Hindawi
Advances in OptoElectronics
Volume 2017, Article ID 9802751, 15 pages
https://doi.org/10.1155/2017/9802751

Research Article

DWT versus WP Based Optical Color Image Encryption Robust to Composite Attacks

M. A. Mohamed,[1] Ahmed Shaaban Samrah,[1] and Mohamed Ismail Fath Allah[2]

[1]*Faculty of Engineering, Mansoura University, Mansoura, Egypt*
[2]*Delta Higher Institute for Engineering and Technology, Talkha, Egypt*

Correspondence should be addressed to Mohamed Ismail Fath Allah; mismail1885@yahoo.com

Received 9 February 2017; Revised 24 April 2017; Accepted 3 May 2017; Published 5 June 2017

Academic Editor: Samir K. Mondal

Intensive studies have been done to get robust encryption algorithms. Due to the importance of image information, optical encryption has played a vital role in information security. Many optical encryption schemes have been proposed but most of them suffer from poor robustness. In this paper six proposed algorithms will be presented for optical encryption to be robust to severe attacks: composite attack. Three of these approaches are based on one level Discrete Wavelet Transform (DWT) and the others are based on Wavelet Packet (WP). Not only will new techniques be presented but also a new proposed chaotic map has been developed as random keys for all algorithms. After extensive comparative study with some traditional techniques, it has been found that the novel algorithms have achieved better performance versus conventional ones. Also it has been found that WP based algorithms have achieved better performance than DWT based ones against severe composite attacks.

1. Introduction

Nowadays, technology has improved rapidly so security issues have become more important for protect the information. There are different approaches to transfer information in ensuring way. Transferring information from sender to receiver has needed to be very confidential so encryption has become essential [1]. Optical techniques have appeared as effective practical tools in validating and securing information [2, 3]. One of the most attractive advantages of optical systems is the possibility of providing many degrees of freedom to handle parameters such as phase, amplitude, and wavelength [4]. Image encryption techniques have attracted a growing attention since the DRPE technique has been proposed by Réfrégier and Javidi [5]. On the other hand, DRPE suffers from poor performance if the transmitted image is corrupted with different types of attacks, for example, rotation and cropping. Color images represent most practical life information, and it has been found that DRPE is not effective for color image encryption against attacks.

In 2015, Vijayaraghavan has performed encryption and decryption of the three color planes based on gray code effect and FFT [6]. Sharma has proposed a novel encryption-compression scheme based on multiple parameters of discrete fractional Fourier transform with random phase matrices [7]. Narayanan has presented an overview on the various encryption based compression techniques [8]. In 2014, Palevicius and Ragulskis had introduced the integration of dynamic visual cryptography (an optical technique based on the interplay of visual cryptography and time-averaging geometric moiré) with Gerchberg–Saxton algorithm. A stochastic moiré grating has been used to embed the secret into a single cover image [9]. Kanchana and Annapurna had provided an approach of image encryption using the concept of sieving, dividing, and shuffling which has been robust to withstand brute force attacks [10]. In 2015, Li et al. had proposed performance-enhanced image encryption schemes based on depth-conversion integral imaging and chaotic maps [11]. In 2014, Shao et al. had described a novel algorithm to encrypt double color images into a single undistinguishable image in quaternion gyrator domain using an iterative phase retrieval algorithm [12]. In 2013, Kester has developed a cipher algorithm for colored image encryption by shuffling the RGB pixel values [13]. In 2015, Liu et al. had designed

a color image encryption algorithm using Arnold transform and DCT [14]. In 2015, Deng and Zhu had introduced a simple color image encryption with the help of quick response (QR) code [15]. In 2015, Mohamed et al. had proposed a hybrid encryption-watermarking algorithm for copyright protection [16]. In 2014, Hussain et al. had presented for an optical image encryption algorithm by implanting secret image into cover image to form stegoimage which has been then encrypted with the help of DRPE and chaotic substitution box transformation [17]. In 2013, Ashutosh and Sharma had proposed a novel method of image encryption using discrete fractional Fourier transform and exponential random phase mask [18]. In 2007, Tao et al. had introduced a novel image encryption technique by utilizing random phase encoding in the fractional Fourier domain to encrypt two images into one encrypted image with stationary white distribution [19]. In 2013, Alfalou et al. introduced a new technique as a double optimization procedure for spectrally multiplexing multiple images using a combination of spectral fusion based on DCT, specific spectral filtering, and quantization of the remaining encoded frequencies using an optimal number of bits [20].

In the last two decades, extensive studies on the application of coherent optical methods to real time communication and image transmission have been carried out. This is especially true when a large amount of information needs to be processed, for example, high-resolution images. In actual transceiver systems, optical images should be converted into digital form in order to transmit, store, compress, and/or encrypt them. This process requires important computing times or image quality reduction. To avoid such problems, an optical compression of the images may be appropriate. The main advantage of optical methods, compared to digital ones, lies in their capability to provide massively parallel operations in a 2D space [21]. In 2015, Alfalou et al. studied theoretically a simultaneous compression and encryption method which was optically implementable and well adapted to color images. The major strength of this method was in its generality and robustness against various known-plain text attacks making this algorithm appealing for color video images [22].

Practical breakthroughs were achieved through studying correlation applications for tracking and identification, 2D and 3D holography, encryption and compression of images, and so forth. Since images are originally optical in nature, numerical processing is usually realized to exploit their information content. Within this context, a survey of the last recent progress in the field of optical processing of information has been made including some schemes to enhance image quality and others for denoising images [23].

Recently, it has been noticed that the wavelet transform (WT) emerged in the field of image processing as an excellent alternative to the Fourier transform (FT) and its related transforms, as, the Discrete Sine Transform (DST) and the Discrete Cosine Transform (DCT). In the Fourier theory, an image is expressed as an infinite sum of sins and cosines, which made the FT suitable for infinite and periodic signal analysis. For several years, the FT dominated the field of signal processing; however, if it succeeded well in providing the frequency information contained in the analyzed signal, it failed to give any information about the occurrence time. This shortcoming, but not the only one, motivated the scientists to scrutinize the transform horizon for a "messiah" transform. The first iteration in this long research was to cut the signal of interest in several parts and then to analyze each part separately. Allowing the extraction of the localization of different frequency components and time information has been the idea at a first glance that seemed to be very promising which has been known as the Short-Time Fourier Transform (STFT). The main question here is how to cut the signal. The best solution to this question was of course to find a fully scalable modulated window in which no signal cutting is needed anymore. This objective was achieved successfully by the use of the WT [24].

In this article, six proposed methodologies for optical encryption will be provided. Three techniques are based on DWT using chaotic maps as random keys; one of them has depended on using only DWT instead of Fast Fourier Transform (FFT), another one has been based on DWT combined with steganography, and the last one has used Fractional Fast Fourier Transform (FRFFT) as well as DWT besides steganography. The other three algorithms are the same as the previous approaches by using Wavelet Packet Decomposition (WPD) instead of DWT and Wavelet Packet Reconstruction (WPR) instead of Inverse DWT (IDWT). The effect of different types of noise has been studied, as salt and pepper noise, Gaussian noise, and speckle noise, and hence it has been found that salt and pepper noise has had the largest effect on most of performance metrics. So three types of attacks have been merged with each other, salt and pepper noise, rotation by 5°, and centralized cropping of size 100×100 attacks called composite attack. Our results will be compared with traditional techniques for DRPE: FFT based DRPE, Discrete Cosine Transform (DCT) based DRPE, and DWT based DRPE which could be represented as a modified technique when imposing plain image to composite attack. Seven performance metrics have been used for that comparative study as will be obtained later.

Dubreuil et al. have tested the resistance of dual polarization encryption scheme against effective attacks as brute force and video sequence and others effective as known plain text and chosen plain text. An optimization of the setup could be achieved by the use of high dynamic range for the key image or by using a phase only spatial light modulator in the target and in the key image channel [25]. In our proposed schemes chaotic maps have been used instead of random phases as random keys which achieved high dynamic range for the key image through the flexibility in changing the parameters as well as initial conditions of the proposed chaotic map which made it difficult for the attacker to decrypt an unknown image in a strong manner from the practical point of view. This result could be achieved through practical experiments on real images.

