shown in Figure 11.

The proposed model is shown in the sequential manner of events in Figure 11. In sequence 1, CPU starts processing, and hypervisor is running in 2 along with OS in sequence 3. After setup of the minimum requirement, application is accessed through any native application. Monitoring of CPU

SandBlast Agent Forensics Analysis: General

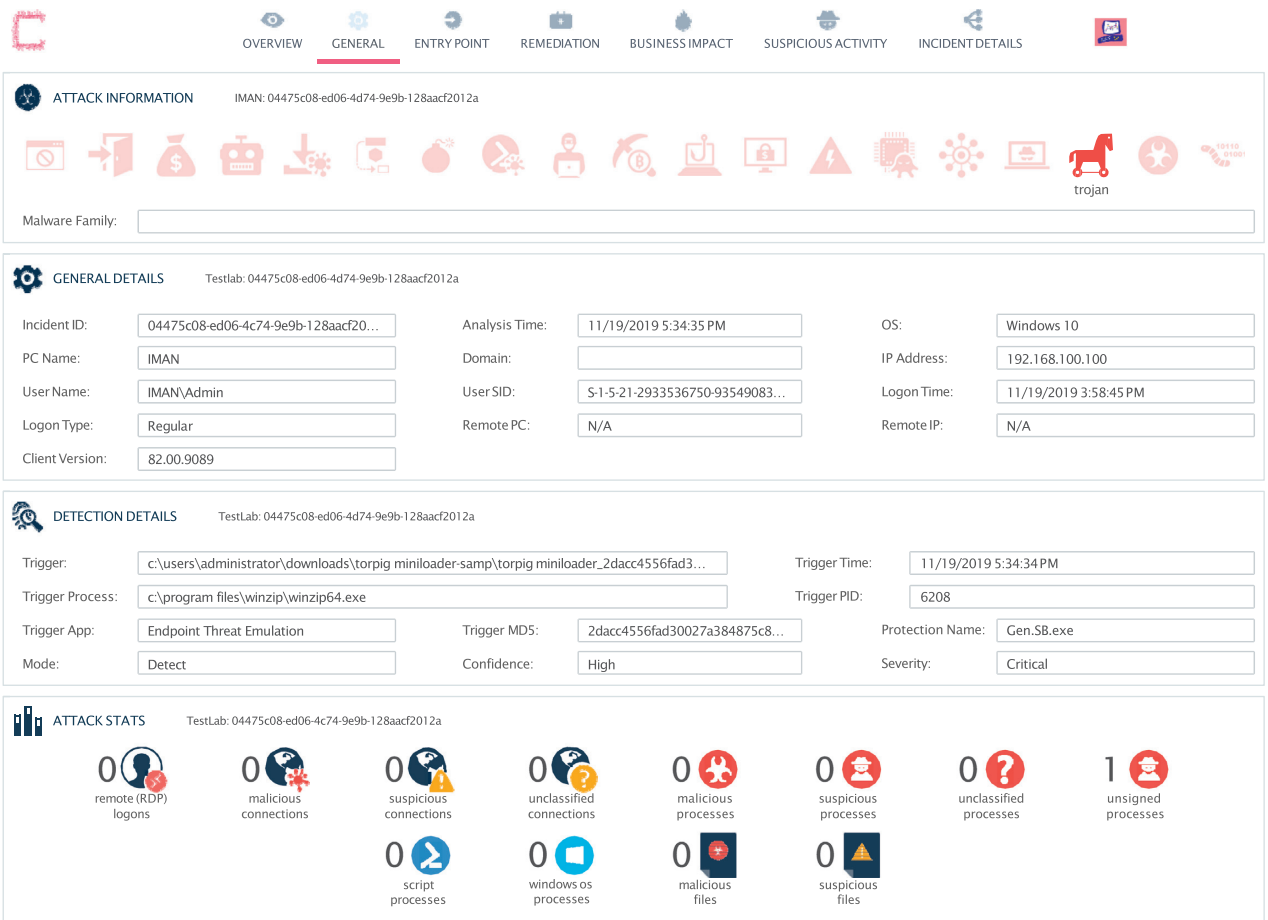


Figure 7: Malicious activity analysis from BYOD endpoint using SandBlast Agent (Figure 3, index 5), Check Point.

activities is in sequence 5 which is a key focused area in this process. If any malicious activities are observed in sequence 6, anomalies detection and protection mechanism is called in sequences 7 and 8. Sequence 9 protects the system before an attack so that BYOD environment cannot be exploited.

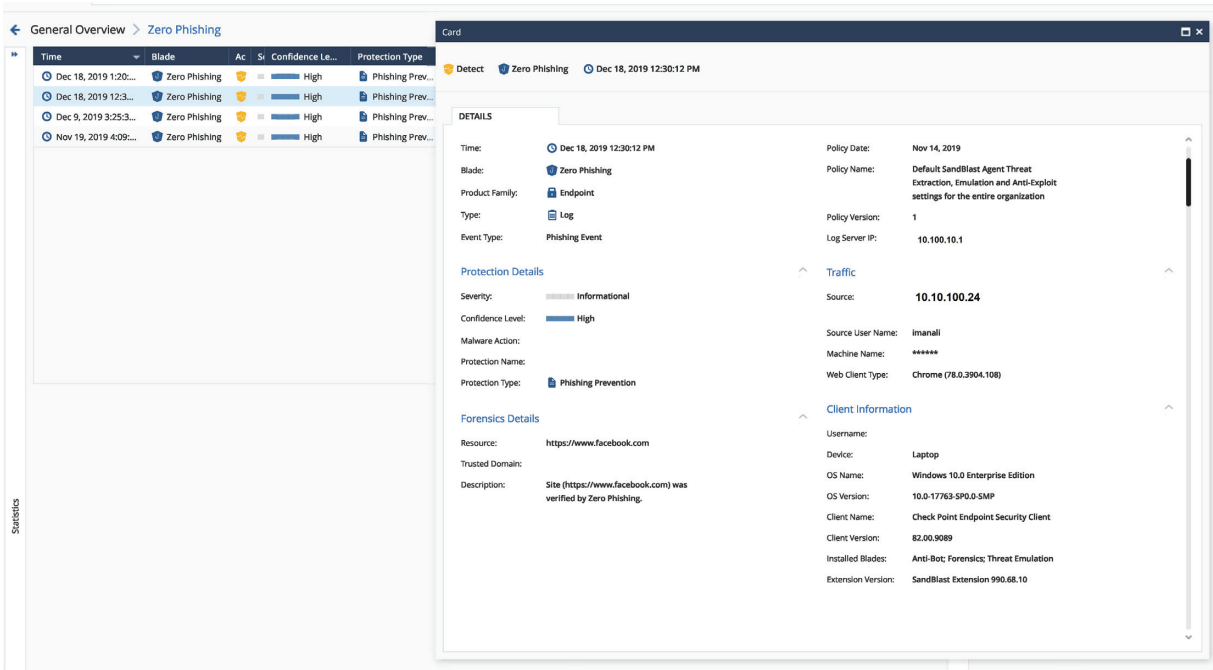
Comparison and benefit of the new technique are provided in Table 10.

The comparison of the existing mechanisms and the proposed mechanism is a comprehensive technique in protecting the organization before a potential attack by analyzing the behavior of the malicious activities from the CPU level in the BYOD environment.

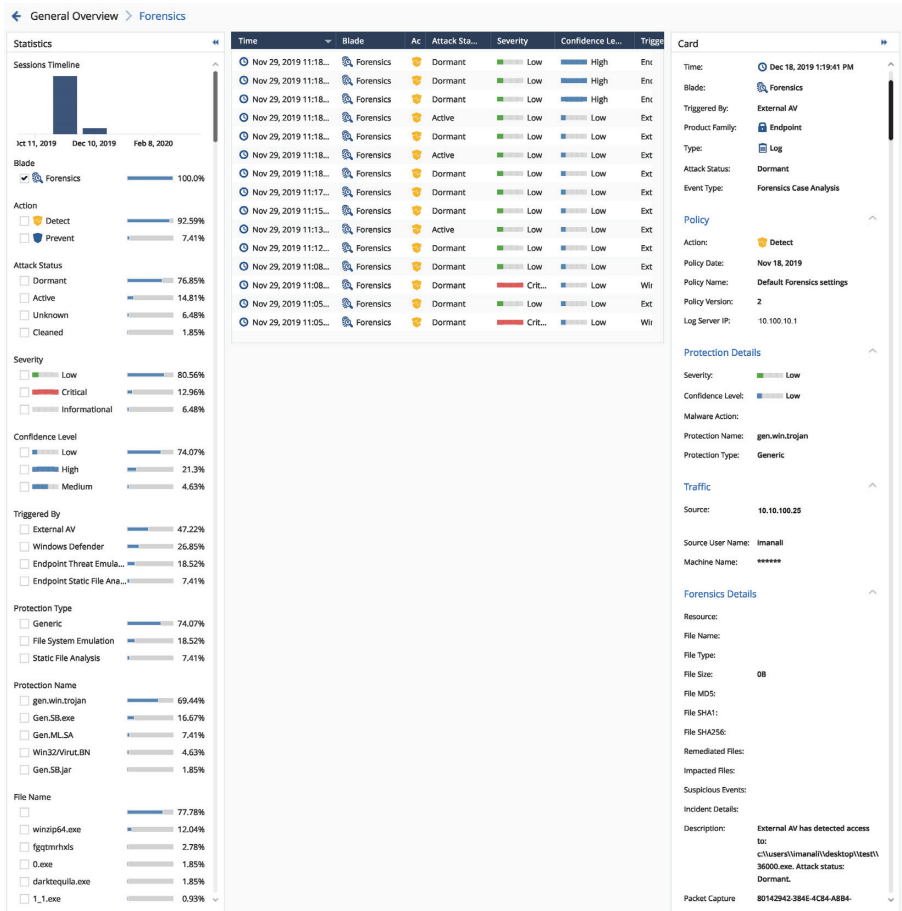
6. Proposed Cyber Forensic NG-DFR Model

After analysis of the results, an advanced level of the cyber forensic model concept is formalized. Next-generation digital forensic (NG-DFR) model is proposed to complete the process of investigation. This model is proposed with the major components as BYOD process definition, then BYOD technology enablement, threat hunting mechanism as the 3rd component, thereafter protection mechanism as the 4th component, and at last forensic process, law, and enforcement as the 5th component. All these 5 components of collaboration approaches in the cyber forensic environment are presented to build a cyber forensic ecosystem. The major 5 component modules described prove the concept of the next-generation DFR model.

6.1. BYOD Cyber Forensic Process Definition. The first and foremost task is the process layout of the BYOD environment. Framework for cyber secured BYOD policy is where untrusted devices are provisioned to access resources over critical infrastructure. In this phase, the security policy definition is framed. After policy of detection mechanism environment is framed, this can comprise multiple technologies and processes. In this phase, the attack detection mechanism is framed. After detection policy violations and acceptance policy are defined, the incident handling mechanism and security operation center mechanism are defined along with the integration of multiple products, and the technology framework is defined in this phase. At last,



(a)



(b)

Figure 8: (a) Phishing attack analysis packet captured. (b) The detailed cyber threat landscape in BYOD environment.

Table 9: Forensic case analysis after attack.

Nov 22, 2019 8:21:57 AM imanali Anti-Bot; Forensics; Threat Emulation Log 2019-11-22T08:35:47Z
Forensics Case Analysis 2019-11-22T13:51:57Z 2019-11-18T14:19:55Z Detect a4640108-ce8b-af06-5dd7-9aa500050000 1 Active 1 ep-demo 0 @A@@B@1574380800@C@52 Gen.SB.exe 46133eec-f86a-480f-a2dc-7483e2c20adf 1.57441E+12 High Endpoint Threat Emulation has detected access to:c:\\users\\imanali\\desktop\\340s.exe. Attack status: Active. Laptop INDELTEST 2 Endpoint Threat Emulation 82.00.9089 Check Point Endpoint Security Client 0 Critical Endpoint Forensics ip-172-28-1-164.ec2.internal (172.28.1.164) 10.0-17763-SP0.0-SMP Default Forensics settings File System Emulation 0 (10.128.140.176) 164.100.1.8 true S-1-5-21-2933536750-935490830-805106884-1003 Generic", "Trojan", Windows 10.0 Enterprise Edition

the complete security posture framework is laid down in this phase as shown in Figure 2.

6.2. BYOD Technology Enablement. BYOD technology enablement is an important key area in this proposed concept of NG-DFR. Different products and technologies enabled the complete service. While choosing products and technology, the most important factor to consider is the integration of different products and technology. If advanced level networking and security products and technology are placed but all these do not talk with each other, then threat intelligence in NG-DFR will be a challenge. Accordingly, in this phase, major service enablement products and technology are factored to work in an integrated way so that each and every threat can be traced without any break of the packet flow. As shown in Figure 4, integration was done along with Cortex for the data lake. Apart from this in Figure 3, integration of next-generation endpoint protection is also introduced for the threat hunting process to enable critical infrastructure. In this section, actual threat detection technology is integrated with the authentication of BYOD users. After secure authentication and onboarding [43], detection of malicious traffic mechanism is proposed [48]. Log management and sandboxing for traffic analysis are considered in this phase.

6.3. Threat Hunting Framework. The most important key part for the forensic investigation ecosystem to develop is the threat hunting mechanism. Monitoring is a continuous action to collect activity logs for potential threat detection in a cyber forensic system. After an attack, finding the source of the attack is a critical task [8]. Detection of malicious [49] traffic which is indeed a major dependent technique required in cyber forensic mechanism is introduced in this phase. Primarily in this section, log analysis is conducted in order to track suspicious traffic. Once the threat is detected in this phase, threat verdict and score are checked to determine whether it is malicious or not. If it is found to be malicious and known pattern, then protection [48] module is called. If the threat pattern is unknown by the threat defender, for example, a zero-day attack [50], then, after extraction of hash, it is sent to threat cloud for verdict and score of the threat and retrospective event is triggered [51]. Finally, logs are preserved for further investigation. In this section, endpoint traffic logs are captured in the external gateway as shown in Figure 3 index 8 and Figure 4 index 23 so that later on logs can be investigated further. Apart from this, all traffic including source IP, destination IP, user information, and user MAC address is captured with all activity details.

6.4. Threat Protection Mechanism. Protection from threat is the foremost task before an attack on the organization. Consistently, researchers are focusing on developing new tactics for threat protection. Different types of novel approaches have been developed in threat protection. One of the advanced level protection mechanisms was developed in BYOD cyber forensic ecosystem study [48]. In this phase, concept of protection of critical infrastructure is covered. After getting the threat category, traffic dropped and logs are preserved for analysis as shown in Figure 3 index 13, and results are shown in Figure 8(b).

6.5. Forensic Investigation, Law, and Enforcement Module. In this phase, a forensic paradigm is presented. In order to complete the forensics of attack, few key areas need to be focused on such as analysis of the logs, preservation of the traffic, and stored log. After analysis, presentation and documentation need to be done. The entire BYOD ecosystem has to have the ability to do all these activities. Preserving evidence and log correlation is focused on the integration of different technologies and products as shown in Figures 3 and 4, where all the gateway perimeter security devices along with AAA, controller, and BYOD users are integrated with Active Directory user database. After integration, end-to-end logs analysis mechanism is developed to enable the forensic system. Finally, forensic correlation of related facts and finding is documented and presented.

7. Next-Generation DFR Model Ecosystem

In this phase, the final framework is represented by next-generation digital forensic readiness (NG-DFR) model. Step by step sequential process is explained to complete the cyber forensic ecosystem. The complete ecosystem comprises process, policies, humans, technology, and integration. Integration of process and technology with human interaction area is covered to build cyber forensic BYOD environment. As shown in Figure 13, complete steps are proposed for next-generation DFR model.

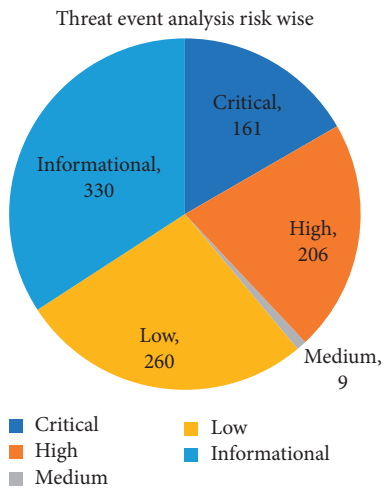


Figure 9: Risk-wise traffic analysis out of 966 packets.

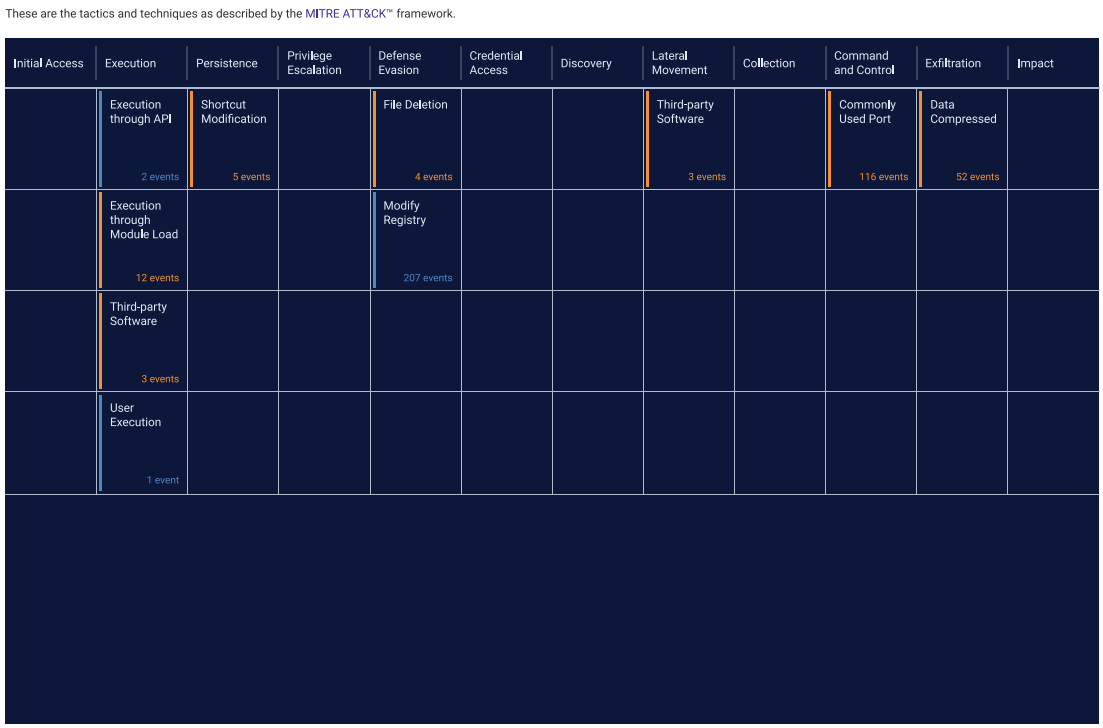


Figure 10: Attack framework as per MITRE ATT&CK.

In Step 1 of the NG-DFR model in Figure 13 planning, policy frameworks are defined with related security and technology enablement paradigm. Service enablement policy, security policy, and detection policies alert mechanism are defined. The integration process is defined.

In Step 2 Service enablement area is focused on. In particular, to build secured BYOD infrastructure with all required products and technology is a key component of this phase.

In Step 3 specially, a detection mechanism is proposed. Detection of various threats and then categorization of the threats are sequential events. Malicious traffic and known threats are detected, and unknown threats are filtered. Unknown threats are sent to the threat cloud in this phase to be analyzed and get the threat score so that appropriate action can be taken.

In Step 4, protection of critical infrastructure is focused on. Protection from different threats before exploiting up to best possible options is taken care of so that the threat landscape can be reduced.

In Steps 5 and 6, the focus area of NG-DFR that is a thorough investigation of the threat is covered. In this phase, outcome of the integration of all tools, techniques, products, and technology are leveraged to build a cyber forensic ecosystem. After analysis from preserved logs, threat hunting mechanism is enabled to carry out the investigation. Finally, storing the logs and artifacts and preparing documentation for submission to law and enforcement are covered.

In a nutshell, this proposed approach of NG-DFR model covered end-to-end system to complete the forensic

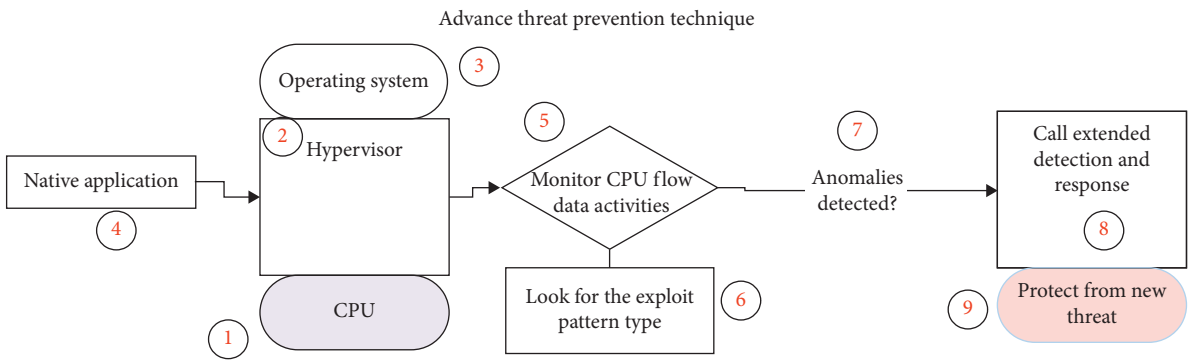


Figure 11: The proposed new approach of the threat detection model.

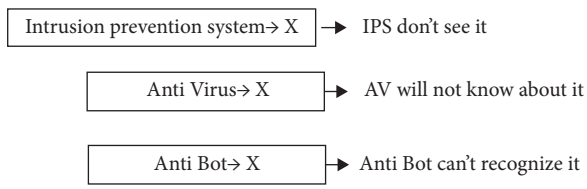


Figure 12: Existing technology to handle the attack.

Table 10: Comparison of the existing solutions and the new simulated solution.

Threat type	IPS (intrusion prevention system)	AntiBot	AntiVirus	New proposed model
Known threat	Yes	Yes	Yes	NA
Unknown threat detection	No, until sandboxing, and more time consuming	No, until sandboxing process which is more time consuming	No, protection mechanism time is higher	Yes, protecting before attack

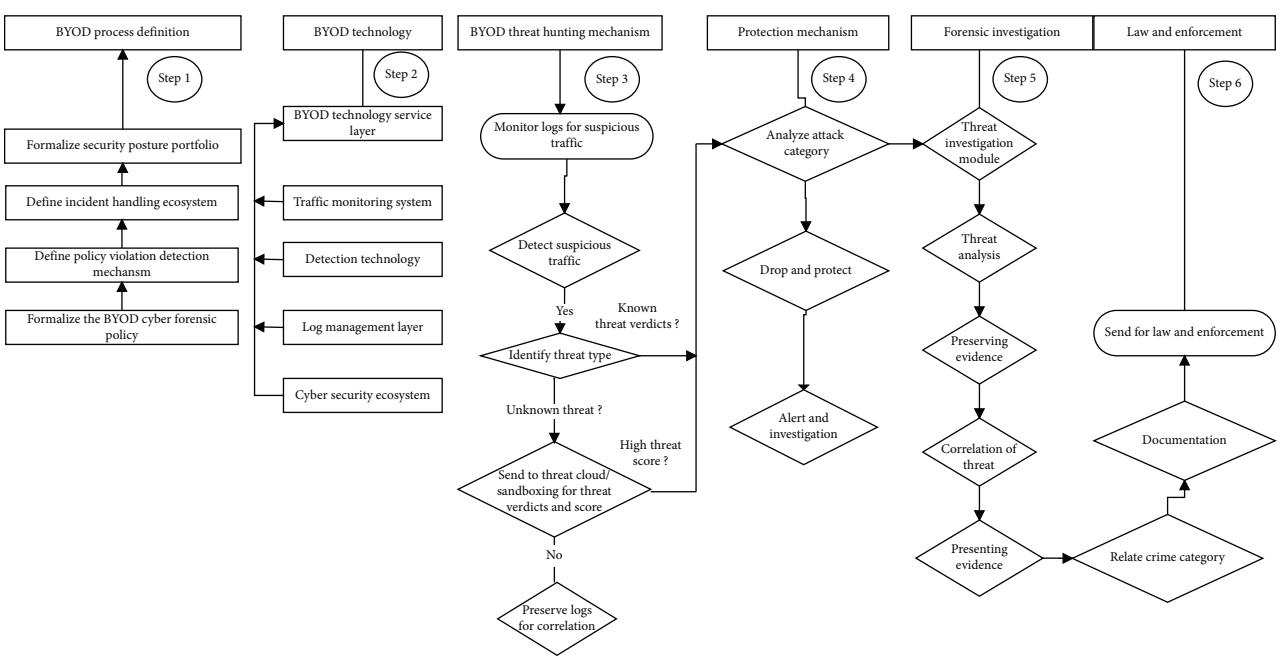


Figure 13: Next-generation digital forensic framework.

```
Step 1: Start
Step 2: Define BYOD security process and policies variables
   P1 = Security policies
   P2 = Detection Polices
   P3 = Incident Response
   P4 = Security violation Protection policy
   P5 = Forensic call policy
Step 3: Technology variables and users
   T1 = Technology portfolio
   T2 = Monitoring system
   T3 = Detection System/Decoy system
   T4 = Protection technology
   T5 = Log management
   T6 = Forensic technology ecosystem
   T7 = Threat category
   U1=BYOD users
Step 4: action and category variables
   violation = V
   Risk acceptable level = A
   Protection = P
   Forensic = F
Step 4: Monitoring of threat
   push U1 through T3 and compare P1
   If Result = A
      then accept request
      stop
   else
      call Step 5
   Then process U1 in T4 for P2
      send U1 logs to T5
   else
      call step 5
Step 5: Detection and Protection
   Push U1 through T3 for P4
      if Result = V
      Drop traffic
   Else
   call step 7
Step 7: identify threat
   If threat category is = known
      if verdict/score = A
         pass the traffic
      else
         drop and send Call step 10 for forensic
   else
         call step 8 for T7 Sandboxing for threat verdicts to
         call step 9
   else
      call step Sandboxing for threat verdicts
Step 8: Analyze threat category
         Analysis of threat type with threat Hash
         return T7 = verdict and score of threat category
Step 9: Unknown threat for forensic
         If T7 = = A compare to P5
            pass and send T5
         else
            send for forensic T6
Step 10: Forensic ecosystem
         if P5=Investigate attack
            do analysis
         Present
Step 9: Present to Law and enforcement
Step 11: Stop
```

Algorithm 1: Detailed algorithm of NG-DFR model.

investigation in order to build an advanced level of the cyber forensic ecosystem.

Detailed algorithm of NG-DFR based model is shown in Algorithm 1.

An algorithmic approach for NG-DFR model is proposed as per architectural flow shown in Figure 13.

8. Discussion

With BYOD, being external devices connected in the infrastructure, it is very sensitive and critical in nature to control threats and postincident analysis of the attack, and finding the source of the attack is a very crucial part. As per Check Point technology research, 99% of organizations [52] do not have a protection mechanism to fight against the ongoing cyber-attack threats. The proposed approach of NG-DFR has addressed the need for an end-to-end cyber forensic ecosystem.

After any cyber incident, finding digital evidence, analyzing the evidence, preserving and presenting the evidence for legal requirement for the court of law are important requirements. This research developed a new model of investigation of a different attack, reaching up to the endpoint of the attack which was targeted during the research. Network security, endpoint security, and critical infrastructure security all are covered in this research with respect to protection of critical infrastructure from BYOD threat.

During the investigation process in BYOD, after an attack, we analyzed all different categories of attack and behavioral analysis of crime. As it was also an important target to protect the infrastructure, detection and prevention were also achieved. Honeypot technology used for detection was not enough to protect the infrastructure. There was a need for prevention technologies after detection by the system without manual intervention. STRIDE-based threat model, which is an interaction between the threat and the corporate network, can be integrated with this model to get a better result.

End-to-end visibility, analysis, investigation, and integration between tools and technologies for building up an advanced model of cyber defense system were needed to fight against today's advanced cyber threat landscape. During the research, an advanced level of cyber forensic model was developed.

Moreover, one important aspect was analyzed during the research, which is run time detection of attack endpoint, status of connection and blocking, and preventing the endpoint from the infrastructure. Detection of threat, visibility of threat associated risk, incident response, and postincident forensic model are key areas explored in this research.

9. Contribution

There are two major novel contributions from this research. The first research contribution is a unique attack detection mechanism. This unique attack detection mechanism helps to detect and protect against zero-day attacks which cannot be detected by traditional tools like IPS, IDS, AV, and AntiBot. The second key contribution is to build a cyber defense BYOD ecosystem. This research has contributed to the area of cyber forensic analysis of a BYOD environment. The complexity of forensic analysis of the malicious activity in a BYOD environment is simplified. The different approaches of forensic investigation are compared using different tools and techniques. Finding the source of an attack in BYOD is analyzed from internal and external threats. The threat prevention mechanism is also an important contribution to this research, and end-to-end BYOD cyber forensic ecosystem framework is also defined.

10. Future Research

Digital forensic investigation becomes complex due to lack of standard procedures depending upon the types of digital crime. The growing complexity of crime becomes a challenge to face with standard tools and techniques. Since BYOD adoption is an upcoming growing phase, new tools and technologies are used by criminals to conduct crimes in zero-day attack behavior. Therefore, ongoing further research is important to fight against crimes. Also, an important area of further research is the collaboration of cyber tools, technology, and cyber law.

11. Conclusion

Due to the lack of a cyber defense ecosystem in the BYOD environment, attacks on the critical infrastructure of the organizations increased, and as a result business ecosystem gets fragmented. Cyber secured BYOD infrastructure is one of the major requirements for organizations today to protect from the advanced level of threats. In this paper, a framework of the cyber forensic model is presented including a cyber-secure BYOD model.

In the first phase of this research, the detection technique of threat is explored with different tools and techniques for further research and analysis.

In the second phase of this research, a major conclusion is a novel approach of detection and protection mechanism of zero-day attacks which cannot be detected by traditional tools like IPS, IDS, AntiBot, and AntiVirus. The proposed method of detection and protection model of unknown threats or zero-day attacks contributed to the protection of the organization's critical infrastructure. The comparison of the outcomes shows a significant advanced incremental positive result, and adoption of this method helped to build the complete cyber forensic ecosystem.

Postincident threat hunting is a critical task in any cyber forensic investigation which is addressed in this research using different tools and techniques like sandblasting and Cortex.

Finally, an advanced level of cyber forensic readiness BYOD infrastructure is developed. Next-generation digital forensic readiness (NG-DFR) model is proposed to mitigate the ongoing need for conducting end-to-end digital forensic investigation including detection and protection framework which also includes the BYOD policy framework and service enablement technology area.

Data Availability

The design/data/architecture used to support the findings of this study are included within the article.

Disclosure

The research, hypothesis, assessments, and analysis articulated in this paper are those of the authors alone and not the organization with which the authors are associated.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Shetty, L. Unden-Farboud, and P. Arriandiaga, "Competitive landscape: managed mobility services," 2020.

[2] "94% enterprises will use IoT by end 2021: Microsoft report," 2019, https://www.livemint.com/technology/tech-news/94-enterprises-will-use-iot-by-end-2021-microsoft-report-1565165449842.html.

[3] B. Tokuyoshi, "The security implications of BYOD," *Network Security*, vol. 2013, no. 4, 13 pages, 2013.

[4] J. Collie, "A strategic model for forensic readiness," *Athens Journal of Sciences*, vol. 5, no. 2, pp. 167–182, 2018.

[5] M. Ratchford, P. Wang, and R. O. Sbeit, "BYOD security risks and mitigations," in *Information Technology-New Generations*, S. Latifi, Ed., pp. 193–197, Springer International Publishing, Cham, Switzerland, 2018.

[6] "Risk or reward: What lurks within your IoT?," 2017.

[7] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, 2018.

[8] G. Suciu, A. Scheianu, I. Petre, L. Chiva, and C. S. Bosoc, "Cybersecurity threats analysis for airports," in *New Knowledge in Information Systems and Technologies*, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds., pp. 252–262, Springer International Publishing, Cham, Switzerland, 2019.

[9] P. Beckett, "BYOD-popular and problematic," *Network Security*, vol. 2014, no. 9, 9 pages, 2014.

[10] "Browse cve vulnerabilities by date." https://www.cvedetails.com/browse-by-date.php, 2019).

[11] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, "Improving forensic triage efficiency through cyber threat intelligence," *Future Internet*, vol. 11, no. 7, p. 162, 2019.

[12] V. R. Kebande, N. M. Karie, and H. S. Venter, "A generic Digital Forensic Readiness model for BYOD using honeypot technology," in *Proceedings of the 2016 IST-Africa Week Conference*, pp. 1–12, Durban, South Africa, May 2016.

[13] "Union Home Minister inaugurates Cyber Crime Unit of Delhi Police and National Cyber Forensic Lab." 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=188700.

[14] Vishnu Institute of Technology, B. V. P. santhi, P. Kanakam, and S. M. Hussain, "Cyber forensic science to diagnose digital crimes-a study," *International Journal of Computer Trends and Technology*, vol. 50, no. 2, pp. 107–113, 2017.

[15] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia, Y. Prayudi, A. Ashari, and T. K. Priyambodo, "A proposed digital forensics business model to support cybercrime investigation in Indonesia," *International Journal of Computer Network and Information Security*, vol. 7, no. 11, pp. 1–8, 2015.

[16] S. Soltani and S. A. H. Seno, "A formal model for event reconstruction in digital forensic investigation," *Digital Investigation*, vol. 30, pp. 148–160, 2019.

[17] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.

[18] L. Columbus, "83% of enterprise workloads will Be in the cloud by 2020," 2020, https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/.

[19] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective android forensics," *Forensic Science International: Digital Investigation*, vol. 33, Article ID 200897, 2020.

[20] S. L. Garfinkel, "Digital forensics research: the next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.

[21] C. Utter, "The "Bring your own device" conundrum for organizations and investigators: an examination of the policy and legal concerns in light of investigatory challenges," *Journal of Digital Forensics, Security and Law*, vol. 10, no. 2, 2015.

[22] "Digital Forensics in the Mobile, BYOD, and Cloud Era,".

[23] S. J. Ngobeni, "Digital forensic readiness for wireless local area networks," 2016.

[24] A. Marotta and M. McShane, "Integrating a proactive technique into a holistic cyber risk management approach," *Risk Management and Insurance Review*, vol. 21, no. 3, pp. 435–452, 2018.

[25] F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, "Enhanced bring your own device (BYOD) environment security based on blockchain technology," *International Journal of Engineering*, vol. 7, 2018.

[26] M. Kaur, D. Singh, V. Kumar, and K. Sun, "Color image dehazing using gradient channel prior and guided L0 filter," *Information Sciences*, vol. 521, pp. 326–342, 2020.

[27] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5 D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[28] S. Brotsis et al., "Blockchain solutions for forensic evidence preservation in IoT environments," 2019, http://arxiv.org/abs/1903.10770.

[29] D. A. Flores, F. Qazi, and A. Jhumka, "Bring your own disclosure: analysing BYOD threats to corporate information," in *Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 1008–1015, Tianjin, China, August 2016.

[30] I. Ali and S. Kaur, "Detection and control of malicious activity and digital forensic in BYOD," 2019.

[31] Z. A. Baig, P. Szewczyk, C. Valli et al., "Future challenges for smart cities: cyber-security and digital forensics," *Digital Investigation*, vol. 22, pp. 3–13, 2017.

[32] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digital Investigation*, vol. 28, pp. S22–S29, 2019.

[33] "Wireshark Go Deep." https://www.wireshark.org/, 2019.

[34] X. Zhang and K.-K. R. Choo, "Digital forensic education an experiential learning approach," 2020.

[35] S. Sathwara, N. Dutta, and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," in *Proceedigns of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–4, Iasi, Romania, Jun. 2018.

[36] E. Casey, "The chequered past and risky future of digital forensics," *Australian Journal of Forensic Sciences*, vol. 51, no. 6, pp. 649–664, 2019.
[37] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.
[38] "IBM Study: Responding to Cybersecurity Incidents Still a Major Challenge for Businesses - Mar 14, 2018," IBM News Room, 2019. https://newsroom.ibm.com/2018-03-14-IBM-Study-Responding-to-Cybersecurity-Incidents-Still-a-Major-Challenge-for-Businesses.
[39] "General Data Protection Regulation (GDPR) guidance," NHS Digital. 2019, https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance.
[40] "2017 Norton Cyber Security Insights Report-Global Results," 2018.
[41] B. Cusack and T. Laurenson, "Systems architecture for the acquisition and preservation of wireless network traffic," 2020.
[42] T. Wiens, "Engine speed reduction for hydraulic machinery using predictive algorithms," 2021.
[43] "BYOD secured solution framework," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 1602–1606, 2019.
[44] "Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide.
[45] D. Ghimire, E. Valle, and S. Robin, "Check point software technologies check point SandBlast agent next generation AV E80.82," 2020.
[46] S. Osterland and J. Weber, "Analytical analysis of single-stage pressure relief valves," *International Journal of Hydromechatronics*, vol. 2, no. 1, p. 32, 2019.
[47] "Cisco Security Report: Majority of Orgs Do Not Monitor DNS," Cisco Umbrella, 2016. https://umbrella.cisco.com/blog/cisco-security-report-more-orgs-should-be-monitoring-dns.
[48] I. Ali, "Byod cyber forensic eco-system," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 9, 2020.
[49] M. I. Ali, S. Kaur, A. Khamparia et al., "Security challenges and cyber forensic ecosystem in IOT driven BYOD environment," *IEEE Access*, vol. 8, pp. 172770–172782, 2020.
[50] A. Lamba, S. Singh, and B. Singh, "Mitigating zero-day attacks in IoT using a strategic framework," *SSRN Electronic Journal*, vol. 4, no. 1, 2016.
[51] Firepower Management Center Configuration Guide, Version 6.0 - File/Malware Events and Network File Trajectory [Cisco Firepower Management Center]," *Cisco*, 2020, https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html.
[52] Security CheckUp, Check Point Software." 2020, https://pages.checkpoint.com/security-checkup.html.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 5536170, 19 pages
https://doi.org/10.1155/2021/5536170

Research Article

A Secured Frame Selection Based Video Watermarking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption

Chirag Sharma,[1] **Bagga Amandeep**,[2] **Rajeev Sobti**,[1] **Tarun Kumar Lohani**,[3] **and Mohammad Shabaz**[1]

[1]*Department of Computer Science and Engineering, Lovely Professional University, Punjab, India*
[2]*Department of Computer Application, Lovely Professional University, Punjab, India*
[3]*Arba Minch University, Arba Minch, Ethiopia*

Correspondence should be addressed to Chirag Sharma; chiragsharma1510@gmail.com

Received 29 January 2021; Revised 10 February 2021; Accepted 16 February 2021; Published 8 March 2021

Academic Editor: Manjit Kaur

The advancement of Internet technologies has led to the availability of audios, images, and videos in different forms. The unauthorized users are exploiting the use of multimedia by transmitting them on various Internet sites to earn money unethically without the intervention of the original copyright holder. Watermarking is a technique used to hide the signal known as watermark inside multimedia data that is not visible to the intruder to manipulate any information. In this paper, a secured watermarking approach is developed to tackle issues related to copyright protection and ownership identification. A Secured Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption hybrid techniques are proposed. The watermark cannot be embedded in every frame of the video as it adds to the size of the video and watermark can be easily retrieved by an intruder. Therefore, the frame selection algorithm has been proposed in the given work. Adding watermark in the frame adds to the challenge of quality loss. The quality loss is addressed in this work. Various attacks have been applied on the watermarked frames to calculate the performance of the proposed technique using quality metrics: Peak Signal to Noise Ratio, Structural Similarity Index, Normalized Correlation, and Bit Error Rate. The results indicate that the proposed technique is effective against various attack scenarios.

