# A Novel Chaotic based Optical Color Image Encryption Technique

M. A. Mohamed
Associate Professor at ECE Department,
Faculty of Engineering,
Mansoura University, Egypt

A. S. Samrah
Professor at ECE-Department,
Faculty of Engineering,
Mansoura University, Egypt

M. I. Fath Allah
Assist Lecturer at ECE-Department,
Faculty of Engineering,
Delta University, Egypt

## ABSTRACT

Nowadays, various types of attacks are imposed to multimedia during transmission. Also in many applications the security of information is very important. So the information encryption has become an important issue. Many encryption techniques have been proposed to achieve high robustness against different types of attacks and to save information from hackers. In this paper, a new chaotic based optical encryption that depends on Discrete Wavelet Transform (DWT) for image transformation will be introduced for color image encryption. Nine chaotic maps have been used in the proposed technique; eight of them were traditional and one is a new proposed map. As a result of extensive simulation results depending on various performance metrics it has been found that the proposed technique has given better robustness comparing to traditional algorithm.

## General Terms

Image Encryption, Optical Encryption, Chaotic Maps, RGB.

## Keywords

Double Random Phase Encoding (DRPE), Fast Fourier Transform (FFT), Discrete Wavelet Transform (DWT), Inverse Discrete Wavelet Transform (IDWT).

## 1. INTRODUCTION

Recently, fast development of Internet technology has improved the schemes to distribute and exchange digital multimedia with less time, lower complexities and better efficiency. Digital multimedia can be manipulated or reproduced easily without the loss of information using effective multimedia processing tools that are widely available [1]. Over the years many researches have been directed toward coherent optics because of the potential for new technological applications in telecommunications [2, 3]. In recent years, optical encryption has reached a level of maturity with the publication of realistic attacks that exploit its inherent weakness of linearity [4-6]. The main objective of image encryption is to convert the original image to another image that is hard to understand, but it differs from text encryption due to some intrinsic features of images which include bulk data capacities, high redundancy, strong correlations among pixels, etc. These features make conventional cipher systems unsuitable for practical image encryption [7, 8]. Due to optical nature of an image; optical encryption is more suitable for image encryption. The chaos theory has been applied in cryptography due to its intrinsic features. These properties of chaos includes; sensitivity to initial conditions and control parameters [8]. The chaotic encryption technique has been developed in [9]. In this paper, Traditional Double Random Phase Encoding (DRPE) using DWT instead of Fast Fourier Transform (FFT) as in [10] will be firstly presented.

After that the proposed algorithm will be introduced. This proposed technique depends on adding the green component of original and host color images followed by multiplying by two chaotic maps of the same type with different parameters and initial conditions. Finally DWT has been applied to get the encrypted image. Nine chaotic maps have been used; eight of them are conventional, and one is our new map, hence not only a novel technique has been introduced, but also a new chaotic map has been proposed for better performance. The main advantage of our technique is its high robustness to different types of attacks such as; noise, rotation, and cropping, as well as the flexibility in control of encryption process by varying the host image or the parameters and initial conditions of chaotic maps until getting the best performance.

The next of this paper is organized as follows; section-2 presents for literature survey, section-3 provides traditional technique, section-4 introduces proposed algorithm, section-5 observes the simulation results and discussions as well as images database, and section-6 discusses the conclusions.

## 2. LITERATURE SURVEY

A new two-dimensional chaos based lossless encryption method that was based on series of confusion and diffusion processes has been developed in [11]. A technique which replaced the traditional preprocessing complex system and utilized the basic operations like confusion, diffusion which provided same or better encryption using cascading of 3D standard and 3D cat map has been presented in [12]. Optical encryption and compression methods have been discussed in [13]. The approach of image encryption using the concept of sieving, dividing and shuffling has been described in [14]. A performance-enhanced image encryption schemes based on depth-conversion integral imaging and chaotic maps have been introduced in [15]. A novel algorithm to encrypt double color images into a single undistinguishable image in quaternion gyrator domain using an iterative phase retrieval algorithm has been described in [16]. The general body of knowledge in the area of cryptography application and developing a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values has been discussed in [17]. A color image encryption algorithm has been designed by use of Arnold transform and discrete cosine transform (DCT) in [18]. A simple and practical color image encryption has been proposed with the help of quick response (QR) code in [19]. A proposed hybrid encryption-watermarking algorithm for copyright protection has been introduced in [20].