The outline of this paper is organized as follows; Section 2 shows DRPE overview, Section 3 introduces the proposed algorithms, Section 4 observes the simulation results and discussions, and Section 5 gives the general conclusions.

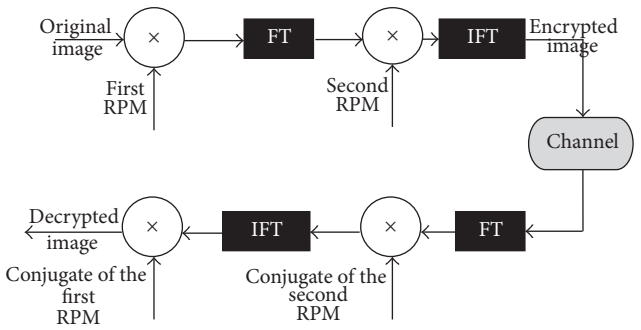


Figure 1: Flow chart of traditional DRPE technique.

2. DRPE Overview

In this section, the main optical encryption scheme based on DRPE will be illustrated. This implementation has been performed using an optical setup called 4f system as depicted in Figure 1 [5, 26]. It is clearly found that the original image to be encrypted is first multiplied by the first random phase mask; then Fourier transform (FT) will be applied. The next step is multiplying this ciphertext by the second random phase mask. The last step in encryption process is applying Inverse-FT (IFT) to get the resulting encrypted image to be transmitted through channel.

The reverse steps will be done for decryption process. FT will first be applied to the received encrypted image, then multiplying by the conjugate of the second random phase mask. After that IFT will be applied followed by multiplication by the conjugate of the first random phase mask to get the resulting decrypted image.

Consider a primary intensity image $\mathrm{OI}(x, y)$ with positive values where x and y denote the spatial domain coordinates. Also u and v represent the Fourier domain coordinates. Let $\mathrm{EI}(x, y)$ denote the encrypted image and $N(x, y)$ and $M(x, y)$ denote two independent white sequences uniformly distributed in $[0, 2\pi]$ interval. To encode $\mathrm{OI}(x, y)$ into a white stationary sequence, two random phase masks (RPMs) are used. $\Psi n(x, y) = \exp[2i\pi N(x, y)]$ and $\Psi m(x, y) = \exp[2i\pi M(x, y)]$. $H(x, y) = M(x, y)$ is a phase function that is uniformly distributed in $[0, 2\pi]$. The second RPM, $\Psi m(u, v)$, is the Fourier transform (FT) of the function $H(x, y)$; that is,

$$\begin{aligned} \mathrm{FT}\left\{H\left(x, y\right)\right\} &= H\left(u, v\right) = \Psi m\left(u, v\right) \\ &= \exp\left[2i\pi M\left(u, v\right)\right]. \end{aligned} \tag{1}$$

The encryption process can be represented by multiplying the original image by the first RPM $\Psi n(x, y)$. Then convolution with the function $H(x, y)$ is applied. The encrypted function is complex with amplitude and phase and is given by the following expression [27]:

$$\mathrm{EI}\left(x, y\right) = \left\{\mathrm{OI}\left(x, y\right)\Psi n\left(x, y\right)\right\} * \mathrm{IFT}\left\{\Psi m\left(u, v\right)\right\}. \tag{2}$$

IFT in (2) indicates Inverse Fourier Transform and $(*)$ denotes convolution process. In the decryption process $\mathrm{EI}(x, y)$ is Fourier transformed, multiplied by the complex conjugate of the second RPM $\Psi m(u, v)$, and then IFT is applied to get the output as follows [28]:

$$\mathrm{IFT}\left\{\mathrm{FT}\left[\mathrm{EI}\left(x, y\right)\Psi m\left(u, v\right)\right]\right\} = \mathrm{OI}\left(x, y\right)\Psi n\left(x, y\right). \tag{3}$$

The absolute value of the output of (3) turns out the decrypted image $\mathrm{DI}(x, y) = \mathrm{OI}(x, y)$.

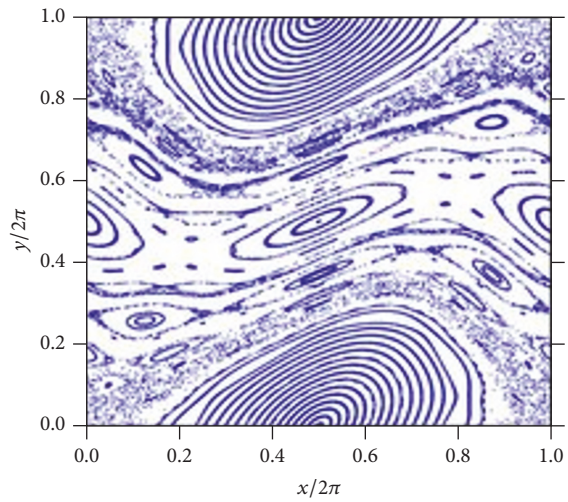


Figure 2: Traditional Chirikov map graph.

3. Proposed Algorithms

In this section the six proposed methods will be illustrated.

3.1. DWT Based Algorithms. First, the main equations of traditional Chirikov map and proposed map as well as their graphs must be discussed to obtain the main advantage of the proposed map over the conventional one. The basic equations of the conventional Chirikov map are as shown below [29]:

$$\begin{aligned} x_{n+1} &= x_n - K\sin y_n, \\ y_{n+1} &= y_n + x_{n+1}. \end{aligned} \tag{4}$$

The graph of this traditional map for $K = 0.9$ is obtained in Figure 2 [29].

The main equations of our proposed map are shown as follows:

$$\begin{aligned} x_{n+1} &= x_n - K\tan y_n, \\ y_{n+1} &= y_n + x_{n+1}. \end{aligned} \tag{5}$$

From these equations, it is clear that the sine function in the traditional Chirikov map has been replaced by tan function. The main graph for this proposed map with the same value of K ($K = 0.9$) is illustrated in Figure 3.

From Figures 1, 2, and 3 it is noticed that the graph of traditional Chirikov map has had a lot of filling spaces. On the contrary the graph of the proposed map has had approximately no filling spaces as it has been obtained as a sharp graph which means more sharpening and hence more

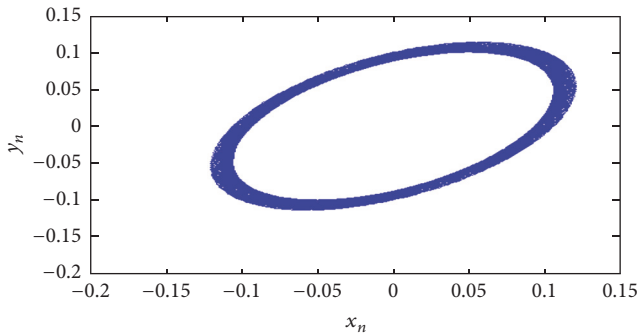


Figure 3: Proposed Chirikov map graph.

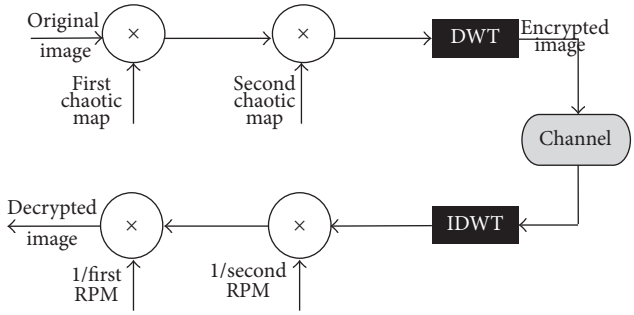


Figure 4: Flow chart of the first DWT based proposed technique.

