Hindawi
Journal of Engineering
Volume 2022, Article ID 6903695, 5 pages
https://doi.org/10.1155/2022/6903695

Research Article

Improving the Security of Video Embedding Using the CFP-SPE Method

Karthick Panneerselvam,[1] K. Rajalakshmi,[2] V. L. Helen Josephine,[3] Dhivya Rajan,[4] L. Visalatchi,[5] K. Mahesh,[1] and Meroda Tesfaye[6]

[1]*Department of Computer Applications, Alagappa University, Karaikudi, India*
[2]*Department of Computer Science, Montfort College, Bengaluru, India*
[3]*Business Analytics, School of Business Management, Christ University, Bengaluru, India*
[4]*Department of MCA, CMR Institute of Technology, Bengaluru, India*
[5]*Department of IT, Dr. Umayal Ramanathan College for Women, Karaikudi, India*
[6]*Addis Ababa Science and Technology University, Addis Ababa, Ethiopia*

Correspondence should be addressed to Meroda Tesfaye; meroda.tesfaye@aastu.edu.et

Received 14 June 2022; Accepted 5 July 2022; Published 30 July 2022

Academic Editor: Karthikeyan Sathasivam

With the amount of data being transferred on a daily basis, it is becoming increasingly dangerous to save data on the Internet in the face of intruders or hackers. This study paper is one of the most effective ways to transmit information in a secure and confidential manner. The authors previously disclosed a way for embedding a secret video inside a cover video in their prior work. The writers have implemented a number of techniques to incorporate the secret video. The current work improves on the existing approach by including encryption and decryption concepts into the video embedding process. The secret data for either a large or little amount of information is put on the cover video utilising the embedding technique. Our proposed method combines compression, encryption, decryption, and secret information embedding to provide a more secure data transfer.

1. Introduction

Video embedding is a new field of study that aims to provide secure data transmission. Frames from the video file were used to hide data in the process of video data concealing [1]. Large amounts of data can readily be embedded behind the frames of a file due to the use of frames. The goal of the secure video data hiding approach is to insert hidden information in multiple bits of pixels. In the discrete wavelet transform domain of the cover video, the concealing approach is applied. Effective decryption is the key issue that arises during the video encryption process. Quantization employing cosine transformations or wavelet transformations may not be able to restore the encrypted input video frame more successfully during the compression process. Pixel information was lost when employing transforms [2]. The pixel information was adequately kept during the encoding process; however the encryption efficiency was not increased. As a result of the existing methods, the video frame size was initially lowered by combining the current and prior pixels [3]. The encryption procedure is based on the pixel grouping and substituting the relevant and recurrent pixels with the message information, and the problem was solved using effective block code creation. The size of the resultant image is approximately half that of the input image [4] (see Table 1).

2. Literature Review

The survey suggests that there are benefits and drawbacks to the current video security methods. However, most methods have significant drawbacks when it comes to embedding videos, such as:

Table 1: Literature review.

Author and year	Technique	Observation
Alhaj (2016)	Multilayer image stegnaography	According to video steganography, six bits of the secret message can be used to decipher the hidden message.
Manimegalai (2014)	Peak-shaped technique	For the purposes of spatial demonstration, multiple steganography algorithms for JPEG images were thoroughly analyzed.
Mstafa et al. (2017)	(MOT) algorithm and error correcting codes (ECC)	Algorithms for video steganography have been developed in the DCT and DWT domains, respectively. Hamming and bose, chaudhuri, and hocquenghem (BCH) codes were used to encrypt the secret data in the communication.

(i) Unreliable compression ratio

(ii) It is less time-efficient, less secure, and requires more effort.

(iii) Memory complexity is another drawback.

The goal of this research is to create a novel method for video embedding in order to solve these problems.

2.1. Advantages of Steganography Over Watermarking. The types of video embedding techniques are watermarking and steganography. Using wavelet coefficients for information concealment, watermarking is an effective technique that is mostly utilized in the field of image authentication and protection. The following are some of the disadvantages of watermarking in comparison to steganography:

(i) Extensive complexity

(ii) The efficiency must be increased using a rate distortion-optimized rate control.

(iii) High sensitivity to document skewing; poor immunity to manipulation; image quality may be reduced as opposed to watermarking, steganography has the following advantages:

(iv) The embedded video is more sophisticated, making it harder for an attacker to abuse it, and the video stream is used as a cover file in this method, which maximises protection against attackers.