1. Introduction

The availability of multimedia data across Internet has prompted unauthorized persons to illegally distribute multimedia data such as videos across the Internet. The issues like copyright protection and ownership identification are prominent and the development of the secured technique is required to counter these issues. Videos are the most attackable multimedia data and unauthorized people are distributing videos for their own benefits and are earning lots of money in this regard. The illegal distribution of video is illustrated in Figure 1 where videos are exposed to the Internet after DVD release or movie release and this problem has led to huge loss of movie industry. The real time videos are gaining lots of popularity with various OTT platforms like NETFLIX and AMAZON PRIME. The problem of copyright protection again emerges as the videos from these platforms are getting released to the Internet and thus drops the number of users accessing these websites. There is a need of a secured technique to identify these unauthorized users, thus stopping this illegal distribution. Watermarking is a technique that embeds secret and unnoticeable signal inside the video which is unidentifiable to any unauthorized user. The watermarking embeds encrypted watermark inside the multimedia data and the process of extraction is done from the researcher's side to test validity of scheme. The videos need to be watermarked before they are distributed across the network.

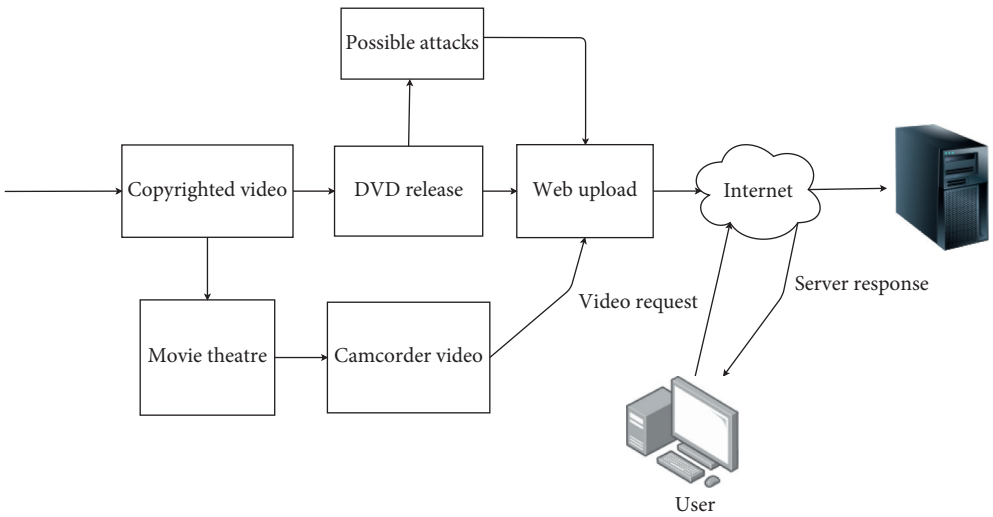


Figure 1: Illegal distribution of multimedia data.

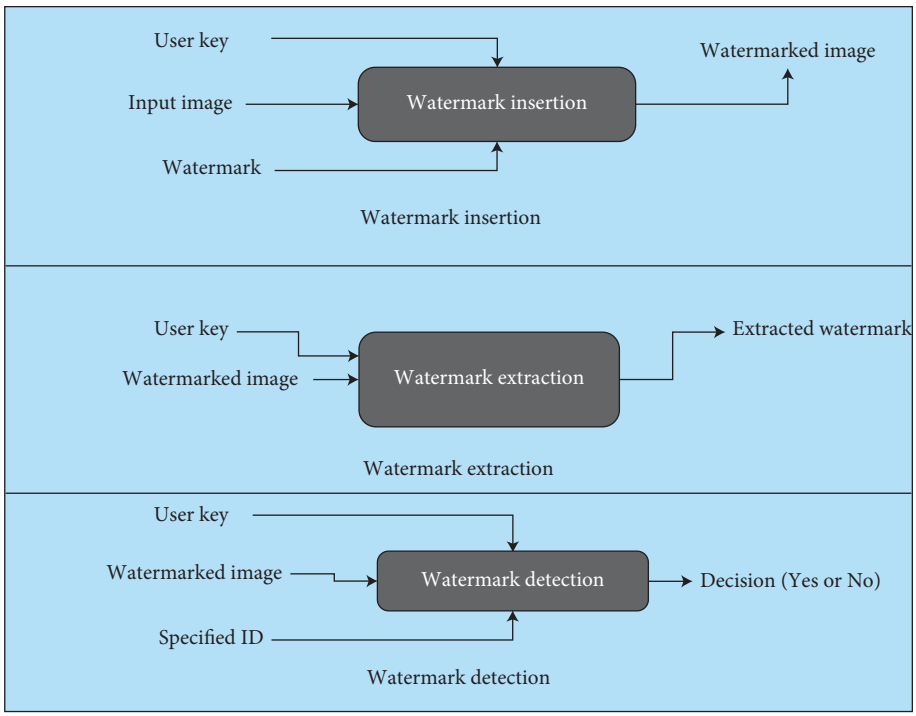


Figure 2: Process of watermarking.

Figure 2 describes the process of watermarking with the addition of key inside the watermark being embedded.

The proposed technique in this paper embeds the secret signal with additional security feature so that unauthorized person cannot identify it. The real time videos are available in compressed domain because it is very challenging to distribute uncompressed domain videos across the Internet. The uncompressed videos are raw videos and compressed domain videos are encoded versions of raw videos. The videos are available in many codecs like XVID, H.264, H.265, and WMV. The codec used for real time video is H.264. The proposed technique will embed the watermark in compressed domain videos. The major challenges in embedding the watermark in the video are the selection of frames and quality loss after embedding.

The selection of frames is done because watermark cannot be embedded in every frame of the video as it will be very easy for the unauthenticated user to detect watermark and remove it. The quality loss is the major constraint in the research as embedding of watermark affects quality of the video. There are many watermarking techniques available. The different types of techniques are described in Figure 3. The most common types of watermarking techniques are frequency domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Many researchers are applying these techniques to provide

solution to these problems. Although these techniques are good, improvement can be done in many aspects. The encryption mechanism used in the proposed technique adds to additional security feature as it would be very difficult for any intruder to detect watermark and recover watermark from watermarked video. The proposed technique used in the research is based on Graph Based Transform along with Singular Valued Decomposition. This combination is applied to encrypted watermark. The encryption can be done in many ways such as Ciphers, AES, and DES. The reason why AES and DES are not used for encrypting watermark is that they are very compressed and make the watermarking algorithm even more complex so the hyperchaotic encryption [1] is used in the research.

The validity of the proposed technique is tested after applying certain signal processing attacks to watermarked video. Gaussian Noise, Sharpening Attack, Rotation, Blurring, and JPEG Compression attacks have been applied on watermarked video. Quality parameters, Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), Normalized Correlation (NC), and Bit Error Rate (BER), have been used in the research. The major contribution of this manuscript is summarized as follows.

(a) We proposed the frame selection algorithm that identifies best suitable frames from the compressed domain video.

(b) We proposed novel technique Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption for watermark embedding.

(c) We evaluated the performance of the proposed technique against various signal processing attacks.

The organization of this paper is as follows: Section 2 reviews all the related work done in this area, Section 3 presents the research methodology of the proposed technique, Section 4 presents results gathered from various experiments performed on selected set of videos, and Section 5 describes conclusion obtained from the given research.

2. Related Work

The number of video watermarking techniques has been proposed in the field of watermarking. The most prominent watermark embedding technique is Discrete Wavelet Transform (DWT). This technique has been applied by many researchers as transformation of a frame to DWT is a reliable method. Spatial Domain Methods given in this paper are fast but not robust enough to handle any signal processing attacks [2, 3]. Frequency domain techniques like DWT and DCT have been used by many researchers. The techniques are good but suffer from the problem of dimensionality reduction; that is why these techniques were coupled with another technique named as Singular Valued Decomposition (SVD). The major constraint in watermarking is the area where watermark is embedded. Many techniques and methods have been proposed nowadays where study is made on feature selection and feature extraction. The fast methods like SLFNs have been proposed in [4] which are based on extreme learning machine. The optimization algorithms such as PSO [5] improve the efficiency of existing algorithms by targeting high values of fitness function with their respective mathematical model. The watermarking technique can be made more secure by adding encryption mechanism in it. The technique proposed in [6] adds security features to the abovementioned mechanism. The performance of the frequency domain techniques can be optimized using optimization algorithms like genetic algorithm [7]. The PSO algorithm [8] also optimizes the performance of watermarking technique by taking quality parameter into consideration. Graph Based Transform is a new kind of transform that interprets graph in the form of signal. A new transform based on graphs was proposed for depth map coding [9]. The process of frame selection is very important aspect of the research. The frame selection algorithm is proposed by using identical frame extraction concept [10]. The process of scene change detection was applied by Masoumi [11]. The proposed work is inspired from the research done over the years on the videos and intends to solve problems of existing research. Different frequency domain techniques are used in watermarking [12] but DWT has been used by many researchers. The application of SVD was to extract good number of features for performing transformation as largest coefficients in S component of SVD Matrix can resist image compression and processing attacks and embedding of watermark will not be affected when any of frequency domain methods is coupled with SVD [13]. Fourier Transform is also the part of Frequency Domain Technique [14] but the technique does not produce good results in terms of imperceptibility. The process of frame selection is done on the basis of number changes in scenes of the frames. The calculation is done using histogram difference [15]. A new Grey Wolf Optimizer is used to solve local optimum problems and find optimal solution from given set of solutions. GWO is an efficient PSO technique [16]. Hybrid combination of DWT-SVD was proposed by

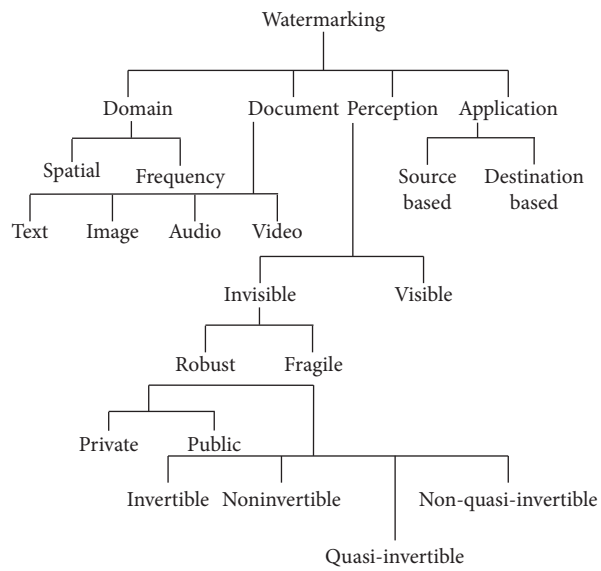


Figure 3: Watermarking techniques.

various researchers. A hybrid technique based on DWT-SVD along with firefly algorithm got high values of quality parameters [17]. A video watermarking technique was proposed using multiple wavelets with the application of DWT-SVD [18]. GBT Transform is applied for data decorrelation [19] which is also an effective transform that can be applied to multimedia data. A semiblind DWT-SVD technique was proposed on compressed domain videos [20]. Graph Fourier Transform is used for depth map coding. This technique produces good results in multimedia data [21]. The hybrid transform DWT-SVD produces favorable results in terms of quality parameters. The hybrid transform is combined with Fuzzy BPN Architecture for grey scale images. It was producing good visual quality of watermarked image [22]. The DWT-SVD was applied on videos by Sharma [23]. The watermark embedding techniques hide the signal in the multimedia data but, to ensure security of data, various encryption techniques have been used along with frequency domain techniques. Wang [24] proposed encrypted watermarking technique using multiple kinds of chaos. A Hybrid Genetic Algorithm combined with fruit fly optimization [25] addresses QOS parameter that helps to solve the problem in less computation time. The same technique can be used in watermarking to produce good results. A hybrid technique that combines BWT-SVD and optimization algorithm was proposed [26] to embed watermark in multimedia data. The blind H.264 compressed domain technique was proposed to find certain areas of the frames to embed watermark. Pattern recognition technique was proposed [27]. Sharma [28] enhanced the work by adding transpositional cipher in the combined transform of DWT-SVD to enhance security. Transpositional cipher used in [29] had issues in security. The cipher used in research [30] enhances security of any watermarking technique. Combined approach on Graph Based Transform and Singular Valued Decomposition was proposed for images in the respective work [31]. Cao [1] proposed an encryption technique that produces good results compared to others. The GBT-SVD Transform produces better results than GBT used in previous research [9, 19]. Table 1 illustrates the gaps found in recent studies in this field.

3. The Proposed Methodology

In this section, we propose a frame selection mechanism followed by watermark embedding and application of certain attacks on the proposed technique. In this research, frame selection process is important as watermark information is sensitive that should not be leaked to any intruder. Embedding watermark in every frame makes the information easily accessible to unidentified user and adding watermark in every frame increases the size of watermarked video. Therefore, frame selection mechanism is important. This mechanism is followed by watermark embedding and then evaluation of proposed technique is done by applying certain attack scenarios.

3.1. Frame Extraction and Selection. The first phase in the proposed work is to find the suitable number of frames from extracted frames of the video. The process of finding suitable frames in real time is done using scene change detection. The watermark cannot be embedded on all frames of the video as it becomes every easy for any intruder to detect the watermark and add watermarking to all frames which also increases the size of the video. The process of finding suitable frames becomes significant. To select significant frames, scene change detection mechanism is applied. The comparison of adjacent frames with one another is performed. The grouping of identical frames is done. The value of the frame difference will decide whether frame will be considered as the part of the same group or different group. If difference is large, then it will be considered as part of different group. The parameter of decision will be taken as threshold; if the value of frame difference is higher than the value of threshold, the next frame will be the part of next group. The same is illustrated in Figure 4. The temporal sampling is performed that enhances the process of frame selection that gives better results compared to [10]. The selection of the first frame is done from all different groups. Frame difference can be represented as histogram difference that can be expressed as

$$\mathrm{FD}_k = \sum_{k=1}^{I} T_k(m) - T_k(m+1), \tag{1}$$

where FD_k is representing frame difference and T_k is the histogram value of kth frame of level m and I is the number of levels of the histogram. The grouping of similar images is based on scene change detection. The threshold is maintained to detect intensity histogram difference to calculate sudden transition amongst frames (in order to find larger frame difference). This scenario is expressed as

$$K_b = \mu + \alpha\sigma, \tag{2}$$

K_b is threshold value. σ and μ are the standard deviation and mean value of selected frame intensity histogram difference. The selected value of α in the research is 2.8. The temporal sampling has also enhanced the process of frame selection. The criteria of frame selection depend upon the comparison of FD_k with K_b. The algorithm was tested on 6 videos. Relevant frame selection was done. The standard frame rate taken is 29.97. A total of 6 videos have been taken as data set for this process.

The videos with a greater number of scene changes will have a greater number of selected frames. This process is illustrated with the help of algorithm given as Algorithm 1.

The Akiyo video did not have any scene changes; hence, no frames will be selected and watermark embedding will not take place. Watermark embedding follows frame selection process only. The evaluation parameter of this step is total frame selection time from extracted frames of the video. The process of frame extraction is done followed by frame selection. Some videos have a smaller number of scene changes; hence, less frames will be selected. In case there is no detection of any scene done, then no selection of frame takes place. The pure storage video has higher number of scene changes;

Table 1: Analysis with related work.

Reference	Main contribution	Gaps
Tabassum [10]	In this research, identical frame extraction technique is proposed with 3-level DWT frame selection done using frame difference method. DWT is applied to higher band coefficients to get robustness against signal processing attacks.	The quality is compromised and watermark embedding technique could be more efficient.
Masoumi [11]	In this research, frame extraction is done by taking motioned part of the video; scene change detection is applied. Color separation of selected frame is done and watermark embedding is done in blue channel. Watermark is considered as pseudorandom numbers; each bit of watermark can be taken as scattered randomly through video frames in order to provide additional security feature.	The proposed algorithm becomes complex by applying a secured, encrypted technique.
Mishra [17]	In this research, DWT-SVD technique is proposed along with optimization firefly algorithm using multiple scaling factors. The optimization adds to high values of quality parameters.	The technique is applied on grey scale images and additional security feature can be added.
Sridhar [18]	In this research, hybrid DWT-SVD is applied on the videos with multiple wavelets. The efficiency of hybrid technique is always better than DWT.	The efficiency of frame selection algorithm is compromised.
Rajpal [29]	In this research, fuzzy frame selection scheme with bidirectional extreme learning machine is done. Fuzzy rules are based on luminance, edge, and texture sensitivity. Fuzzy frame selection is based on scene change detection; weighting factor is based on these 3 parameters.	Security is compromised using transposition cipher.

hence more frames will be selected. The importance of frame selection comes from the fact that watermarking on still number of frames will give a chance to any unauthorized person to get access of watermark content because of similar properties [32]. Figure 4 depicts the process of frames selection. Frame selection using scene change detection is giving better results especially in uncompressed domain. The grouping of similar images is done and threshold is calculated using (2); the moment scene change is detected, the first frame in the individual frame is selected and the same process follows till all the extracted frames are processed [33]. The process is fast avoiding similar frames to be selected, thus saving the time for frame selection and saving overall embedding time for embedding process. The results are formulated in MATLAB 2019b using i5 processor.

3.2. The Proposed Technique of Watermarking. The next step after selection of frames is to embed encrypted watermark. Watermark is encrypted before it is embedded to selected frame [34]. Watermark embedding poses a great challenge of quality loss. To counter the problem of quality loss after embedding, the technique is supposed to be proposed that aims at high values of quality parameters like PSNR. Hybrid combination of Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption is proposed to counter the security issues in multimedia data. Graph Based Transform (GBT) is a transform that uses signal in the form of graph and produces better results in terms of adapting signal structure of an image [35]. GBT is used as it is robust against various attack scenarios in the field of image processing. Singular Valued Decomposition counters the issues of dimensionality reduction [36]. After frame selection is done, selected frames are applied with GBT Transform followed by SVD and at the same time watermark is encrypted with Hyperchaotic Encryption before being applied to selected frame. The selected frame is taken as a signal in the form of a graph and transformation is applied using GBT [37]. The S value is taken after SVD is applied. The watermark is encrypted using Hyperchaotic Encryption and SVD is applied to it [38]. The S values of the selected frame and watermark are combined to form modified S value of watermarked frame. The proposed watermark embedding technique is further discussed in the following sections.

3.2.1. Embedding Technique. Graph Based Transform is a newly formed transform that is represented by $G = \{V; E; s\}$ where V and E are the vertices and edges of the graph, and s represents the frame signal [39] for graph G

$$M(i, j) = \left\{ \begin{array}{ll} \sum mi, j, & \text{if } i = j, \\ 0, & \text{otherwise} \end{array} \right\}, \tag{3}$$

where $m_{i,\ j}$ represents the weight of the edge. The degree matrix $D \in N \times N$ is a diagonal matrix, where elements are

$$K(i, j) = \left\{ \begin{array}{ll} \sum mi, j, & \text{if } i = j, \\ 0, & \text{otherwise} \end{array} \right\}. \tag{4}$$

Then, the Laplacian-Graph Matrix L would be defined as

$$L = K - M, \tag{5}$$

where the operator L is also known as Kirchhoff operator, which is represented as adjacency matrix A. Eigenvalue decomposition is done to set of real nonnegative eigenvalues which are represented by $\wedge = \{\lambda 1, \lambda 2, \ldots \lambda \mathbf{N}\}$; orthogonal eigenvectors are represented by $\mathbf{V} = \{v1, \ldots vN\}$, derived as

$$L = V \Lambda V^T. \tag{6}$$

Decorrelation of the signal defined on the graph is done using eigenvectors.

$$C = V^T s, \tag{7}$$

$$A = \sum_{A=1}^{r} EA * SA * (RA)^T = \sum_{i=1}^{r} Ei * Si * (Ri)^T, \tag{8}$$

$$E_A = [e1, e2, e3, e4 \ldots\ldots eN], \tag{9}$$

$$R_A = [r1, r2, r3, r4 \ldots\ldots rN], \tag{10}$$

$$S_y = \begin{pmatrix} S_1 & \ldots & N \\ \vdots & \ddots & \vdots \\ 0 & \cdots & S_N \end{pmatrix}, \tag{11}$$

$$A = \mathrm{E}SR^T, \tag{12}$$

$$WF''(i, j) = A(i, j) + \alpha W(i, j). \tag{13}$$

Singular Valued Decomposition is done using equation number 10 where transform is done using S as it is more resistant to image processing attacks.

3.2.2. Encryption of Watermark before Embedding. The watermark embedded on selected frames is encrypted using Hyperchaotic Encryption to add security feature to the proposed technique [1]. The value of x, y, z, and w calculated from above equation will be used for encrypting the watermark image to be used in a frame. The standard values of a, b, and c were taken as per the values in reference [1]. The second step is the conversion of R; S is done into x, y for column and row of the encrypted watermark image. The 3rd step is to interchange the coefficients of mth row and $x(m)^{\text{th}}$ row of image $W - m = 1, 2, \ldots i$, $N = 1, 2, \ldots j$; see Algorithm 2.

$$\begin{Bmatrix} x = a(y - x) + w \\ y = cx - y - xz \\ z = xy - bz \\ w = -yz + rw \end{Bmatrix}, \tag{14}$$

$$X = \mathrm{mod}(\mathrm{floor}(R + 100) * 105, i) + 1, \tag{15}$$

$$Y = \mathrm{mod}(\mathrm{floor}(S + 100) * 105, j) + 1, \tag{16}$$

$$W(m, :) = W(x(m), :), \tag{17}$$

$$W1 = W, \tag{18}$$

$$W1(:, n) = W1(:, y(n)). \tag{19}$$

The encryption of a watermark image is represented as $W(i, j)$ where image size is represented as $m * n$. The first step is generating the sequence of R, S using Lorenz system. The security feature added here adds to security feature by encrypting watermark before being embedded, thus making the technique more secure. Real time applications like broadcasting face security issues and copyright protection; the proposed technique combined with Hyperchaotic Encryption adds to security feature and also adds to copyright protection. Figure 5 depicts watermark embedding process.

3.3. Extraction Procedure. The next section in the proposed work describes watermark extraction procedure so as to recover watermark from watermarked video. The extraction of a watermarked from watermarked video is a reverse process of embedding when watermark was embedded with the help of (13). The extraction of frames is followed by applying GBT and SVD and the extraction is calculated as per the following equation. This is followed by inverse GBT and inverse SVD; then decryption is done using a key; then watermark is recovered. Figure 6 depicts watermark extraction process:

$$W_{i,j} = WF'_i - \frac{A_{i,j}}{\alpha}, \tag{20}$$

where $W(i, j)$ is extracted watermark, $\mathrm{WF}'(i, j)$ is watermarked frame, and $A(i, j)$ is selected frame.

The extraction procedure is used to find the difference between original and extracted watermarks. High difference between both of the watermarks suggests that the technique is not efficient; however, as per result calculation, it was found that there is a negligible difference amongst both watermarks after extraction is done, as shown in Algorithm 3.

3.4. Performance Evaluation. The performance evaluation of the watermarking technique is typically calculated in terms of quality parameters of the video and robustness against various attack scenarios such as Gaussian Noise, Sharpening, Rotation, Blurring, and JPEG Compression. The parameters are PSNR, SSIM, NC, and BER.

(a) PSNR (Peak Signal to Noise Ratio) is a major quality parameter that differentiates original and watermark frame based on Mean Square Error. The average PSNR is sum of PSNR of all selected frames divided by number of frames. The objective of the proposed technique is obtaining high values of PSNR as embedding of watermark causes quality loss. Higher values of PSNR indicate the efficiency of the technique. It is calculated by following equation:

$$\mathrm{MSE} = \sum_{i=0\,j=0}^{G-1H-1} \frac{1}{G * H} ([AI(i, j) - EI(i, j)])^2, \tag{21}$$

where G and H are rows and columns of the image:

$$\mathrm{PSNR} = \frac{10 \log_{10} (255)^2}{\mathrm{MSE}}, \tag{22}$$

$\mathrm{AI}(i, j)$ is selected frame;

$\mathrm{EI}(i, j)$ is watermarked frame.

$$\text{Average PSNR} = \frac{\sum_i^n \mathrm{PSNR}_i}{n}. \tag{23}$$

(b) Normalized Correlation (NC): this parameter is used to find correlation between watermarked frame and

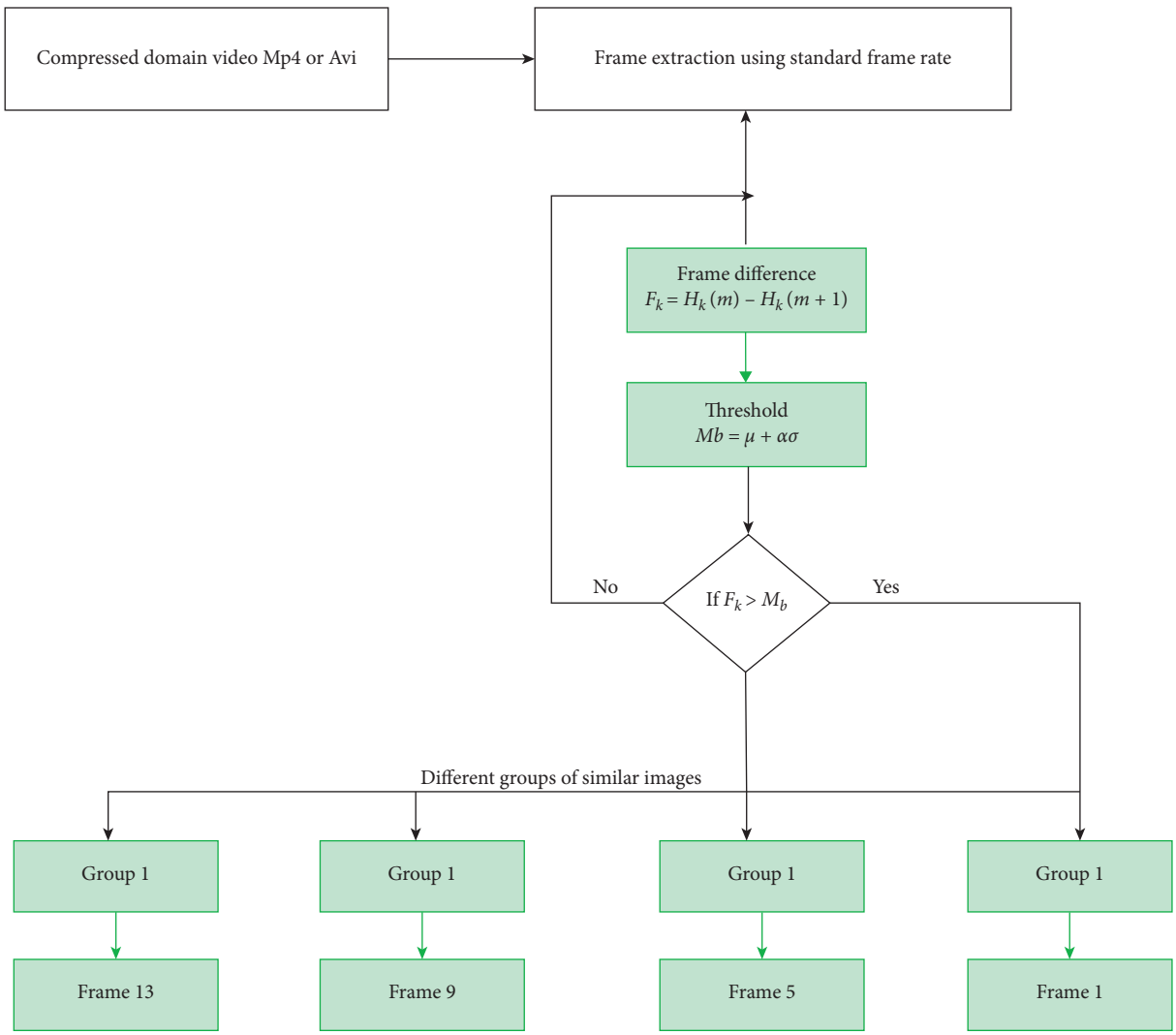


Figure 4: Selected frames to be watermarked from different groups.

Input: $T \longleftarrow$ No. of Frames, $\mathbf{K} \longleftarrow$ Mean(T), $\mathbf{S} \longleftarrow$ Std Deviation
$\mathbf{K_b} \longleftarrow K + \alpha S$
$\mathbf{FD_k} \longleftarrow$ Frame difference
Output-Selected T
(1) **for** $i \longleftarrow 1$ to T
(2) **Read** (T) and store in variables
(3) **Compute** the difference amongst frames and group them in different groups and store in FD_k.
(4) **if** ($\mathrm{FD}_k > K_b$)
(5) **Select** and group them
(6) **Apply** random key amongst frames from different groups and write them to disk
(7) **End if**
(8) **Write** selected frames on disk
(9) **End for**
(10) **End**

Algorithm 1: Frame selection algorithm.

Input: Selected Frames
Output: Watermarked Video
Begin
(1) **for** selected frames from 1 to k
(2) **Input** binary image watermark (i, j).
(3) **Implement** layer separation on selected RGB frame $A(i, j)$ and watermarked image $W(i, j)$.
(4) **Encrypt** the watermark image $W(i, j)$.
(5) **Convert** selected frame into GBT Transform on each layer of $A(i, j)$.
(6) **Use** SVD Transform and extract S Feature of USV of $A(i, j)$ and $W(i, j)$.
(7) **Target** S value from both sides to be merged.
(8) **Embed** watermark $W(i, j)$ to $A(i, j)$ using value α as 0.02 using equation $WF'(i, j) = A(i, j) + \alpha W(i, j)$
(9) **Get** modified S value from both $A(i, j)$ and $W(i, j)$
(10) **Repeat** steps from 1 to 9 till all the selected frames are processed.
(11) **End for**
(12) **for** frames $1 : m$
(13) **Replace** watermarked frames with selected frames from the directory.
(14) **Use** same frame rate to combine all frames including watermarked and rest of extracted frames
(15) **End for**
(16) **End**

Algorithm 2: GBT-SVD-chaotic algorithm.

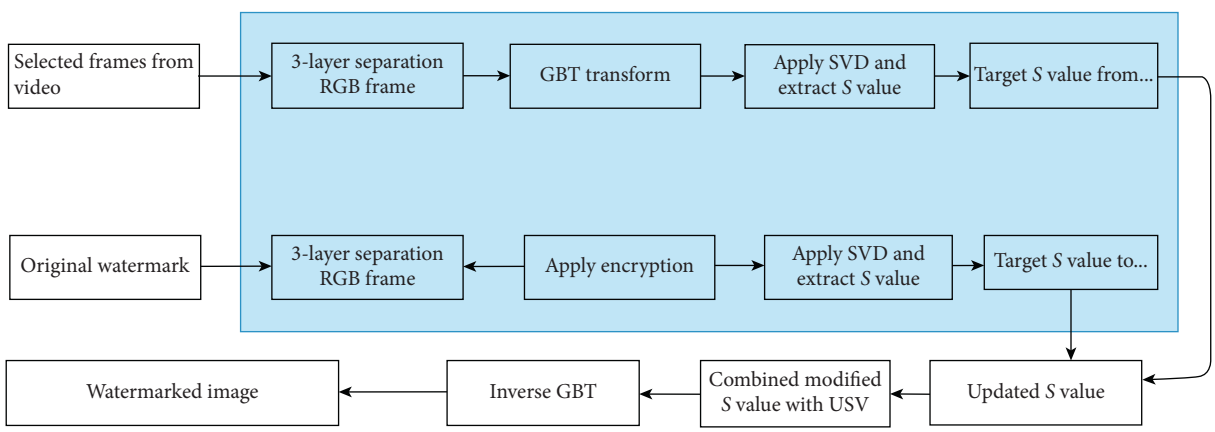


Figure 5: Watermark embedding procedure.

selected frame. It is calculated using the following equation:

$$\mathrm{NC} = \frac{\sum_{i=1}^{G}\sum_{j=1}^{H} A(i,j)E(i,j)}{\sum_{i=1}^{G}\sum_{j=1}^{H} E(i,j)^2}. \tag{24}$$

(c) Structural Similarity Index Measure (SSIM): this parameter is used to find structural similarity between watermarked frame and selected frame. It is calculated from the following equation:

$$\mathrm{SSIM}(m,n) = \frac{(2P_mP_n + c1)(2K_{mn} + c2)}{(P_m^2 + P_n^2 + c1)(K_m^2 + K_n^2 + c2)}, \tag{25}$$

where P_m and P_n represent average of m and n column; K_m and K_n represent variance of m and n; K_{mn} represents covariance of m and n and $c1$ and $c2$ are variables.

(d) Bit Error Rate (BER): this is the inverse of PSNR calculated in the following equation:

$$\mathrm{BER} = \frac{1}{\mathrm{PSNR}}. \tag{26}$$

The numerical values of NC, SSIM, and BER lie in the range of [0, 1]. While SSIM and NC measure the similarity, so high values of them are preferred and BER is inversely proportional to PSNR so lower values indicate the efficiency of technique.

4. Experimental Results

The results were evaluated in MATLAB 2019b using i5 processor. The frame selection time and embedding time are dependent on the type of processor used. The compiled results are dependent upon watermark embedding time and

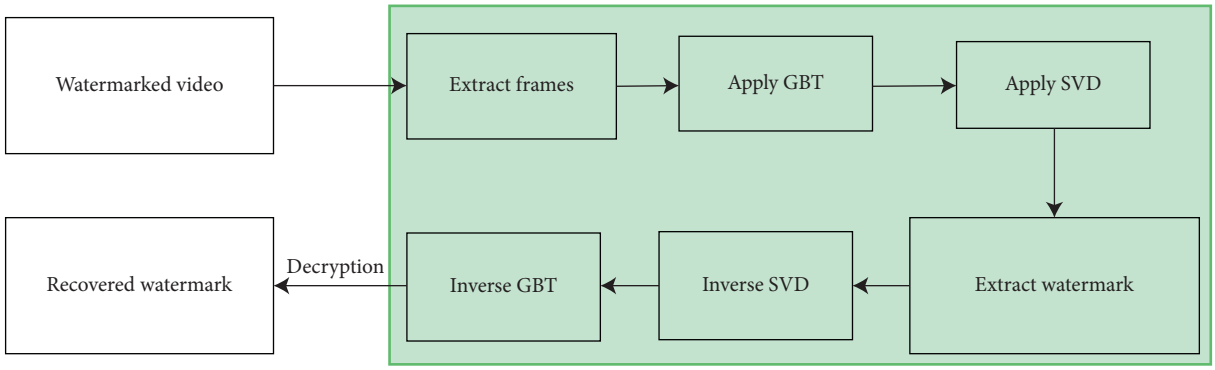


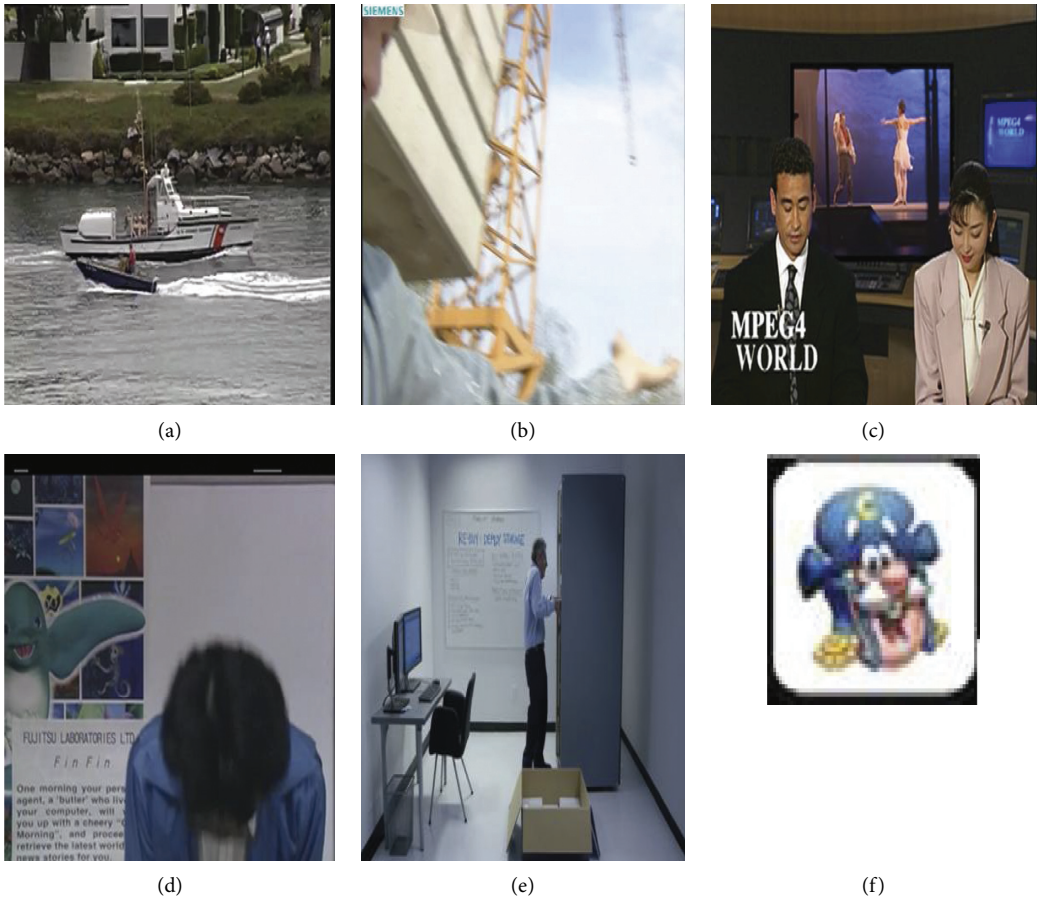
Figure 6: Watermark extraction procedure.

Input: Watermarked Video
Output-Recovered Watermark
Begin
(1) **Input** watermarked video
(2) **Apply** frame extraction mechanism using frame rate 29.97
(3) **for** frames from 1 to k
(4) **Implement** layer separation of watermarked frame
(5) **Convert** Watermarked frame into GBT Transform on each layer of $WF'(i, j)$.
(6) **Perform** extraction of USV feature of each layer of $WF'(i, j)$.
(7) **Extract** S value of watermarked frame.
(8) **Extract** watermark $W(i, j)$ from $WF'(i, j)$ using formula $W(i, j) = (WF'(i, j) - A(i, j))/\alpha$
(9) **Extract** S value of the watermark
(10) **Perform** inverse SVD to combine S value with USV of each layer.
(11) **Perform** inverse GBT Transform of watermark images
(12) **Apply** decryption mechanism to get extracted watermark
(13) **Repeat** Steps 4–12 to get extracted watermark.
(14) **End for**
(15) **End**

Algorithm 3: Watermark extraction algorithm.

frame selection time. A total of 6 Common Interchange Format (Cif) encoded videos have been taken and frame selection mechanism entirely depends upon number of scene changes in the video. Some videos have a greater number of scene changes; hence more frames will be selected. Akiyo did not have sufficient scene change detection so the watermarking technique could not be applied on that as the value of FD_k (frame difference) was not greater than K_b (threshold) so no significant frames were selected from the video; rest of the videos have significant frames selected as per frame selection algorithm.. The data sets of the videos were obtained from Figures 7(a)–7(e) which signifies some selected frames from the data set of videos. Along with these videos 2 binary watermarks and their encrypted versions have been shown; the compressed domain videos taken in the research are the same type of videos used in broadcast application; to remove unauthorized access to these videos, the given videos are embedded with encrypted watermark that addresses the issues faced by real time application. The encrypted watermark not only addresses security issues but also adds to copyright protection to achieve ownership identification. Higher values of PSNR and lower values of BER implicate the proposed technique to be efficient that leads to less loss in quality of output video. Every video will have different properties that mean frame selection in every video will be different. The same is demonstrated in this research where different videos have different number of frames getting selected.

4.1. Experimental Tests for Quality Check. The experimental results were divided into certain phases, starting with taking the input video in Avi or Mp4 file; this phase is followed by frame extraction. Frames are extracted in.png format as.jpeg is a compression format. Frames are extracted using a standard frame rate 29.97. The next phase is to embed the watermark by combining both S values of watermark and selected frames. The last phase is to check efficiency of the proposed technique by applying signal processing attacks on them which are taken in further section. The watermark embedding is done on selected frames depicted in Figures 7(a)–7(e); the videos are taken in compressed domain as uncompressed domain videos will take more time to process. The Cif format is known as Common Interchange



(a) (b) (c)

(d) (e) (f)

Figure 7: (a–e) Watermarked frames from the video; (f) selected binary watermark.