## 3. TRADITIONAL TECHNIQUE

In this section, the conventional optical encryption technique based on DRPE by replacing FFT with DWT will be demonstrated in Fig. 1. As illustrated in this figure, the original image is first multiplied by the first random phase mask and then it is multiplied by the second random phase mask. After that, DWT is applied to obtain the encrypted image. Obviously the reversed steps are applied on the encrypted image to get the original color image as included in decryption process.

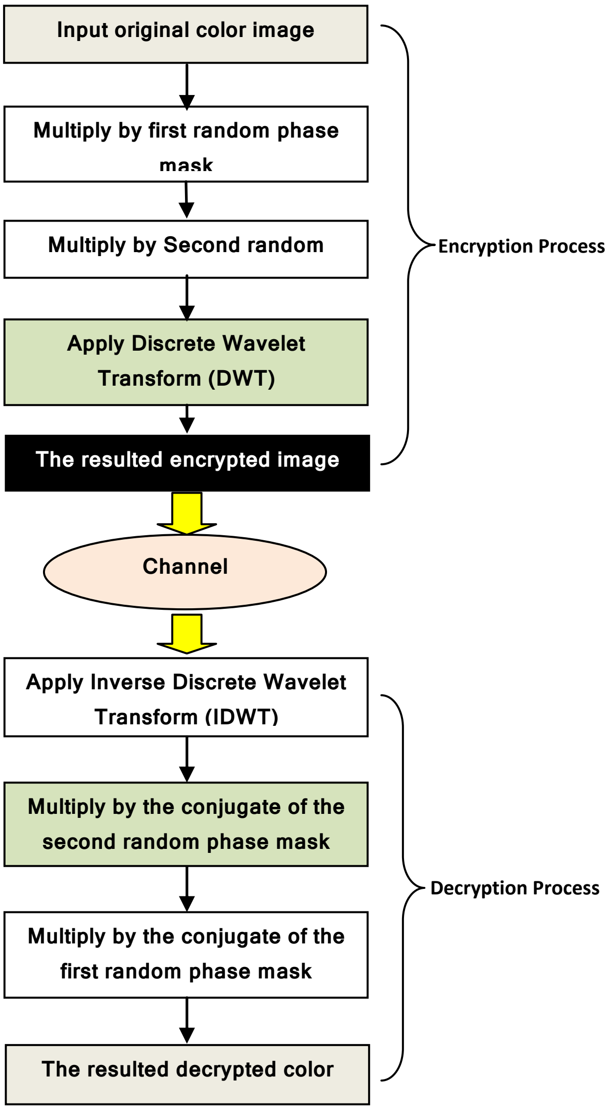

Input original color image
Multiply by first random phase mask
Multiply by Second random
Apply Discrete Wavelet Transform (DWT)
The resulted encrypted image
Encryption Process
Channel
Apply Inverse Discrete Wavelet Transform (IDWT)
Multiply by the conjugate of the second random phase mask
Multiply by the conjugate of the first random phase mask
The resulted decrypted color
Decryption Process

**Fig 1: Flow Chart of DWT Based Traditional Technique**

## 4. PROPOSED ALGORITHM

In this section the proposed technique that depends on using chaotic maps to randomize the original image as well as DWT for image transformation will be introduced. The main flow chart of this proposed algorithm is shown in Fig. 2. From this figure, we get that the first step is adding the green component of both original and host color images; so we could get more varieties to adapt the performance to be better by using specific host image. It was found that changing the host image has changed the performance and we have chosen the best host image that gave the best performance. Also this step will make hacking slightly harder. The second step is multiplying this summation by the two chaotic maps with specific parameters and initial values. Nine chaotic maps have been used, eight of them are conventional and one is the new proposed map; hence we not only a novel technique for optical color image encryption has been introduced, but also a new chaotic map. The last step in encryption process is applying DWT for image transformation to get the resulted encrypted image.