(v) Additionally, it reduces the payload and additional strain.

(vi) Offers both high-quality images and videos.

Thus, the goal of this work was to use steganography to conduct video embedding. When processing video as a series of frames, it conceals the information to provide great security. Additionally, it removes redundant data while enhancing security.

3. Proposed Work

The input and secret video are pre-processed by the supple rectification method and contaminated in the pixel grouping in the proposed method. In this work, the video's white Gaussian noise is removed using preprocessing. The shade picture element (SPE) algorithm is used to process the embedded segment. The code is made up of the results of each patch [5]. Decrypted images can be retrieved by performing a similar operation on the receiver side. Because it is completely reversible, the technology can be utilized to transmit sensitive information in extremely secure videos. The process' performance is assessed using the input and decompressed image's MSE, PSNR, capacity, BER, and SSIM picture quality analyses, and compression ratios. The new method outperforms the old one in terms of effectiveness [6]. Figure 1 shows the block diagram of proposed work.

In this method, following the major steps involved a complete process of information hiding in video sequences.

(1) Input the cover and Stego video

(2) Frame conversion

(3) Preprocessing

(4) Generate the embedding

(5) Encoding the process

(6) Decoding the process with reversible extraction.

(7) Measure the performances.

We have two distinct ways for video embedding:

(i) We can use the supple rectification algorithm to preprocess the video frames.

(ii) We can use the shade picture element algorithm to incorporate the video.

The MATLAB software is used to simulate and evaluate this strategy. The major steps in developing the embedding algorithm are listed below.

3.1. Embedding Part

(i) Read cover video and Stego video file

(ii) Divide the video into frames.

(iii) Using the supple rectification filtering algorithm, select the frames for preprocessing (SRF).

(iv) Initially, this SRF method is utilized to reduce noise in the cover and stego videos.

(v) Use the shade picture element (SPE) approach to group pixels after preprocessing.

(vi) The precompiled cover image pixel is combined with the precompiled secret picture pixel to conduct the embedding procedure.

(vii) For video encoding, the cipher frame pattern (CFP) is used after the embedding procedure.