Format and it is referred to as a standardized format for picture resolution and the data has been obtained from website named https://media.xiph.org/video/derf/. Figures 8(a)–8(h) describe selected frames along with selected watermark. All videos are of the same resolution and selection of frame I s done in real time. The videos are encoded to standardized MPEG-4 format using codec x264. The value of quality parameters is taken as per comparison with original and watermarked frames.

Table 2 represents the comparison of the input videos and the number of frames selected from the given videos. It was found that Pure Storage video has higher number of frames selected out of all videos. Table 3 represents the embedding of watermark 1 on selected frames without any attack. The performance of the proposed technique is calculated with various factors represented in Table 3. Figures 9(a)–9(d) describe the performance of embedding technique against no attacks applied to it.

4.2. Experimental Tests for Time Complexity. Table 4 compiles the processing time (in seconds) required to carry out frame selection, embedding time taken for the given set of videos. The time is entirely based on processor requirements. The total time consumed depends upon selection of frames from the video. Pure Storage video has got 5 frames selected and the time for every frame varies from 20 to 35 seconds for every frame. The value of embedding time is directly proportional to number of selected frames. Total of 5 frames were selected from Pure Storage video; thus, total embedding time is the highest for the same video. The watermark embedding factor is kept being 0.02 and GBT was followed by SVD on selected frames and mixed with S value of watermark. The proposed technique is fast and, as per processor requirements, works considerably at good speed. The plots in Figures 10(a) and 10(b) signify time taken for selection of frame from 5 videos. More number of changes in the video is directly proportional to the frame selection time and watermark embedding in selected frames for a single video is dependent upon number of frames selected. The plot in Figures 10(a) and 10(b) signifies the embedding time taken by selected frames from the video. Table 4 represents the total frame selection time and embedding time of the input videos.

4.3. Processing Attacks. The robustness of the proposed technique is tested against various attack scenarios such as Gaussian Noise, Sharpening, Rotation, Blurring, and JPEG Compression. A series of experiments have been conducted to attack every watermarked frame to measure quality loss. The robustness of the technique entirely depends upon the values of PSNR, SSIM, NC, and BER.

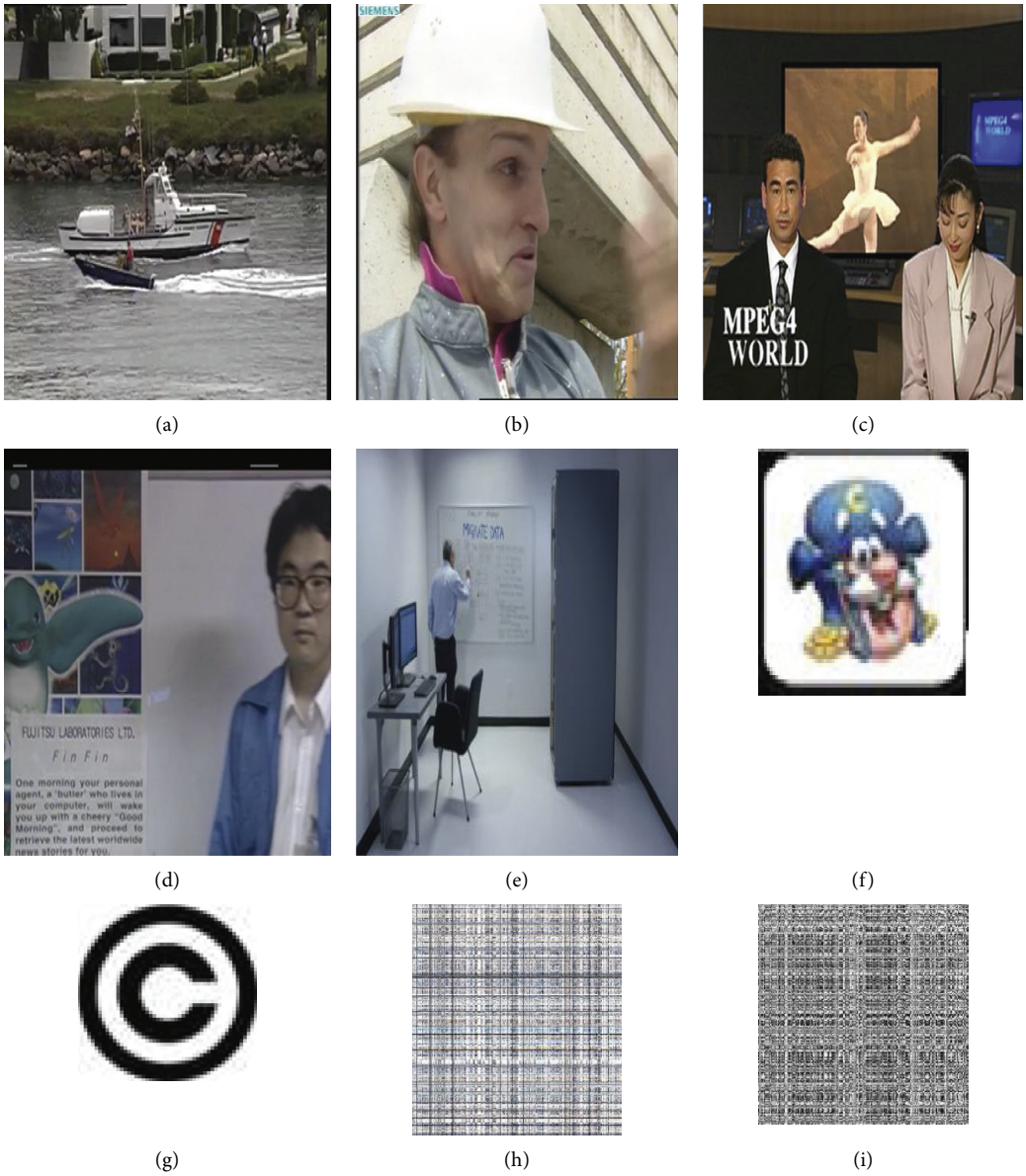


Figure 8: (a-i): Selected frames from videos: (a) Coastguard (frame # 64), (b) Foreman (frame # 134), (c) News (frame # 78), (d) Bowing (frame # 48), and (e) Pure Storage (frame #57); (f) original watermark 1, (g) original watermark 2, (h) encrypted watermark 1, and (i) encrypted watermark 2.

Table 2: Comparison of videos in terms of frame selection.

S. no.	Video name	Selected frames
1	Akiyo	0
2	Coastguard	1
3	Foreman	2
4	News	3
5	Bowing	4
6	Pure Storage	5

Table 3: Results after embedding of watermark 1 on selected frames.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	36.5062	0.99862	0.99987	0.027393
Foreman	36.6527	0.997625	0.999885	0.027284
News	36.6823	0.996863	0.99978	0.027261
Bowing	36.27048	0.99862	0.999955	0.027571
Pure Storage	36.32226	0.998002	0.999924	0.027531

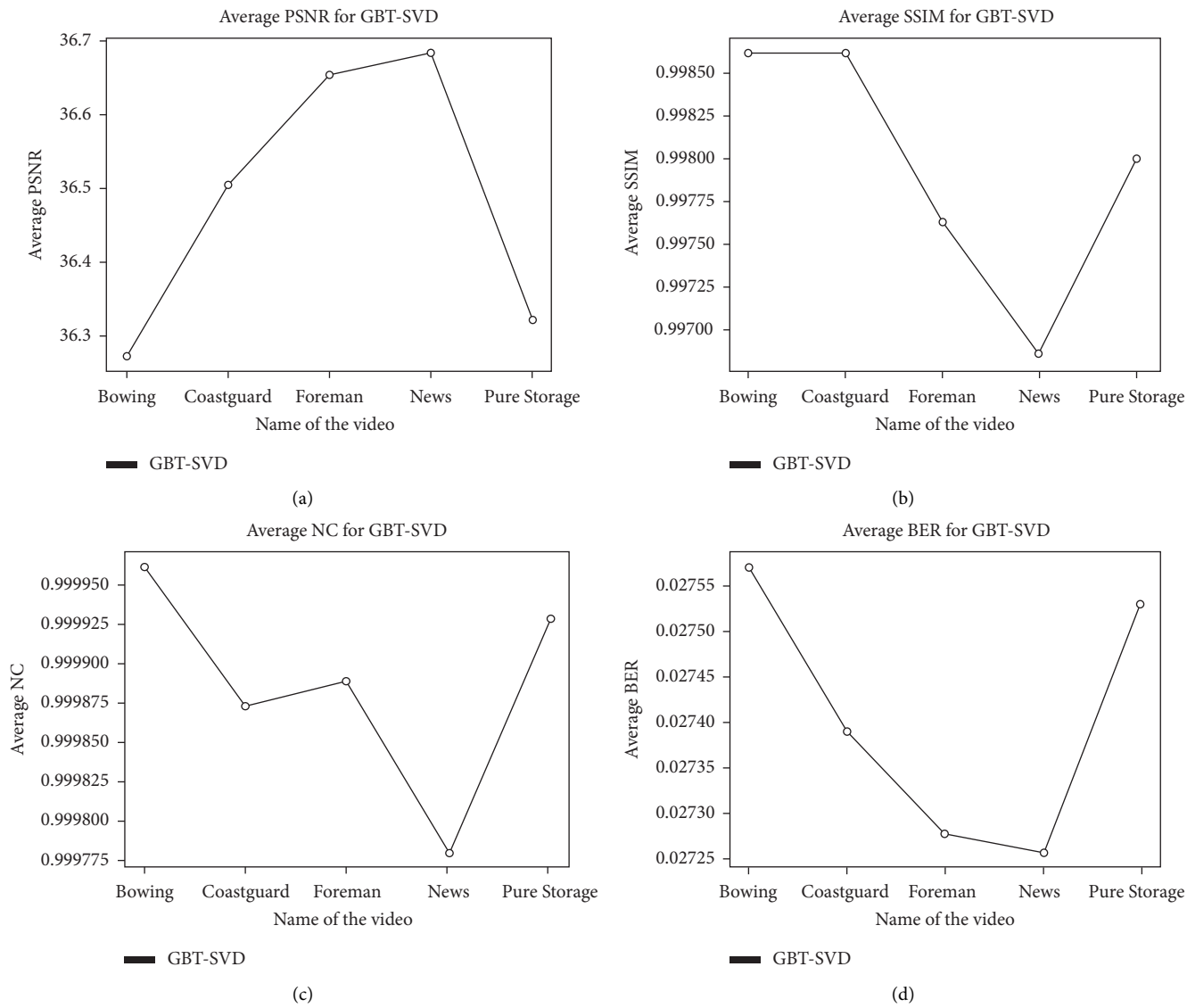


Figure 9: (a–d) Plot of PSNR, SSIM, NC, and BER w.r.t the videos taken in the proposed work for watermark 1 against no attack. (a) Average PSNR vs. no attack using watermark 1. (b) Average SSIM vs. no attack using watermark 1. (c) Average NC vs. no attack using watermark 1. (d) Average BER vs. no attack using watermark 1.

Table 4: Results of embedding time using watermark 1.

Video	Frame selection time	Embedding time
Coastguard	0.31845	1.2614
Foreman	0.94113	2.5288
News	1.19484	4.9685
Bowing	1.41451	5.3493
Pure Storage	1.16416	5.9485

4.4. Gaussian Noise Attack. In Gaussian Noise attack, a random Gaussian sequence of real values {0.01} is added to all selected frames of the watermarked video using watermark 1. It can be seen from plots in Figures 11(a)–11(d) that average PSNR, NC, and SSIM decrease with increase in attack value and BER increases with increase in attack value. Figures 11(a)–11(d) compile real time testing by applying this attack of 0.01 Gaussian value; Table 5 represents results of quality parameters after Gaussian Noise attack.

4.4.1. Sharpening Attack. In Sharpening Attack, a random sequence real value {0.01} is added to all frames of the watermarked video using watermark 1. It can be seen from plots in Figures 12(a)–12(d) that average PSNR, NC, and SSIM decrease with increase in attack value and BER increases with increase in attack value. The Sharpening Attack is applied to highlight details of the image. Sharpening Attack is an attack that enhances changes in high and low frequencies of selected frames. More changes lead to more distortion in the image. It is applied

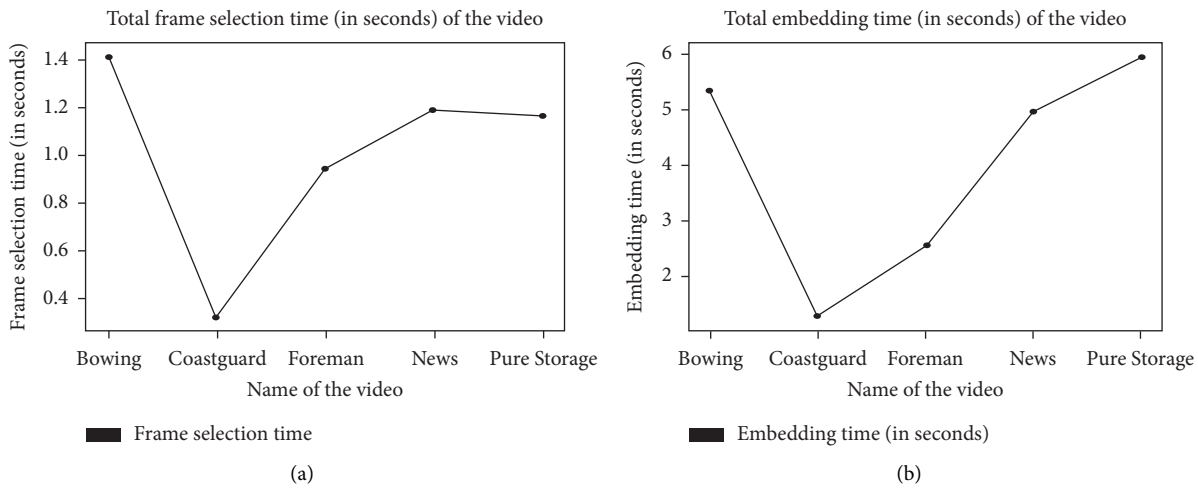


Figure 10: (a-b) Plot of total frame selection time and total embedding time (in seconds). (a) Total frame selection time (in seconds) for 5 videos. (b) Total embedding time (in seconds) for 5 videos.

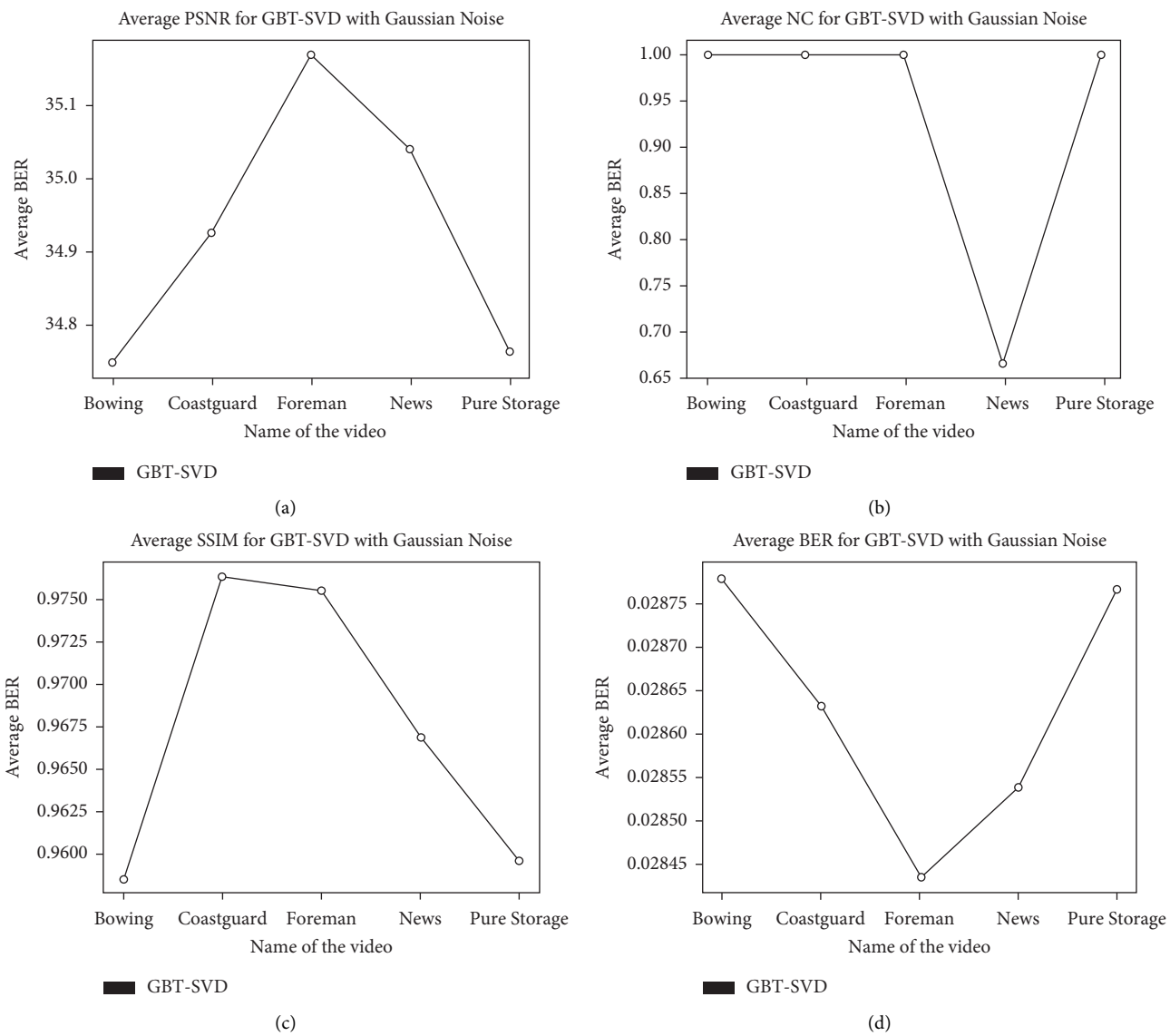


Figure 11: (a-d): Plot of PSNR, NC, SSIM, and BER w.r.t Gaussian Noise variance using watermark 1. (a) Average comparison of PSNR vs. Gaussian Noise variance. (b) Average comparison of NC vs. Gaussian Noise variance. (c) Average comparison of SSIM vs. Gaussian Noise variance. (d) Average comparison of BER vs. Gaussian Noise variance.

Table 5: Results after applying Gaussian Noise attack on watermarked frames using watermark 1 using value 0.01.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	34.9263	0.9763	0.99895	0.028632
Foreman	35.1684	0.97538	0.998965	0.028435
News	35.04007	0.966793	0.998997	0.028539
Bowing	34.74843	0.958563	0.998855	0.028778
Pure Storage	34.76392	0.959552	0.998698	0.028766

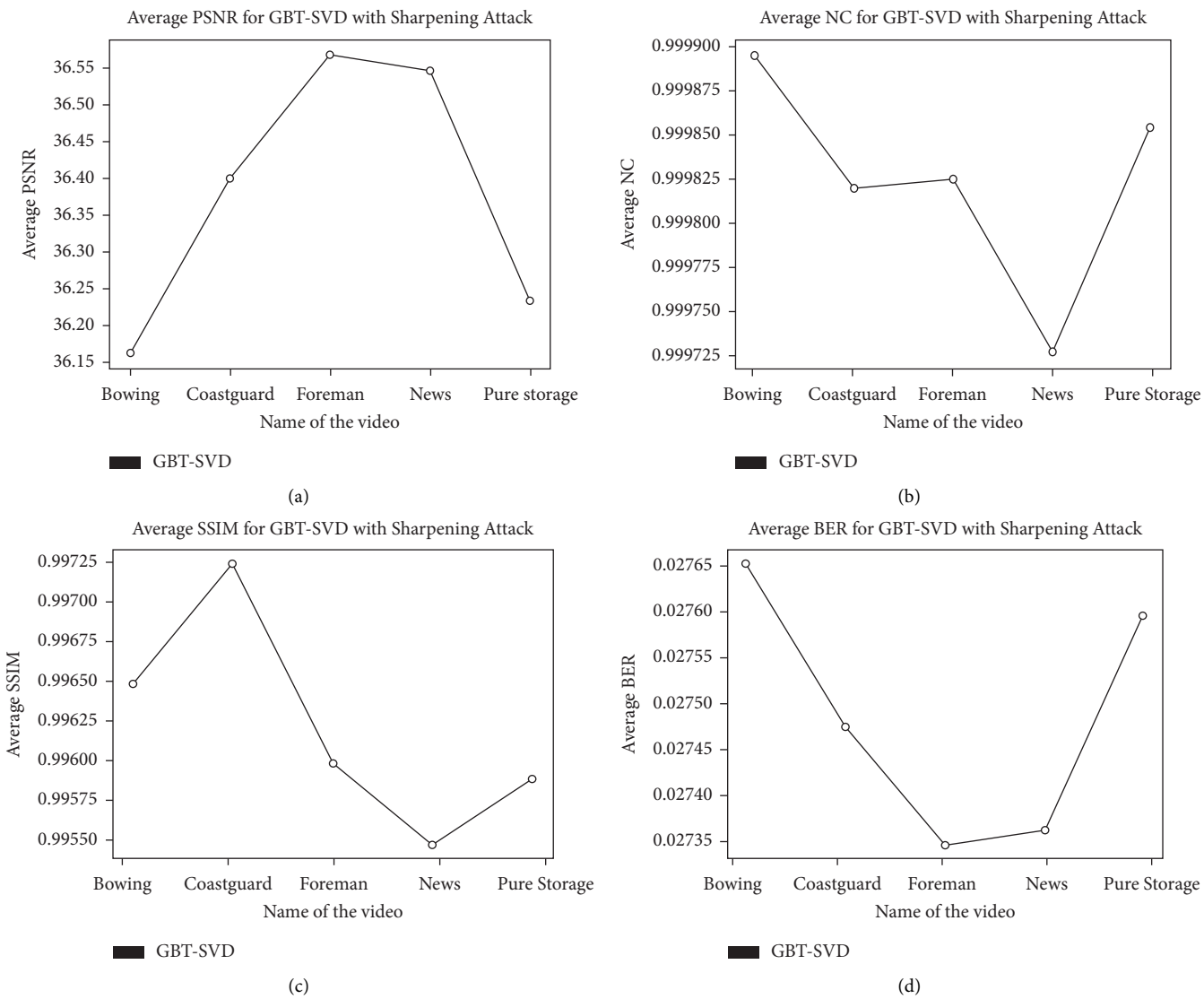


Figure 12: (a-d) Plot of PSNR, NC, SSIM, and BER w.r.t Sharpening Attack using watermark 1. (a) Average comparison of PSNR vs. Sharpening Attack variance. (b) Average comparison of NC vs. Sharpening Attack variance. (c) Average comparison of SSIM vs. Sharpening Attack variance. (d) Average comparison of BER vs. Sharpening Attack variance.

to low and high frequency bands of the image. In our research, this attack is applied to find out difference in watermarked frames with this attack and without it. The results of quality parameters after Sharpening Attack are represented in Table 6.

4.4.2. Rotation Attack. In Rotation attack, a watermarked frame is rotated with an angle of 90 using watermark 1. Higher value of Rotation attack will affect PSNR of the watermarked frame. The quality metrics of Rotation attack is affected by the higher angle in which the frame is rotated. It can be seen from plots in Figures 13(a)–13(d) that average PSNR, NC, and SSIM deteriorate with increase in attack value and BER increases with increase in attack value. The Rotation attack is carried out by rotating the watermarked frame and normal selected frame. The technique is vulnerable against Rotation attack as it does not achieve good results in that attack. The addition of optimization algorithm

Table 6: Results after applying Sharpening Attack.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	36.3996	0.99724	0.99982	0.027473
Foreman	36.56795	0.99597	0.999825	0.027347
News	36.5464	0.995467	0.999727	0.027362
Bowing	36.163	0.996473	0.999895	0.027653
Pure Storage	36.2352	0.995882	0.999854	0.027597

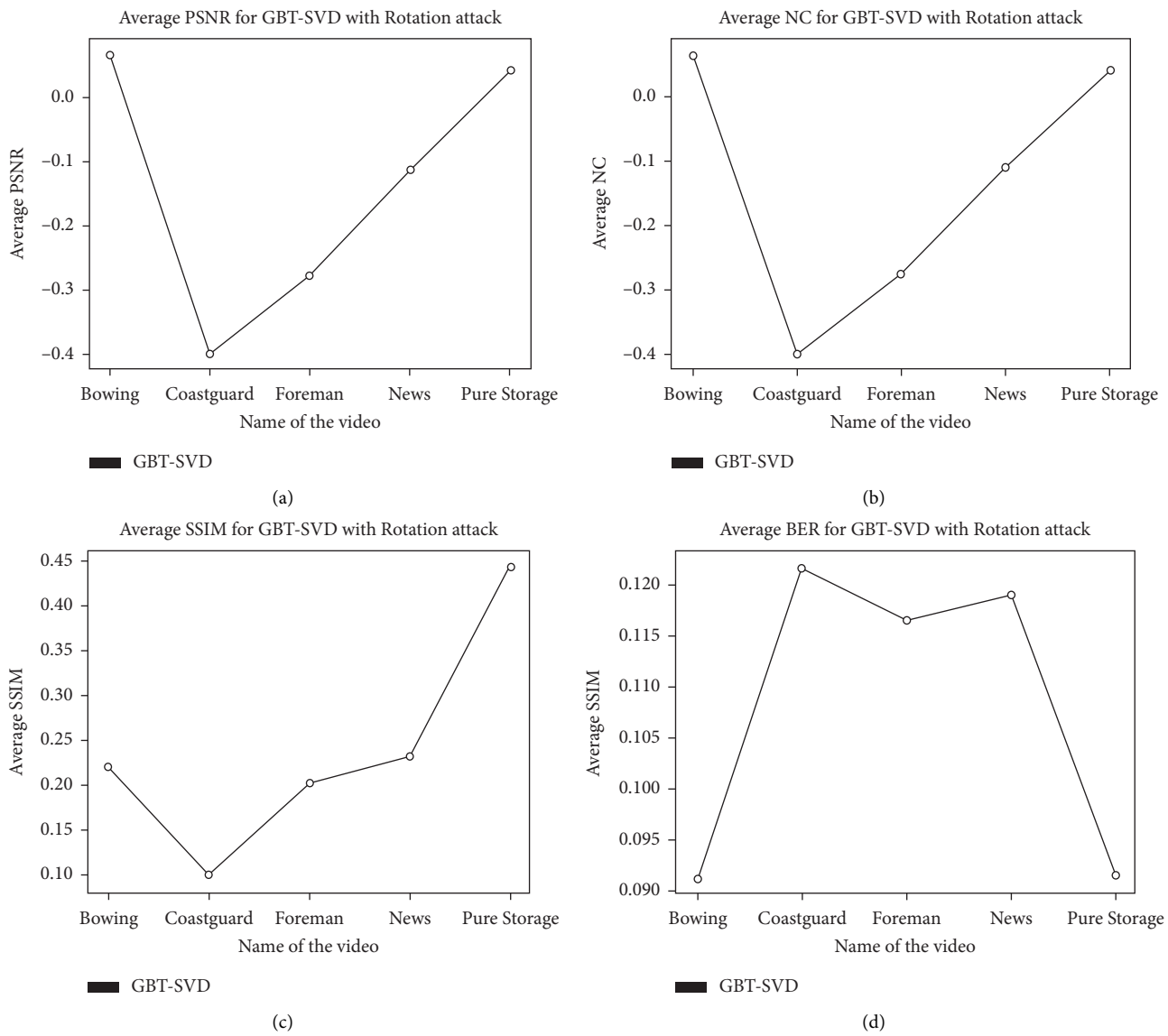


Figure 13: (a-d) Plot of PSNR, NC, SSIM, and BER against Rotation attack using watermark 1. (a) Average comparison of PSNR vs. Rotation attack variance. (b) Average comparison of NC vs. Rotation attack variance. (c) Average comparison of SSIM vs. Rotation attack variance. (d) Average comparison of BER vs. Rotation attack variance.

to find best fitness function can improve the values of quality metrics against this attack. Table 7 represents results of quality parameters after applying Rotation attack.

4.4.3. Blurring Attack. In Blurring attack, a random sequence of real values {2.05} is added to all frames of the watermarked video using watermark 1. The Blurring attack is caused by motion of an object. The more the object is moved, the lower the value of PSNR will be. It can be seen from plots in Figures 14(a)–14(d) that average PSNR, NC, and SSIM decrease with increase in attack value and BER increases with increase in attack value. In the research, we applied Blurring attack to check the motion of watermarked frame. Higher values of PSNR will indicate effectiveness of the technique. Table 8 represents results of quality parameters after applying Blurring attack.

Table 7: Results after applying Rotation attack on watermarked frames using watermark 1 using value 90.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	8.2061	0.097794	−0.39927	0.12186
Foreman	8.593	0.201262	−0.27613	0.116745
News	8.404067	0.23115	−0.1115	0.118997
Bowing	10.98838	0.220308	0.066108	0.091297
Pure Storage	11.00918	0.44313	0.041094	0.091474

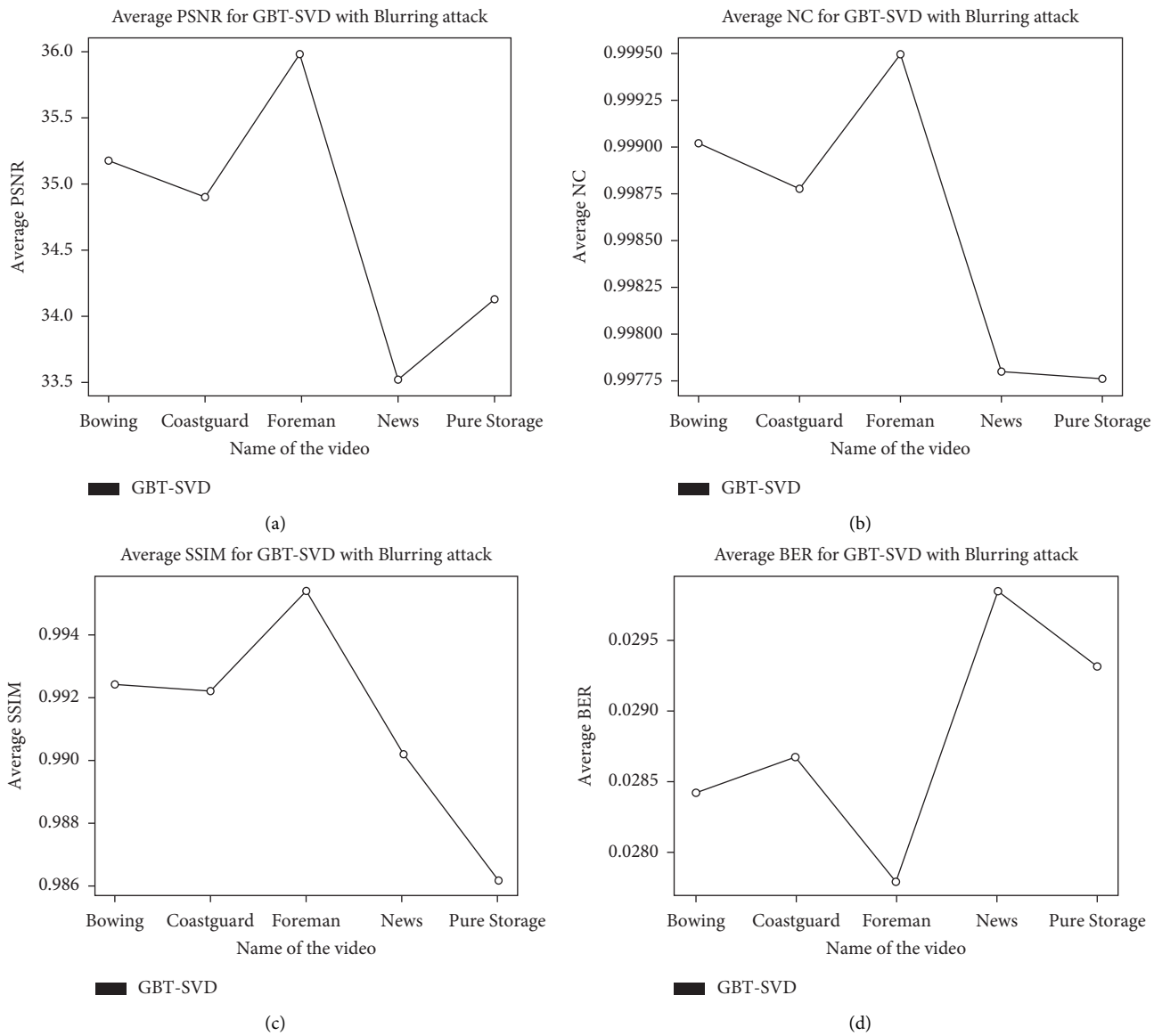


Figure 14: (a-d) Plot of PSNR, NC, SSIM, and BER w.r.t Blurring attack variance using watermark 1. (a) Average comparison of PSNR vs. Blurring attack variance. (b) Average comparison of NC vs. Blurring attack variance. (c) Average comparison of SSIM vs. Blurring attack variance. (d) Average comparison of BER vs. Blurring attack variance.

4.4.4. JPEG Compression Attack. In JPEG Compression attack, value {98} is taken and applied to all frames of watermarked video. JPEG Compression number decides how much compression attacks can be applied. JPEG Compression application on watermarked frame indicates no significant change. It can be seen from plots in Figures 15(a)–15(d) that average PSNR, NC, and SSIM decrease with decrease in value of compression attack value and BER increases with decrease in attack value. Table 9 represents results of quality parameters after applying JPEG Compression attack.

Table 8: Results after applying Blurring attack on watermarked frames using watermark 1 using value 2.05.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	34.8924	0.99216	0.99878	0.02866
Foreman	35.9857	0.995365	0.9995	0.027789
News	33.5081	0.990213	0.997803	0.029844
Bowing	35.17803	0.992393	0.999025	0.028427
Pure Storage	34.1216	0.986148	0.997758	0.029309

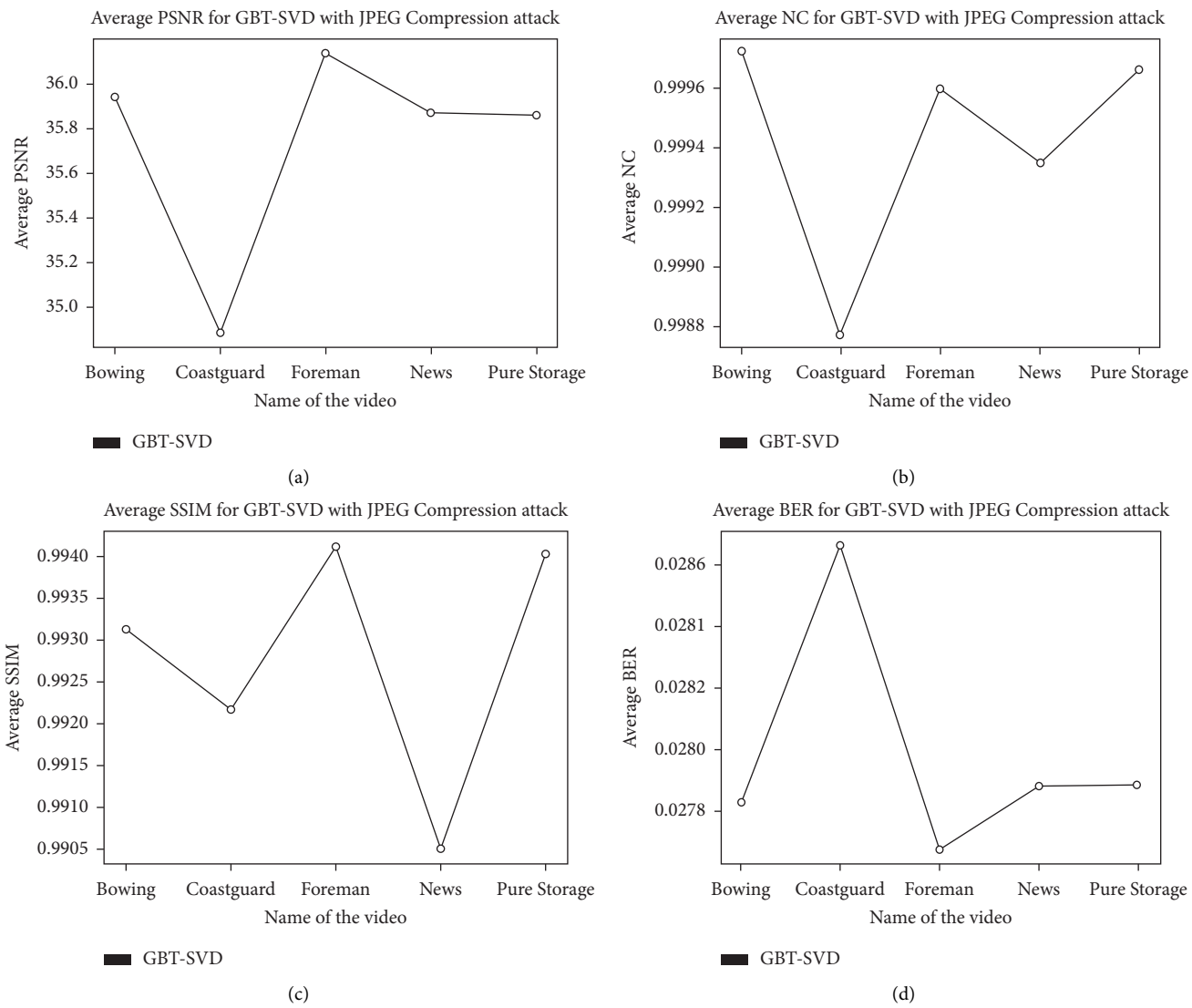


Figure 15: (a-d): Plot of PSNR, NC, SSIM, and BER w.r.t JPEG Compression attack variance using watermark 1. (a) Average comparison of PSNR vs. JPEG Compression attack variance. (b) Average comparison of NC vs. JPEG Compression attack variance. (c) Average comparison of SSIM vs. JPEG Compression attack variance. (d) Average comparison of BER vs. JPEG Compression attack variance.

Table 9: Results after JPEG attack (98 value).

Video	PSNR (db)	SSIM	NC	BER
Coastguard	34.8924	0.99216	0.99878	0.02866
Foreman	36.13615	0.99411	0.9996	0.027675
News	35.8682	0.9905	0.999357	0.02788
Bowing	35.93805	0.993125	0.999728	0.027826
Pure Storage	35.86234	0.99403	0.999662	0.027885

5. Conclusion and Future Work

We proposed a novel frame selection based watermarking technique (GBT-SVD-hyperchaotic) to address quality loss of data. Frame selection algorithm is proposed to select appropriate number of frames as addition of watermark in every frame leads to time complexity of the embedding algorithm. Frame selection is done on the basis of number of scene changes done in the video. The hybrid combination of Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption provides efficient results for watermark embedding. The proposed technique was found to be robust against many signal processing attacks, Gaussian Noise, Sharpening Attack, Rotation, Blurring, and JPEG Compression. The additional security mechanism applied in the proposed work gives added advantage over transpositional ciphers in related work. The proposed technique is fast; however, it faces the limitation of absence of optimized algorithms. The performance of the proposed technique can be improved by applying optimization algorithms like Grey Wolf Optimization that will optimize the embedding factor, thus targeting high values of PSNR.

Data Availability

The data are open and available on request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] Z. Cao and L. Wang, "A secure video watermarking technique based on hyperchaotic Lorentz system," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26089–26109, 2019.

[2] S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A survey on different video watermarking techniques and comparative analysis with reference to H. 264/AVC,"in Proceedings of the 2006 IEEE International Symposium on Consumer Electronics, St. Petersburg, Russia, pp. 1–6, 2006.

[3] D. Ye, C. Zou, Y. Dai, and Z. Wang, "A new adaptive watermarking for real-time MPEG videos," *Applied Mathematics and Computation*, vol. 185, no. 2, pp. 907–918, 2007.

[4] G.-B. Huang and L. Chen, "Convex incremental extreme learning machine," *Neurocomputing*, vol. 70, no. 16–18, pp. 3056–3062, 2007.