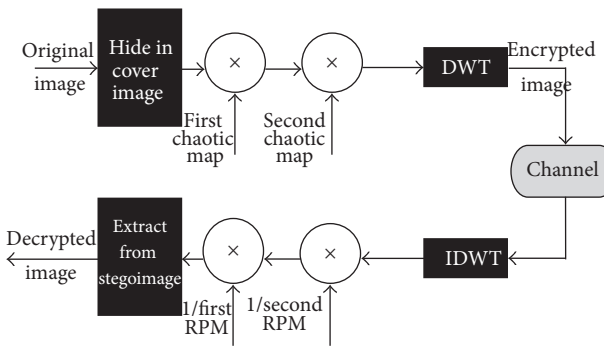


Figure 5: Flow chart of the second DWT based proposed technique.

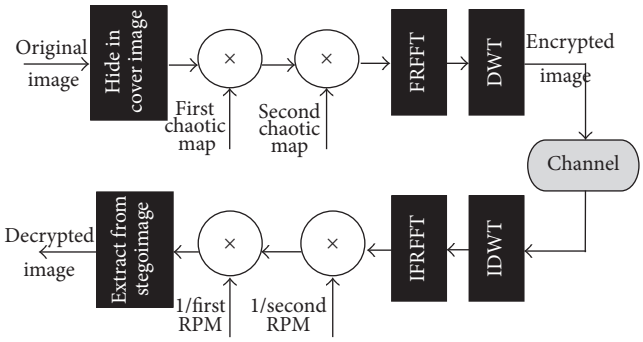


Figure 6: Flow chart of the third DWT based proposed technique.

enhancement for the decrypted image as well as achieving better randomness property over traditional map.

The main steps of the first DWT based proposed technique are represented by the flow chart in Figure 4. As observed from this figure, the green component of original color image is first multiplied by the first chaotic map: the proposed chaotic map, and this stage is followed by multiplying by the second chaotic map: the proposed map with different initial conditions. After that, DWT has been applied to end the encryption process by obtaining the encrypted image. Here, random phase masks in other traditional techniques, FFT based DRPE, DCT based DRPE, and traditional DWT based DRPE, have been replaced by chaotic maps to get powerful randomization of an image. Also, chaotic maps give more varieties to enhance the performance by varying its parameters and initial conditions.

The main steps of the second DWT based proposed algorithm will be discussed. Firstly, the original image has been hidden in the lower pixels of the cover image to form the stegoimage. After that this image has been multiplied by the first random key followed by multiplication by the second random key. Finally DWT has been applied to get the encrypted image to be transmitted through the channel. The reverse steps could be applied to get the decrypted image as shown in Figure 5.

The main flow chart of the third DWT based proposed algorithm will be demonstrated. The only difference between this proposed approach and the first one is applying FRFFT before applying DWT in the encryption process. In the decryption process, applying Inverse FRFFT (IFRFFT) has been needed after applying Inverse DWT (IDWT) as obtained in Figure 6.

Table 1: Plain color images database.

Image	Name	Extension	Size	Entropy
Original	My picture	JPEG	450 × 300	6.0302
Cover	Water lilies	.JPEG	600 × 800	7.0650

3.2. WP Based Algorithms. The remaining three proposed algorithms are the same as the previous ones except replacing DWT by WP. DWT in the encryption process has been replaced by WPD and IDWT in the decryption process has been replaced by WPR. The block diagrams of fourth, fifth, and sixth techniques are illustrated in Figures 7, 8, and 9.

4. Results and Discussions

4.1. Data Collection. The traditional as well as proposed techniques performance has been tested using the color images obtained in Table 1 providing the name, the extension, the size, and the entropy of each plain image.

The original image as well as cover image will be shown in Figure 10. These images are different in their histogram as will be illustrated in Figure 11.

4.2. Performance Metrics. Eight performance metrics have been used to test the performance, elapsed time, entropy analysis, Mean Square Error (MSE), Peak Signal-to-Noise Ratio

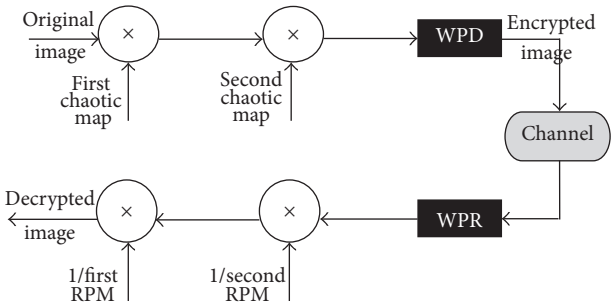


Figure 7: Flow chart of the fourth WP based proposed technique.

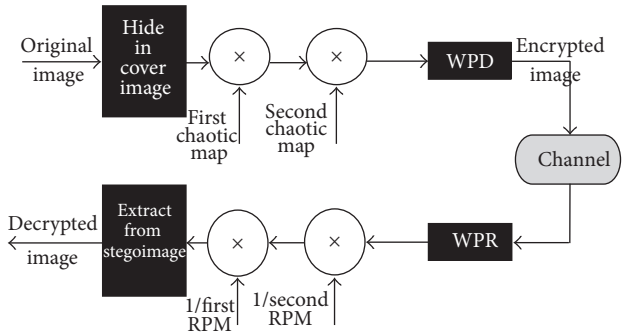


Figure 8: Flow chart of the fifth WP based proposed technique.

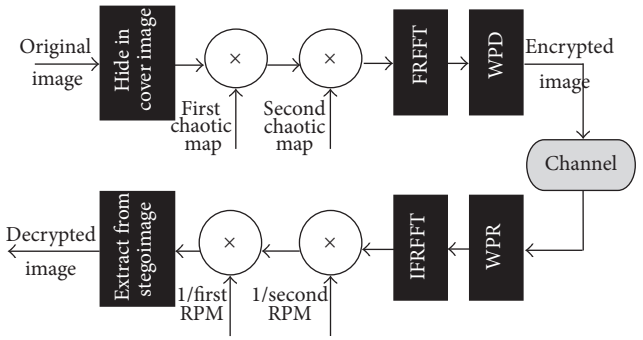


Figure 9: Flow chart of the sixth WP based proposed technique.

(a) (b)

Figure 10: The color images: (a) original image (the first image in Table 1) and (b) cover image (the second image in Table 1).

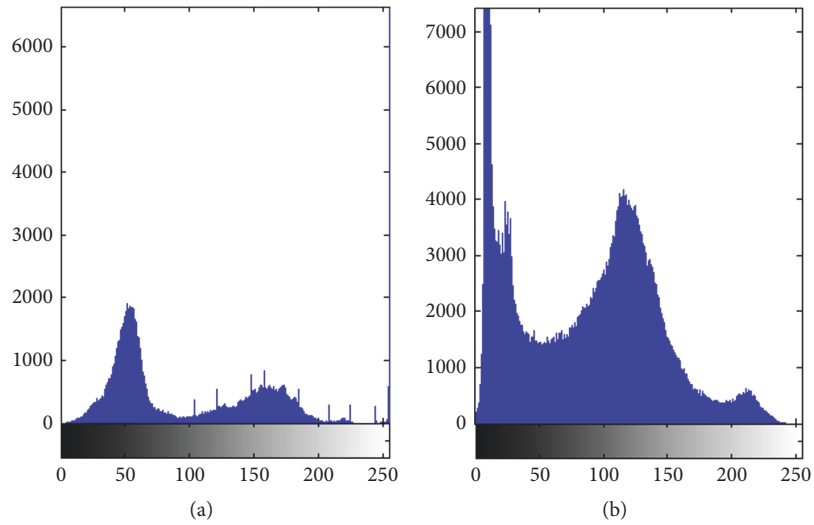


Figure 11: The color image histogram of (a) original image and (b) cover image.