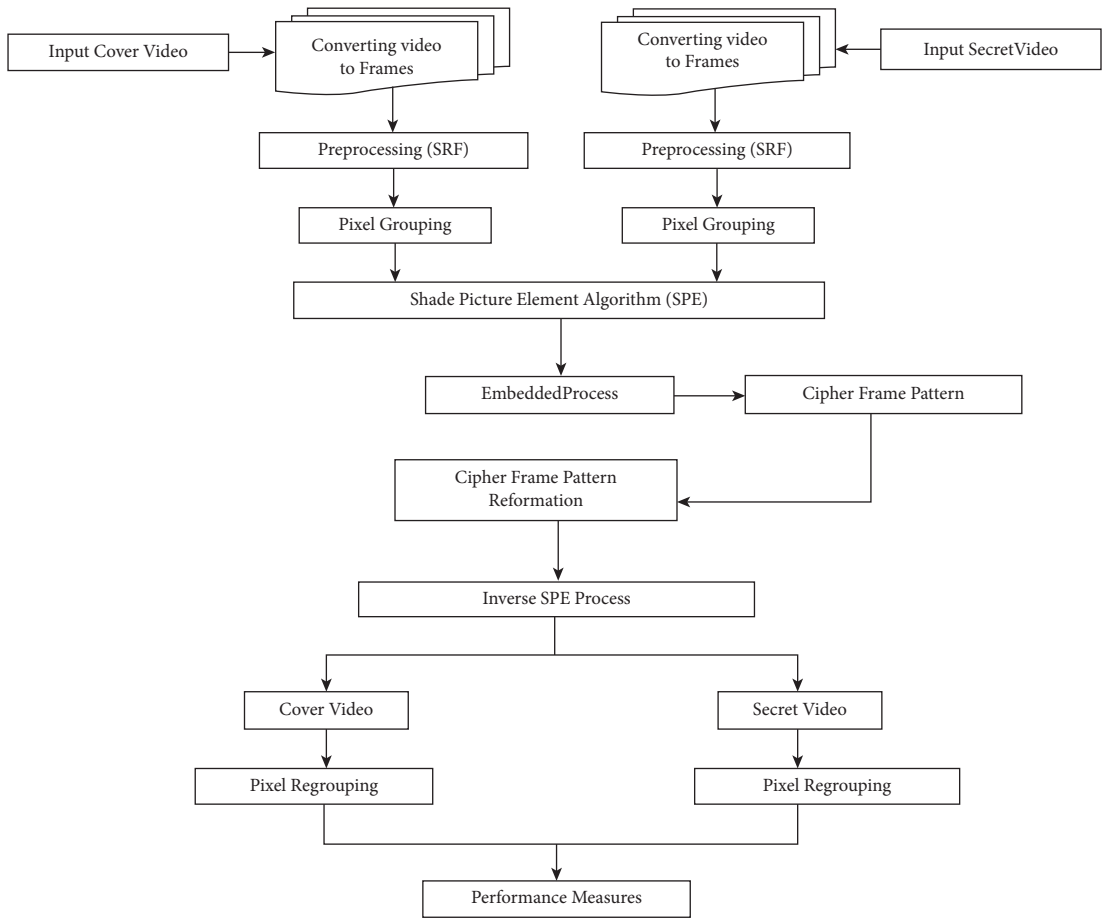

Figure 1: Block diagram of proposed work.

3.2. Extraction Part

(i) Using the reverse technique, extract the hidden video from the stego video.

(ii) To extract cover and stego video, use reversible CFP.

(iii) Using the SPE algorithm's reverse process, regroup the pixels.

(iv) Using the reverse procedure, decode the encrypted video and obtain the original video

4. Experimental Results

This proposed method was used to make common video sequences like news, container, mobile, Akiyo, etc. Here are the results:

Figure 2 depicts a screenshot of a selected video file that is used as a cover video, while Figures 3 and 4 depict a screenshot of a selected video file that is used as a stego video. After then, when the video is delivered to the target receiver, the secret video is embedded using the SPE algorithm, and the video is then reconstructed after the cover and stego video is extracted [7]. A screenshot of the reconstructed video is shown in Figure 5. The reverse methods of picture embedding and pixel grouping are used at this level. In this case, reverse encoding is used to extract the embedded frame from the compressed video sequence. The video is finally

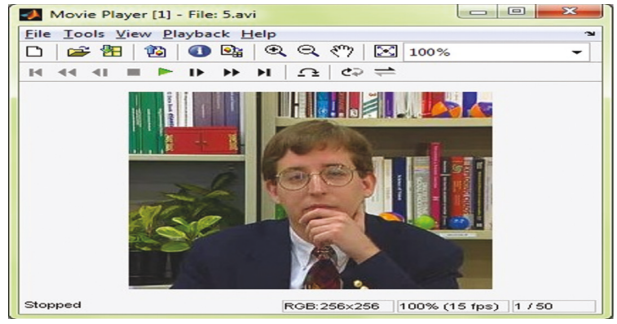

Figure 2: Cover video.

rebuilt by mixing the message frame and cover frame with the least amount of pixel loss possible. There are additional video clips available for the experimental outcomes. As an illustration, we included one sample in a paper. However, we tested a total of 20 samples.

4.1. Performance Analysis. In the first step of testing, video data is taken and hidden using the proposed method. To check the influence of data hiding in the quality of the stego frames [8], performance measurements such as the peak signal-to-noise ratio (PSNR) and mean squared error (MSE) are utilized.

Figure 3: Stego video.

Figure 4: Embedded video.

Figure 5: Reconstructed video.

4.1.1. Peak Signal-To-Noise Ratio (PSNR). Peak signal-to-noise ratio (PSNR) is a common metric used to compare encoded and unencoded video quality. The decibel (db) scale is used to characterize it, as seen in the following [9].

R is the maximum allowable pixel value in the image, and MSE is the mean squared error.

4.1.2. Mean Squared Error (MSE). The MSE is the difference between some of the encoded video's pixel value and the uncompressed video's pixel value.

Table 2: Performance analysis of proposed techniques.

Video sequences	PSNR (dB)	MSE
News	58.42	0.09
Bus	48.56	0.91

Table 3: PSNR value of both existing and proposed techniques.