[5] F. Tao, D. Zhao, Y. Hu, and Z. Zhou, "Resource service composition and its optimal-selection based on particle swarm optimization in manufacturing grid system," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 4, pp. 315–327, 2008.

[6] X. Wang and M. Wang, "A hyperchaos generated from Lorenz system," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 14, pp. 3751–3758, 2008.

[7] A. Al-Haj and A. Abu-Errub, "Performance optimization of discrete wavelets transform based image watermarking using genetic algorithms," journal of Computer Science, vol. 4, no. 10, pp. 834–841, 2008.

[8] C. H. Wu, Y. Zheng, W. H. Ip, C. Y. Chan, K. L. Yung, and Z. M. Lu, "A flexible H.264/AVC compressed video watermarking scheme using particle swarm optimization based dither modulation," *AEU-International Journal of Electronics and Communications*, vol. 65, no. 1, pp. 27–36, 2011.

[9] G. Cheung, W. Kim, A. Ortega, J. Ishida, and A. Kubota, "Depth map coding using graph based transform and transform domain sparsification," in Proceedings of the 2011 IEEE 13th International Workshop on Multimedia Signal Processing, Hangzhou, China, October, 2011.

[10] T. Tabassum and S. M. M. Islam, "A digital video watermarking technique based on identical frame extraction in 3-Level DWT," in Proceedings of the 2012 15th International Conference on Computer and Information Technology (ICCIT), pp. 101–106, Chittagong, Bangladesh, 2012.

[11] M. Masoumi and S. Amiri, "A blind scene-based watermarking for video copyright protection," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 6, pp. 528–535, 2013.

[12] R. Rewani, M. Kumar, and A. Pundir, "Digital image watermarking: a survey," *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 4, pp. 1750–1753, 2013.

[13] O. S. Faragallah, "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 3, pp. 189–196, 2013.

[14] M. Kumar and R. Rewani, "Digital image watermarking using fractional fourier transform via image compression," in Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1–4, Enathi, India, 2013.

[15] P. Venugopala, H. Sarojadevi, N. Chiplunkar, and V. Bhat, "Video watermarking by adjusting the pixel values and using scene change detection," in Proceedings of the 2014 Fifth International Conference on Signal and Image Processing (ICSIP), pp. 259–264, Bangalore, India, 2014.

[16] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey Wolf optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014.

[17] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858–7867, 2014.

[18] B. Sridhar and C. Arun, "An enhanced approach in video watermarking with multiple watermarks using wavelet," *Journal of Communications Technology and Electronics*, vol. 61, no. 2, pp. 165–175, 2016.

[19] J. Hou, H. Liu, and L. Chau, "Graph-based transform for data decorrelation," in proceedings of the 2016 IEEE International Conference on Digital Signal Processing (DSP), pp. 177–180, Beijing, China, 2016.

[20] D. Kaur and S. Jindal, "A Semi Blind-DWT-SVD Video Watermarking," *Procedia Computer Science*, vol. 46, pp. 1661–1667, 2015.

[21] I. Daribo, D. Florencio, and G. Cheung, "Arbitrarily shaped motion prediction for depth video compression using arithmetic edge coding," *IEEE Transactions on Image Processing*, vol. 23, no. 11, pp. 4696–4708, 2014.

[22] C. Agarwal, A. Mishra, and A. Sharma, "A novel gray-scale image watermarking using hybrid Fuzzy-BPN architecture," *Egyptian Informatics Journal*, vol. 16, no. 1, pp. 83–102, 2015.

[23] C. Sharma, G. Singh, and G. Singh, "Efficient video watermarking technique for quality loss of data," *Indian Journal of Science and Technology*, vol. 2016, 2016.

[24] W. Wang, HY. Tan, P. Sun, Y. Pang, and B. B. Ren, "A Novel Digital Image Encryption Algorithm Based on Wavelet

Transform and Multi-Chaos," *Wireless Communication and Sensor Network*, vol. 2016, 2016.

[25] F. Seghir and A. Khababa, "A hybrid approach using genetic and fruit fly optimization algorithms for QoS-aware cloud service composition," *Journal of Intelligent Manufacturing*, vol. 2016, 2016.

[26] A. Sake and R. Tirumala, "Bi-orthogonal wavelet transform based video watermarking using optimization techniques," *Materials Today: Proceedings*, vol. 5, no. 1, pp. 1470–1477, 2018.

[27] A. Mansouri, A. Aznaveh, and F. Azar, "Blind H.264 compressed video watermarking with pattern consideration," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Texas, MA, USA, 2010.

[28] C. Sharma and A. Bagga, "Video Watermarking Scheme Based on DWT, SVD, Rail Fence for Quality Loss of Data," in Proceedings of the 2018 4th International Conference on Computing Sciences (ICCS), pp. 84–87, Jalandhar, India, 2018.

[29] A. Rajpal, A. Mishra, and R. Bala, "A novel Fuzzy selection based watermarking scheme for MPEG-4 videos using Bi-directional extreme learning machine," *Applied Soft Computing Journal*, vol. 2018, 2018.

[30] W. Wang, M. Si, Y. Pang et al., "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.

[31] M. Shabaz and C. Garg, "Clustering Yelp's sentiment data through various approaches and estimating the error rate," *Materials Today: Proceedings*, 2020.

[32] M. Kaur, D. Singh, and R. S. Uppal, "Parallel strength Pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2019.

[33] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[34] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[35] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Applied Cryptography and Noise Resistant Data Security*, vol. 1-20, 2018.

[36] H. Santoyo-Garcia, E. Fragoso-Navarro, R. Reyes-Reyes, C. Cruz-Ramos, and M. Nakano-Miyatake, "Visible watermarking technique based on human visual system for single sensor digital cameras," *Security and Communication Networks*, vol. 1–20, 2017.

[37] M. Fateh, M. Rezvani, and Y. Irani, "A new method of coding for steganography based on LSB matching revisited," *Security and Communication Networks*, vol. 1–15, 2021.

[38] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Security and Communication Networks*, vol. 1–15, 2021.

[39] S. Qin, S. Tan, F. Zhou, J. Xu, and Z. Zhang, "A verifiable steganography-based secret image sharing scheme in 5G networks," *Security and Communication Networks*, vol. 1–14, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 6617944, 17 pages
https://doi.org/10.1155/2021/6617944

Research Article

Robust Secure Color Image Watermarking Using 4D Hyperchaotic System, DWT, HbD, and SVD Based on Improved FOA Algorithm

Hira Nazir, Imran Sarwar Bajwa, Muhammad Samiullah, Waheed Anwar, and Muhammad Moosa

Department of Computer Science & IT, The Islamia University of Bahawalpur, Bahawalpur, Pakistan

Correspondence should be addressed to Imran Sarwar Bajwa; imran.sarwar@iub.edu.pk

Received 25 December 2020; Revised 1 February 2021; Accepted 12 February 2021; Published 28 February 2021

Academic Editor: Manjit Kaur

In the recent past, a different set of algorithms for watermarking and securing the color images have been developed by using transformation, decomposition, and optimization techniques for watermark embedding and extraction. In this paper, we propose an optimized and robust watermarking algorithm coupled with a 4D hyperchaotic system, and its performance is analyzed by extending and differentiating the existing work. Our contribution in the presented work is watermarking and securing the color images by an optimized algorithm that uses transformation technique such as Discrete Wavelet Transformation (DWT) and decomposition techniques such as Hessenberg decomposition (HbD) and singular value decomposition (SVD) coupled with the 4D hyperchaotic system, while the optimization is carried out by improved evolution fruit fly optimization algorithm (IEFOA). The experimental results based on different types of attacks (filter attacks, noise attacks, cropping attack, JPEG compression, motion blur, sharpening, and rotation), key sensitivity, normalized correlation, peak signal-to-noise ratio, and structural similarity index measure are done for measuring the algorithm's performance regarding invisibility and robustness. The experimental results show that the proposed scheme has excellent invisibility and keeps a good trade-off between invisibility and robustness. The experiment results show that the proposed approach outperforms the previous approaches.

1. Introduction

In the age of cloud computing and for computing, the security of data whether the sensor's data or cloud's data has become the dire need of today's age to secure it from malicious attacks. Similarly, copyright infringement problems and illegal distribution and modification while disseminating information over the Internet may arise quite frequently [1, 2]. Therefore, watermarking coupled with hyperchaotic encryption can cope up with the emerging challenges of copyright infringement, watermarking attacks, and security issues. In watermarking, a logo or secret message is hidden in the host image on the transmitting side while this logo or secret message is extracted at receiving side in order to judge the digital ownership of the received data. With the advancement of computing such as DNA and quantum-based computing, the probability to breach currently highly secured watermarks may also increase. The techniques such as HbD, DWT, and SVD have been widely used by researchers in various watermarking methods to watermark the grayscale and color images. The trade-off between invisibility and robustness has always been a challenging issue in watermarking methods and it needs optimization.

Recently, several algorithms such as the firefly algorithm [3], artificial bee colony (ABC) [4], and particle swarm and fruit fly optimization algorithms [5, 6] are employed to optimize the watermarking technique. The problem of entrusting the watermarking to cloud service provider is addressed in [7], in which the authors made the following contributions: (1) modern public-key cryptosystems are employed to avoid the associated security hazards and implementation costs of key exchange are also considered, (2) reversible watermarking techniques compatible with homomorphic cryptosystems are studied, (3) storage efficiency is studied by encrypting a long sequence of bits, (4)

data preprocessing prior to encryption is not required, and (5) both offline and online content-adaptive predictors are developed for various operational requirements. The proposed schemes achieve a remarkable balance between fidelity and reversibility under the given capacity constraints. Moreover, it significantly reduces the size of the encrypted data and improves the space efficiency. Most of the existing watermarking techniques suffer from certain watermarking attacks, are not optimized, and are not coupled with hyperchaotic maps. A few studies have been published on watermarking followed by hyperchaotic encryption [8]. To this end, a novel watermarking technique by exploiting the interblock coefficient correlation for embedding the watermark is proposed by [9], in which chaos and Arnold transform is used for improving security. The modifications are done in such a way that image processing and geometric attacks are resisted. Furthermore, it is testified that watermarking based on DWT has certain advantages such as good compression and imperceptibility; however, DWT-based watermarking schemes are not too much robust against geometric attacks [10]. Therefore, in order to make the scheme more robust against image processing and geometric attacks, matrix decomposition such as SVD and HbD is commonly used. The SVD-based schemes decompose the transformed host image into three vectors called U, S, and V. The digital watermark can be embedded into U or S or V. The S matrix is mostly used for watermark embedding owing to its robust nature against attacks [11]. Additionally, a little change in singular values does not influence the visual quality of the host image. On another note, FPP arises when singular values are used for watermark insertion. The matrices U and V can be replaced by the attacker's desired matrices for the extraction of a new watermark (that has never been inserted) to profess the false ownership. Computer science researchers have proposed the change in singular values with the help of scaling factor to control the strength of digital watermark to be embedded as shown in Sections 4.2 and 4.3 (Eq. (13) and Algorithm 3). The scaling factor can be further optimized by using different algorithms such as particle swarm and improved fruit fly optimization algorithms and bioinspired computing algorithms [5, 6, 12]. The FPP can be solved by encrypting the SVD components by using hyperchaotic systems or by using the one-way hash functions [13, 14]. Hyperchaotic encryption owing to excellent security results is the main source of strong security; i.e., the FPP can be solved. For example, the author in [15] verified the better confusion and diffusion by using the 5D hyperchaotic map to create secret keys for encryption and decryption. The initial parameters for 5D hyperchaotic are tuned by using the dual local search based multiobjective optimization, and the encryption architecture is based on two levels of permutation and diffusion. Similarly, the authors in [16–18] also used the hyperchaotic maps in a novel way for encrypting the images and obtained better results.

Specifically, in this paper, a novel digital watermarking method consisting of DWT, HbD, and SVD based on hyperchaotic encryption, gauging function (GF), and improved evolution fruit fly algorithm (IEFOA) is proposed. Specifically, GF abets IEFOA to find the optimal scaling factor α, for balancing the trade-off between imperceptibility and robustness, while hyperchaotic encryption of watermark before the use of SVD and chaotic encryption of SVD components solves the FPP effectively at a less computational cost. The main contributions of this paper include the following: (1) scheme has shown a good balance of trade-off even with the multiple size watermarks, (2) robustness is improved by coefficient modification through HbD, (3) encryption of color watermark by the 4D hyperchaotic system before SVD procedure and chaotic encryption of SVD components is also applied to make the scheme more secure, and (4) GF and IEFOA are employed to help in finding the optimal scaling factor.

The proposed work is organized as follows. Section 2 gives the related work, Section 3 highlights the preliminaries, Section 4 presents the proposed scheme, and Section 5 contains experimental results and analysis. Concluding remarks with future directions are given in Section 6.

2. Related Work

This section deals with the earlier research work done in designing color watermark embedding and extracting schemes. The list of abbreviations used in this study is shown in Table 1. Imperceptible and robust digital watermarking schemes can be a potential solution for the privacy and security of sensitive information such as Electronic Patient Records (EPRs). To this end, a combination of fast curvelet transform and SVD embeds watermark (EPR) after encoding into patient's healthy and diseased optical coherence tomography (OCT) scans [19]; this scheme has shown a high level of imperceptibility, robustness, and security of EPRs as compared to existing watermarking schemes. A digital watermark protocol proposed by [20] solves the false-positive problem by using a chaotic Kbest gravitational search algorithm in two domains, i.e., SVD and DCT. An efficient watermarking scheme in terms of imperceptibility, security, and robustness proposed by [21] embeds the watermark by Fractional Moments of Charlier–Meixner. The proposed method by [22] achieves robustness against geometric and filtering attacks and shows a better trade-off among robustness and distortion than the state-of-the-art methods. The proposed watermarking scheme in [10] uses a double encryption method based on fractional Fourier transform and DCT in the hybrid wavelet domain. The author in this scheme used multiparameter particle swarm optimization (MP-PSO) for obtaining the optimized embedding factors and reveals high security and invisibility and is robust against geometrical attacks. A robust and secure watermarking scheme to improve the management of medical images is presented in [23]. In this scheme, the techniques of invisible and zero watermarking avoid the detachment between medical images and EPRs and provide authenticity for the identification of patients. Another digital watermarking scheme comprises six modules (level shifting, mixed modulation, sign correlation, orthonormal restoration, distortion compensation, and iterative regulation) that overwhelm the inadequacies of existing SVD-based watermarking schemes while improving

Table 1: List of abbreviations.

Abbreviation	Full form
DCT	Discrete cosine transform
DFT	Discrete fractional angular transform
SVD	Singular value decomposition
LWT	Lifting wavelet transform
FOA	Fruit fly optimization algorithm
DWT	Discrete wavelet transform
HbD	Hessenberg decomposition
IEFOA	Improved evolution fruit fly optimization algorithm
FrMT	Fractional Mellin transform
WL	Wang–Landau
DE	Differential evolution
DNA	Deoxyribonucleic acid

robustness and imperceptibility [24]. In order to provide the copyright protection and ownership of digital data, the authors in [25] present an adaptive and robust watermarking scheme in which the color host and watermark images of the same size are scrambled through Arnold's chaotic map. Then, the approximate subband generated from redundant-DWT goes through SVD to produce the principal component. The principal component of scrambled host image is then embedded with scrambled watermark by using optimized Artificial Bee Colony (ABC) adaptive multiscaling factor. The use of redundant-DWT gives higher embedding capacity while adaptive multiscaling factor improves robustness, security, and visual transparency. Another scheme based on wavelet transformation followed by best-fit equation and Cuckoo Search (CS) algorithm is robust to common attacks, and the watermark is imperceptible to human eyes [26]. On the other hand, the fusion of multiple watermarking techniques such as DCT, DFT, SVD, and LWT improved the security, robustness, imperceptibility, and false-positive problem to a great extent but the authors did not perform scaling factor optimization [27]. SVD and three-level wavelet transform with global optimization scheme based on WL method in [28] keep a better trade-off between robustness and imperceptibility and obtained a better embedding coefficient. A color watermarking scheme presented in [29] converts RGB to YIQ space, separates the luminance component Y, and uses SVD, Arnold Transform, and DWT with DE algorithm for embedding, extraction, and optimization of scalar factors. The reason to choose luminance component Y is that the human eye is not sensitive to this component; thus, embedding watermark information into this component will give strength to invisibility. Watermark encryption and then embedding it in the host image proposed by [8] make use of FrMT, DPMs, and SVD, provide enhanced security due to the nonlinear transformation, and keep a balance between invisibility and robustness to some extent. Combining IWT, DWT, contourlet transform, and 3D Henon Map in embedding and extracting watermark has good imperceptibility and acceptable robustness [30]. The authors in this scheme suggested that the chaotic sequence produced by Henon Map can be used as a pseudorandom number generator after testing it on NIST, DIEHARD, and ENT test suites. To perform the watermarking, the authors in [31] divided the algorithm into four phases called image scaling, block separation by DCT, feature vector computation, watermark spotting regions, message transformation, watermark embedding, IDCT, and message restoration followed by an optimized FCM clustering with Least Favorable Whale Optimization Algorithm based watermarking scheme and obtained the effective results in terms of robustness and invisibility. A substitution scheme for RGB images watermarking based on Fourier transform is proposed in [32]. In this approach, several variants of Fourier transforms are applied to R, G, and B components of an image separately, the watermark is embedded in medium frequency band based on the combined parity of coefficients, and the obtained results are satisfactory in terms of average PSNR greater than 40 decibels for integration into a variant of Fourier transform coefficients. Another blind image watermarking scheme in the transform domain, where there is no need for a watermark and host image for extracting the watermark, gives good imperceptibility and robustness with less computational cost [33]. In this scheme, the host image is split into nonoverlapping blocks each of size 8×8, and DCT coefficients of each block are computed; then, two datasets (d1 and d2) are created from the selected blocks, and DCT coefficients of d1 and d2 are compared with the prefixed threshold values (k1 and k2) as follows: if the watermark bit value is 1, then corresponding d1 and d2 coefficient values are modified with set α value; else, the corresponding d1 and d2 coefficient values are set to zero.

3. Preliminaries

Hessenberg decomposition (HbD) is a transformation of the square matrix A into the unitary matrix Q and Hessenberg matrix H such that $A = QHQ^T$, computed by household matrices, and aids in improving the watermark invisibility [34]. To this end, watermarking based on R level DWT, HbD, SVD, logistic map, and optimization based on FOA through objective evaluation function showed a good trade-off between robustness and invisibility [13]. This scheme can further be improved by using improved FOAs.

Although basic FOA [6] has advantages including fewer parameters and simple principles but has shortcomings such as local optimization, lack of robustness, and slow convergence that can be overcome by IEFOA [35]. The inclusion of two parameters called step control denoted by λ and evolution/elimination control (ec) in IEFOA makes it different and provides an advantage over basic FOA. In basic FOA, the number of iterations in which the algorithm needs to find an optimal solution is the main drawback. In the early stage of iterations with the vast domain, a small search radius (search step) makes basic FOA weak to approach the optimal solution. In the final stage of iterations when the swarm location is close to an optimal solution, a very small scope is a better option for fine-tuning solution vectors. Therefore, a search radius with the big to small (BS) feature may overcome this drawback. The (BS) feature means that a big search step in the early stage can refine the global search ability and a small search step in end stage can refine the local search

ability by determining the scale of step for each fruit fly flexibly. Step control parameter (λ) provides the (BS) feature and can be expressed as

$$\lambda = \lambda_{\max} \times \exp\left[\log\left(\frac{\lambda_{\min}}{\lambda_{\max}}\right)\frac{\text{Iter}}{\text{Iter}_{\max}}\right], \quad (1)$$

where λ is the search radius in each iteration, while $\lambda_{\min}$, $\lambda_{\max}$, and Iter are the minimum radius, maximum radius, and iteration number, respectively. The fruit fly gets a bigger search step and hence eludes falling in local optimum value, while in the later iterations, λ decreases slower than linear decreasing.

The second parameter is called elimination parameter ev, in which the inferior swarm is eliminated and the dominant swarm is saved. The *ec* can be expressed as

$$\text{ec} = 1 - \text{elc}, \quad (2)$$

where elc is the elimination coefficient and can be defined as

$$\text{elc} = \text{elc}_{\max} \times \exp\left[\log\left(\frac{\text{elc}_{\min}}{\text{elc}_{\max}}\right)\frac{\text{Iter}}{\text{Iter}_{\max}}\right], \quad (3)$$

where $\text{elc}_{\min}$, $\text{elc}_{\max}$, Iter, and $\text{Iter}_{\max}$ are the minimum elimination coefficient, maximum elimination coefficient, iteration number, and maximum iteration number. Many bad performance swarms are removed as the search starts and the remaining advanced fly swarms will produce a new population. The repetitive process of swarm elimination will lead to the preservation of only a few swarms. The elimination procedure offers the advantage of letting IEFOA jump out of the local extremum (an extreme point having maximum or minimum value) to find a better global optimum. The beauty of IEFOA is the fact that it not only adopts λ but also segregates the inferior swarms by using ec.

The main process of IEFOA can be illustrated as follows:

Step 1. Randomly generate multiple swarms' center locations.

Step 2. Generate N new swarms; PSF in each swarm represents the population size according to the update rule of the Osphresis foraging stage.

Step 3. The optimal fruit fly is selected in each swarm as a new center location by vision foraging phase according to the fitness function value (fval).

Step 4. Center locations of all the new swarms are sorted in ascending order according to their fval.

Step 5. A certain number of inferior swarms are eliminated; the remaining dominant swarms become the next iteration swarm center locations according to the coefficient of elc and the number of swarm locations at present.

Step 6. Repeat Steps 2 to 5 till the satisfaction of termination condition. The global optimum is only obtained when the optimized process is terminated.

4. Proposed Scheme

The watermark encryption algorithm is introduced in Section 4.1 and the embedding algorithm is introduced in Section 4.2, while the extraction and decryption algorithm is introduced in Sections 4.3 and 4.4. Optimization of the proposed watermarking method to achieve the trade-off between invisibility and robustness is given in Section 4.5. The flowchart of the proposed scheme is given in Figure 1.

4.1. Watermark Encryption. A color watermark of multiple sizes ($N \times N$), where $N = 2, 4, 8, 16, 32, 128, 256, 512$ is input to the watermark encryption algorithm. Initial conditions based on the DNA sequence taken from the NCBI dataset are calculated. External key xK is extracted from the DNA sequence taken from the NCBI dataset. For example, we downloaded a DNA sequence of some animals having a length of 183015. The mean intensity value of the watermark image is used as a starting index to cut the DNA sequence from this location having a length of 128. After cutting the DNA sequence of length 128, each nucleotide base is converted into a two-bit binary equivalent according to the DNA mapping rules [36], shown in Table 2, which meet the Watson–Crick complement rule. In this way, a 256-bit binary key binK is obtained. In order to create the initial conditions $x(0)$, $y(0)$, $z(0)$, $u(0)$ for the 4D hyperchaotic system, we divide binK into 32 subgroups where each subgroup g is comprised of 8 bits and is expressed as follows:

$$\text{binK} = \{g1, g2, \ldots, g32\}. \quad (4)$$

Now, the initial conditions using binK are computed as follows:

$$\begin{cases} x(0) = \dfrac{(g1 \oplus g2 \oplus g3 \oplus g4 \oplus g5 \oplus g6 \oplus g7 \oplus g8)}{256} \\ y(0) = \dfrac{(g9 \oplus g10 \oplus g11 \oplus g12 \oplus g13 \oplus g14 \oplus g15 \oplus g16)}{256} \\ z(0) = \dfrac{(g17 \oplus g18 \oplus g19 \oplus g20 \oplus g21 \oplus g22 \oplus g23 \oplus g24)}{256} \\ u(0) = 256\dfrac{}{(g25 \oplus g26 \oplus g27 \oplus g28 \oplus g29 \oplus g30 \oplus g31 \oplus g32)} \end{cases}. \quad (5)$$

Initial conditions with control parameters (a, b, c, d, e) are input to the 4D hyperchaotic system (Equation (1)). The 4D hyperchaotic at any given initial conditions with control parameters ($a = 27.5$, $b = 3$, $c = 19.3$, $d = 2.9$, $e = 3$)

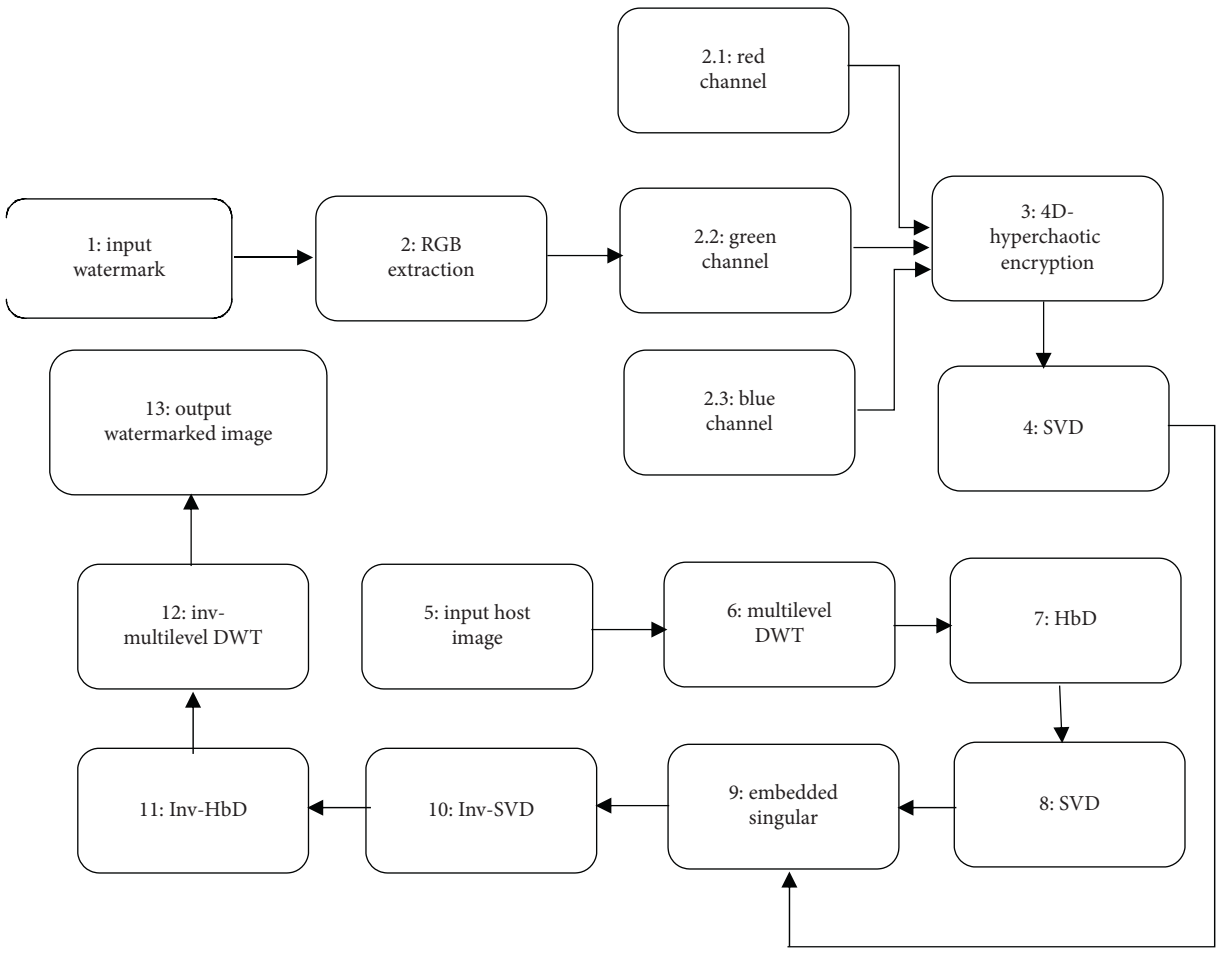


Figure 1: Watermark embedding procedure.

Table 2: DNA mapping rules.

	R1	R2	R3	R4	R5	R6	R7	R8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

behaves hyperchaotic and generates a hyperchaotic key called hyp-K which is used to encrypt the watermark.

$$\begin{cases} \dot{x}_1 = a\left(x_2 - \dot{x}_1\right) \\ \dot{x}_2 = bx_1 + cx_2 - x_1x_3 + x_4 \\ \dot{x}_3 = x_2^2 - dx_3 \\ \dot{x}_4 = -ex_1 \end{cases} \tag{6}$$

Encryption steps based on hyp-K to encrypt the watermark image are as follows (Algorithm 1).

In Algorithm 1, C_o is a constant number ranging from 0 to 255 and mEW is the mean intensity value of EW produced in Step 3.

4.2. Watermark Embedding. The inputs to the watermarking embedding algorithm are the EW of size $(N \times N)$ and the host image HI of size $(M \times N)$. And the output is watermarked host image WHI of size $(M \times N)$. The embedding steps are as follows (Algorithm 2).

4.3. Watermark Extraction. Watermark extraction takes WHI as input and the output is XW, similar to the original color watermark. The size of WHI is $M \times N$ and the size of XW is $N \times N$. The extraction steps are as follows (Algorithm 3).

4.4. Watermark Decryption. Watermark decryption is shown in Algorithm 4.

4.5. Algorithm Optimization Using IEFOA. In this section, an improved evolution fruit fly optimization algorithm (IEFOA) discussed in Section 3 is used to find the optimal scaling factor to solve the trade-off problem between invisibility and robustness. The flowchart to find the optimal scaling factor is shown in Figure 2. Invisibility is measured by PSNR and SSIM while robustness is measured by Normalized Correlation (NC). The steps to find the optimal scaling factor are given as follows.

Step 1. Initialize the parameters $S1 = \beta, \omega_i$ and $S2 = \mathrm{NS}, \mathrm{PS}, \lambda_{\max}, \lambda_{\min}, \mathrm{Iter}_{\max}, \mathrm{elc}_{\max}, \mathrm{elc}_{\min}$. The parameters in S1 such as β are the weight factor and ω_i $(i = 1, 2, 3)$ are the quantization coefficients that directly reflect the proportion of invisibility or robustness. The parameters in S2 such as $\mathrm{NS}, \mathrm{PS}, \lambda_{\max}$, $\lambda_{\min}$, $\mathrm{Iter}_{\max}$, $\mathrm{elc}_{\max}, \mathrm{elc}_{\min}$ represent the number of swarms, the population size of the fruit fly, maximum search radius, minimum search radius, maximum iteration number, maximum elimination coefficient, and minimum elimination coefficient, respectively. The set S1 with different scaling factors will be used in the gauging function (GF) which is based on the objective evaluation function (OEF) [13] and is given by

$$\mathrm{GF}(\beta, \omega_i) = \omega_1 \frac{1}{\beta} \mathrm{PSNR}(\mathrm{HI}, \mathrm{WHI}) + \omega_2 \mathrm{SSIM}(\mathrm{HI}, \mathrm{WHI}) + \omega_3 \frac{\left(\sum_{i=1}^{K} \mathrm{NC}(W, \mathrm{DW}_i)\right)}{K}, \tag{7}$$

where DW_i is the *decrypted* watermark, i.e., decrypted from extracted watermark EW_i under i_{th} attack.

The scaling factor *array* is denoted by α_i $(i = 1, 2, \ldots, n)$, where n is the max number index. The scaling factors are used in computing PSNR, SSIM, and NC. For example, the scaling factor array α_i is used to embed the watermark to produce the watermarked image, and i_{th} attack is applied on the watermarked image to produce the attacked watermarked image. After that, the PSNR and SSIM between the cover and attacked watermarked images is calculated. Similarly, NC between original and decrypted watermarks is computed. S2 will be used in IEFOA mentioned in the related work section.

Step 2. The GF values of each location for smell judgment are calculated according to Equation (7).

Step 3. In order to get the optimal scaling factor, apply IEFOA discussed in Section 3. The only modification that will be in the IEFOA is to use GF in Step 3 of IEFOA, and repeat Steps 2 to 5 of IEFOA for updating the fruit fly population location when the iterative smell concentration is superior to the previous smell concentration.

5. Experimental Results and Analysis

The invisibility and robustness of the proposed scheme are analyzed in this section. The optimal scaling factor is computed in Section 5.1, invisibility and robustness analysis is carried out in Section 5.2, false-positive problem is done in Section 5.3, and comparison with related works whenever the data is available is done in Section 5.4. Intel(R) core i3 4010 CPU@1.7 GHz with 4.0 GB RAM and MATLAB version R2015a installed on Windows 7, a 64-bit operating system, is used for experimental purposes. Except for the other images, the standard color host images Lena and Pepper each of size 512×512 and color watermark images with sizes of 256×256, 128×128, and 64×64 shown in Figure 3 are used in the experiments. The initial population size of 50 and the maximum number of iterations of 200 are empirically selected in the experiments. Aside from the above parameters, the other parameters are set according to the improved fruit fly optimization algorithm (IFFO) [35, 37]; i.e., $\lambda_{\max} = (UB - LB)/2$, $\lambda_{\min} = 10^{-14}$ $\mathrm{elc}_{\max} = 0.1$, and $\mathrm{elc}_{\min} = 0.05$.

5.1. Finding Optimal Scaling Factor. Optimal state performance is characterized by an optimal scaling factor. According to Section 4.5, an optimal n is decided and is input to gauging function (Equation (7)) to find the optimal scaling factor. The Normalized Correlation (NC) is normally used to evaluate the robustness of the watermarking algorithm and is defined by [13]

$$\mathrm{NC} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} W_{i,j} \mathrm{DW}_{i,j}}{\sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} W_{i,j}^2} \sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} \mathrm{DW}_{i,j}^2}}. \tag{8}$$

The NCs between original watermark (W) and extracted-decrypted DW watermark under various attacks and scaling factors are shown in Figure 4. The attacks used in the simulations are shown in Table 3. NC values vary in the range of $[0 : 0.06]$ and get stabilized to large extent in the range of $[0.09 : 0.2]$; therefore, the starting value can be set as $n_1 = 0.09$. Similarly, the curves for PSNR and SSIM are also shown in Figures 5 and 6. Similarly, the starting value for PSNR can be set as $n_2 = [0{:}\ 0.02]$ as values of PSNR have negative correlations with α_i within the range of $[0.009{:}\ 0.2]$, and for SSIM, it can be set as $n_3 = [0{:}\ 0.2]$ as SSIM values are almost constant within this range. And n can be calculated as $n = (n_{\max} - n_s)/M_i$, where $n_{\max} = 0.2$, n_s is a set containing all elements of n_1 that also belong to n_2 and n_3, and M_i is the minimum interval. The value of nn is then used in GF for obtaining the optimal scaling factor. Table 4 shows the better NCs under certain attacks at the scaling factor $\alpha = 0.115$.

5.2. Invisibility and Robustness Analysis. For invisibility performance, we used color images of lena and peppers as host images and colorful logos of the Islamia University of Bahawalpur, Pakistan, as watermarks with different dimensions. Except for visual representation, we also used three metrics, PSNR, SSIM, and NC, to quantify the invisibility. The invisibility performance of the proposed algorithm under no attacks, shown in Figure 7, reflects excellent invisibility. Robustness needs to be assessed when the invisibility is acceptable. In robustness, the quality of extracted watermarks is checked under certain attacks. Several cases of attacks on lena color image (512×512) embedded with watermark (128×128) are shown in Figure 8. Watermarks are extracted from attacked images by the extraction algorithm and are decrypted by the decryption algorithm. The corresponding NC values of extracted-decrypted watermarks are shown in Figure 9. The NC values

Input: color watermark image (W), initial conditions, control parameters.
Output: encrypted watermark image EW.
Step 1. Solve the 4D hyperchaotic system by using initial conditions and control parameters to produce **hyp-K**.
Step 2. $\mathrm{key}(i) = \mathrm{mod}(C_o + \mathrm{hyp} - \mathrm{K}(i), 256)$.
Step 3. $\mathrm{EW}(i) = \mathrm{XOR}(W(i), \mathrm{Key}(i))$.
Step 4. $\mathrm{key}(i) = \mathrm{mod}(\mathrm{mEW} + \mathrm{hyp} - \mathrm{K}(i), 256)$.
Step 5. $\mathrm{EW}(i) = \mathrm{XOR}(\mathrm{EW}(i), \mathrm{Key}(i))$.

Algorithm 1: Watermark encryption.

Input: **EW**, color host image (**HI**).
Output: **WHI**.
Step 1. Obtain a low-frequency subband $\mathrm{SB1}_{\mathrm{HI}}$ of RGB components of **HI** using **HW**.
$\mathrm{SB1}_{\mathrm{HI}} = \mathrm{DWT}(\mathrm{HI})$.
Step 2. Perform Hessenberg decomposition (HbD) on RGB components.
$\mathrm{HQ} = (\mathrm{Id}^n - 2\mu\mu^T)/\mu\mu^T$.
Here, $\mathrm{HQ}, \mathrm{Id}^n$, μ, μ^T are household orthogonal matrix, identity matrix, nonzero vector, and the transpose of μ, respectively. For example, HbD on $\mathrm{SB1}_{\mathrm{HI}}$ is given as:
$\mathrm{P} = (\mathrm{HQ1}, \mathrm{HQ2}, \mathrm{HQ3}, \ldots, \mathrm{HQ}_{n-2})^T \mathrm{SB1}_{HI}(\mathrm{HQ1}, \mathrm{HQ2}, \mathrm{HQ3}, \ldots, \mathrm{HQ}_{n-2})$,
$\Rightarrow H = (P^T)\mathrm{SB1}_{\mathrm{HI}}(P)$,
$\Rightarrow \mathrm{SB1}_{\mathrm{HI}} = \mathrm{PHP}^T$.
Step 3. Perform SVD on H and EW as shown in the following equations. Only the singular value S from $\mathrm{P} = (\mathrm{HQ1}, \mathrm{HQ2}, \mathrm{HQ3}, \ldots, \mathrm{HQ}_{n-2})^T \mathrm{SB1}_{HI}(\mathrm{HQ1}, \mathrm{HQ2}, \mathrm{HQ3}, \ldots, \mathrm{HQ}_{n-2})$ is used here. The other components such as U and V^T are used as a source of information in the extraction process. Similarly, SVD is also applied to the RGB components of EW. Note that components are also encrypted by a logistic map in order to avoid the false-positive problem.
$S = \mathrm{SVD}(H)$,
$U_{\mathrm{ew}}, S_{\mathrm{ew}}, V_{\mathrm{ew}}^T = \mathrm{SVD}(\mathrm{EW})$.
Step 4. Calculate the modified singular values by using the scaling factor α as follows:
$S^* = \alpha S_{\mathrm{ew}}$,
$S^{**} = S + S^*$.
Step 5. Perform an inverse SVD to get H^*.
$H^* = \mathrm{inverseSVD}(U_{\mathrm{ew}}, S^{**}, V_{\mathrm{ew}}^T)$.
Step 6. Perform an inverse HD to get $\mathrm{SB1}_{\mathrm{HI}}^*$.
$\mathrm{SB1}_{\mathrm{HI}}^* = \mathrm{inverseHD}(P, H^*, P^T)$.
Step 7. Perform inverse DWT to get watermarked host image **WHI**.

Algorithm 2: Watermark embedding.

Input: **WHI**.
Output: extracted watermark **XW**.
Step 1. WHI is decomposed into 4 subbands: $\mathrm{SB1}_{\mathrm{WHI}}, \mathrm{SB2}_{\mathrm{WHI}}, \mathrm{SB3}_{\mathrm{WHI}}, \mathrm{SB4}_{\mathrm{WHI}}$ by using DWT.
Step 2. Perform HbD on $\mathrm{SB1}_{\mathrm{WHI}}$ and get $P_{\mathrm{WHI}}, H_{\mathrm{WHI}}, P_{\mathrm{WHI}}^T$.
Step 3. Apply SVD on H_{WHI} and obtain $U_{\mathrm{WHI}}, S_{\mathrm{WHI}}, V_{\mathrm{WHI}}^T$.
Step 4. The extracted singular value S^{***} is obtained as follows:
$S^{***} = (S_{WHI} - S^{**})/\alpha$.
Here, $S^{***}$is taken from $S^{**} = S + S^*$.
Step 5. Apply inverse SVD on $U_{\mathrm{ew}}, S^{***}, V_{\mathrm{ew}}^T$ and get **XW**.