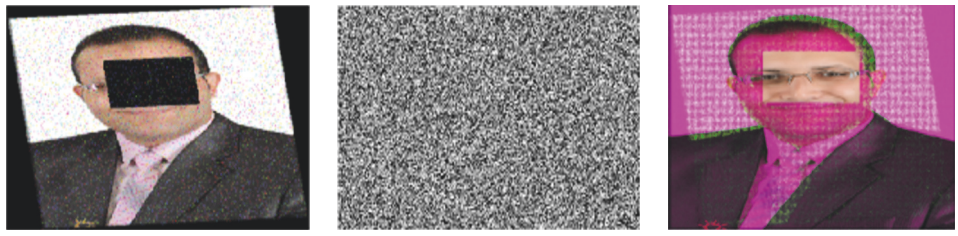


Figure 12: The simulation results of (a) original, (b) encrypted, and (c) decrypted images for both FFT and DCT based traditional techniques.

(PSNR), cross correlation coefficient (R) between original and decrypted images, Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), and the histogram analysis for both plain and resulting decrypted images. The basic definitions and equations for all the above performance metrics are listed in [16, 26]. Besides all of the above performance metrics, the simulation results for original, encrypted, and decrypted images for each technique will be observed.

4.3. Simulation Results and Discussions. The simulation results for the proposed algorithms as well as traditional ones will be discussed in this section using a personal computer with the following specifications: (i) Intel processor 3.2 GHZ Pentium-IV; (ii) 2 MB cache RAM; (iii) 2 GB RAM; (iv) SATA hard disk 250 GB.

From Figures 12–27 it has been found that the proposed techniques have given more similar histogram for encrypted and decrypted images than other traditional ones as well as realistic uniform distribution for encrypted image. Other performance metrics for all techniques will be listed in Table 2.

From these measurements we find that the proposed algorithms have given the best performance against composite attacks. They have obtained the closest entropy of decrypted image (DI) to that of original image listed in Table 1, the least MSE, the largest PSNR, the maximum cross correlation coefficient between original and decrypted images, and the least value for UACI. The elapsed time has been minimum in case of the first proposed DWT based technique. Also it could be easily noticed that DWT based proposed algorithms had achieved better performance than WP based ones before using any type of filters. These results can be represented more obviously through Figure 28. The value of NPCR has been the same for all techniques 0.0007 and 1 − NPCR = 0.9993 which achieved the practical value of it.

Different types of filters have been tested to get rid of the effect of salt and pepper noise and it has been found that median filter has given the best results. So in Table 3 the performance metrics results after using median filter for both traditional and proposed algorithms will be observed. After that the graphical representation of these results will be demonstrated through Figure 29.

From these measurements it could be found that generally WP based algorithms have given better performance versus DWT based ones except the elapsed time. It has been found that the first proposed technique has achieved the best robustness over DWT based schemes; on the other hand the fifth algorithm has obtained the best robustness over WP based approaches. By comparing these two algorithms (first and fifth) it has been found that the fifth proposed method has given better performance than the first one but with

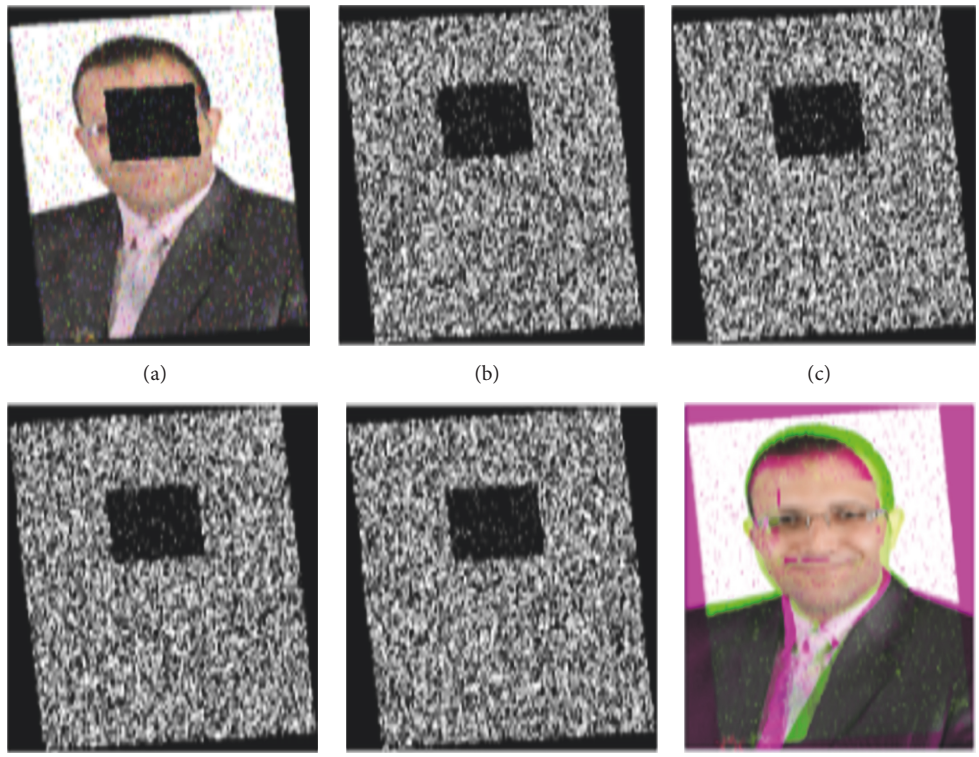


Figure 13: The simulation results of (a) original, (b) LL component, (c) LH component, (d) HL component, and (e) HH component of encrypted and (f) decrypted images for modified DWT based technique.

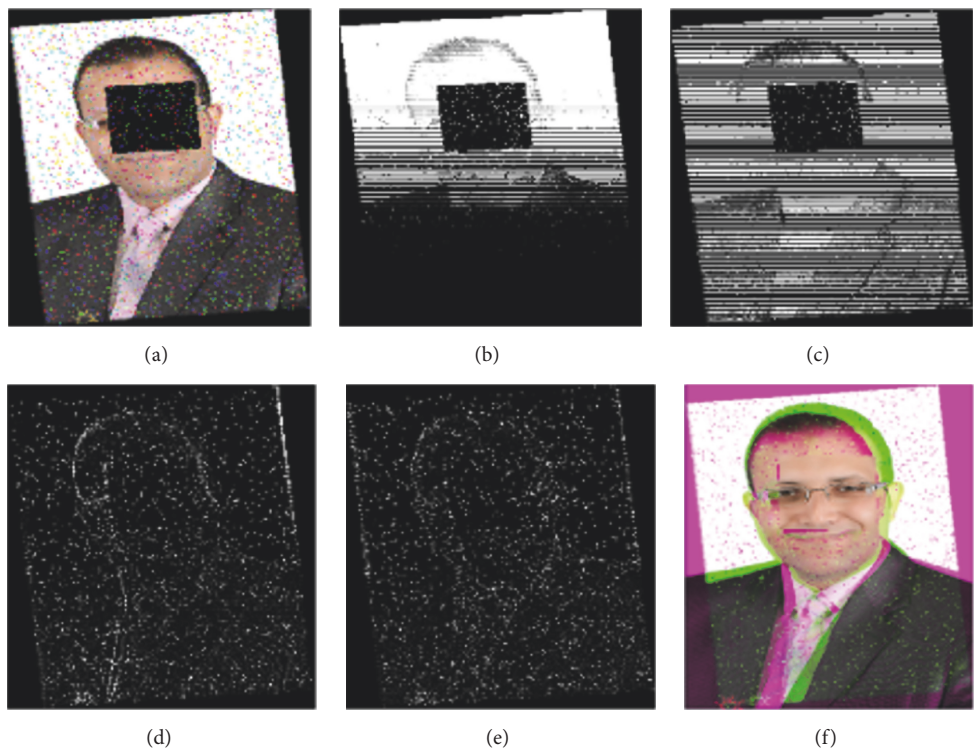


Figure 14: The simulation results of (a) original, (b) LL component, (c) LH component, (d) HL component, and (e) HH component of encrypted and (f) decrypted images for the first proposed technique.