Video sequences	PSNR original frame	PSNR of reconstructed frame	
		Shamir's (t, n) with DCT	Proposed result
News	37.74	37.19	37.5
Bus	36.47	35.62	36.11

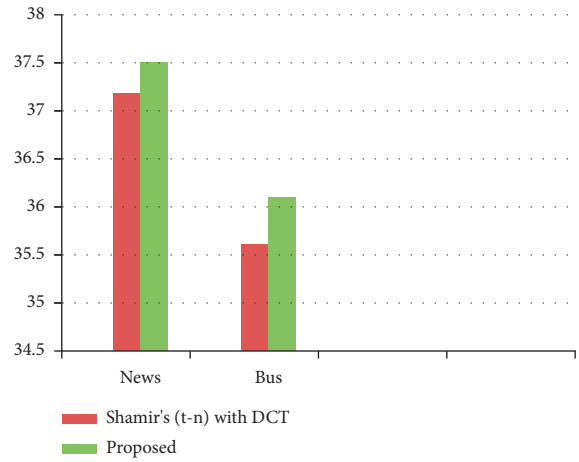

Figure 6: PSNR value comparison.

The MSE is estimated by applying Eq. to arrive at the PSNR (2). HSI band image rows and columns are R and C, respectively [10]. Based on the metrics of time and memory usage during the steganography process, the complexity of the proposed job is validated. By taking into account how long pixel grouping and frame fusion take, the work's time complexity is calculated.

Table 2 illustrates the results of the proposed strategies' performance evaluations. When compared to other video sequences, the news and bus footage has a higher PSNR value and lower MSE value.

Several characteristics, such as PSNR and MSE, are shown in Table 3 to compare the proposed CFP-performance SPE's to that of the existing Shamir's (t, n) with the DCT technique. This study's findings show that the CFP-SPE algorithm, as presented, delivers improved embedding results with great visual quality and great robustness [11]. The results show that the suggested technique produces the best outcomes for all of the video sequences. Therefore, the suggested technique is better suited for various video samples. The PSNR and MSE of each and every video can then differ, and this is entirely dependent on the type of video. As a result, the PSNR and MSE serve as the foundation for the video embedding system's performance rate. Figure 6 shows the PSNR value comparison.

4.2. Features of Our Advanced Video Embedding

(i) Highly secure
(ii) Accuracy
(iii) Improves capacity
(iv) Less Impressibility
(v) Video error correction
(vi) More privacy

5. Conclusions

A video embedding method was proposed in this study to address the challenges that come during the data concealment process. The problem of lossy information is solved by including pixel grouping as well as preprocessing into the embedding process. Optimization and SRF analysis employing varying boundary coefficients of cover and secret video frames are the preprocessing techniques used in the supple correction algorithm approach. The SPE algorithm is used to blend the secret message's pixel information with the necessary pixel information from the cover frame. Last but not least, the video encoding process, also referred to as the suggested method, accomplishes security using the CFP algorithm.

Data Availability

The data used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was performed as a part of the employment of institutions.

References

[1] S. Alzhair and A. Borici, "An innovative lossless compression method for discrete- color images," *IEEE Transactions on Image Processing*, vol. 21, no. 1, 2015.
[2] S. khosla and P. Kaur, "Secure data hiding technique using video steganography and watermarking—a review," *International Journal of Computer Applications*, vol. 95, 2014.
[3] B. A. Usha, N. K. Srinath, and N. K. Cauvery, "Analysis of video steganalysis techniques to defend against statistical attacks—a survey," *International Journal of Engineering Research and Technology*, vol. 1, 2021.
[4] B. RaviKumar and P. R. K. Murti, "Data security and authentication using stegnaography," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 4, pp. 1453–1456, 2011.
[5] S. Sonali, S. Ekhande, P. Sonavane, and P. J. Kulkarni, "Universal steganalysis using feature selection strategy higher-order video," *Statistics and Information*, vol. 1, p. 19, 2013.
[6] K. Rajalakshmi and K. Mahesh, "A review on video compression and embedding techniques," *International Journal of Computer Applications*, vol. 141, p. 12, 2016.
[7] S. Khosla and P. Kaur, "Secure data hiding technique using video steganography and watermarking," *International Journal of Computer Application*, vol. 95, no. 20, pp. 7–12, 2014.
[8] T. M. Thomas, ""Efficient video watermarking with SWT and empirical PCA based decoding" IOSR," *Journal of Computer Engineering (IOSRJCE) ISSN*, vol. 16, no. 5, 2014.
[9] K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 10, pp. 1499–1512, 2009.
[10] P. Roy and A. Nath, "New Steganography approach using encrypted secret message inside Audio and Video media," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, pp. 46–59, 2014.
[11] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 596–606, 2014.