Algorithm 3: Watermark extraction.

(Figure 9) are acceptable for the median, Gaussian noise, salt and pepper, speckle noise, and JPEG compression. Moreover, NC values of extracted-decrypted watermarks under different parameters suffering from numerous attacks are also shown in Figure 10.

5.3. False-Positive Problem Analysis. Digital watermark ownership protection and authentication is a vital application of watermarking schemes; i.e., only the actual owner should be able to extract the embedded digital watermark from the images correctly. FPP problems are very common

Input: **XW**.
Output: decrypted watermark **DW**.
Steps: inverse steps of Algorithm 1 are carried out in the reverse order.

Algorithm 4: Watermark decryption.

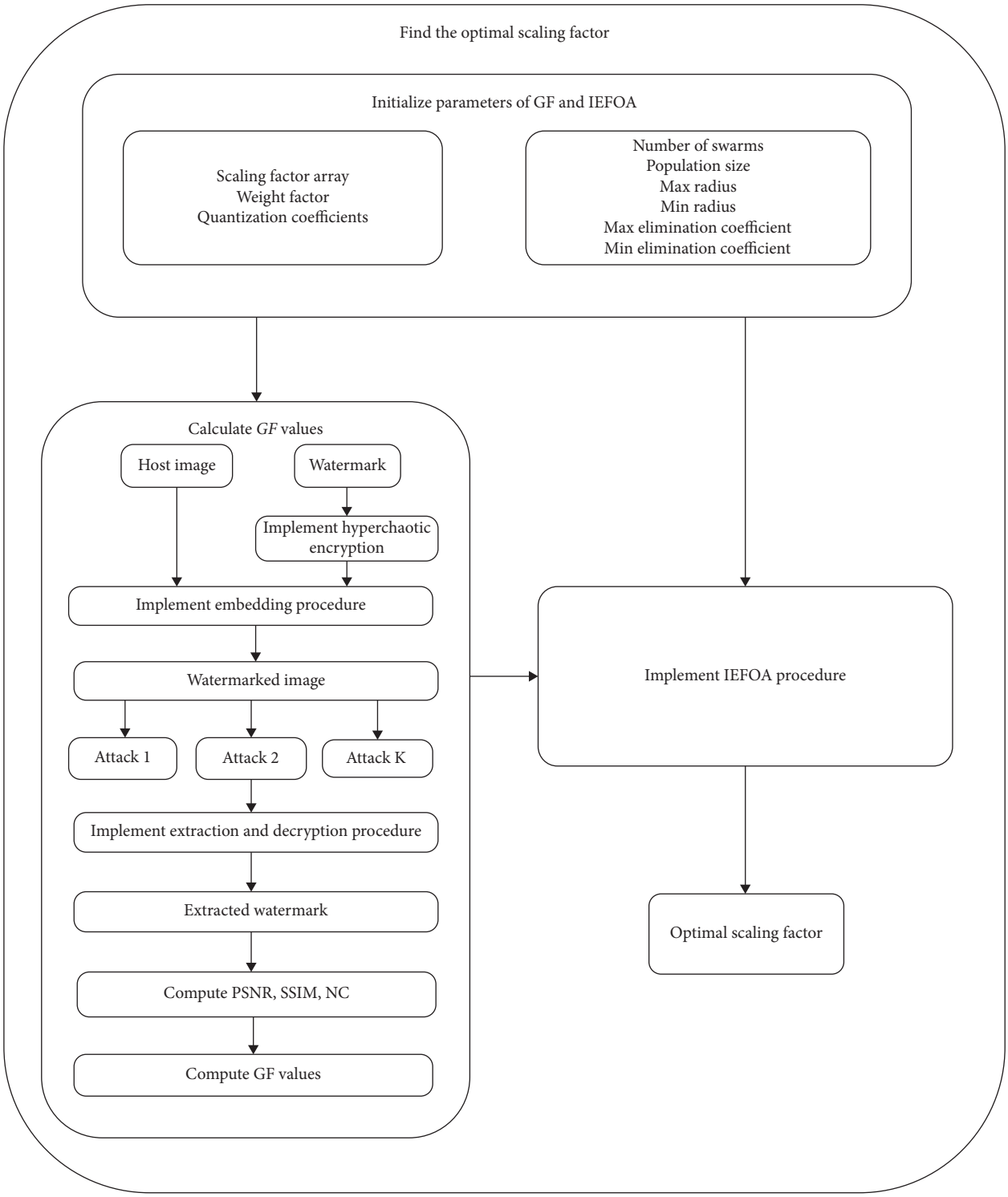


Figure 2: Scaling factor optimization.

FIGURE 3: (a-b) Host images of size 512×512. (c–e) Watermarks of size 256×256, 128×128, and 64×64, respectively.

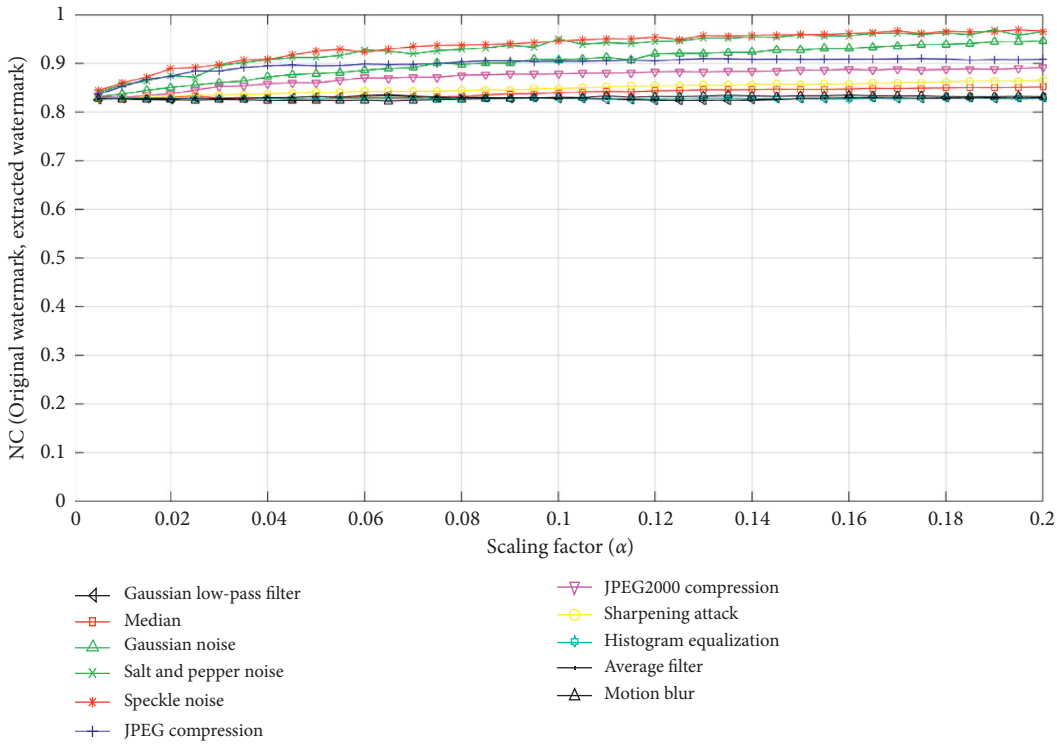


FIGURE 4: NC values under various scaling factors and attacks.

Table 3: Attacks used for experimental purpose.

Attack	Specification
Filter attack	Wiener filter (3×3) Median filter (3×3) GLP filter (3×3) Average filter (3×3)
Noise attack	Salt and pepper noise (0.001) Speckle noise (0.001) Gaussian noise (0.001)
Cropping attack	Percentage 2%
JPEG compression	QF = 50
Motion blur	Theta = 4, len = 7
Sharpening	0.8
Rotation	2 degrees

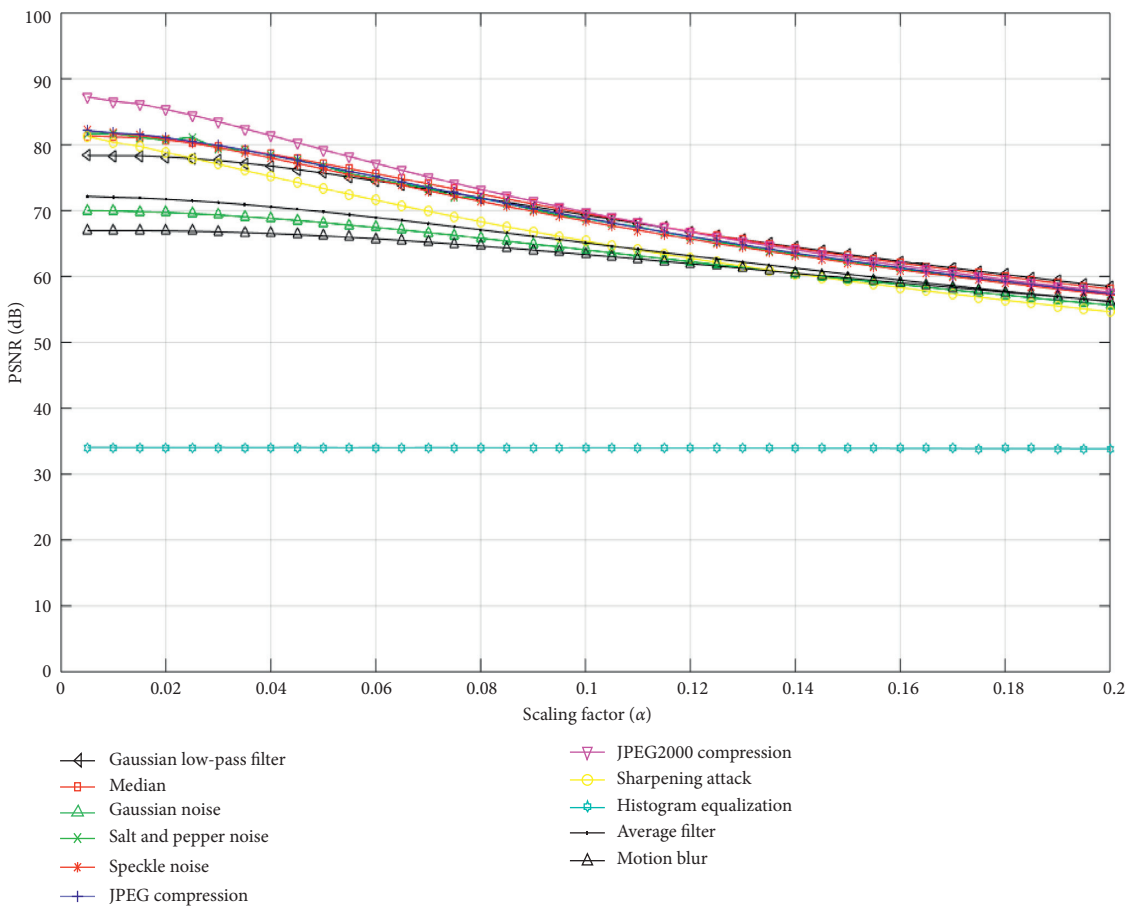


Figure 5: PSNR values under various scaling factors and attacks.

and become a challenging issue in digital watermarking schemes, where an attacker claims false ownership of the watermark by embedding and extracting the forged watermarks. This state is a serious security matter that creates a barrier in confirming the real ownership of digital media [25]. There are two approaches to embed the watermark in the SVD domain: (i) computing the singular values of watermark and cover images and then embedding the singular values of the watermark into the singular values of the cover image or (ii) by directly embedding the watermark bits into the singular values of the cover image. Generally, SVD-based watermarking schemes satisfy the criteria of invisibility and robustness but may be exposed to the increased probability of FPP.

To solve the FPP problem, we have implemented two solutions in our study. First, we have performed encryption on U and V^T components by using the logistic map. Secondly, a 4D hyperchaotic system is used to encrypt the

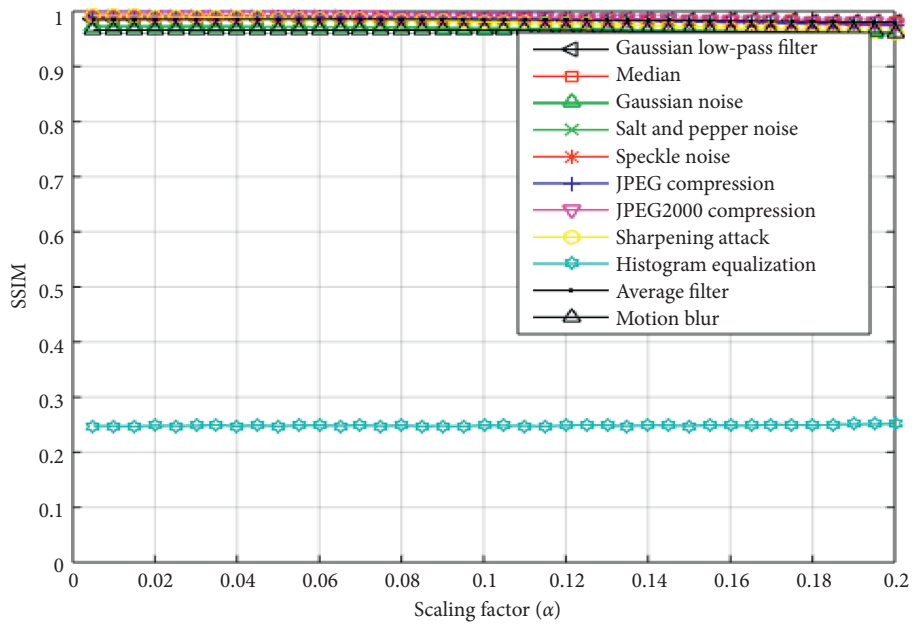


Figure 6: SSIM values under various scaling factors and attacks.

Table 4: NCs for the watermark images extracted from the attacked color watermarked images. Images shown in Figures 3(a) and 3(c) are used to compute the values of NCs under certain attacks.

Attacks	NCs at $\alpha = 0.115$
No attack	1.0
Gaussian low-pass filter	0.827244
Median filtering (5, 1)	0.887447
Gaussian noise	0.908452
Salt and pepper noise	0.944562
Speckle noise	0.951758
JPEG compression	0.900064
JPEG2000 compression	0.880474
Sharpening attack	0.99612
Histogram equalization	0.826685
Average filter	0.826939
Motion blur	0.830194

watermark before embedding it into the cover image. This gives an additional layer of security against FPP. Therefore, it will be mandatory to decrypt again the watermark after extraction. In the experimental setup of FPP, a watermark (64×64) is chosen as shown in Figure 11(a). A decrypted watermark with correct parameters having NC = 1.0000 is shown in Figure 11(b), while Figure 11(c) is the extracted watermark (NC = 0.62) with incorrect parameters which is not recognizable.

5.4. Performance Comparison. In this section, the proposed watermarking scheme is compared with some recently published schemes. The robustness comparison based on NC values after applying some attacks is shown in Table 5. It is obvious that, under some attacks, our results are better when compared with the recently published schemes. The improved results are written in bold format. The imperceptibility comparisons listed in Table 6 are based on the average NC, PSNR, and SSIM between the cover and watermarked images. It is clear that imperceptibility results are better than some recently published works when compared in most cases. Computational time consisting of watermark embedding time, watermark extraction time, watermark encryption, and decryption time is given in Table 7. The computational time is verified by using five test host images having a dimension of 512×512 taken from the USC-SIPI image database while the three RGB images (Figures 2(c)–2(e)) having dimensions of 256×256, 128×128, and 64×64 are used as watermarks. The improved results such as watermark embedding and extraction time are written in bold format.

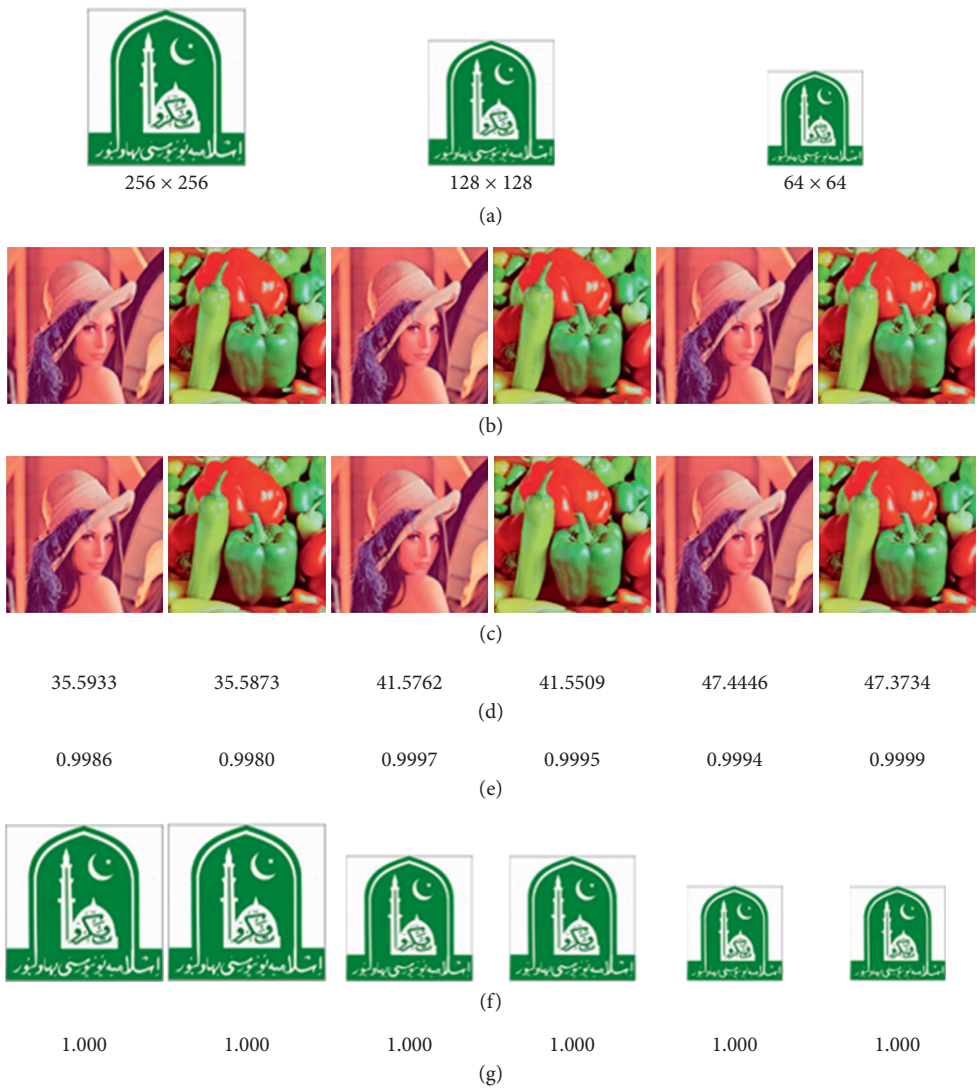
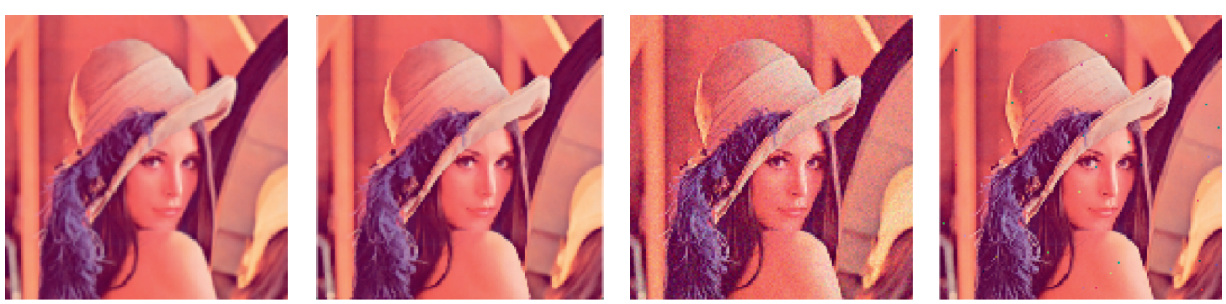


Figure 7: Invisibility test results at the scaling factor of 0.115. (a) Watermark. (b) Host image 1024 × 1024. (c) Watermarked images. (d) PSNR (db). (e) SSIM. (f) Extracted watermark. (g) NC (without attack).



(a) (b) (c) (d)

Figure 8: Continued.

Figure 8: Various attacks on watermarked images. (a) Gaussian low-pass filter, (b) median, (c) Gaussian noise, (d) salt and pepper noise, (e) speckle noise, (f) JPEG compression, (g) JPEG2000 compression, (h) sharpening attack, (i) histogram equalization, (j) average filter, (k) motion blur.

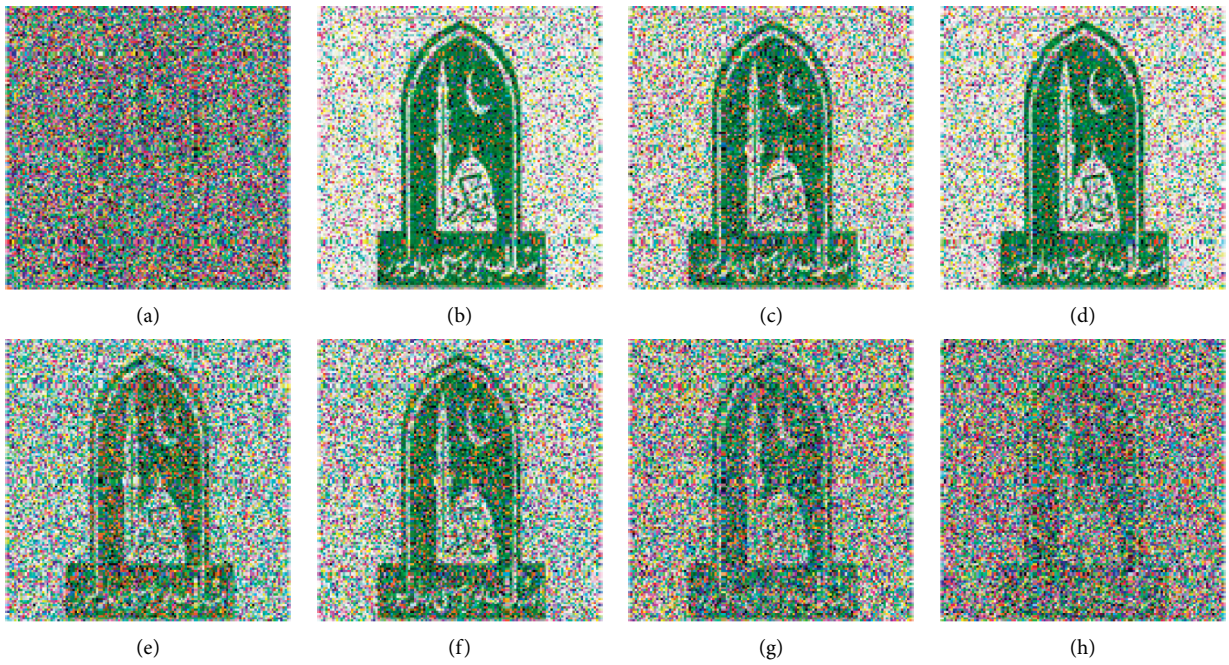


Figure 9: Continued.

(i) (j) (k)

Figure 9: Watermarks extracted from attacked watermarked images given in Figure 8. (a) Gaussian low-pass filter: NC = 0.79286. (b) Median: NC = 0.94175. (c) Gaussian noise: NC = 0.9124. (d) Salt and pepper noise: NC = 0.93241. (e) Speckle noise: NC = 0.85761. (f) JPEG compression: NC = 0.88661. (g) JPEG2000 compression: NC = 0.85736. (h) Sharpening attack: NC = 0.82034. (i) Histogram equalization: NC = 0.76479. (j) Average filter: NC =0.79288. (k) Motion blur: NC = 0.76144.

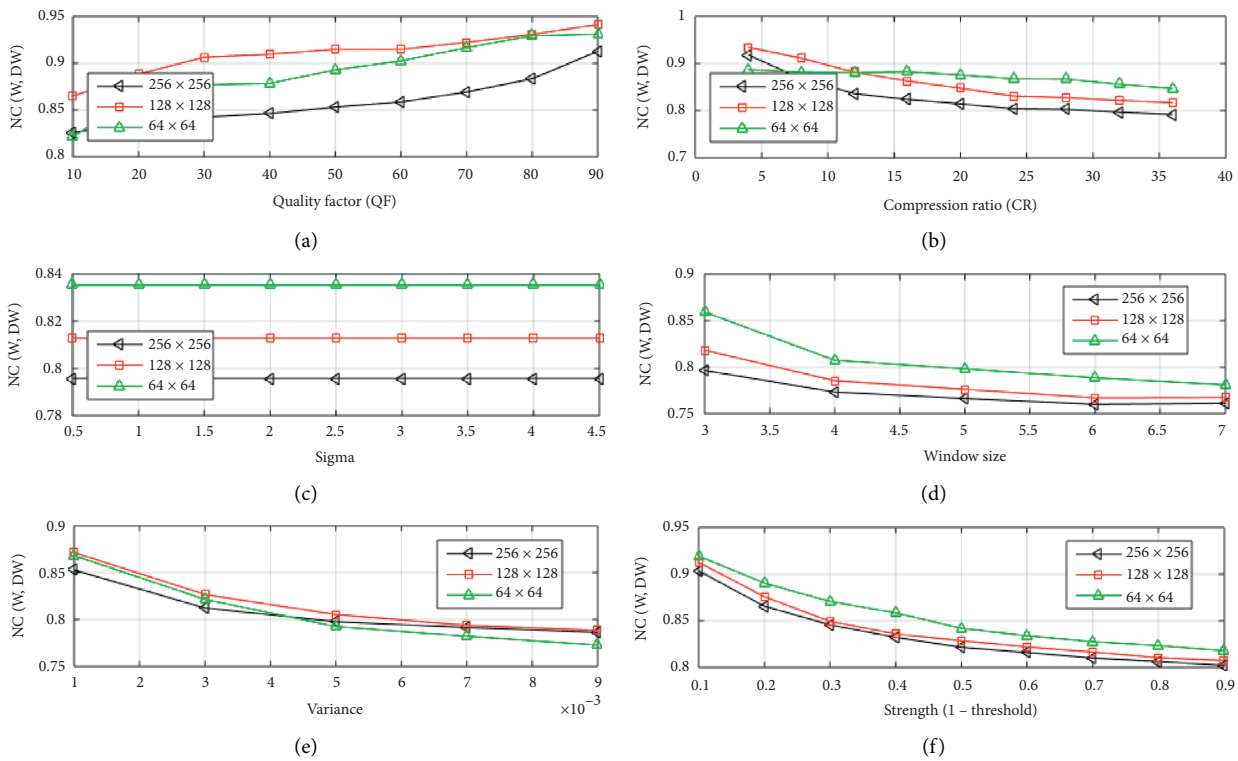


Figure 10: NC results under different attacks and parameters. (a) JPEG compression, (b) JPEG2000 compression, (c) Gaussian low-pass filter, (d) median filter, (e) Gaussian noise, and (f) sharpening attack.

(a) (b) (c)

Figure 11: FPP results with correct and incorrect parameters. (a) Original watermark, (b) the decrypted watermark with correct parameters, and (c) the decrypted watermark with incorrect parameters.

Table 5: Robustness comparison on the bases of NCs under certain attacks, whenever the data are available.

Attacks	Our NC (ref NC)
No attack	1.0 (1.0 [25], 1.0 [38])
Gaussian low-pass filter	0.827244
Median filtering (5, 1)	0.8874 (0.9968 [25], 0.5743 [39], 0.9356 [40], 0.8814 [38], 0.8370 [41])
Median filtering (3, 3)	0.847447 (0.7897 [42], 0.9188 [30], 0.9258 [9])
Average filter' (3, 3)	**0.826939** (0.7569 [42])
Gaussian noise ($M = 0$, $V = 0.0001$)	0.94806 (0.9706 [25], 0.9256 [39], 0.9387 [40], 0.9131 [38])
Salt and pepper noise (0.001)	0.984562 (0.9952 [25], 0.9287 [39], 0.9122 [40], 0.9902 [38], 0.9421 [43])
Speckle noise	0.951758
JPEG compression (Qf = 30)	0.87903 (0.9968 [25], 0.8594 [39], 0.9789 [40], 0.8469 [38])
JPEG compression (Qf = 90)	0.92956 (0.9862 [30], 0.9061 [43], 0.89109 [32])
Sharpening attack (0.2)	**0.96612** (0.9138 [42], 0.9579 [9])
Sharpening attack (0.8)	0.856457
Sharpening attack (1.0)	0.8052 (0.9638 [25], 0.9877 [39], 0.9366 [40], 0.9999 [38])
Histogram equalization	0.8785 (0.8805 [11])
Motion blur	0.830194
Flip (horizontal/Vertical)	0.9912 (1.0 [19])

The optimized scaling factor is $\alpha = 0.115$.

Table 6: Average NC, PSNR, and SSIM comparison between original and watermarked images whenever the data are available.

Image dimensions, watermark dimensions	Our NC (ref NC)	Our PSNR (ref PSNR)	Our SSIM (ref SSIM)
512×512, 256×256	0.999830	29.2385	0.9941
512×512, 128×128	0.999959	35.2342	0.9987
512×512, 64×64	0.999990	**41.1389** (40.77 [32], 35.97 [43], 38.95 [44])	**0.9997** (0.9885 [43])

The scaling factor is $\alpha = 0.115$.

Table 7: Computational time comparison whenever the data are available.

Computational time (s)	Our value (ref value)
Watermark encryption time	0.127723
Watermark embedding time	**0.350738** (0.8509 [42], 0.611810 [30], 0.7901 [41])
Watermark extraction time	**0.140354** (0.2295 [42], 0.2015 [41])
Watermark decryption time	0.127649

6. Conclusions and Future Directions

This paper is an attempt toward developing an imperceptible, secure, and robust watermarking framework with the procedure of scaling factor optimization based on IEFOA to solve the issues of authentication, integrity, and FPP. Host images can be embedded with color watermarks of multiple dimensions efficiently. Prior to the embedding procedure, the color watermark is encrypted by using a hyperchaotic system whose initial parameters are found from a DNA sequence taken from the NCBI dataset. After encrypting the RGB components of the watermark image, the embedding procedure consisting of logarithmic-based DWT, HbD, and SVD is utilized to obtain the watermarked image. Host images embedded with watermarks have shown an average PSNR greater than 35 which is considered acceptable and makes watermark invisible to the human visual system. This scheme also accomplishes excellent imperceptibility but with comparable robustness results. Moreover, the double encryption (before SVD and after SVD) makes it more secure to cope up with the security issues. A slight modification in the SVD parameters or hyperchaotic key makes the extracted watermark completely unrecognizable.

In the future, we intend to extend the proposed scheme to DICOM imaging such as ultrasound, X-rays, and magnetic resonance imaging. We also intend to make it more robust against attacks in which it is not robust. Moreover, we intend to adapt this scheme with other frequency transforms by combining it with higher-dimensional hyperchaotic systems to achieve high-efficiency batch processing.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] X. Li, S.-T. Kim, and I.-K. Lee, "Robustness enhancement for image hiding algorithm in cellular automata domain," *Optics Communications*, vol. 356, no. 1, pp. 186–194, 2015.

[2] Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "A blind double color image watermarking algorithm based on QR decomposition," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 987–1009, 2014.

[3] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858–7867, 2014.

[4] I. A. Ansari, M. Pant, and C. W. Ahn, "Artificial bee colony optimized robust-reversible image watermarking," *Multimedia Tools and Applications*, vol. 76, no. 17, pp. 18001–18025, 2017.

[5] V. Aslantas, A. Dogan, and S. Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer," in *Proceedings of the 2008 IEEE International Conference on Multimedia and Expo*, pp. 241–244, Hannover, Germany, June 2008.

[6] W.-T. Pan, "A new Fruit Fly Optimization Algorithm: taking the financial distress model as an example," *Knowledge-Based Systems*, vol. 26, pp. 69–74, 2012.

[7] C. Chang, S. Member, C. Li, and S. Member, "Privacy-aware reversible watermarking in cloud computing environments," *IEEE Access*, vol. 6, pp. 70720–70733, 2020.

[8] H. Singh, "Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain," *IET Image Processing*, vol. 12, no. 11, pp. 1994–2001, 2018.

[9] N. A. Loan, S. Member, N. N. Hurrah, and S. Member, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.

[10] Y.-M. Li, D. Wei, and L. Zhang, "Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain," *Information Sciences*, vol. 551, pp. 205–227, 2021.

[11] T. K. Araghi, A. A. Manaf, and S. K. Araghi, "A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition," *Expert Systems with Applications*, vol. 112, pp. 208–228, 2018.

[12] A. Shaik and V. Masilamani, "A novel digital watermarking scheme using dragonfly optimizer in transform domain," *Computers & Electrical Engineering*, vol. 90, Article ID 106923, 2021.

[13] S. U. Yang, D. Wei, and R. Zhou, "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019.

[14] M. Begum and M. S. Uddin, "Analysis of digital image watermarking techniques through hybrid methods," *Advances in Multimedia*, vol. 2020, no. 2, pp. 1–12, 2020.

[15] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, pp. 281–301, 2020.

[16] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[17] M. Kaur, D. Singh, and R. Singh Uppal, "Parallel strength Pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2020.

[18] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B: Lasers and Optics*, vol. 126, no. 9, 2020.

[19] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement," *IEEE Access*, vol. 7, pp. 69758–69775, 2019.

[20] R. Singh and A. Ashok, "An optimized robust watermarking technique using CKGSA in frequency domain," *Journal of Information Security and Applications*, vol. 58, Article ID 102734, 2021.

[21] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Image watermarking using separable fractional moments of Charlier–Meixner," *Journal of the Franklin Institute*, 2021.

[22] M. Sadeghi, R. Toosi, and M. A. Akhaee, "Blind gain invariant image watermarking using random projection approach," *Signal Processing*, vol. 163, pp. 213–224, 2019.

[23] M. Cedillo-Hernandez, A. Cedillo-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Improving the management of medical imaging by using robust and secure dual watermarking," *Biomedical Signal Processing and Control*, vol. 56, p. 101695, 2020.

[24] H.-T. Hu, L.-Y. Hsu, and H.-H. Chou, "An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated," *Information Sciences*, vol. 519, pp. 161–182, 2020.

[25] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing Journal*, vol. 84, pp. 1–30, 2019.

[26] M. Sundararajan and G. Yamuna, "Optimization of colour image watermarking using area of best fit equation and Cuckoo search algorithm," *Materials Today: Proceedings*, vol. 5, no. 1, pp. 1138–1146, 2018.

[27] N. R. Zhou, A. W. Luo, and W. P. Zou, "Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm," *Multimedia Tools and Applications*, vol. 78, no. 2, pp. 2507–2523, 2019.

[28] B. Wang, "An adaptive image watermarking method combining SVD and wang-landau sampling in DWT domain," *Mathematics*, vol. 8, pp. 1–20, 2020.

[29] X. Cui, Y. Niu, X. Zheng, and Y. Han, "An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image," *PLoS ONE*, vol. 13, no. 5, pp. 1–15, 2018.

[30] M. Yousefi Valandar, M. Jafari Barani, and P. Ayubi, "A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map," *Soft Computing*, vol. 24, no. 2, pp. 771–794, 2020.

[31] K. Soppari and N. S. Chandra, "Development of improved whale optimization-based FCM clustering for image watermarking," *Computer Science Review*, vol. 37, Article ID 100287, 2020.

[32] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik*, vol. 208, pp. 1–9, 2020.

[33] Sunesh and R. R. Kishore, "A novel and efficient blind image watermarking in transform domain," *Procedia Computer Science*, vol. 167, no. 2019, pp. 1505–1514, 2020.

[34] Q. Su, "Novel blind colour image watermarking technique using Hessenberg decomposition," *IET Image Processing*, vol. 10, no. 11, pp. 817–829, 2016.

[35] X. Yang, W. Li, L. Su, Y. Wang, and A. Yang, "An improved evolution fruit fly optimization algorithm and its application," *Neural Computing and Applications*, vol. 32, no. 14, pp. 9897–9914, 2019.

[36] J. Sun, M. Peng, F. Liu, and C. Tang, "Protecting compressive ghost imaging with hyperchaotic system and DNA encoding," *Complexity*, vol. 2020, Article ID 8815315, 13 pages, 2020.

[37] Q.-K. Pan, H.-Y. Sang, J.-H. Duan, and L. Gao, "An improved fruit fly optimization algorithm for continuous function optimization problems," *Knowledge-Based Systems*, vol. 62, pp. 69–83, 2014.

[38] Q. Su, G. Wang, and X. Zhang, "A new algorithm of blind color image water- marking based on LU decomposition," *Multidimensional Systems and Signal Processing*, vol. 29, no. 2018, pp. 1055–1074, 2018.

[39] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, vol. 22, no. 1, pp. 91–106, 2017.

[40] S. Roy and A. K. Pal, "An SVD based location specific robust color image watermarking scheme using RDWT and arnold scrambling," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2223–2250, 2018.

[41] K. Prabha and I. Shatheesh Sam, "An effective robust and imperceptible blind color image watermarking using WHT," *Journal of King Saud University-Computer and Information Sciences*, 2020.

[42] H. Zhang and C. Wang, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 45, pp. 1–16, 2017.

[43] Y. Cao, F. Yu, and Y. Tang, "A digital watermarking encryption technique based on FPGA cloud accelerator," *IEEE Access*, vol. 8, no. 1, pp. 1–15, 2020.

[44] H. Xu, X. Kang, Y. Chen, and Y. Wang, "Rotation and scale invariant image watermarking based on polar harmonic transforms," *Optik*, vol. 183, pp. 401–414, 2019.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 6659371, 6 pages
https://doi.org/10.1155/2021/6659371

Research Article

Exposing Speech Transsplicing Forgery with Noise Level Inconsistency

Diqun Yan, Mingyu Dong, and Jinxing Gao

Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China

Correspondence should be addressed to Diqun Yan; yandiqun@nbu.edu.cn

Received 7 December 2020; Revised 8 January 2021; Accepted 13 January 2021; Published 27 January 2021

Academic Editor: Manjit Kaur

Splicing is one of the most common tampering techniques for speech forgery in many forensic scenarios. Some successful approaches have been presented for detecting speech splicing when the splicing segments have different signal-to-noise ratios (SNRs). However, when the SNRs between the spliced segments are close or even same, no effective detection methods have been reported yet. In this study, noise inconsistency between the original speech and the inserted segment from other speech is utilized to detect the splicing trace. First, noise signal of the suspected speech is extracted by a parameter-optimized noise estimation algorithm. Second, the statistical Mel frequency features are extracted from the estimated noise signal. Finally, the spliced region is located by utilizing a change point detection algorithm on the estimated noise signal. The effectiveness of the proposed method is evaluated on a well-designed speech splicing dataset. The comparative experimental results show that the proposed algorithm can achieve better detection performance than other algorithms.

1. Introduction

With the wide spread of social networks and the rapid development of powerful audio editing tools (such as Adobe Audition and GoldWave), digital speech can be easily accessed, manipulated, and distributed. Such tools have provided lots of convenience in various aspects such as social activity, news media, entertainment, and so forth. These modified speeches, however, may cause unpredictable results when they are presented in a scene such as justice or criminal investigation. Digital speech forensics [1–3] is a valuable technique for determining the authenticity of digital speech. By analyzing the modification traces left in the suspected speech, digital forensics can identify the tampering type and locate the tampering position [4].

Deletion, insertion, and splicing are three most commonly tampering operations that can significantly change the content of the original speech. Splicing is an operation in which one or more speech segments are inserted in the original one to change the content of the target speech. In general, splicing is always accompanied by deletion and insertion. According to whether the inserted speech segment is from the original speech or not, splicing can be further divided into self-splicing and transsplicing, respectively. Specifically, self-splicing refers to copying a segment in the original speech and inserting it into the other region in the same speech. Since the self-splicing will introduce high-similarity regions in the spliced speech, the detector can take the similarity of speech features as criterion to find the splicing matching regions. In real scenarios, transsplicing is relatively more common than self-splicing. On the one hand, the forgers tend to splice speech components from different source/scenes. On the other hand, it is a hard task for the forgers to find the splicing segment from the original speech in most cases. In this work, we focus on the detection of speech transsplicing.