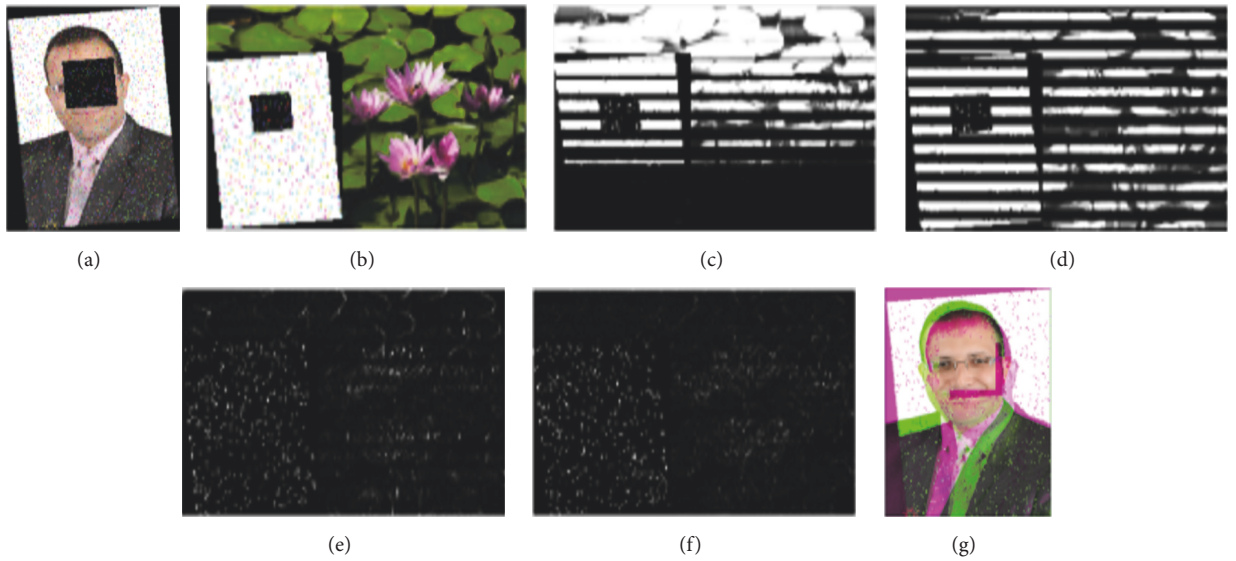


Figure 15: The simulation results of (a) original image, (b) stegoimage, (c) LL component, (d) LH component, (e) HL component, and (f) HH component of encrypted and (g) decrypted images for the second proposed technique.

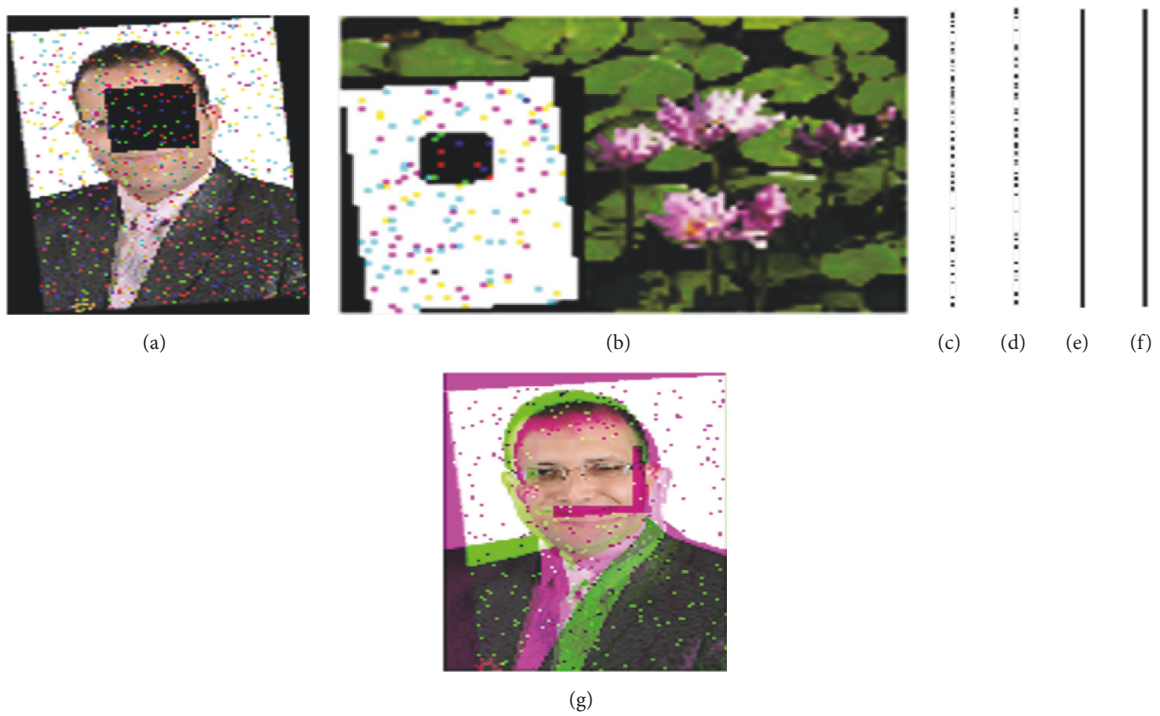


Figure 16: The simulation results of (a) original image, (b) stegoimage, (c) LL component, (d) LH component, (e) HL component, and (f) HH component of encrypted and (g) decrypted images for the third proposed technique.

higher value for elapsed time. So after using median filter it is recommended by using the first proposed technique to achieve reasonable robustness and to be suitable for real time applications. In other words, for achieving more robustness with slightly larger elapsed time values it is recommended by using the fifth proposed technique.

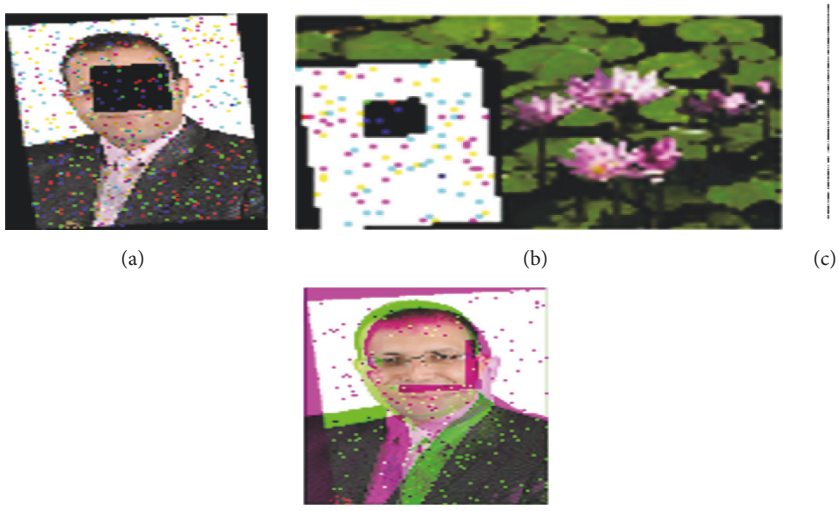
Note that the traditional DWT based technique itself could be considered as a modified technique. The main reason behind considering it as a modified technique not proposed one is that the complex random phases were still used as random keys as traditional DRPE technique. On the other hand it differed from DRPE in using DWT instead of

(a) (b) (c)

Figure 17: The simulation results of (a) original, (b) encrypted, and (c) decrypted images for the fourth proposed technique.

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

Figure 18: The simulation results for (a) original image, (b) stegoimage, (c) encrypted image, and (d) decrypted image for the fifth proposed technique.



(a) (b) (c)

(d)

Figure 19: The simulation results for (a) original image, (b) stegoimage, (c) encrypted image, and (d) decrypted image for the sixth proposed technique.

FFT to get higher resolution compatibility with color images encryption.

As a general discussion, it is clearly found that the modified as well as proposed algorithms have achieved higher performance over that of traditional ones against severe composite attacks. It has been found that there were significant enhancement ratios in most performance metrics values when using proposed techniques. These ratios before using any types of filters were about 190.62% enhancements in cross correlation coefficient (R), 36.38% improvements in MSE, 32% enhancements in PSNR, and about 97.17% improvements in UACI. After using median filter, these enhancement ratios have become as follows: 162.49% in R, 39.88% in MSE, 35.29% in PSNR, and 98.17% in UACI.

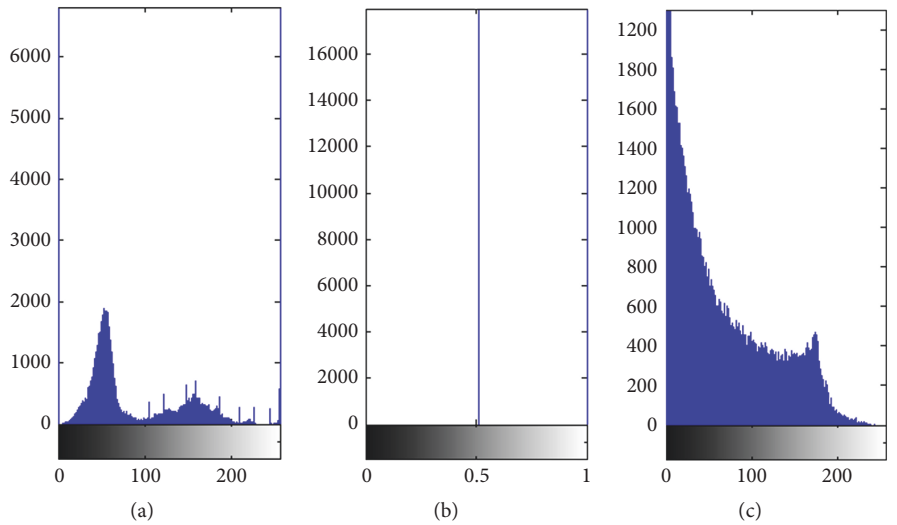


Figure 20: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for both FFT and DCT based traditional techniques.

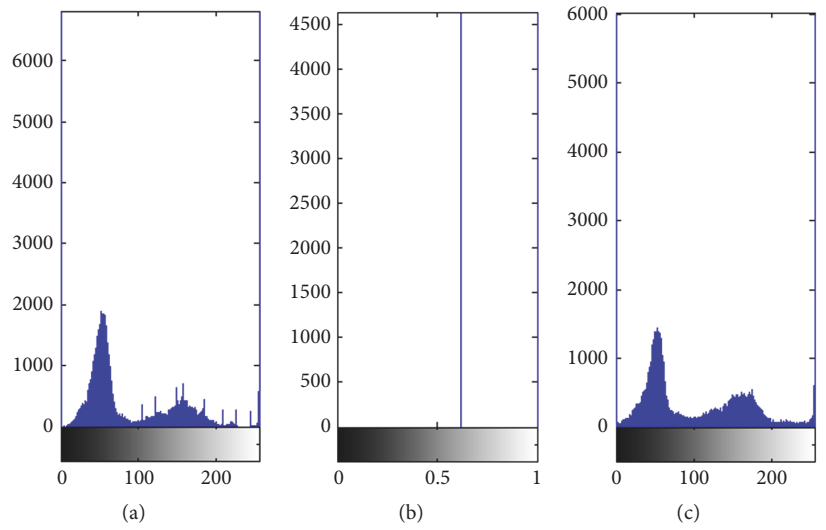


Figure 21: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for DWT based modified technique.

Table 2: Performance metrics for DWT versus WP based proposed techniques without using filters.

Technique	Performance metrics							
	Entropy of DI	Elapsed time (Sec)	R	MSE	NMSE	PSNR (dB)	UACI	NPCR
Traditional FFT	7.2628	0.5007	0.1557	15828	1	6.1365	28.317	0.00074
Traditional DCT	7.2638	0.7704	0.1545	15819	0.999	6.1391	28.221	0.00074
Modified DWT	5.9133	0.6259	0.4341	10495	0.663	7.9209	5.6079	0.00074
First proposed	*5.9132*	*0.4907*	*0.4365*	*10446*	*0.660*	*7.9412*	*5.5848*	*0.00074*
Second proposed	*5.5161*	*0.7326*	*0.4526*	*10070*	*0.636*	*8.1005*	*0.8016*	*0.00074*
Third proposed	*5.5167*	*0.9310*	*0.4509*	*10101*	*0.638*	*8.0871*	*0.8815*	*0.00074*
Fourth proposed	*5.9201*	*1.9768*	*0.4354*	*10456*	*0.661*	*7.9370*	*5.5808*	*0.00074*
Fifth proposed	*5.5170*	*2.5886*	*0.4510*	*10098*	*0.638*	*8.0884*	*0.8421*	*0.00074*
Sixth proposed	*5.5175*	*11.975*	*0.4506*	*10104*	*0.638*	*8.0860*	*0.8273*	*0.00074*

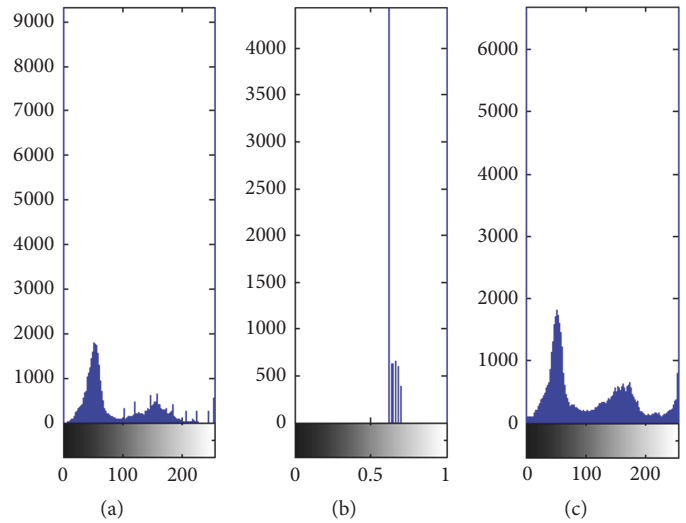


Figure 22: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for the first technique.

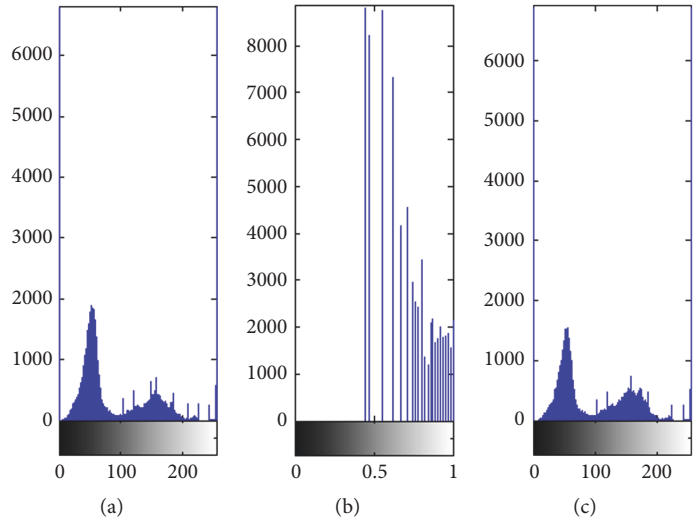


Figure 23: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for the second proposed technique.

Table 3: Performance metrics for DWT versus WP based proposed techniques after using median filter.