As an important branch of multimedia security [5, 6], many splicing detection algorithms [7–9] for digital speech have been proposed over the last decade. The ENF- (electric network frequency) based method [10] is effective for detecting speech splicing, in which the ENF signal is extracted from a questioned audio recording and matches it with the reference signal in an ENF database. Reis et al. [11] proposed an ESPRIT-Hilbert ENF estimator with an outlier

detector based on the kurtosis of the estimated ENF. Then, the kurtosis is taken as an input for a support vector machine classifier to indicate the presence of splicing. However, ENF-based detection algorithms may not be applicable when the speech is recorded with the well-designed or battery-operated devices. On the other hand, the reference ENF dataset is needed during an ENF-based forensic investigation process. Imran [12] proposed a splicing detection algorithm based on intrinsic statistical properties of suspected speech. The speech is first divided into segments using voice activity detection, and the histogram of one-dimensional LBP (local binary pattern) is exploited as the detection feature. Zhao et al. [13] introduced channel impulse response to detect speech splicing. The impulse response amplitude and background noise are used to determine the location of the splicing.

In real scenarios, in order to remove the splicing trace, the forger would try best to keep the SNR (signal-noise ratio) of the processed speech as consistent as possible between the spliced and the original regions. This will greatly increase the difficulty of the splicing detection task. As far as we know, there is no prior work on transsplicing detection with the same SNR. In this study, we proposed an approach for detecting transsplicing with the same SNR. First, the Sorensen algorithm [14] is utilized to estimate the noise level of the suspected speech. Then, the variances of Mel frequency cepstral coefficient (MFCC) [15] for estimated noise signal are calculated as the detecting features. Finally, the spliced region is located by a change point detection algorithm based on the penalty cost function [16]. The performance of the proposed algorithm is evaluated on a well-designed speech splicing dataset. The experimental results show that the proposed algorithm achieves better detection accuracy compared with other algorithms.

The rest of the study is organized as follows. The main work of this study is described in Section 2, in which noise estimation, feature extraction, and the change point detection algorithm are described in detail. Section 3 will present the splicing dataset and the experimental results. Finally, the conclusion is drawn in Section 4.

2. Proposed Transsplicing Detection Algorithm

The proposed framework for transsplicing detection and localization is shown in Figure 1. First, the Sorensen algorithm is adopted to estimate the noise signal. Next, the estimated noise is framed, and its Mel-frequency cepstral coefficients are extracted. The variance of the coefficients is calculated as the detecting feature. Finally, the change point detection algorithm is applied on the variance sequence to detect and locate the splicing.

2.1. Noise Estimation. Sorensen [14] proposed a recursive averaging noise estimation algorithm. The idea is that different attenuation rules are adopted to different regions to estimate the noise in the speech accurately. Figure 2 shows the flowchart of this algorithm.

Let $y(i)$ be the suspected speech at time i, which consists of clean speech $s(i)$ and additive noise $n(i)$. First, the windowed and framed speech signal is subjected to short-time Fourier transform (STFT):

$$Y(\lambda, k) = S(\lambda, k) + N(\lambda, k), \tag{1}$$

where $\lambda \in Z$ is the time index, $k \in \{0, 1, \ldots, K-1\}$ is the frequency bin index, L is the window length, and $S(\lambda, k)$ and $N(\lambda, k)$ are the STFT coefficients of $s(i)$ and $n(i)$, respectively.

Then, the periodograms P_Y can be calculated as

$$P_Y(\lambda, k) \triangleq |Y(\lambda, k)|^2. \tag{2}$$

Next, P_Y is spectrally smoothed to produce $p_Y(\lambda, k)$ and then temporally smoothed to $p(\lambda, k)$. Then, the temporal minimum values $p_{\min}(\lambda, k)$ could be tracked within a minimum search window of length $D_{\min}$, that is,

$$p_{\min}(\lambda, k) = \min\left(p(\psi, k) \mid \lambda - D_{\min} < \psi \le \lambda\right), \tag{3}$$

where $\psi \in Z$, and $D_{\min} = U * V$. Window D represents an analysis window length. Since it is computationally expensive to find minimum in each frequency band for each frame, an efficient procedure [17] is proposed in which the analysis window is divided into U subwindows of V samples. Hence, the minimum is updated for every V samples, stored it for later use, and reduced the number of comparation operations per frame and frequency bin on $1 + (U-1)V$.

For $D(\lambda, k) = 1$, the noise periodogram estimation is equal to a time-varying power scaling of the minimum tracks $p_{\min}(\lambda, k)$. For $D(\lambda, k) = 0$, it is equal to the noisy speech periodogram $P_Y(\lambda, k)$, that is,

$$P_{\widehat{N}}(\lambda, k) = \left\{ \begin{array}{ll} R_{\min}(\lambda) p_{\min}(\lambda, k), & \text{if } D(\lambda, k) = 1, \\ P_Y(\lambda, k), & \text{if } D(\lambda, k) = 0, \end{array} \right\}, \tag{4}$$

where $D(\lambda, k)$ is used to determine whether speech exists. $R_{\min}(\lambda)$ is a bias compensation factor, and it only updates in the nonspeech frames.

A smooth estimate of the noise magnitude spectrum can be obtained by

$$|\widehat{N}(\lambda, k)| = \sqrt{\widetilde{P}_{\widehat{N}}(\lambda, k)}. \tag{5}$$

After the above steps, we obtained the enhanced speech $\widehat{s}(i)$. Finally, the estimated noise signal $\widehat{n}(i)$ can be obtained by subtracting the enhanced speech $\widehat{s}(i)$ from the noisy speech $y(i)$, that is,

$$\widehat{n}(i) = y(i) - \widehat{s}(i). \tag{6}$$

It is seen from equation (3) that $D_{\min}$ plays an important role in the noise estimation process. $D_{\min}$ is mainly used to control a fixed-length window. In the noise estimation process of each frame, the minimum $p_{\min}(\lambda, k)$ in the window is tracked, and the value obtained by the tracking is used to continuously update $p_{\min}(\lambda, k)$. Finally, the noise power spectrum $P_{\widehat{N}}(\lambda, k)$ is calculated by $p_{\min}(\lambda, k)$. It can be seen from the above analysis that reasonable adjustment

Figure 1: Framework of proposed splicing detection and localization.

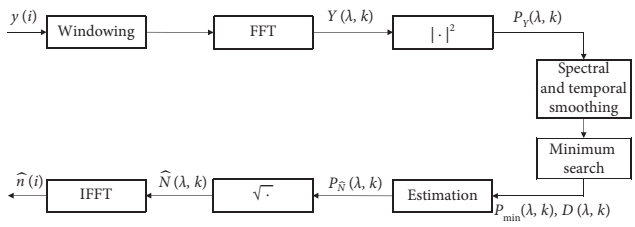


Figure 2: Flowchart of the Sorensen noise estimation algorithm.

of U and V can effectively improve the noise estimation performance of the algorithm.

2.2. Detection Feature Extraction. For each frame of the estimated noise, Mel frequency cepstral coefficients are extracted, which is based on the human peripheral auditory system. Figure 3 shows the diagram of MFCC extraction.

First, the estimated noise signal $\widehat{n}(i)$ is subjected to DFT to obtain a linear spectrum $\widehat{N}(k)$. Then, $\widehat{N}(k)$ is filtered by the Mel frequency filter bank $H_m(k)$ to obtain the Mel spectrum. In order to make the result more robust to noise and spectral estimation errors, the logarithmic energy of the Mel spectrum is generally taken, that is,

$$L(m) = \ln\left[\sum_{k=1}^{N} |\widehat{N}(k)|^2 H_m(k)\right], \quad m = 1, 2, \ldots, M, \tag{7}$$

where m is the number of filter banks.

Next, $L(m)$ is subjected to DCT to obtain the MFCC coefficient:

$$mfcc(j) = \sum_{m=1}^{M} L(m)\cos\left(n(m-0.5)\frac{\pi}{m}\right), \quad (1 \le j \le J), \tag{8}$$

where j is the index of the cepstral coefficients.

Finally, for each frame, the variance of $mfcc(j)$ can be calculated by equation (9), and we can obtain a variance sequence for each suspected speech.

$$V = \frac{1}{J}\sum_{j=1}^{J}(mfcc(j) - \overline{mfcc})^2. \tag{9}$$

2.3. Change Point Detection. Since the segments of trans-splicing come from the different sources/scenes, we consider the inconsistencies of the noise characteristics mixed in the suspected speech to be a clue of splicing. It means that there will be a change on noise characteristics where the splicing happened. Hence, the splicing detection and localization can be transformed into a change point detection problem. Algorithms for change points' detection [18–20] have made good progress in recent years. Lavielle [16] proposed a model selection method based on a penalized contrast which is applied to the change point problem. It can be used for estimating the number of change points and their location. In this work, Lavielle's algorithm is adopted to find the splicing positions.

Let $V = (V_1, V_2, \ldots, V_n)$ be the variance sequence of estimated noise signal and K be some integer. Similarly, let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{K-1})$ be a sequence of integers satisfying $0 < \alpha_1 < \alpha_2 <, \cdots, < \alpha_{K-1} < n$. For any $1 \le k \le K$, let $M(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}; \beta)$ be a contrast function for estimating the unknown true value of the parameter β in the segment k. It means that there will be an estimated value of β ($\widehat{\beta}$) when the contrast function reaches it minimum. In other words, the minimum contrast estimate $\widehat{\beta}(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K})$, computed on segment k of α, is defined as a solution of the following minimization problem:

$$M\left(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}; \widehat{\beta}\left(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}\right)\right) \le M\left(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}; \beta\right). \tag{10}$$

Then, we define the contrast function $J(\alpha, v)$ as

$$J(\alpha, s) = \frac{1}{n}\sum_{k=1}^{K} M\left(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}; \widehat{\beta}\left(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}\right)\right), \tag{11}$$

where $\alpha_0 = 0$, $\alpha_K = n$.

As an example, consider the flowing model:

$$V_i = \mu_i + \sigma_i \varepsilon_i, \quad (1 \le i \le n), \tag{12}$$

where ε_i is a sequence with zero mean and unit variance. In the case of changes in the variance, μ_i is a constant sequence and σ_i is a piecewise one. The contrast function can be defined as a Gaussian log-likelihood, even if ε_i is not a Gaussian sequence.

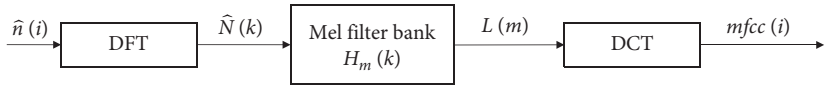


Figure 3: Diagram of MFCC extraction.

$$M\left(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_K}; \sigma^2\right) = (\alpha_k - \alpha_{k-1})\log\left(\sigma^2\right) + \frac{1}{\sigma^2}\sum_{i=\alpha_{k-1}+1}^{\alpha_K}(V_i - \mu)^2. \quad (13)$$

Then,

$$\mathrm{J}(\alpha, v) = \frac{1}{n}\sum_{k=1}^{K}(\alpha_k - \alpha_{k-1})\log\left(\hat{\tau}^2_{\alpha_{k-1}+1:\ \alpha_k}\right), \quad (14)$$

where $\hat{\tau}^2_{\alpha_{k-1}+1:\ \alpha_k} = (1/(\alpha_k - \alpha_{k-1}))\sum_{i=\alpha_{k-1}+1}^{\alpha_K}(V_i - \overline{V})^2$ is the variance of $(V_{\alpha_{k-1}+1}, V_{\alpha_{k-1}+2}, \ldots, V_{\alpha_k})$. For instance, when the maximum number of segments $K_{\max} = 3$, the number of change points is $K_{\max} - 1 = 2$, and the change boundary is (α_1, α_2).

Finally, we summarize our splicing detection algorithm as follows. First, we estimate the power spectral density $P_{\hat{N}}(\lambda, k)$ of the noise in the noisy speech signal $y(i)$ and then use $P_{\hat{N}}(\lambda, k)$ to obtain the enhanced speech signal $\hat{s}(i)$. Therefore, the noise signal $\hat{n}(i)$ can be estimated with the noisy speech $y(i)$ and the enhanced speech $\hat{s}(i)$. Then, the estimated noise $\hat{n}(i)$ is framed and windowed, and then for each frame, M-dimensional MFCC coefficients are calculated. The variance sequence $V = (V_1, V_2, \ldots, V_n)$ of MFCC coefficients is obtained and taken as the input of the change point detection algorithm, and then, the penalty cost function is constructed by equation (11). Finally, the estimated parameters of the penalty cost function $K^* - 1$ and $(\alpha_{K^*-2}, \alpha_{K^*-1})$ represent the number of change points and the boundaries of the change segments, respectively. Among them, the boundary of the change segment is the final detected tampering position.

3. Experimental Results

In this section, we first describe the dataset adopted in this work. Additionally, as mentioned in subsection 2.1, the performance of the proposed detection algorithm depends strongly on the effectiveness of the noise estimation. Hence, the noise estimation algorithm is evaluated to find the optimal parameters. Then, the performance of the proposed splicing detection method with optimal noise estimation is present.

3.1. Splicing Dataset. The transsplicing speech samples in this study are created based on NOIZEUS speech corpus [21] which is derived from the clean speech contaminated by various kinds of noise in the real world. The clean speech comes from 30 IEEE statements containing three male and three female pronunciations. The noise signals in NOIZEUS come from the AURORA-2 database [22], including noise from train stations, airports, exhibition halls, streets, and restaurants, as well as car noise, noise from commuter trains, and babble noise from multiperson speech. During noise contamination, various SNR cases including 0 dB, 5 dB, 10 dB, and 15 dB have been considered.

The creation process of the splicing speech dataset is as follows. First, the samples of NOIZEUS corpus are divided into two classes: the original samples and the samples to be spliced. Then, for each sample to be spliced, we further cut it into 4 different segments by using random numbers. For each original sample, a pseudorandom generator is used to determine where the segment will be spliced. Next, the splicing is performed, and the spliced speech is saved with the original sampling rate. In this work, the SNR of the original sample is kept the same as the segment to be spliced.

In the experiment, there will be 42 types of samples in each splicing subset, and each type contains 30 samples. As a result, there will be 1260 samples in each splicing subset. Each sample is 8 KHz, mono, 16 bit quantized, and the duration is 3-4 seconds.

3.2. Performance Evaluation on Noise Estimation. It can be seen from the analysis in Section 2.1 that the parameters U and V will affect the performance of the noise estimation algorithm. In order to find the optimal U and V, we first adjust the U and V values in the Sorensen algorithm to estimate the noise of 1260 segments of each subset and then calculate the average SNR of the 1260-segment speech under each U and V case. The experimental results for 0 dB and 5 dB speech are given in Tables 1 and 2.

It can be clearly seen from Tables 1 and 2 that U and V have a great influence on the performance of the Sorensen algorithm. For example, the estimation error for 0 dB case is minimized at −0.0737 dB when (U, V) is (2, 5). And the best choice for 5 dB case is (4, 4). Table 3 gives the optimal U and V for various SNR cases.

Additionally, we compared the optimized Sorensen algorithm with other typical noise estimation algorithms. From Table 4, the optimized algorithm achieves the best estimated results in various SNR cases.

3.3. Performance Evaluation on Splicing Detection. In MFCC extraction, we set the number of filters m to 27 and the number of cepstral coefficients J to 12. For Lavielle's algorithm [16], we set the maximum number of segments $K_{\max}$ to 3 and only variance change is considered.

Table 1: Noise estimation for 0 dB.

		V						
		8	7	6	5	4	3	2
U	5	1.9714	1.7684	1.5395	1.2562	0.8877	0.4256	−0.2804
	4	1.6638	1.4731	1.2296	0.9308	0.5658	0.0819	−0.6422
	3	1.2830	1.0713	0.8185	0.5161	0.1296	−0.3664	−1.0596
	2	0.7330	0.5187	0.2536	**−0.0737**	−0.4621	−0.9503	−1.5494

The value in bold is used to emphasise that the noise estimation algorithm achieves the best performance when (U, V) is (2, 5).

Table 2: Noise estimation for 5 dB.

		V						
		8	7	6	5	4	3	2
U	5	7.0750	6.8253	6.5178	6.1066	5.5315	4.7870	3.5437
	4	6.6826	6.4245	6.0547	5.5989	**5.0011**	4.1934	2.8933
	3	6.1350	5.8040	5.4229	4.9272	4.2658	3.4006	2.1375
	2	5.2449	4.9374	4.4928	3.8981	3.1890	2.3344	1.2947

The value in bold type is used to emphasise that the noise estimation algorithm achieves the best performance when (U, V) is (4, 4).

Table 3: Optimal parameters in various SNRs.

	SNR (dB)			
	0	5	10	15
U	2	4	3	4
V	5	4	7	7

F score is introduced as an objective metric to evaluate the performance of the proposed algorithm, which can be expressed as follows:

$$F = \frac{(2 * \text{precision} * \text{recall})}{(\text{precision} + \text{recall})},$$
$$\text{Precision} = \frac{\tilde{\chi} \cap \chi}{\tilde{\chi}}, \tag{15}$$
$$\text{Recall} = \frac{\tilde{\chi} \cap \chi}{\chi},$$

where precision is the accuracy rate, recall is the recall rate, χ is the actual splicing region, and $\tilde{\chi}$ is the detected splicing region. It can be seen from equation (15) that the larger the F value, the better the detection capability of the algorithm.

As a comparison to [7, 9], we adopt the optimal parameters in Table 3 to detect the splicing trace. The F scores are shown in Table 5. It can be seen that the proposed method achieves better detection performance in all SNR cases. Meanwhile, it can be seen from Table 3 that the detection performance of the algorithm gradually deteriorates with the SNR increases. This is consistent with the situation in the actual scene, that is, the lower the noise energy contained in the speech signal, the more difficult the noise estimation algorithm is to extract the noise. In addition, according to the results in Tables 3 and 5, the detection result of the algorithm tends to become better with the decrease of U and V. It indicates that the speed of the noise estimation will be beneficial to improve the detection rate of the algorithm.

Table 4: SNR estimation for various algorithms.

Algorithm	0 dB	5 dB	10 dB	15 dB
[23]	4.7419	9.8905	14.7146	18.5088
[24]	2.6064	7.7292	12.5088	16.5755
[25]	3.5518	8.2249	12.3533	15.6897
[26]	3.3987	8.7689	13.7923	17.8140
[27]	4.3277	8.5393	12.1390	14.7518
Optimized Sorensen	**0.1296**	**5.0011**	**10.0396**	**15.0139**

The value in bold type is used for emphasis that the performance of the optimized algorithm is better than other algorithms.

Table 5: F scores of splicing detections.

Algorithms	SNR cases (dB)			
	0-0 dB	5-5 dB	10-10 dB	15-15 dB
[7]	0.7459	0.7317	0.6734	0.6605
[9]	0.7924	0.7999	0.7805	0.7672
Proposed	**0.8302**	**0.8137**	**0.7923**	**0.7685**

The values in bold type is used for emphasis that the performance of the proposed algorithm is better than other two algorithms.

4. Conclusion and Future Work

In this study, a novel method for the speech transsplicing detection algorithm has been proposed. Considering that the segment to be spliced and the original segment have different noise levels, the noise of the suspected speech is estimated first. Then, we extract the variance of the 12-dimensional MFCC coefficients from the estimated noise and utilize the change point detection algorithm based on the penalty cost function to locate the splicing region, finding that the variance of the spliced region is significantly lower than that of the nonspliced regions. Experimental results show that the detection algorithm can accurately determine the starting position of splicing and can detect the entire splicing region. Compared with the splicing detection methods based on grid frequency and intrinsic statistical law of speech, the proposed method has fewer assumptions and can be applied to more forensic scenarios. The future work will focus on extracting more efficient hybrid features to further improve detection accuracy, and more scenarios closer to the real world such as reverberation will be considered.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61300055), Ningbo Natural Science Foundation (Grant No. 202003N4089), and K. C. Wong Magna Fund in Ningbo University.

References

[1] Q. Yan, R. Yang, and J. Huang, "Detection of speech smoothing on very short clips," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2441–2453, 2019.

[2] D. Luo, R. Yang, B. Li, and J. Huang, "Detection of double compressed AMR audio using stacked autoencoder," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 432–444, 2017.

[3] T. Bianchi, A. Rosa, M. Fontani, G. Rocciolo, and A. Piva, "Detection and localization of double compression in MP3 audio tracks," *EURASIP Journal on Information Security*, vol. 2014, pp. 1–14, 2014.

[4] L. Verdoliva, "Media forensics and DeepFakes: an overview," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, 2020.

[5] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[6] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[7] X. Meng, C. Li, and L. Tian, "Detecting audio splicing forgery algorithm based on local noise level estimation," in *Proceedings of the 2018 5th International Conference on Systems and Informatics (ICSAI)*, pp. 861–865, Nanjing, China, November 2018.

[8] X. Lin and X. Kang, "Supervised audio tampering detection using an autoregressive model," in *Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2142–2146, New Orleans, LA, USA, March 2017.

[9] J. Chen, S. Xiang, H. Huang, and W. Liu, "Detecting and locating digital audio forgeries based on singularity analysis with wavelet packet," *Multimedia Tools and Applications*, vol. 75, no. 4, pp. 2303–2325, 2016.

[10] A. Hajj-Ahmad, R. Garg, and M. Min Wu, "Spectrum combining for ENF signal estimation," *IEEE Signal Processing Letters*, vol. 20, no. 9, pp. 885–888, 2013.

[11] P. M. G. I. Reis, J. P. C. Lustosa da Costa, R. K. Miranda, and G. Del Galdo, "ESPRIT-Hilbert-based audio tampering detection with SVM classifier for forensic analysis via electrical network frequency," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 853–864, 2017.

[12] M. Imran, Z. Ali, S. Bakhsh, and S. Akram, "Blind detection of copy-move forgery in digital audio forensics," *IEEE Access*, vol. 5, pp. 12843–12855, 2007.

[13] H. Zhao, Y. Chen, R. Wang, and H. Malik, "Audio splicing detection and localization using environmental signature," *Multimedia Tools and Applications*, vol. 76, no. 12, pp. 13897–13927, 2017.

[14] K. Sorensen and S. Andersen, "Speech enhancement with natural sounding residual noise based on connected time-frequency speech presence regions," *EURASIP Journal on Advances in Signal Processing*, vol. 2005, pp. 2954–2964, 2005.

[15] S. Davis and P. Mermelstein, "Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 28, no. 4, pp. 357–366, 1980.

[16] M. Lavielle, "Using penalized contrasts for the change-point problem," *Signal Processing*, vol. 85, no. 8, pp. 1501–1510, 2005.

[17] R. Martin, "Noise power spectral density estimation based on optimal smoothing and minimum statistics," *IEEE Transactions on Speech and Audio Processing*, vol. 9, no. 5, pp. 504–512, 2001.

[18] F. Desobry, M. Davy, and C. Doncarli, "An online kernel change detection algorithm," *IEEE Transactions on Signal Processing*, vol. 53, no. 8, pp. 2961–2974, 2005.

[19] L. I. Kuncheva and W. J. Faithfull, "PCA feature extraction for change detection in multidimensional unlabeled data," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 25, no. 1, pp. 69–80, 2014.

[20] S. Liu, M. Yamada, N. Collier, and M. Sugiyama, "Change-point detection in time-series data by relative density-ratio estimation," *Neural Networks*, vol. 43, pp. 72–83, 2013.

[21] Y. Hu and P. Loizou, "Subjective comparison of speech enhancement algorithms," *Speech Communication*, vol. 49, no. 7-8, pp. 588–601, 2006.

[22] H. Hirsch and D. Pearce, "The AURORA experimental framework for the performance evaluation of speech recognition systems under noise conditions," in *Proceedings of the Sixth International Conference on Spoken Language Processing, ICSLP 2000/INTERSPEECH 2000*, pp. 29–32, Beijing, China, October 2000.

[23] H. G. Hirsch and C. Ehrlicher, "Noise estimation techniques for robust speech recognition," in *Proceedings of the 1995 International Conference on Acoustics, Speech and Signal Processing*, pp. 153–156, Detroit, MI, USA, May 1995.

[24] I. Cohen and B. Berdugo, "Noise estimation by minima controlled recursive averaging for robust speech enhancement," *IEEE Signal Processing Letters*, vol. 9, no. 1, pp. 12–15, 2002.

[25] S. Rangachari and P. C. Loizou, "A noise-estimation algorithm for highly non-stationary environments," *Speech Communication*, vol. 48, no. 2, pp. 220–231, 2006.

[26] I. Cohen, "Noise spectrum estimation in adverse environments: improved minima controlled recursive averaging," *IEEE Transactions on Speech and Audio Processing*, vol. 11, no. 5, pp. 466–475, 2003.

[27] G. Doblinger, "Computationally efficient speech enhancement by spectral minima tracking in subbands," *Proceedings of Eurospeech*, vol. 2, pp. 1513–1516, 1995.

Hindawi
Security and Communication Networks
Volume 2020, Article ID 8889317, 8 pages
https://doi.org/10.1155/2020/8889317

Research Article

High-Resolution SAR Image Despeckling Based on Nonlocal Means Filter and Modified AA Model

Qiao Ke,[1] Sun Zeng-guo,[2] Yang Liu,[3] Wei Wei,[4] Marcin Woźniak,[5] and Rafał Scherer[6]

[1]*School of Software, Northwestern Polytechnical University, Xi'an 710129, China*
[2]*School of Computer Science, Shaanxi Normal University, Xi'an 710119, China*
[3]*College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China*
[4]*School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China*
[5]*Institute of Mathematics, Silesian University of Technology, Kaszubska 23, Gliwice 44-100, Poland*
[6]*Czestochowa University of Technology, Al. Armii Krajowej 36, Czestochowa 42-200, Poland*

Correspondence should be addressed to Sun Zeng-guo; sunzg@snnu.edu.cn

Received 7 September 2020; Revised 8 October 2020; Accepted 7 November 2020; Published 29 November 2020

Academic Editor: Manjit Kaur

A new speckle suppression algorithm is proposed for high-resolution synthetic aperture radar (SAR) images. It is based on the nonlocal means (NLM) filter and the modified Aubert and Aujol (AA) model. This method takes the nonlocal Dirichlet function as a linear regularization item, which constructs the weight by measuring the similarity of images. Then, a new despeckling model is introduced by combining the regularization item and the data item of the AA model, and an iterative algorithm is proposed to solve the new model. The experiments show that, compared with the AA model, the proposed model has more effective performance in suppressing speckle; namely, ENL and DCV measures are 21.75% and 4.5% higher, respectively, than for NLM. Moreover, it also has better performance in keeping the edge information.

1. Introduction

Synthetic aperture radar (SAR) is widely used in many aspects, such as ecology, hydrology, ocean monitoring, and topographic mapping for its advantageous of all-day, all-weather, multiangle of view, and penetration of ground objects. Because of the coherent imaging system of SAR images, speckle inevitably appears in the imaging process. Especially, imaging of high-resolution SAR images is more complex and demanding. However, the existence of speckle seriously affects the quality of images, makes the interpretation and subsequent processing of images difficult, and cannot correctly reflect the characteristics of the object. Therefore, the speckle suppression in high-resolution SAR images is of great significance [1–3].

There are two main aims of speckle suppression in SAR images. One is to effectively suppress speckle in homogeneous regions, and the other is to preserve edges and fine details as much as possible. SAR image despeckling algorithm has been deeply studied. Traditional filtering algorithms based on local statistics [4] derive local statistics based on homogeneous regions, so the image structure is not preserved enough, the edge is blurred to some extent, and the point target is filtered out. The despeckling method based on wavelet transform [5–7] is the filter based on a fixed window, and image edge information can produce Gibbs phenomenon [8]. In recent years, the method based on partial differential equation (PDE) has become the focus of speckle suppression in SAR images due to its good edge preservation [9, 10]. Many PDE methods are limited to images with additive noise. Based on this, Aubert and Aujol propose a multiplier speckle suppression model, namely, AA model, in which speckle obeys gamma distribution [11]. The AA model can suppress speckle to a certain extent, but the effect is not very ideal in image edge and texture preservation.

Buades et al. [12] propose a nonlocal means (NLM) filtering algorithm. The algorithm extends the local feature

statistics of traditional speckle suppression algorithm to nonlocal domain and uses structural similarity to measure the difference between pixels. Compared with traditional filtering algorithm, the NLM filter can preserve image details and texture information well [13–15]. In addition, based on the PDE method, Kindermann et al. [16] propose a general form of energy functional regularization item based on nonlocal means. Some authors use clustering [17] or neural networks [18] for processing satellite images.

Gilboa and Osher [19] construct weights and regularization items by measuring the similarity of images and propose a nonlocal Dirichlet function as a regularization item. In this paper, a new despeckling model of high-resolution SAR images is introduced by combining the regularization item and the data item of AA model, and an iterative algorithm is proposed to solve the new model. Despeckling experiments on different kinds of SAR images demonstrate that, compared with the AA model, the proposed model has more effective performance in suppressing speckle, and it also has better performance in keeping the edge information.

2. AA Model

For SAR images, let u be the restored image, f be the observed image, and v be the speckle. Then,

$$f = uv. \tag{1}$$

Based on the Bayesian framework, assuming that the speckle v obeys Gamma distribution, the probability density function is written as follows:

$$g_v(v) = \frac{L^L}{\Gamma(L)} v^{L-1} e^{-Lv}, \tag{2}$$

where L denotes the number of looks of images and $\Gamma(\cdot)$ denotes the gamma function. By reasoning, Aubert and Aujol proposed a multiplicative noise denoising model, namely, the AA model, as follows:

$$\arg\min_u \left(TV(u) + \frac{\lambda}{2} \int_\Omega \log u(x) + \frac{f(x)}{u(x)} \mathrm{d}x \right), \tag{3}$$

where regularization item $TV(u)$ is the total variation of u, which guarantees the smoothness of the restored image. Data item $\int_\Omega \log u(x) + (f(x)/u(x))\mathrm{d}x$ is used to ensure that the restored image u retains the main features of the observed image f and λ is a scale parameter used to balance the regularization item and the data item.

The AA model is a problem of minimizing the total variation and is solved discretely. The discrete iteration form is obtained as follows:

$$u_{n+1} = u_n + \Delta t \operatorname{div}\left(\frac{\nabla u}{|\nabla u|} \right) - \Delta t \lambda \left(\frac{u_n - u_0}{u_n^2} \right), \tag{4}$$

where Δt is the time step and $\operatorname{div}(\cdot)$ is the divergence. Figure 1 shows the despeckling results of the AA model for a real high-resolution SAR image, and the SAR image is acquired by the Sandia National Laboratories in the United States. When the maximum peak signal-to-noise ratio (PSNR) of the speckle suppression image is reached, the iteration is stopped. It can be seen that the AA model suppresses speckle well in homogeneous regions, but the effect is not ideal in image edge and texture preservation, which blurs image edge structure information to a certain extent.

3. NLM Filter

Buades et al. proposed a NLM filter [12]. Its basic idea is to open a window centered on each pixel i in the image and use every pixel j in the window to estimate the value of the pixel i. The estimation uses two smaller window similarities as evaluation criteria. The centers of the two windows are i and j, respectively. And weights are calculated using the Gaussian weighted Euclidean distance between the two windows. When the current pixel is estimated, the weight of the pixel which is similar to the central pixel structure in the local structure is larger, and noise can be effectively removed by the weighted mean. The mathematical expression of the NLM filter is written as follows:

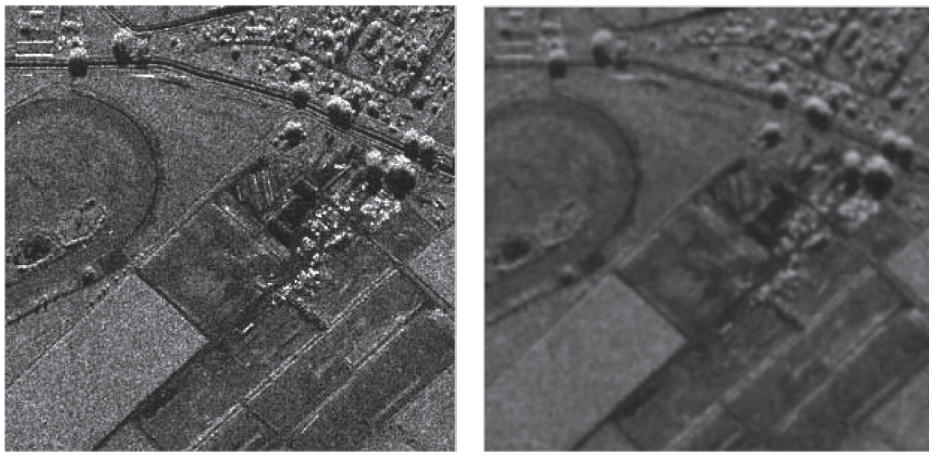
$$\mathrm{NLM}(u)(i) = \frac{1}{C(i,j)} \sum_{j \in \Omega} w(i,j) u(j), \tag{5}$$

where $\mathrm{NLM}(u)(i)$ is the weighted filtering result, $w(i,j) = e^{-d(i,j)/h^2}$ is a filtering weight, $d(i,j)$ is a similarity distance function of pixels i and j, h is the filtering parameter, $C(i,j) = \sum_{j \in \Omega} w(i,j)$ is a normalized function, and Ω is a neighborhood size of pixel i. Parameters h and Ω affect the final denoising effect.

The SAR image speckle obeys the multiplicative model, and the NLM filtering algorithm is deduced based on the additive Gaussian noise. Therefore, original SAR images are usually transformed logarithmically before processing them. Figure 2 shows the despeckling results of the NLM filter for a real high-resolution SAR image, and SAR images were acquired by the Sandia National Laboratories in the United States. It can be seen that the NLM filter has a weak ability to suppress speckle in homogeneous regions but has stronger ability to preserve edge and point targets than the AA model in texture regions.

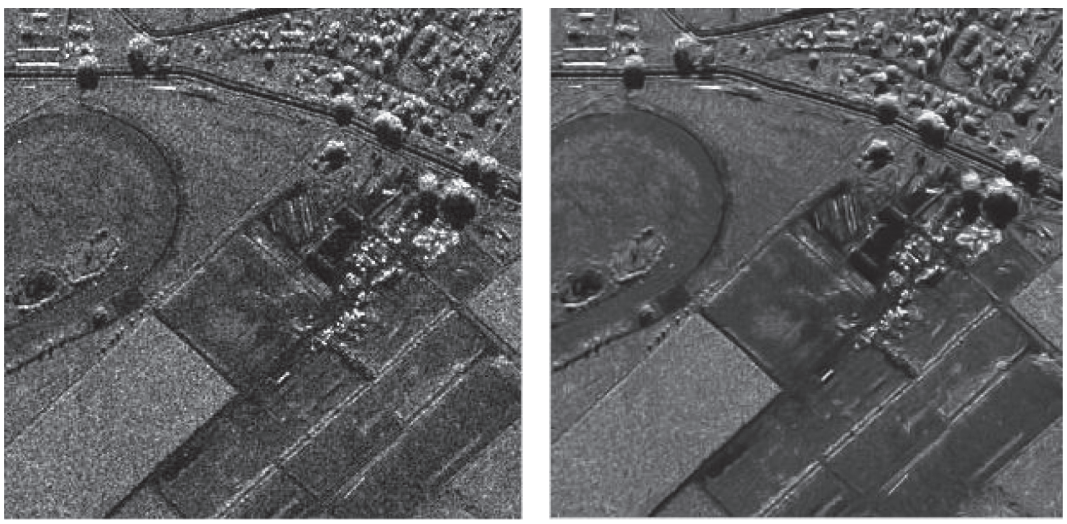
4. Modified Model Based on the NLM Filter and the AA Model

The above results show that the AA model has more effective performance in suppressing speckle in homogeneous regions, but it has weak performance in keeping the edge information. In contrast, the NLM filter has weak performance in suppressing speckle in homogeneous regions, but it has more effective performance in keeping the edge information. Thus, in this paper, a modified model based on the NLM filter and the AA model is proposed.



(a) (b)

Figure 1: Despeckling results of SAR image. (a) SAR image; (b) AA model.



(a) (b)

Figure 2: Despeckling results of SAR image. (a) SAR image; (b) NLM filter.

4.1. Establishment of the Model. Gilboa and Osher constructed weights and regularization terms by measuring the similarity of images based on the NLM filter and proposed a nonlocal Dirichlet function as a regularization item:

$$D(u) = \frac{1}{4}\int_{i\in\Omega} \left|\nabla_{NL}u\right|^2(i)\mathrm{d}i = \frac{1}{4}\iint_{\Omega\times\Omega} (u(i)-u(j))^2 w(i,j)\mathrm{d}i\mathrm{d}j, \tag{6}$$

where $w(i,j) = e^{-d(f(i),f(j))/h^2}$ is a weight function, $d(f(i), f(j))$ is a similarity distance function of pixel i and pixel j, and h is a filtering parameter. The weight function is used to calculate the similarity between the speckle in the window and the unsuppressed speckle.

In this paper, a modified despeckling model of SAR images is proposed by combining the regularization item and data item of the AA model:

$$\arg\min_u \left\{\frac{1}{4}\iint_{\Omega\times\Omega}(u(i)-u(j))^2 w(i,j)\mathrm{d}i\mathrm{d}j + \frac{\lambda}{2}\int_{\Omega}\left(\log u(i) + \frac{f(i)}{u(i)}\right)\mathrm{d}i\right\}. \tag{7}$$

4.2. Solution of the Model. Using variational method, the Euler–Lagrange equation corresponding to model (7) is shown as follows:

$$\int_{\Omega}(u(i)-u(j))(w(i,j))\mathrm{d}y + \lambda\left(\frac{u(i)-f(j)}{u(i)^2}\right) = 0. \tag{8}$$

Using the steepest descent method, the steepest descent flow is shown as follows:

$$u_t = \int_{\Omega} (u(i) - u(j))w(i, j)\mathrm{d}y + \lambda\left(\frac{u(i) - f(j)}{u(i)^2}\right), \quad (9)$$

where scale parameter λ can be seen as a Lagrange multiplier and obtained by the following formula:

$$\lambda = \frac{1}{|\Omega|\sigma^2} \int_{\Omega} (u(i) - f(i))\left[\int_{\Omega} (u(j) - u(i))w(i, j)\mathrm{d}j\right]\mathrm{d}i. \quad (10)$$

The iteration form of the discretized steepest descending flow (9) is as follows:

$$u_i^{n+1} = u_i^n + \Delta t \sum_j w_{ij}\left(u_i^n - u_j^n\right) + \lambda\Delta t \frac{\left(u_i^n - f_i^0\right)}{\left(u_i^n\right)^2}, \quad (11)$$

where u_i denotes the value of pixel i, u_j denotes a pixel value in the neighborhood of pixel i, w_{ij} is the weight function $w(i, j)$, and Δt is the time step. In the actual implementation of the algorithm, a small value ε is added to the denominator to avoid the denominator being zero; then, the discretized iteration form becomes as follows:

$$u_i^{n+1} = u_i^n + \Delta t \sum_j w_{ij}\left(u_i^n - u_j^n\right) + \lambda\Delta t \frac{\left(u_i^n - f_i^0\right)}{\left(u_i^n\right)^2 + \varepsilon}. \quad (12)$$

The flow chart of the improved filtering algorithm is shown in Figure 3. Firstly, in high-resolution SAR images, pixel i is taken and its neighborhood Ω and a block to be estimated $N(i)$ are determined. Secondly, in neighborhood Ω of pixel i, the filter weights of $N(i)$ and $N(i)$are calculated by taking the similar block $N(j)$ of pixel j. And then, filter weights of all pixels in the neighborhood and pixel i are calculated by traversing whole neighborhood Ω. Finally, the despeckling result is obtained by putting an iterative formula of the improved model after discretization.