Technique	Performance metrics							
	Entropy of DI	Elapsed time (Sec)	R	MSE	NMSE	PSNR (dB)	UACI	NPCR
Traditional FFT	7.2307	0.5542	0.1858	15375	0.999	6.2627	29.0707	0.00074
Traditional DCT	7.2331	0.7911	0.1846	15388	1	6.2590	29.1083	0.00074
Modified DWT	5.6448	0.6296	0.4601	10066	0.654	8.1021	5.3108	0.00074
First proposed	*5.6431*	*0.5132*	*0.4602*	*10061*	*0.653*	*8.1043*	*5.2961*	*0.00074*
Second proposed	*5.5673*	*0.7451*	*0.4877*	*9243*	*0.601*	*8.4727*	*0.5308*	*0.00074*
Third proposed	*5.5654*	*0.9521*	*0.4877*	*9245.7*	*0.601*	*8.4714*	*0.5267*	*0.00074*
Fourth proposed	*5.6422*	*3.5743*	*0.4599*	*10071*	*0.654*	*8.0999*	*5.3114*	*0.00074*
Fifth proposed	*5.5663*	*2.5712*	*0.4880*	*9239.4*	*0.600*	*8.4744*	*0.5328*	*0.00074*
Sixth proposed	*5.5643*	*10.567*	*0.4876*	*9245.1*	*0.601*	*8.4717*	*0.5242*	*0.00074*

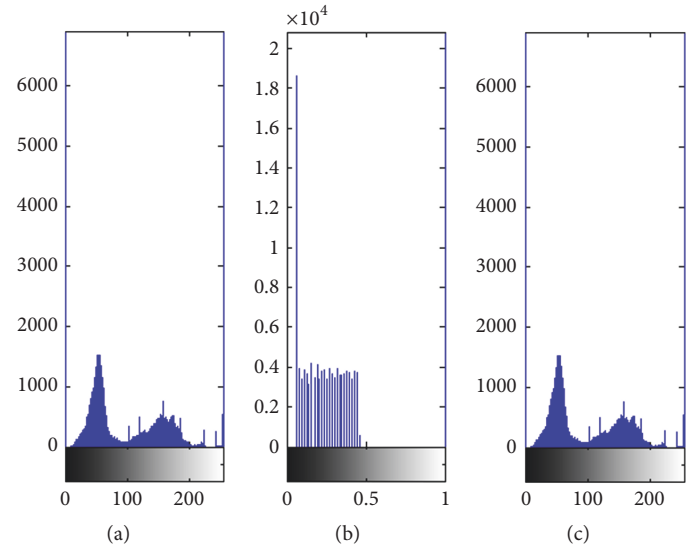


Figure 24: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for the third proposed technique.

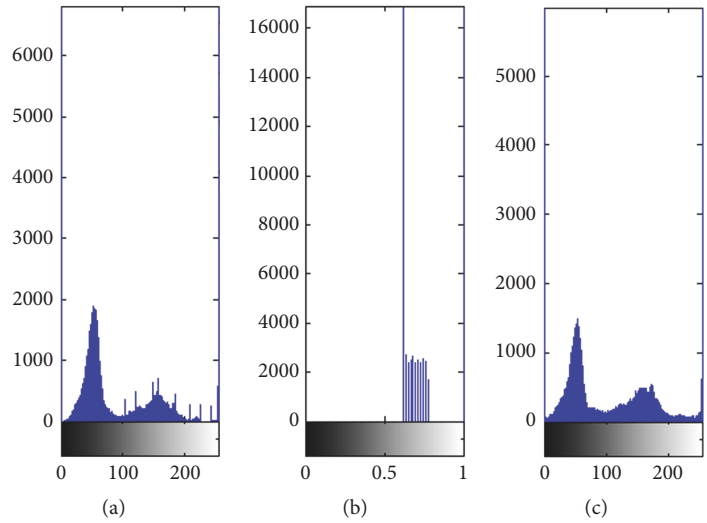


Figure 25: The histogram analysis for (a) original, (b) encrypted, and (c) decrypted images for the fourth proposed technique.

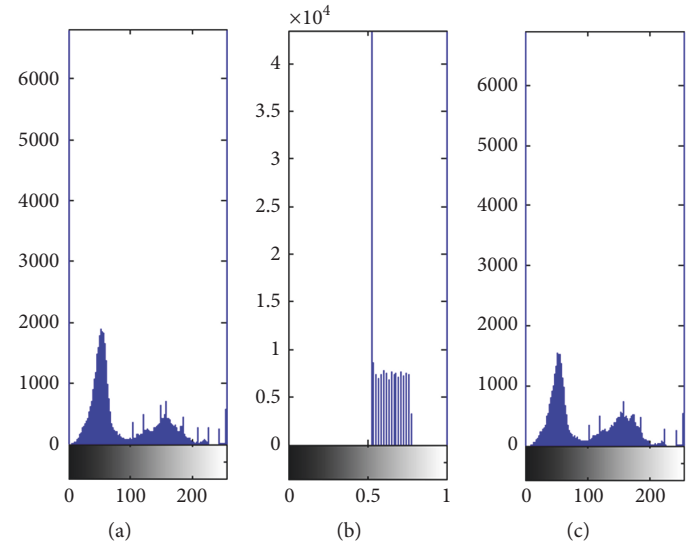


Figure 26: The histogram analysis for (a) original, (b) encrypted, and (c) decrypted images for the fifth proposed technique.

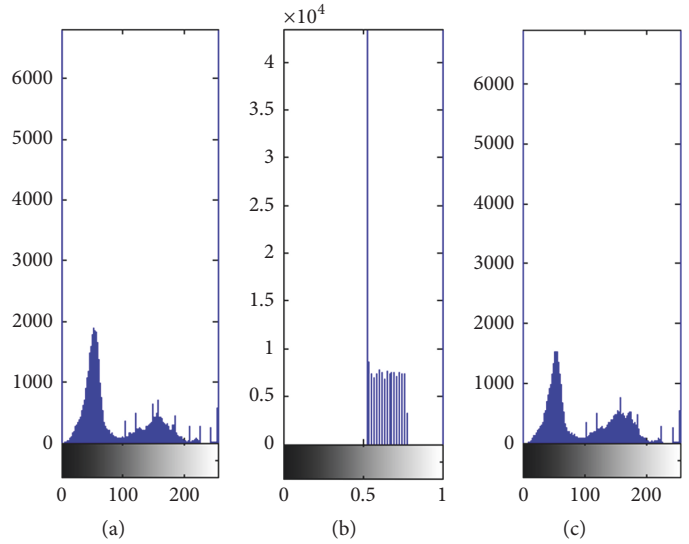


Figure 27: The histogram analysis for (a) original, (b) encrypted, and (c) decrypted images for the sixth proposed technique.

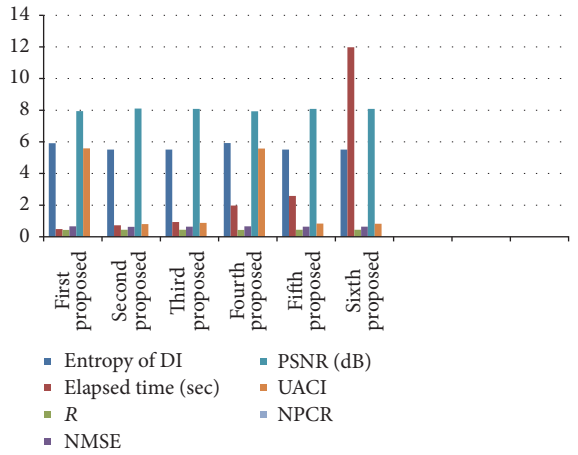


Figure 28: The performance metrics for DWT versus WP based proposed algorithms without using filters.

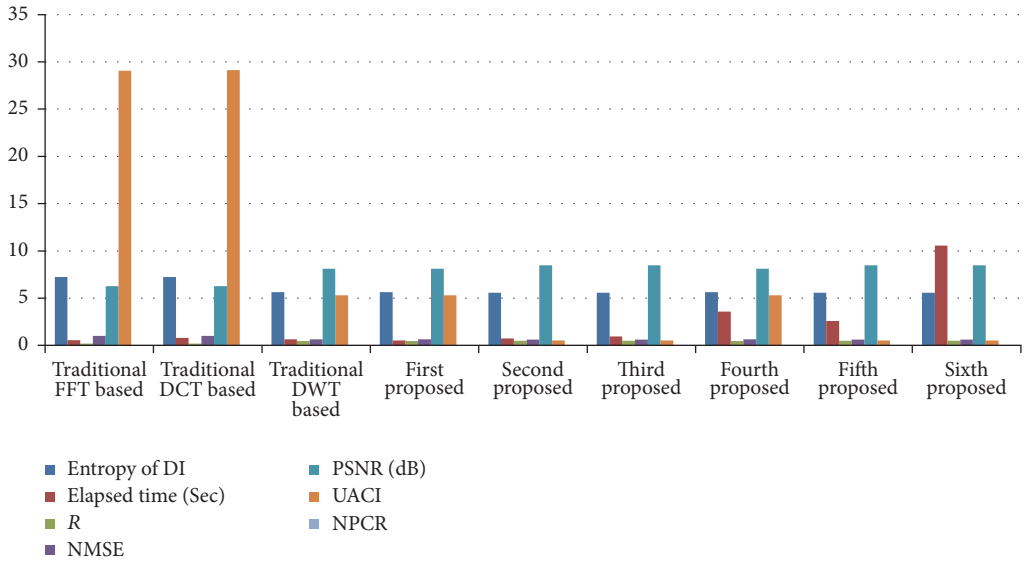


Figure 29: The performance metrics for DWT versus WP based proposed algorithms after using median filter.

One of the most attractive strength points is recovering the decrypted images without any occlusion parts. The occlusion itself has represented a severe type of attacks when imposing individually on the original image, but also it has been composed of other hard attacks: noise and rotation attacks; however all proposed techniques could retrieve the decrypted image effectively.

5. Conclusions

In this paper six proposed optical encryption algorithms have been introduced. Three of them have been based on DWT and other ones have been based on WP. The random keys used in these techniques have been represented using a new chaotic map based on Chirikov map. The performance of these algorithms as well as a set of traditional algorithms has been studied on color images. As a result of extensive comparative study it has been found that the proposed algorithms provided improved results with respect to traditional techniques: (i) the minimum value for MSE, (ii) the maximum value for PSNR, (iii) the largest value of R, (iv) the closest value of decrypted image entropy to those of the plain images, and (v) the minimum values for UACI. DWT based algorithms have given better performance than WP based ones before using any type of filters, and vice versa, after using median filter. So for real time applications in which low security level is needed using the first traditional algorithm is recommended. For acceptable level of security as well as compatibility with real time applications, it is recommended by using the first DWT based proposed algorithm. Finally, for high level of security but with slightly larger value for elapsed time by using median filter using the fifth proposed method is recommended. The practical applications of these provided algorithms introduced the advantage of high robustness against composite-severe attacks. On the other hand, the theoretical implications of these algorithms were the increased complexity of the overall system. In the future the proposed techniques can be implemented on a reasonable hardware platform as Field Programmable Gate Array (FPGA). Also all of proposed schemes can be applied on optical holographic images instead of digital images.

Conflicts of Interest

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

References

[1] R. Vijayaraghavan, S. Sathya, and N. R. Raajan, "Encryption for an image using circular budge on bit-planes," *International Journal of Applied Engineering Research*, vol. 9, no. 2, pp. 60–153, 2014.

[2] M. A. Mohamed, A. S. Samarah, and M. I. Fath Allah, "Optical encryption techniques: an overview," *International Journal for Computer Science Issues (IJCSI)*, vol. 11, no. 2, pp. 125–129, 2014.

[3] F. Mosso and M. Tebaldi, "All-optical encrypted movie," *Optical Society of America*, vol. 19, no. 6, pp. 5706–5712, 2011.

[4] Y. Liu, J. Lin, J. Fan, and N. Zhou, "Image encryption based on cat map and fractional fourier transform," *Journal of Computational Information Systems*, vol. 8, no. 18, pp. 7485–7492, 2012.

[5] P. Réfrégier and B. Javidi, "Optical Image Encryption Based on Input Plane & Fourier Plane Random Encoding," *Optics. Letters*, vol. 20, pp. 767–769, 1995.

[6] R. Vijayaraghavan, S. Sathya, and N. R. Raajan, "Image encryption based on the reflected binary code method with the combination of FFT," *Indian Journal of Science and Technology*, vol. 8, no. 36, Article ID 87852, 2015.

[7] D. Sharma, R. Saxena, and N. Singh, "Hybrid Encryption-Compression Scheme Based on Multiple Parameter Discrete Fractional Fourier Transform with Eigen Vector Decomposition Algorithm," *International Journal of Computer Network & Information Security*, vol. 10, pp. 1–12, 2014.

[8] C. S. Narayanan and S. A. Durai, "A critical study on encryption based compression techniques," *Journal of Computers*, vol. 11, no. 5, pp. 380–399, 2015.

[9] P. Palevicius and M. Ragulskis, "Image communication scheme based on dynamic visual cryptography and computer generated holography," *Optics Communications*, vol. 335, pp. 161–167, 2015.

[10] M. V. Kanchana and V. K. Annapurna, "An enhanced VCS of image encryption using SDS algorithm without secret keys," *International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC)*, vol. 2, no. 7, pp. 1794–1798, 2014.

[11] X. Li, C. Li, S. T. Kim, and I. K. Lee, "An optical image encryption scheme based on depth conversion integral imaging and chaotic maps," preprint submitted to Elsevier, pp. 1–18.

[12] Z. Shao, H. Shu, J. Wu, Z. Dong, G. Coatrieux, and J. L. Coatrieux, "Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain," *Optics Express*, vol. 22, no. 5, pp. 4932–4942, 2014.

[13] Q. Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling," *International Journal of Computer Network and Information Security*, vol. 5, no. 7, pp. 43–50, 2013.

[14] Z. Liu, L. Xu, T. Liu et al., "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123–128, 2011.

[15] X. Deng and X. Zhu, "A simple and practical color image encryption with the help of QR code," *Optica Applicata*, vol. 45, no. 4, pp. 513–521, 2015.

[16] M. A. Mohamed, H. M. Abdel-Atty, A. M. Abutaleb, M. G. Abdel-Fattah, and A. S. Samrah, "Hybrid watermarking scheme for copyright protection using chaotic maps cryptography," *International Journal of Computer Applications*, vol. 128, no. 1, pp. 1–14, 2015.

[17] I. Hussain, N. A. Azam, and T. Shah, "Stego optical encryption based on chaotic S-box transformation," *Optics & Laser Technology*, vol. 61, pp. 50–56, 2014.

[18] Ashutosh and D. Sharma, "Robust Technique for Image Encryption and Decryption Using Discrete Fractional Fourier Transform with Random Phase Masking," *Procedia Technology*, vol. 10, pp. 707–714, 2013.

[19] R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Optics Express*, vol. 15, no. 24, pp. 16067–16079, 2007.

[20] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," *Optics Express*, vol. 21, no. 7, pp. 8025–8043, 2013.

[21] G. Cristobal, P. Schelkens, and H. Thienpont, *Optical and digital image processing: fundamentals and applications*, Wiley-VCH Verlag GmbH & Co. KGaA, 2011.

[22] A. Alfalou, C. Brosseau, and N. Abdallah, "Simultaneous compression and encryption of color video images," *Optics Communications*, vol. 338, pp. 371–379, 2015.

[23] A. Alfalou and C. Brosseau, "Recent Advances in Optical Image Processing," *Progress in Optics*, vol. 60, pp. 119–262, 2015.

[24] N. Soorma, J. Singh, and M. Tiwari, "Feature Extraction of ECG Signal Using HHT Algorithm," *International Journal of Engineering Trends and Technology*, vol. 8, no. 8, pp. 454–460, 2014.

[25] M. Dubreuil, A. Alfalou, and C. Brosseau, "Robustness against attacks of dual polarization encryption using the Stokes-Mueller formalism," *Journal of Optics (United Kingdom)*, vol. 14, no. 9, Article ID 094004, 2012.

[26] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Advances in Optics and Photonics*, vol. 1, no. 3, pp. 589–636, 2009.

[27] P. W. M. Tsang, T.-C. Poon, and K. W. K. Cheung, "Fast numerical generation and encryption of computer-generated Fresnel holograms," *Applied Optics*, vol. 50, no. 7, pp. B46–B52, 2011.

[28] G. K. Anusha and R. M. Nilajkar, "Optical method for images encryption based on chaotic baker map and double random phase encoding," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, no. 6, 2014.

[29] 2017, http://www.scholarpedia.org/article/Chirikov_standard_map.