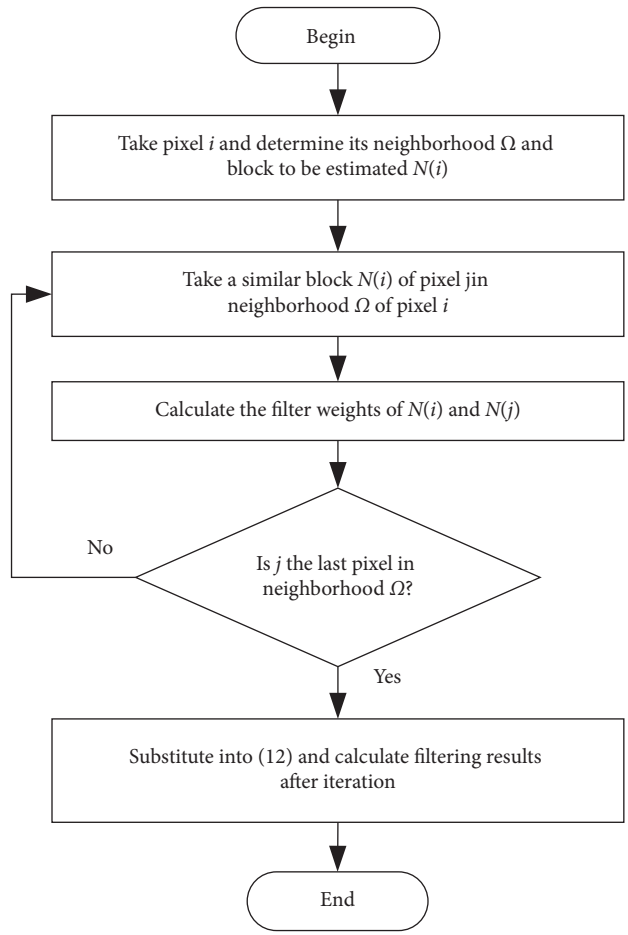


Figure 3: Flow chart of the proposed method.

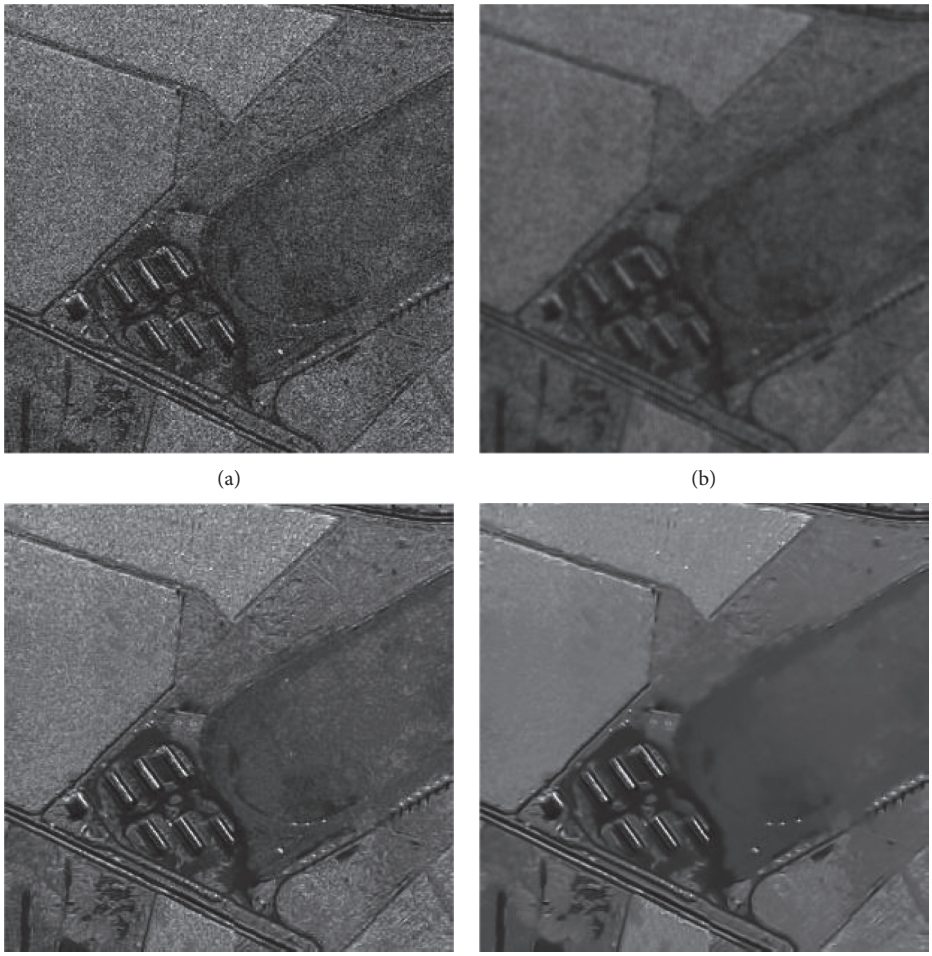
5. Despeckling Experiments

Figure 4 shows the despeckling results of a real high-resolution SAR image to illustrate the speckle suppression effect of the proposed algorithm. SAR images are acquired by the Sandia National Laboratories in the United States. In order to verify the filtering performance of the proposed algorithm more objectively, some objective evaluation indicators are used to compare the AA model, the NLM filter, and the proposed algorithm. The experiment results are shown in Table 1. An equivalent number of looks (ENL) and difference of the coefficient of variation (DCV) are indexes to evaluate the filtering effect [20–22]. ENL is the most commonly used criterion for SAR image speckle suppression, and its calculation range is homogeneous regions. ENL is defined as the ratio of the square of the mean value of a pixel to the square of the standard deviation in a homogeneous region. The larger the ENL value is, the stronger the speckle suppression ability of the despeckling algorithm is. The calculation range of DCV is edge regions, and it is defined as the difference of the coefficient of variation between the real image and speckle suppression image in one edge region. The closer the DCV value is to 0, the stronger the preservation ability of speckle suppression algorithm for edge information is.

Table 1: Quantitative measures evaluating the performance of various methods in Figure 4.

	ENL	DCV
AA model	5.8427	0.1935
NLM filter	3.5489	0.0723
Proposed algorithm	7.8692	0.0756

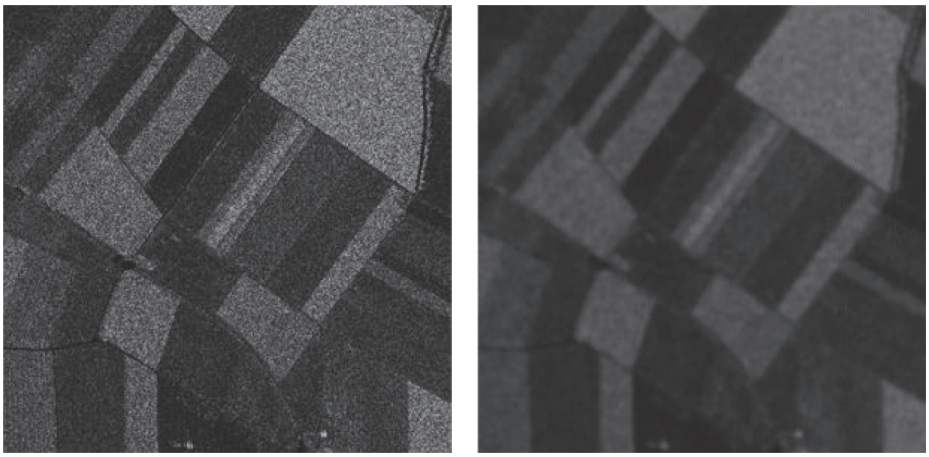
As can be seen from Figure 4, the AA model achieves a better speckle suppression effect in homogeneous regions but largely blurs the edge of the image. In Table 1, the DCV value of the AA model for speckle suppression is the largest, which also confirms that the edge preservation ability of the AA model is the worst. By converting speckle into an additive noise model, the NLM filter is superior to the AA model in preserving edge structure information, and its corresponding DCV value is closer to 0 than that of the AA model. However, the NLM filter has a worse ability to suppress speckle in homogeneous regions than the AA model, and its corresponding ENL value is also smaller than



(a) (b)

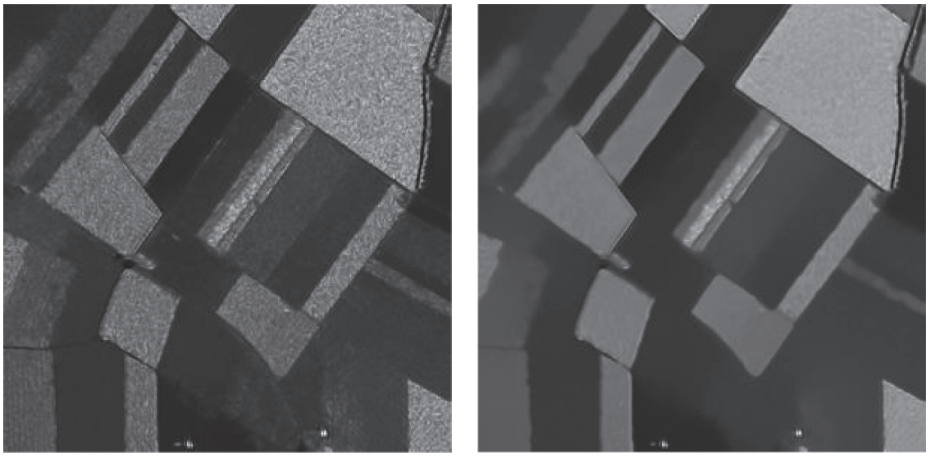
(c) (d)

Figure 4: Despeckling results of a SAR image. (a) SAR image; (b) AA model; (c) NLM filter; (d) the proposed method.



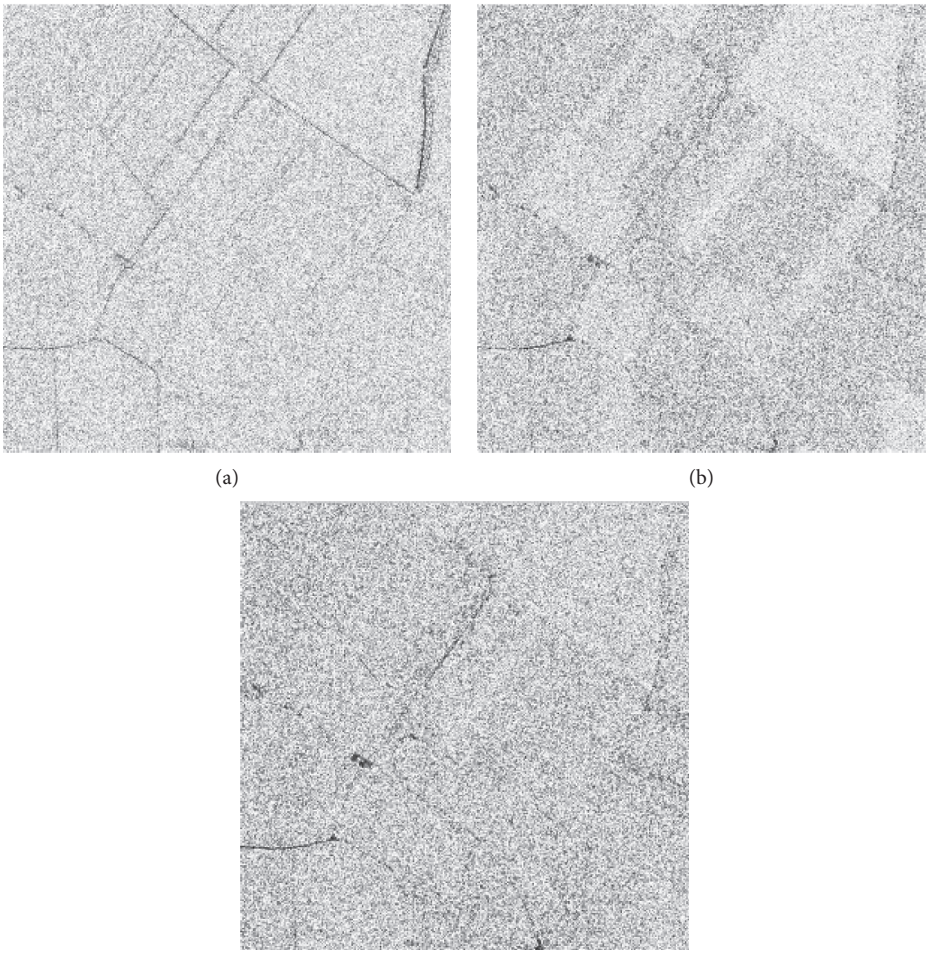
(a) (b)

Figure 5: Continued.



(c) (d)

Figure 5: Despeckling results of SAR image. (a) SAR image; (b) AA model; (c) NLM filter; (d) the proposed method.



(a) (b)

(c)

Figure 6: Speckle patterns of various methods in Figure 5. (a) AA model; (b) NLM filter; (c) the proposed method.

that of the AA model. In contrast, the proposed algorithm can suppress speckle in homogeneous regions more thoroughly and preserve edge details better. It can also be seen from Table 1 that the ENL value of the proposed algorithm is the largest, which shows that the proposed algorithm has a more thorough ability of the speckle suppression in

homogeneous regions than the traditional AA model and the NLM filter. At the same time, the DCV value of the proposed algorithm is closer to 0 than that of the traditional AA model, which shows that the edge preservation ability of the proposed algorithm is stronger.

In order to further illustrate the speckle suppression ability and edge preservation ability of the proposed algorithm for SAR images, the results of the speckle suppression for a SAR image of farmland and the corresponding speckle image are given in Figures 5 and 6, respectively [23–33]. The speckle image is defined by the ratio of the observed image to image after speckle suppression. The amount of edge information on the speckle image reflects the degree of preservation of edge structure information by the speckle suppression method. The less the edge structure information on speckle image, the stronger the edge preservation ability of the corresponding speckle suppression method. The ideal speckle suppression method can completely suppress speckle without losing any edge structure information. In addition, the speckle is not only in homogeneous regions but also in edge regions [33–47].

From the results of the speckle suppression in Figure 5, it can be seen directly that the proposed algorithm is superior to the AA model and the NLM filter in speckle suppression and preserves the edge information of the image. Furthermore, the speckle image in Figure 6 shows that the speckle image corresponding to the proposed algorithm is obviously covered by granular speckle, which shows that the proposed algorithm has better speckle suppression ability than the AA model and the NLM filter. In addition, the AA model has more edge information on the speckle image, while the proposed algorithm has less edge information on the speckle image. This shows that the AA model has a poor edge preservation ability and the proposed algorithm has a strong edge preservation ability.

6. Conclusions

In this paper, a new speckle suppression algorithm is proposed for high-resolution SAR images. This method takes the nonlocal Dirichlet function as a linear regularization item, which constructs the weight by measuring the similarity of images. Then, an improved despeckling model is introduced by combining the regularization item and the data item of the AA model, and an iterative algorithm is proposed to solve the new model. Moreover, we compared the proposed method with the AA model and the NLM filter algorithm. The experiments show that the proposed model is more effective in suppressing speckle in homogeneous regions, and it also has a better performance in keeping the edge information. Thus, it turned out to be an effective speckle suppression method for SAR images.

The limitation of our work is a limited number of images. In the future, we plan to perform broader experiments. Besides, we plan to finetune the method parameters.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the US Sandia National Laboratories for providing some SAR images to perform despeckling experiments in this paper. This work was supported by the China Postdoctoral Science Foundation (Nos. 2020TQ0247 and 2020M683567), Development Program of Shaanxi Province (No. 2018ZDXM-GY-036), Shaanxi Key Laboratory of Intelligent Processing for Big Energy Data (No. IPBED7), the Fundamental Research Funds for the Central Universities (No. GK201903085), and the Key Laboratory of Land Satellite Remote Sensing Application Center, Ministry of Natural Resources of the People's Republic of China (No. KLSMNR-202004).

References

[1] Y.-N. Zhang and L. I. Ying, *The Key Technology of SAR Image Processing*, Publishing House of Electronics Industry, Beijing, China, 2014.

[2] J. I. A. O. Li-Cheng and B. Hou, *Intelligent SAR Image Processing and Interpretation*, Science Press, Beijing, China, 2008.

[3] P. I. Yi-Ming, J.-Y. Yang, F. U. Yu-Sheng et al., *Synthetic Aperture Radar Imaging Principle*, University of Electronic Science and Technology Press, Chengdu, China, 2007.

[4] V. Bhateja, A. Tripathi, A. Gupta et al., *An Improved Local Statistics Filter for Denoising of SAR Images*, Springer International Publishing, Berlin, Germany, 2014.

[5] R. Tao, H. Wan, and Y. Wang, "Artifact-free despeckling of SAR images using contourlet," *IEEE Geoscience and Remote Sensing Letters*, vol. 9, no. 5, pp. 980–984, 2012.

[6] J. Ji, X. Li, S.-X. Xu, H. Liu, and J.-J. Huang, "SAR image despeckling by sparse reconstruction based on shearlets," *Acta Automatica Sinica*, vol. 41, no. 8, pp. 1495–1501, 2015.

[7] S. Lang, X. Liu, B. Zhao, X. Chen, and G. Fang, "Focused synthetic aperture radar processing of ice-sounding data collected over the east antarctic ice sheet via the modified range migration algorithm using curvelets," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 53, no. 8, pp. 4496–4509, 2015.

[8] J.-J. Xu, *SAR Image Despeckling Based on Nonlocal Means Filtering*, Xidian University, Xi'an, China, 2010.

[9] Y. Zhao, J. G. Liu, B. Zhang, W. Hong, and Y.-R. Wu, "Adaptive total variation regularization based SAR image despeckling and despeckling evaluation index," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 53, no. 5, pp. 2765–2774, 2015.

[10] Q. Liu, Z. Yao, and Y. Ke, "Solutions of fourth-order partial differential equations in a noise removal model," *Electronic Journal of Differential Equations*, vol. 22, no. 3, pp. 249–266, 2007.

[11] G. Aubert and J.-F. Aujol, "A variational approach to removing multiplicative noise," *SIAM Journal on Applied Mathematics*, vol. 68, no. 4, pp. 925–946, 2008.

[12] A. Buades, B. Coll, and J. M. Morel, "A review of image denoising algorithms, with a new one," *Multiscale Modeling & Simulation*, vol. 4, no. 2, pp. 490–530, 2005.

[13] Y. I. Zi-Lin, D. Yin, and H. U. An-Zhou, "SAR image despeckling based on non-local means filter," *Journal of Electronics and Information Technology*, vol. 34, no. 4, pp. 950–955, 2012.

[14] Z.-M. Zhao, Y.-J. Zhao, and N. I. U. Chao-Yang, "Improved polarimetric SAR speckle filter based on non-local means," *Journal of Image and Graphics*, vol. 18, no. 8, pp. 1038–1044, 2013.

[15] Y. Jin, J. Jost, and G. Wang, "A new nonlocal H 1 model for image denoising," *Journal of Mathematical Imaging and Vision*, vol. 48, no. 1, pp. 93–105, 2014.

[16] S. Kindermann, S. Osher, and P. W. Jones, "Deblurring and denoising of images by nonlocal functionals," *Multiscale Modeling & Simulation*, vol. 4, no. 4, pp. 1091–1115, 2005.

[17] G. Capizzi, G. L. Sciuto, M. Woźniak, and R. Damaševičius, "A clustering based system for automated oil spill detection by satellite remote sensing,"*Artificial Intelligence and Soft Computing*, Berlin, Germany, Springer, pp. 613–623, 2016.

[18] G. Chen, C. Li, W. Wei et al., "Fully convolutional neural network with augmented atrous spatial pyramid pool and fully connected fusion path for high resolution remote sensing image segmentation," *Applied Sciences*, vol. 9, no. 9, p. 1816, 2019.

[19] G. Gilboa and S. Osher, "Nonlocal linear image regularization and supervised segmentation," *Multiscale Modeling & Simulation*, vol. 6, no. 2, pp. 595–630, 2007.

[20] A. Lopes, R. Touzi, and E. Nezry, "Adaptive speckle filters and scene heterogeneity," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 28, no. 6, pp. 992–1000, 1990.

[21] R. Touzi, "A review of speckle filtering in the context of estimation theory," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 40, no. 11, pp. 2392–2404, 2002.

[22] A. Lapini, t. Bianchi, F. Argenti, and L. Alparone, "Blind speckle decorrelation for SAR image despeckling," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 52, no. 2, pp. 1044–1058, 2014.

[23] S. U. N. Zeng-Guo and H. A. N. Chong-Zhao, "Combined despeckling algorithm of synthetic aperture radar images based on region classification, adaptive windowing and structure detection," *Acta Physica Sinica*, vol. 59, no. 5, pp. 3210–3220, 2010.

[24] P. Zheng, Y. Qi, Y. Zhou, P. Chen, J. Zhan, and M. R.-T. Lyu, "An automatic framework for detecting and characterizing the performance degradation of software systems," *IEEE Transactions on Reliability*, vol. 63, no. 4, pp. 927–943, 2014.

[25] H. Dou, Y. Qi, W. Wei, and H. Song, "A two-time-scale load balancing framework for minimizing electricity bills of Internet Data Centers," *Personal and Ubiquitous Computing*, vol. 20, no. 5, pp. 681–693, 2016.

[26] P. Wang, Y. Qi, and X. Liu, "Power-aware optimization for heterogeneous multi-tier clusters," *Journal of Parallel and Distributed Computing*, vol. 74, no. 1, pp. 2005–2015, 2014.

[27] Y.-n. Qiao, Q. Yong, and H. Di, "Tensor Field Model for higher-order information retrieval," *Journal of Systems and Software*, vol. 84, no. 12, pp. 2303–2313, 2011.

[28] J. Yan, Y. Qi, and Q. Rao, "Detecting malware with an ensemble method based on deep neural network," *Security And Communication Networks*, vol. 2018, 16 pages, Article ID7247095, 2018.

[29] X. Wang, Y. Qi, Z. Wang et al., "Design and implementation of SecPod: a framework for virtualization-based security systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 44–57, 2019.

[30] W. Wei and Y. Qi, "Information potential fields navigation in wireless Ad-Hoc sensor networks," *Sensors*, vol. 11, no. 5, pp. 4794–4807, 2011.

[31] X. Fan, H. Song, X. Fan, and J. Yang, "Imperfect information dynamic stackelberg game based resource allocation using hidden markov for cloud computing," *IEEE Transactions on Services Computing*, vol. 11, 2018.

[32] H. Song, W. Li, P. Shen, and A. Vasilakos, "Gradient-driven parking navigation using a continuous information potential field based on wireless sensor network," *Information Sciences*, vol. 408, pp. 100–114, 2017.

[33] Q. Xu, L. Wang, X. H. Hei, P. Shen, W. Shi, and L. Shan, "GI/Geom/1 queue based on communication model for mesh networks," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3013–3029, 2013.

[34] Z. Sun, H. Song, H. Wang, and X. Fan, "Energy balance-based steerable arguments coverage method in WSNs," *IEEE Access*, vol. 99, 2017.

[35] H. Song, H. Wang, and X. Fan, "Research and simulation of queue management algorithms in ad hoc network under DDoS attack," *IEEE Access*, vol. 5, 2017.

[36] X. Fan, H. Song, and H. Wang, "Video tamper detection based on multi-scale mutual information," *Multimedia Tools & Applications*, vol. 78, pp. 1–18, 2019.

[37] X. L. Yang, B. Zhou, J. Feng, and P. Y. Shen, "Combined energy minimization for image reconstruction from few views," *Mathematical Problems in Engineering*, vol. 2012, Article ID 154630, 15 pages, 2012.

[38] X. L. Yang, P. Y. Shen, and B. Zhou, "Holes detection in anisotropic sensornets: topological methods," *International Journal of Distributed Sensor Networks*, vol. 8, no. 10, p. 135054, 2012.

[39] W. Wei, Y. Qiang, and J. Zhang, "A bijection between lattice-valued filters and lattice-valued congruences in residuated lattices," *Mathematical Problems in Engineering*, vol. 2013, Article ID 908623, 6 pages, 2013.

[40] H. M. Srivastava, Y. Zhang, L. Wang, P. Shen, and J. Zhang, "A local fractional integral inequality on fractal space analogous to Anderson's inequality," *Abstract and Applied Analysis*, vol. 2014, Article ID 797561, 14 pages, 2014.

[41] S. Liu, W. Li, and D. Du, "Fractal Intelligent Privacy Protection in Online Social Network Using Attribute-Based Encryption Schemes," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 736–747, 2019.

[42] X. Fan, M. Woźniak, H. Song, W. Li, Y. Li, and P. Shen, "H∞ control of network control system for singular plant," *Information Technology And Control*, vol. 47, no. 1, pp. 140–150, 2018.

[43] Q. Ke, J. Zhang, H. Song, and Y. Wan, "Big data analytics enabled by feature extraction based on partial independence," *Neurocomputing*, vol. 288, pp. 3–10, 2018.

[44] J. Zhang, D. P. WeiWei, M. Woźniak, L. Kośmider, and R. Damaševičius, "A neuro-heuristic approach for recognition of lung diseases from X-ray images Author links open overlay panel," *Expert Systems with Applications*, vol. 126, pp. 218–232, 2019.

[45] J. zhang, W. Wei, R. Damasevicius, and M. Wozniak, "Adaptive independent subspace analysis (AISA) of brain magnetic resonance imaging (MRI) data," *IEEE Access*, vol. 7, no. 1, pp. 12252–12261, 2019.

[46] Q. Ke, J. Zhang, M. Wozniak, and W. Wei, "The phase and shift-invariant feature by adaptive independent subspace analysis for cortical complex cells," *Information Technology and Control*, vol. 48, 2019.

[47] J. Su, H. Song, H. Wang, and X. Fan, "CDMA-based anti-collision algorithm for EPC global C1 Gen2 systems," *Telecommunication Systems*, vol. 67, no. 3, pp. 1–9, 2018.

Hindawi
Security and Communication Networks
Volume 2020, Article ID 6627178, 13 pages
https://doi.org/10.1155/2020/6627178

Research Article

On the Value of Order Number and Power in Secret Image Sharing

Yongqiang Yu, Longlong Li, Yuliang Lu, and Xuehu Yan

National University of Defense Technology, Hefei 230037, China

Correspondence should be addressed to Xuehu Yan; publictiger@126.com

Received 7 October 2020; Revised 10 November 2020; Accepted 13 November 2020; Published 23 November 2020

Academic Editor: Jialiang Peng

Shadow images generated from Shamir's polynomial-based secret image sharing (SSIS) may leak the original secret image information, which causes a significant risk. The occurrence of this risk is closely related to the basis of secret image sharing, Shamir's polynomial. Shamir's polynomial plays an essential role in secret sharing, but there are relatively few studies on the power and order number of Shamir's polynomial. In order to improve the security and effectiveness of SSIS, this paper mainly studies the utility of two parameters in Shamir's polynomial, order number and power. Through the research of this kind of utility, the choice of order number and power can be given under different security requirements. In this process, an effective shadow image evaluation algorithm is proposed, which can measure the security of shadow images generated by SSIS. The user can understand the influence rule of the order number and power in SSIS, so that the user can choose the appropriate order number and power according to different security needs.

1. Introduction

With the development and application of computer network and multimedia technology, the production, transmission, and storage of digital images have increased exponentially. The increasing problem of information leakage and the improvement of people's awareness of network information security have led to more and more individuals and organizations beginning to pay attention to and study the security issues in image transmission and storage. To protect the secret images of the national government and military departments, it is particularly urgent to solve such security problems.

For information security, digital images need to be protected during transmission and storage [1]. Traditional image protection technologies include image encryption [2–4] and image hiding [5–7]. Encryption is the use of a specific algorithm to present the secret in another way. Using a secure encryption algorithm to encrypt the image can effectively protect the security of the image content. Image hiding is to hide the secret existence in other carriers or modules through hiding algorithms. Both of these secret image protection technologies have a common feature: transmission through a single channel. When the channel fails or is destroyed, the recipient cannot normally recover the secret image. The same problem also occurs in storage. If the encrypted secret image and the carrier hiding the secret image are tampered with or destroyed, the secret image cannot be completely restored. In addition to image encryption and image hiding, there are also image sharing [8–12]. Secret image sharing (SIS) not only has the function of protecting secret images, but also has the advantages of loss tolerance that other conventional methods do not have [13].

Secret sharing (SS) is to share the original secret into multiple subsecrets and distribute the generated shares to different participants. When the shares contributed by participants meet the required conditions, the secret can be recovered. SS solves the problem that secrets may be destroyed or tampered with in transmission and storage by using multiple channels for transmission and storage. Secret sharing based on Shamir's polynomial principle is an important branch of SS [14, 15]. Thien et al. introduced the principle of secret sharing into the field of images and proposed SSIS [16]. The proposal of SSIS is of great significance to the protection of secret images. However, some shadows generated by SSIS may leak the original secret image information, which has a significant impact and

challenge on the security of SSIS. It is found that information leakage of shadows occurs at different order numbers, and the degree of leakage varies from order number to order number. Similarly, the change of power also has some influence on the leakage of shadow images. It has been proved that the occurrence of SSIS's information leakage is related to the order number, power, and image itself.

This paper mainly uses theoretical analysis and experimental validation to study the impact of order number and power on the security of SSIS. This paper finds out the influence rule of order number and power and gives different selection schemes of order number and power so that users can select order number and power more effectively and conveniently according to different security needs. In order to evaluate the security of shadows more objectively, this paper also proposes a new shadow security evaluation algorithm. The degree to which the shadows leak the secret of the original image can be objectively measured by the parameters obtained by the evaluation algorithm, thus avoiding the subjective error of the human visual system (HVS).

2. Preliminary

In 1979, Shamir [17] and Blakley [18] proposed classical threshold SS schemes using algebra and geometry, respectively. Shamir's polynomial-based secret sharing (SSS) is to split secret S into n shares, which are assigned to n participants. Any k or more shares can be used to reconstruct S, while less than k shares cannot get any information on S. SSS is a threshold sharing scheme, which shares the secret S into n shadows by $f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod p$, in which $a_0 = S, a_1, a_2, \ldots, a_{k-1}$ are selected randomly in $[0, p]$. SIS can only embed one bit at a time, which is sufficient for sharing ordinary text data, but it is far from enough for sharing secret images. Every pixel in a secret image needs to be shared. If a secret pixel is shared every time, the space occupied by the sharing and the efficiency of sharing will be greatly reduced. In order to improve the efficiency of sharing and the space occupied by sharing, Thien and Lin sequentially embed the pixels of the secret image into all the coefficients of the Shamir's polynomial [16], and the specific measures are as follows:

(1) a_i is the ith pixel value of each group in the secret image sharing process.

(2) p is selected as 251, and the pixels above 250 are treated as 250.

The increase in sharing efficiency also brings about a problem: the shadow images generated by some images will leak the original secret image information [19, 20]. When the pixel correlation of the original secret image is strong, leakage is more likely to occur. It is worth noting that although the images are different, the leakage always occurs on some specific order numbers. In the application of the Thien–Lin's scheme, the choice of order number is of great significance to the security of the secret image, which has been extensively studied [21–23]. Tompa and Woll [21] proposed random generation of order numbers in theory but did not propose specific and effective generation schemes. In reference [22], when using the Thien–Lin's method, change p to 257, and the order number is defined as an integer from 1 to n. Literature [23] uses Thien–Lin's method on GF(2^8), taking order number as image ID number, so it cannot be randomly generated. These studies have noticed the importance of order numbers in SSIS, but they have not given a feasible order number selection scheme. Like the order number, the power is also a coefficient in the polynomial, and its role in sharing the polynomial cannot be ignored. Unfortunately, there is relatively little research on the power of Shamir's polynomial.

The rest of the paper is organized as follows. Section 3 introduces the research motivation of this paper and our contribution. The proposed scheme is introduced in Section 4, including parameter analysis, shadow image security evaluation algorithm, and order number and power selection scheme. Section 5 gives the experimental process and data. Finally, Section 6 concludes this paper.

3. Motivation

SIS has gradually developed into a popular research direction, so many SIS schemes have been proposed. Although there are many SIS schemes, SSIS is a simple and efficient SIS scheme. This simplicity is reflected in the easy-to-understand sharing principle and easy-to-use sharing steps, without other operations such as image preprocessing. The efficiency is reflected in the low time complexity of sharing, and the shadow image generated by sharing takes up less space, which is only $1/k$ of the original secret image. The advantages of time and space make the study of SSIS valuable.

Most of the shadow images generated by SSIS are noise images, which ensures the security of SIS. However, part of the shadow image of some images will leak part of the information of the original secret image. The leaked shadow image of this part destroys the confidentiality of SS and affects the security of sharing to a certain extent. In this paper, the purpose of our research on order number and power is to avoid such information leakage and improve the security of SIS. Order number and power are important parameters for SSIS. The occurrence of shadow image leakage must be related to the order number and power, but there is no research to prove this relationship. The influence of order number and power on SSIS can be found through research, and suggestions for selecting safer order number and power are given. When the user performs SSIS, by selecting a safe order number and power, the appearance of insecure shadow images is reduced, the generated shadow images are prevented from leaking the original secret image information, and the security of SSIS is provided to a great extent.

3.1. Our Contributions

(1) The function of each parameter in Shamir's polynomial is analyzed, and the selection suggestions of

the order number and power under different security conditions are given.

(2) A security evaluation algorithm for shadow images generated by SSIS is proposed, which can measure the degree to which the shadow image leaks the original secret image, that is, the security of the shadow image.

4. The Proposed Scheme

In this section, we describe the function of each parameter in Shamir's polynomial in detail and give some suggestions on the selection of order number and power, which solves the utility problem and selection problem of order number and power in Shamir's polynomial.

4.1. Parameters Analyses. In this section, the function of each parameter in Shamir's polynomial is described in detail, the security evaluation algorithm of the shadow image is proposed, and some suggestions are given for the choice of order number and power, which solves the utility problem of the order number and power in Shamir's polynomial and choice issues.

The position and number of secret pixels are inserted. When using SSS to share a secret image, that is, when only the first coefficient a_0 is inserted into the secret pixel s, and the remaining coefficients a_i are randomly selected from the finite field p, the shadow image will not leak the original secret image information, because the existence of random numbers ensures the security of shadow images. If a single pixel is inserted into the other coefficients a_i of Shamir's polynomial, and the coefficients other than a_i are random numbers, then the shadow image will not leak the original secret image information. This shows that the secret insertion position is not directly related to the leakage of the shadow image.

As the number of inserted secret pixels increases, the location of the secret pixels will have different options. Research has found that no matter how the position and number of the inserted secret pixels change, as long as the number of inserted secret pixels is less than k, the shadow image will not leak information visually. It is not difficult to find that the visual security of the shadow image can be protected as long as there are random coefficients in the polynomial, no matter the position or number of the inserted secret pixels is studied. The existence of random numbers causes shadow images to resemble noisy images. It can be seen that the existence of random numbers ensures the security of SIS, which has nothing to do with the selection of order number and power. However, there is no randomness of coefficient in Thien–Lin's scheme, so the security of its sharing should be maintained by other parameters.

4.1.1. The Type of Secret Image. In Thien–Lin's scheme, different secret images have different degrees of leakage, so we broadly divide the secret images into three categories: monochrome images, strong correlation images, and weak correlation images.

4.1.2. For Monochrome Images. A monochrome image is an image with all the same pixels. Sharing a secret image requires multiple participations of polynomials. But for monochromatic image, there is only one situation: the shared pixels are the same for each group, which leads to the fact that the shared values must be the same. This means that the shadow image is just a color change, which cannot guarantee the security of the secret image content.

4.1.3. For Strongly Correlated Images. In a strong correlation image, the pixel correlation degree is relatively close, and the adjacent pixel values are similar or the same, but they are not exactly the same as monochrome images, so there will be a problem of partial shadow images leaking part of original secret image content. We can deduce the formula as follows: when $k = 2$, $f(x) = (a_0 + a_1 x) \mod p = (a_1 (x+1) + (a_0 - a_1)) \mod p = (a_1 X + \Delta a) \mod p$. Adjacent pixels are the same or similar, so Δa is visually unchanged, that is, $\Delta a = 0$. The randomness of pixels in the shadow image mainly comes from the influence of $a_1 X$. Using λX to represent a_1, we get $a_1 X = \lambda X^2$. This means that when $k = 2$, randomness is related to x^2. Similarly, the following formula can be obtained.

$$\begin{aligned} k &= 2 \sim x^2 \bmod p, \\ k &= 3 \sim x^3 \bmod p, \\ k &= 4 \sim x^4 \bmod p, \\ &\cdots \qquad . \end{aligned} \tag{1}$$

In order to better observe the influence of order numbers on the randomness of shadow pixels, corresponding scatterplots are drawn, as shown in Figure 1.

The randomness of the shadow image is closely related to the order number. By analyzing formula (1) and observing Figure 1, we get the following conclusion:

The larger the k, the greater the randomness of shadow pixels, and the greater the range of safe selection of order numbers .

This conclusion can be explained in many ways:

(1) The more regular the distribution of shadow pixels, the smaller the randomness, and the greater the risk of shadow image leakage. For example, in Figure 2, the distribution of green, blue, and red dots is regular, which means that the randomness is small.

(2) The larger the k, the smaller the probability of continuous k pixels being the same.

(3) The larger the k, the larger the pixel grouping, and the smaller the shadow image.

4.1.4. For Weakly Correlated Image. The correlation degree of pixels in weakly correlated images is small, and each group of pixels can be regarded as a group of random numbers.

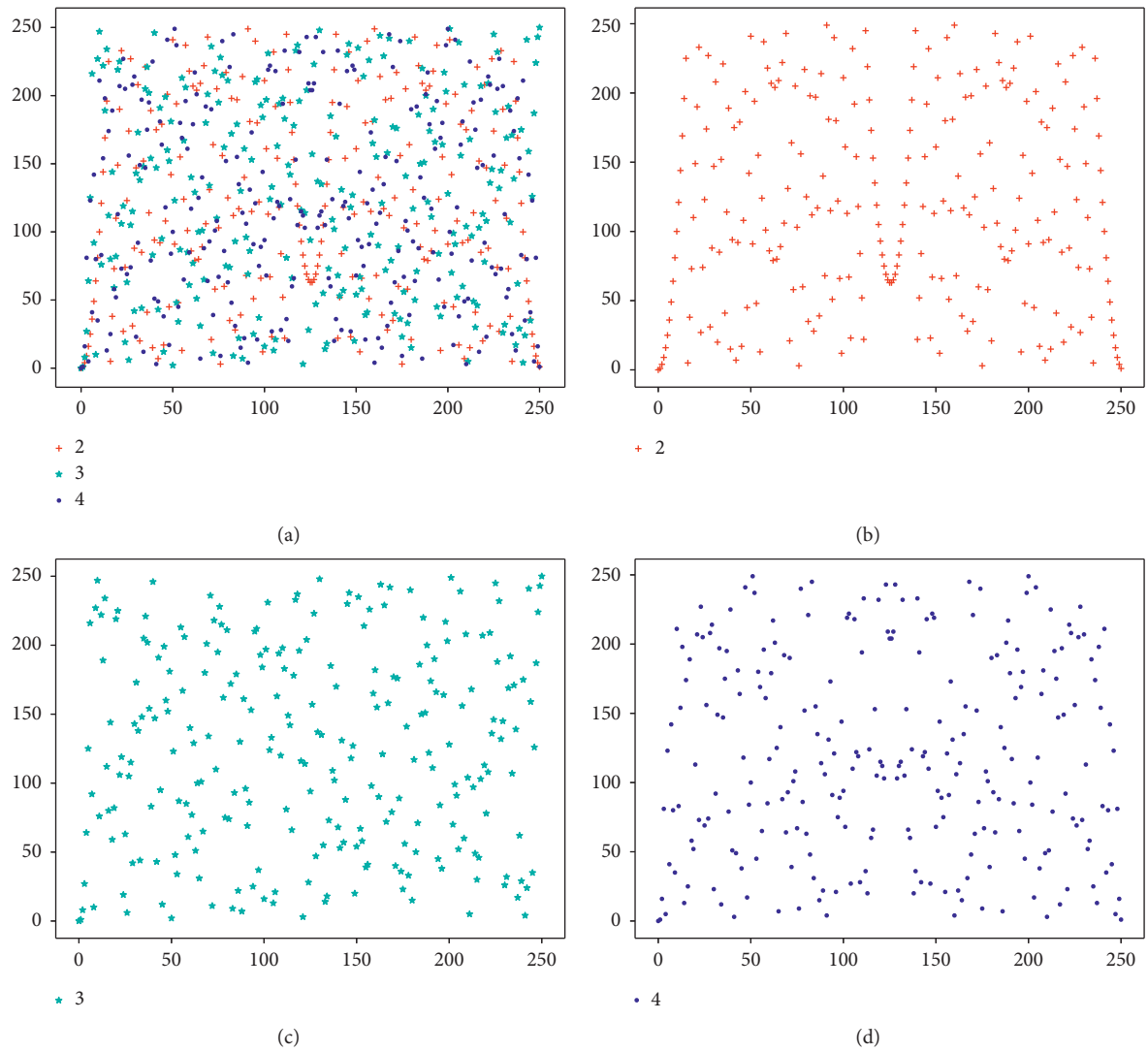


Figure 1: Random distribution. (a) $k = 2, 3, 4$. (b) $k = 2$. (c) $k = 3$. (d) $k = 4$.

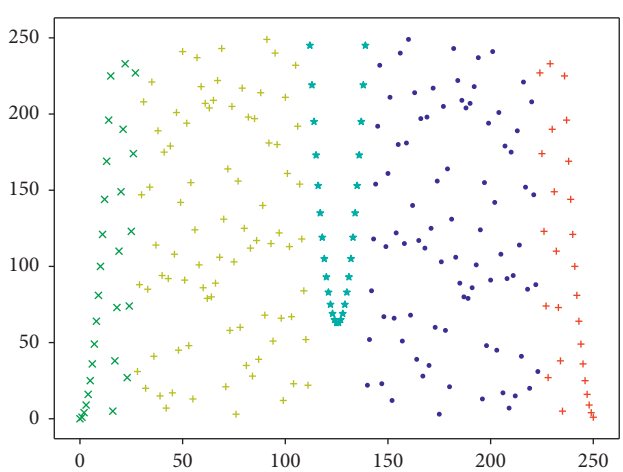


Figure 2: Distribution of $k = 2$.

This guarantees the security of SIS. But it is affirmative that applying the conclusion of strongly correlated images to weakly correlated images can greatly improve the security of sharing.

In this section, we have come to the conclusion that monochrome images are not suitable for sharing with SSIS and that the sharing of strong or weak correlation images requires a reasonable choice of order number and power.

4.2. Shadow Image Security Evaluation Algorithm. If the human visual system (HVS) is used to determine whether a shadow is unsafe, it is not only subjective and arbitrary, but also may have more or less errors. In order to remove human visual errors and subjective factors, we propose an algorithm for evaluating the quality of shadow images. After trying many evaluation methods such as information entropy and mutual information entropy, a new method is proposed. The algorithm is as follows Algorithm 1:

The algorithm is based on randomness, which guarantees the security of shadow images. Parameter ε represents the weighted variance of the distribution of shadow pixels after the corresponding pixels are shared.

Combining the above knowledge and the distribution histogram of shadow image pixels, we will introduce the design ideas of the algorithm. Here, we mainly introduce the algorithm with the classic threshold $k = 2$ as an example. Figure 3(a) is a comparison image, and Figure 3(b) is its pixel distribution histogram. Figures 4 and 5 are the shadow images with order numbers 1 and 59 and their corresponding shadow pixel histograms, respectively. We can clearly see that when the order number is equal to 1, the content of the secret image is leaked, and when the order number is equal to 59, the shadow image is safe. Corresponding to the distribution histogram of the pixels, we can see that when the order number is 1, the general rule of most pixels has not changed, there is only an offset, and the random degree of the pixels has not changed substantially. However, when the order number is 59, the distribution of secret pixels has undergone major changes, and the degree of randomness of pixels has been increased. The more the pixel distribution in the shadow image changes relative to the pixel distribution of the original secret image, the greater the randomness is, and the greater the visual change it brings.

In order to achieve the purpose of evaluating the randomness in the shadow image, we will judge each pixel and calculate the sum according to the weight of each pixel. To evaluate the randomness in a shadow image, we will determine each pixel and weigh it according to its weight. Here, as an example of a pixel with a pixel value of 52, Figure 6(a) shows the corresponding pixel distribution when the order number is 1, and Figure 6(b) shows the corresponding pixel distribution when the order number is 59.

We can see that when the order number is 59, the randomness of the corresponding pixels is greater. The distribution of other pixels is similar to that. After calculating them by weight, the randomness of the shadow image relative to the original secret image can be better evaluated.

The algorithm outputs a parameter ε, and the larger the parameter ε is, the safer it will be. According to the distribution rule of ε, we have established a security system in Table 1. Level A has an obvious leak and is not suitable for application. According to different safety needs, Levels B, C, and D can be chosen.

Based on the algorithm, it can be confirmed that the discrimination of shadow images requires images of equal size. So, we get the required contrast images by embedding the sharing algorithm, as shown in Figure 7.

The actual effect proves that leakage can be completely represented by parameter ε, as shown in Figure 8. When $k = 2$, Figures 8(a) and 8(b) have obvious leakage and cannot be applied in practice. The leakage of Figures 8(c) and 8(d) is not obvious; it can be used optionally. Figures 8(e) and 8(f) are noisy images, which can be used more safely.

The shadow image evaluation algorithm is feasible in practical applications, and the algorithm complexity will be analyzed. Steps 1 and 2 of the algorithm require statistics on the distribution of each pixel in secret and shadow images. In this process, all the pixels in the image need to be traversed, and the time complexity is $O(n^2)$. Steps 3 and 4 perform simple operations with less time complexity. Therefore, the overall time complexity of the algorithm is $O(n^2)$. After analysis, the feasibility and computability of the algorithm have apparent advantages.

4.3. Research and Suggestions on the Selection of Order Number and Power

4.3.1. Research and Analysis on Order Number. With the default power of $0 \sim (k-1)$, we find the following rules:

Rule 1: Information disclosure will be roughly symmetrical.

Rule 2: Information leakage is easy to happen at both ends.

Rule 3: The leakage of different thresholds is different, and the leakage degree is $k = 2 > k = 3 > k = 4$.

Rule 4: There is no simple relationship between information leakage and whether the order number is prime or sum.

Some selection suggestions are given, and users can choose according to their own security requirements.

Refer to Table 2 when $k = 2, 3, 4$:

When users use $f(x) = (a_0 + a_1 x + \cdots + a_{k-} \ 1x^{k-1}) \bmod p$ for secret image sharing, we give the top five order numbers, as shown in Table 3:

4.3.2. Research and Analysis on Power. It is impossible to exhaust all combinations of powers, because the space for power combinations is too large. Some representative power combinations have been selected; see Table 4 for details.

After extensive testing, the following rules are found:

Rule 1: There is no uniform distribution law, which is related to the combination of power.

Rule 2: Shadow image information leaks much less when the first power is not zero than when the first power is zero.

Rule 3: When the power combination is even, the order number is symmetrical.

Rule 4: Shared security increases with the highest power.

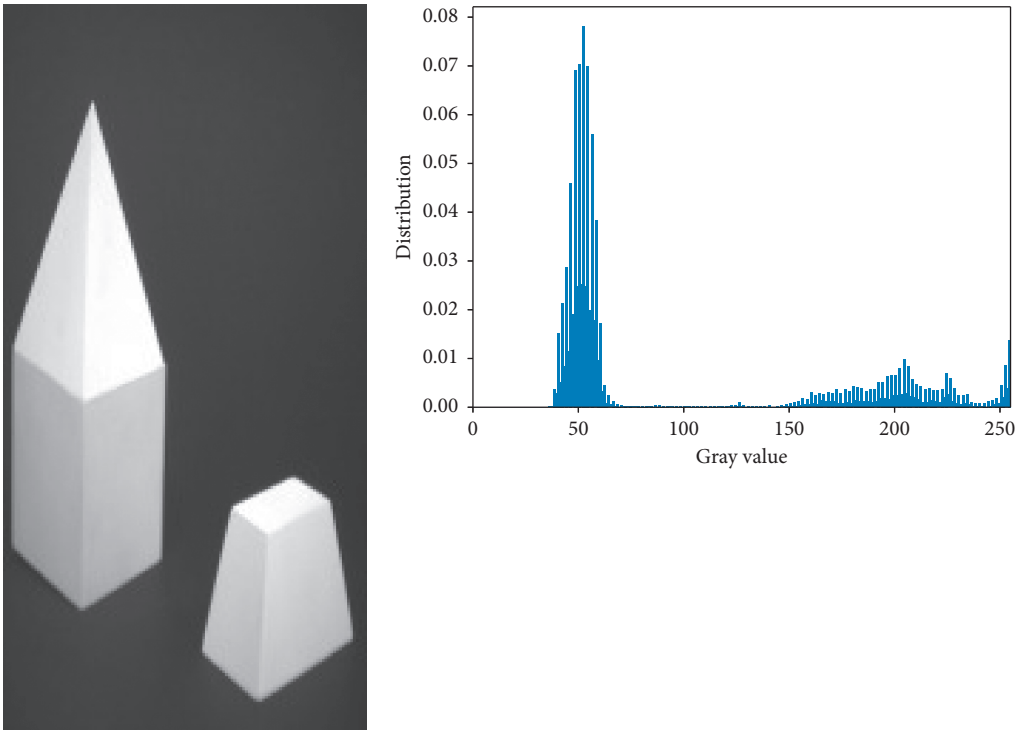
Rule 5, 6: Rules 3 and 4 in order number also apply here.

After comparative analysis, it is recommended that the first power is not zero, and all powers are not even at the same time.

For example,

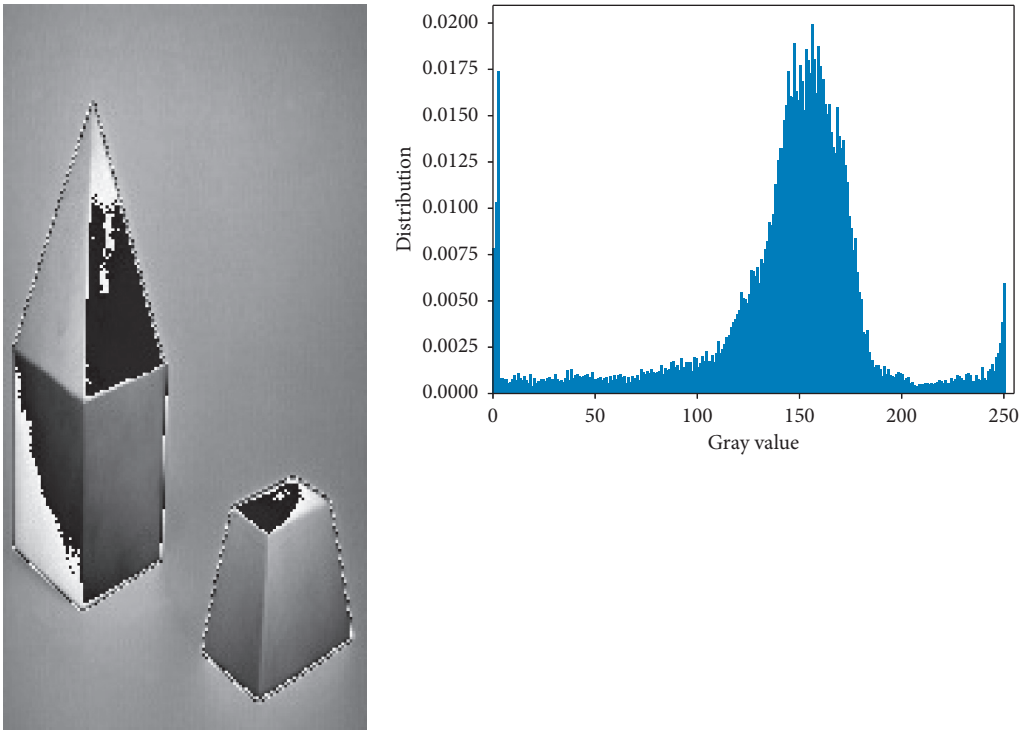
(1) when $k = 2$, the power combination that can be selected is $(1, 2)$.

(2) when $k = 3$, the power combination that can be selected is $(1, 2, 3)$.



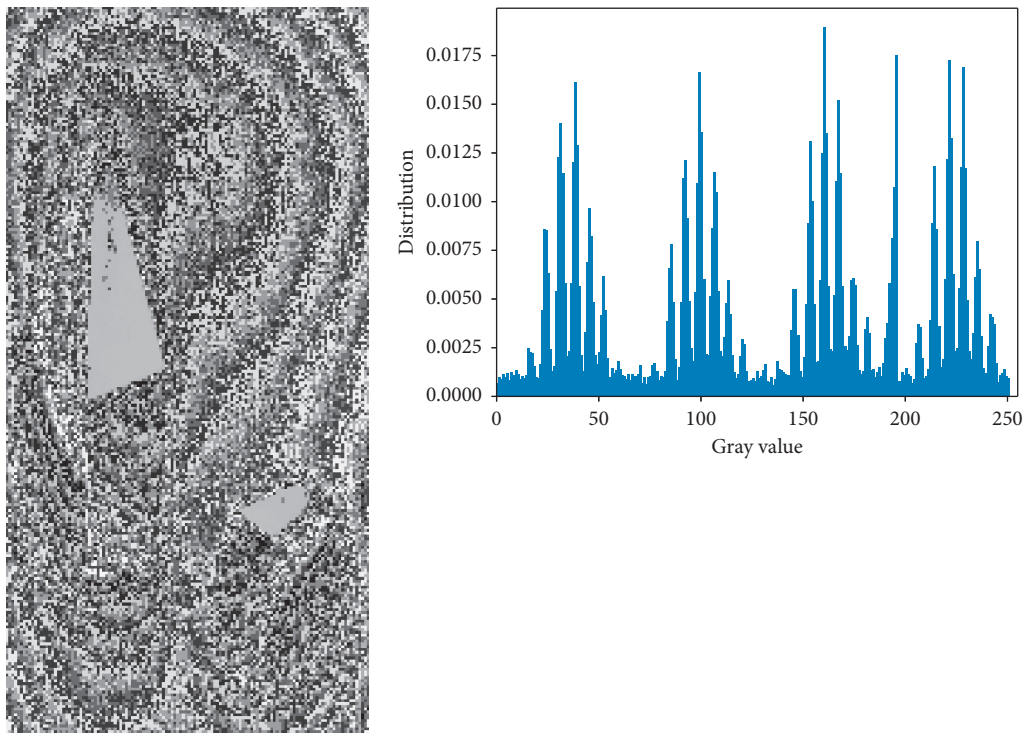
(a) (b)

Figure 3: Indor.



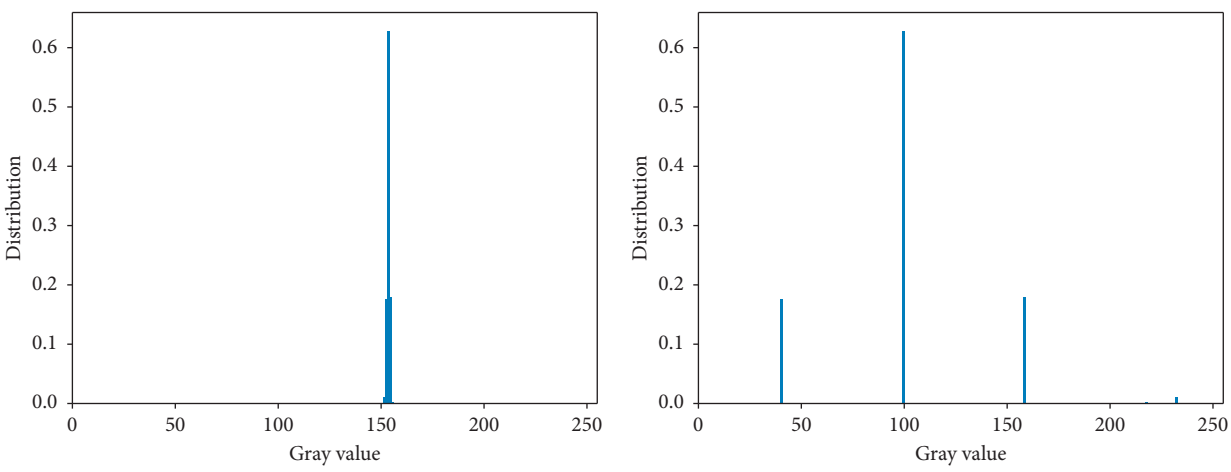
(a) (b)

Figure 4: $X = 1$.



(a) (b)

Figure 5: $X = 59$.

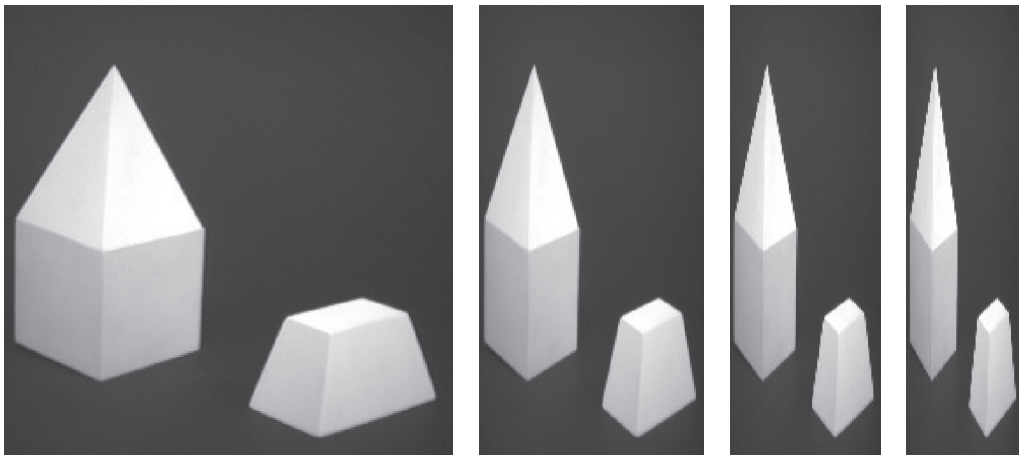


(a) (b)

Figure 6: When $k = 2$, pixel = 52.

Input: original image, Shadow images
Output: evaluating indicator ε
Step 1: statistics of the distribution $D(o)$ and probability $P(o)$ of the pixels in the original secret images.
Step 2: $D(s)$ is obtained by counting the pixels of the corresponding location of $D(o)$ in shadow image.
Step 3: calculate the variance of $D(s)$ to get $V(s)$.
Step 4: get the weighted variance wv of a single pixel through $V(s)P(o)$.
Step 5: add up all wv and output Evaluating indicator ε.

Algorithm 1: Shadow image security evaluation algorithm.

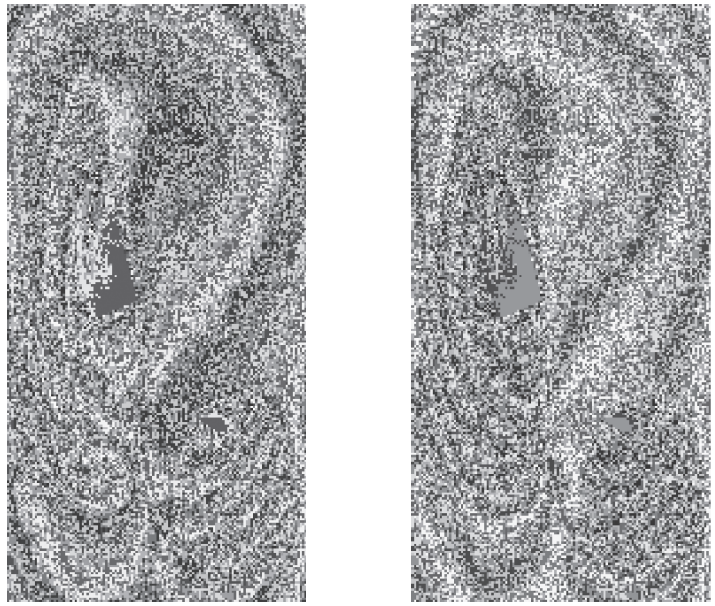


(a) (b) (c) (d)

Figure 7: Contrast image. (a) Indor; (b) 1/2Indor; (c) 1/3Indor; (d) 1/4Indor.

(a) (b) (c) (d)

Figure 8: Continued.



(e) (f)

Figure 8: The number below the image is the parameter ε corresponding to the shadow image. (a, b) belong to Level A. (c, d) belong to Level B. (e, f) belong to Level C. (a) 1145 (b) 2471 (c) 3310 (d) 3980 (e) 4202 (f) 4351.

Table 1: Safety level table.

Security level	A	B	C	D
ε	<3000	>3000	>4000	>5000

Table 2: Selection suggestions of order number.

	Security level	B	C	D
$k = 2$	Range of order numbers	[35,217]	[61,119; 130,186]	—
	Example shadow	Figure 9(a)	Figures 9(b) and 9(c)	—
$k = 3$	Range of order numbers	[5,244]	[7,242]	[18,227]
	Example shadow	Figure 10(a)	Figure 10(b)	Figure 10(c)
$k = 4$	Range of order numbers	[2,249]	[3,247]	[6,243]
	Example shadow	Figure 11(a)	Figure 11(b)	Figure 11(c)

(3) when $k = 4$, the power combination that can be selected is $(1, 2, 3, 4)$.

The security level of the shadow image obtained by sharing is mostly distributed in B, C, and D levels, which meets the requirements of safe sharing. User can choose safe order number between 10 and 240.

5. Experiments

In this section, we will introduce the process and design of the experiment. The experiment follows the following principles:

(1) Choose a strongly correlated image, Indor image for experimentation, and validate it with a weakly correlated image, Lena image.

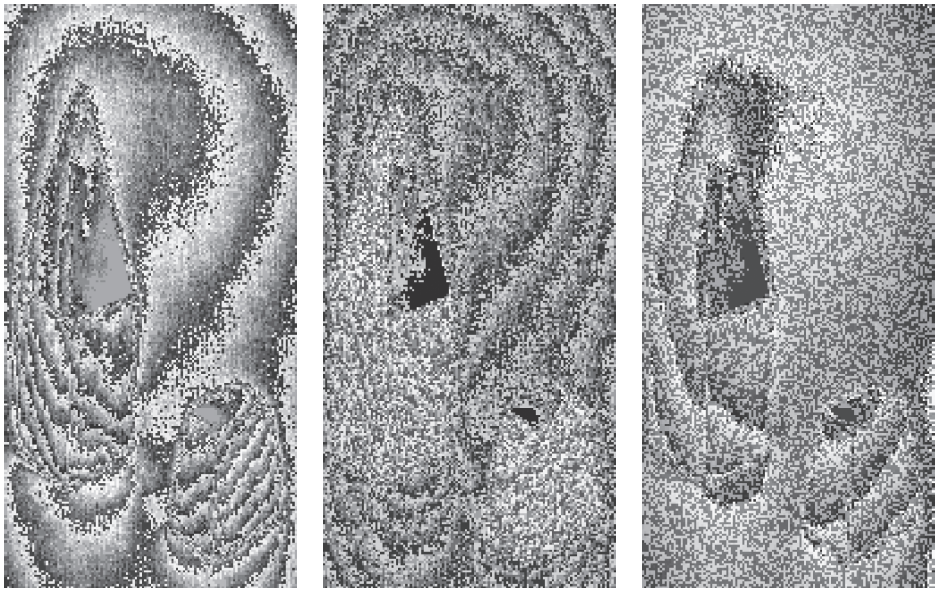
(2) In order to facilitate changing the insertion position, number, and power, the operation of polynomials is changed to the operation of matrix.

(3) List all order numbers, and select $n = 250$.

(4) Select some power combinations for experiments.

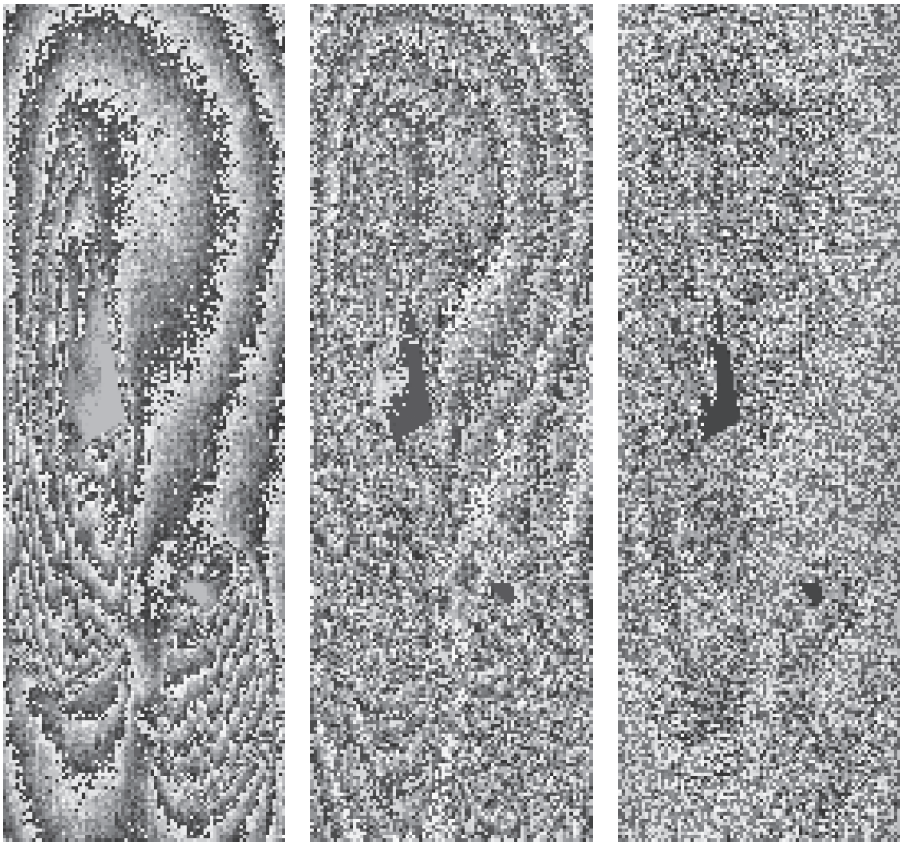
An experiment on SSIS verifies that there is a partial order number leak problem. Here, $k = 2$ is used as an example to show a set of pictures with varying degrees of leaks, such as Figure 12. It can be clearly seen that almost all of them have the problem of leaking the original secret image information, but the degree of leakage is different.

In the experiment, we not only used Indor images, but also other images for auxiliary verification. We find that the shadow image shared by Lena image is leaked, and the



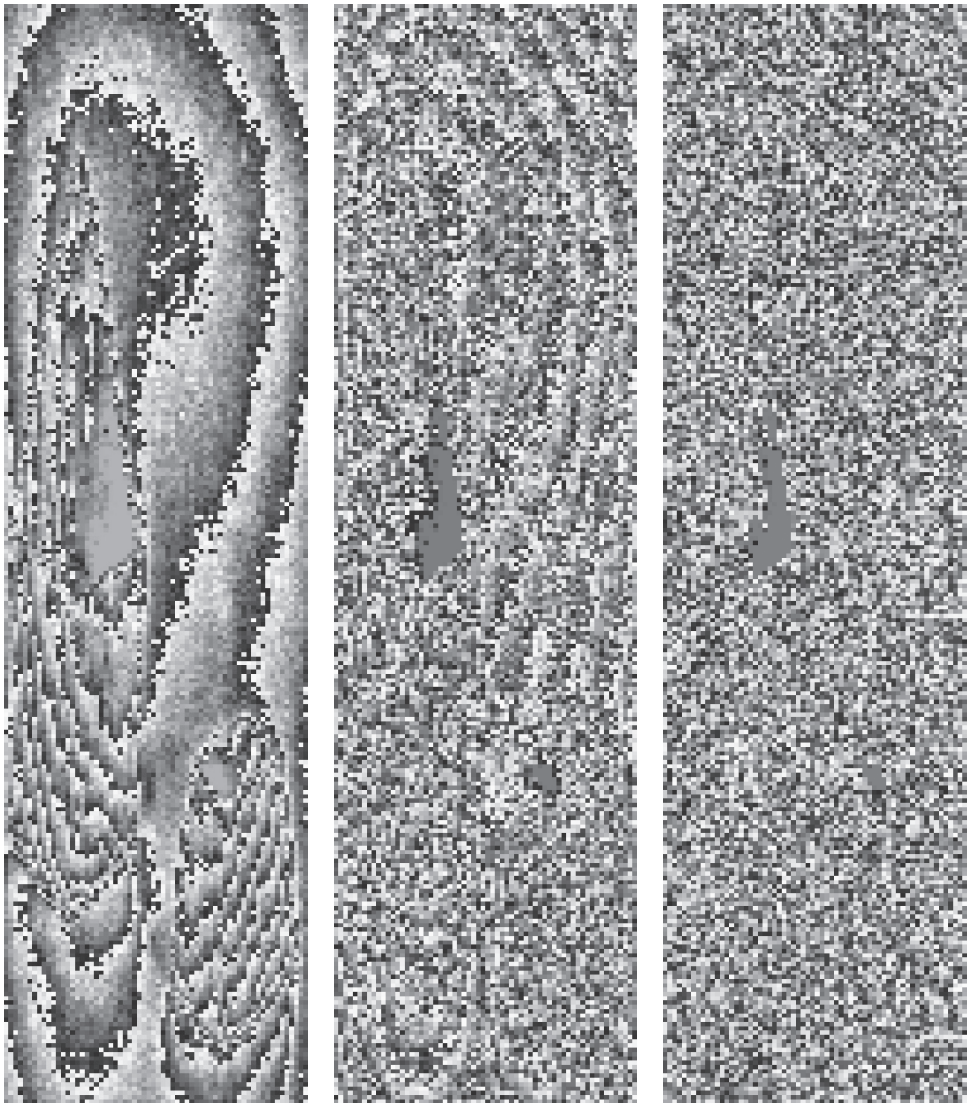
(a) (b) (c)

Figure 9: Shadow images in Table 2. The number below the image is the order number of the shadow image. (a) 35 (b) 61 (c) 130.



(a) (b) (c)

Figure 10: Shadow images in Table 2. The number below the image is the order number of the shadow image. (a) 5 (b) 7 (c) 18.



(a) (b) (c)

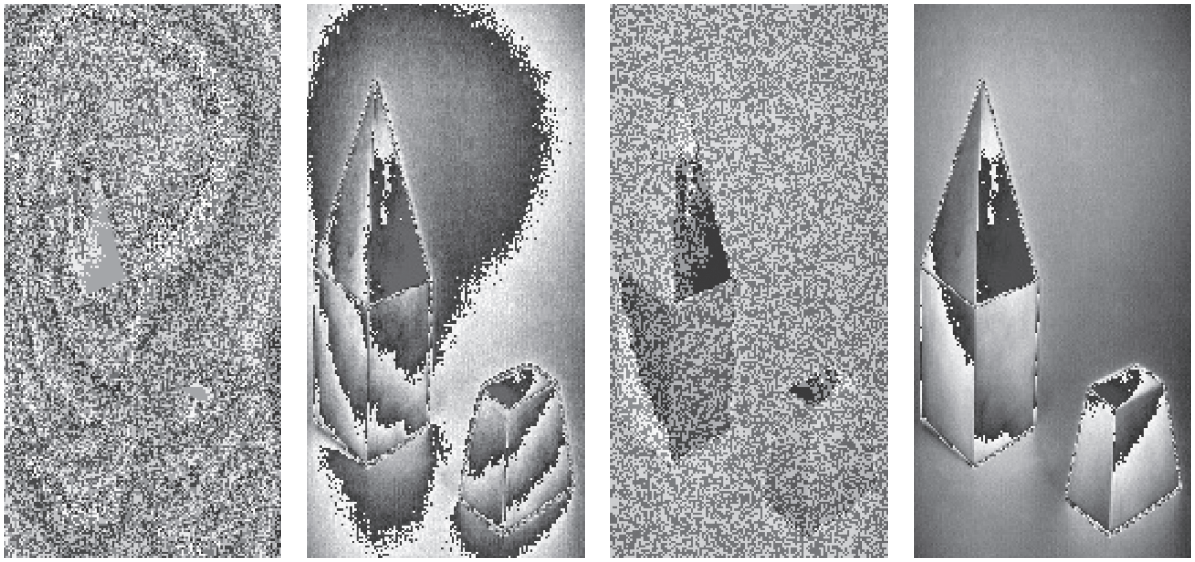
Figure 11: Shadow images in Table 2. The number below the image is the order number of the shadow image. (a) 2 (b) 3 (c) 6.

Table 3: The top five order numbers.

k	Order numbers
$k = 2$	109, 77, 152, 88, 185
$k = 3$	21, 145, 103, 197, 51
$k = 4$	56, 219, 178, 11, 161

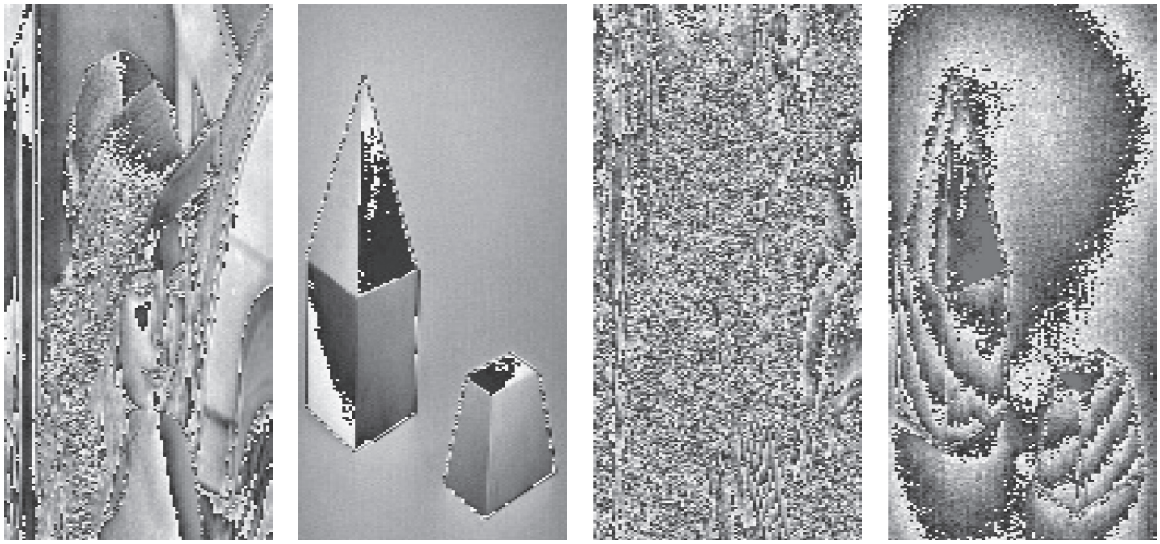
Table 4: Power combination.

The value of k	The value of power
2	(0,1); (0,2); (0,3); (1,2); (3,5); (3,8)
3	(0,1,2); (0,3,8); (0,5,7); (1,2,3); (1,3,5); (2,4,6); (3,5,7)
4	(0,1,2,3); (0,2,5,8); (0,5,7,11); (3,5,7,11)



(a) (b) (c) (d)

Figure 12: When $k = 2$. (a) No leaks; (b–d) is leakage, but the degree of leakage is different. The number below the image is the order number of the shadow image. (a) 159 (b) 13 (c) 125 (d) 5.



(a) (b) (c) (d)

Figure 13: When $k = 3, X = 245, 248$. (a, b) Both Lena's shadow and Indor's shadow leakage. (c, d) Lena's shadow has no leakage, but Indor's shadow has leakage. (a) L248 (b) I248 (c) L245 (d) I245.

corresponding shadow image shared by Indor image must be leaked; the shadow image shared by Indor image is leaked, but the corresponding shadow image shared by Lena image does not have to be leaked. Therefore, strongly correlated image's conclusions apply to the weakly correlated image. See, for example, Figure 13.

Other experimental results are given in other parts of this paper and are not discussed here. In this section, the result of the experiment fully proves that the security evaluation algorithm of the shadow image and the selection scheme of order number and power proposed by us are correct.

6. Conclusion

The shadow image shared by SSIS has the problem of leaking the secret information of the original image. This paper studies the utility of SSIS sharing order numbers and power. We analyzed the utility of each parameter in SSIS and gave suggestions for selecting the order number and power. Users can choose order power and number before sharing according to different security needs. The convenient selection of safe order number and power greatly improves the efficiency and security of SSIS. In this process, a security

algorithm to evaluate the security of shadow image is proposed, which greatly facilitates the detection of shadow images. Further theoretical analyses and application of the evaluation algorithm will be our future work.s

Data Availability

This article contains data to support the results of this study. If other data are needed, the data used to support the results of this study can be obtained from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (Number: 61602491).

References

[1] J. A. Calvert, M. J. Schuster, and S. P. Radziszowski, "Security in computing," *Computers & Security*, vol. 16, no. 3, pp. 2645–2666, 1997.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, Boca Raton, FL, USA, 2007.

[3] J. Peng, B. Abd-El-Atty, H. S. Khalifa, and A. A. A. El-Latif, "Image watermarking algorithm based on quaternion and chaotic lorenz system," in *Proceedings of the Eleventh International Conference on Digital Image Processing (ICDIP 2019)*, Guangzhou, China, May 2019.

[4] L. Li, B. Abd-El-Atty, A. A. El-Latif, and A. Ghoneim, "Quantum color image encryption based on multiple discrete chaotic systems," in *Proceedings of the 2017 Federated Conference on Computer Science & Information Systems*, Prague, Czech Republic, September 2017.

[5] Y.-X. Sun, B. Yan, J.-S. Pan, H.-M. Yang, and N. Chen, "Reversible data hiding in encrypted color halftone images with high capacity," *Applied Sciences*, vol. 9, no. 24, p. 5311, 2019.

[6] R. L. Rivest, A. Shamir, and L. M. Adleman, "Cryptographic communications system and method (September 20 1983)," US Patent 4,405,829, 1983.

[7] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Exploiting the homomorphic property of visual cryptography," *International Journal of Digital Crime and Forensics*, vol. 9, no. 2, pp. 45–56, 2017.

[8] C.-N. Yang, Y.-C. Lin, and P. Li, "Cheating immune k-out-of-n block-based progressive visual cryptography," *Journal of Information Security and Applications*, vol. 55, Article ID 102660, 2020.

[9] X. Yan, X. Liu, and C. N. Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of Real-Time Image Processing*, vol. 14, pp. 61–73, 2015.

[10] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3848–3858, 2020.

[11] L. Li, M. S. Hossain, A. A. A. El-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for internet of things system," *Cluster Computing*, vol. 22, pp. 2293–2307, 2017.

[12] P. Li, J. Ma, and Q. Ma, "(t, k, n) xor-based visual cryptography scheme with essential shadows," *Journal of Visual Communication and Image Representation*, vol. 72, Article ID 102911, 2020.

[13] S. K. Chen and J. C. Lin, "Fault-tolerant and progressive transmission of images," *Pattern Recognition*, vol. 38, no. 12, pp. 2466–2471, 2005.

[14] N. A. Ebri, J. Baek, and C. Y. Yeun, "Study on secret sharing schemes (SSS) and their applications," in *Proceedings of the International Conference for Internet Technology & Secured Transactions*, Abu Dhabi, United Arab Emirates, December 2012.

[15] X. Yan, Y. Lu, C.-n. Yang, X. Zhang, and S. Wang, "A common method of share authentication in image secret," *IEEE Transactions on Circuits and Systems for Video Technology*, 2020.

[16] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[18] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, pp. 313–317, IEEE Computer Society, New York, NY, USA, June 1979.

[19] Z. Zhou, C. N. Yang, and Y. Cao, "Secret image sharing based on encrypted pixels," *IEEE Access*, vol. 6, pp. 15021–15025, 2018.

[20] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, *Security Analysis of Secret Image Sharing*, Springer, Singapore, Singapore, 2017.

[21] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.

[22] S.-J. Lin and J.-C. Lin, "VCPSS: a two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," *Pattern Recognition*, vol. 40, no. 12, pp. 3652–3666, 2007.

[23] C.-N. Yang and C.-B. Ciou, "Image secret sharing method with two-decoding-options: lossless recovery and previewing capability," *Image and Vision Computing*, vol. 28, no. 12, pp. 1600–1610, 2010.