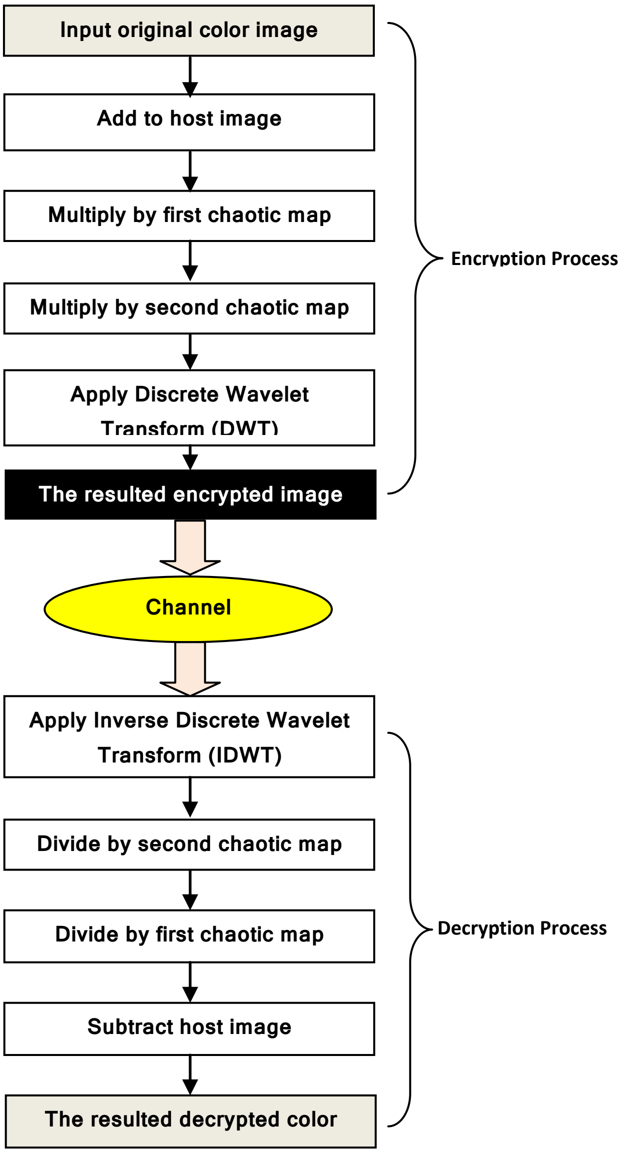

Input original color image
Add to host image
Multiply by first chaotic map
Multiply by second chaotic map
Apply Discrete Wavelet Transform (DWT)
The resulted encrypted image
Encryption Process
Channel
Apply Inverse Discrete Wavelet Transform (IDWT)
Divide by second chaotic map
Divide by first chaotic map
Subtract host image
The resulted decrypted color
Decryption Process

**Fig. 2 Flow Chart of the Proposed Technique**

The decryption process steps are the inverse of those of the encryption process as obtained in Fig. (2). First Inverse Discrete Wavelet Transform (IDWT) has been applied to the encrypted image, and then it has been divided by the second chaotic map followed by dividing by the first one. The last step is subtracting the host image to get the resulted decrypted color image. The main equations of eight predefined chaotic maps; Chirikov, Henon, Logistic, Quadratic, Ikeda, Baker, CAT, and Open-CAT maps have been presented in [21, 22].

The proposed chaotic map depends on Chirikov map by replacing sin function with tan function. It has been found that this new map gave the best performance as will be illustrated in the following section. The main equations of a novel chaotic map are shown in the following equations.

$$x_{n+1} = x_n - K \tan y_n \qquad (1)$$

$$y_{n+1} = y_n + x_{n+1} \qquad (2)$$

# 5. 5. SIMULATION RESULTS & IMAGES DATABASE

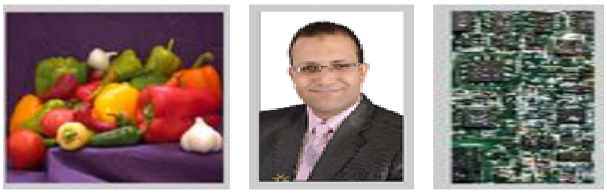
In this section the color images database that has been used in simulation process as well as simulation results and discussions will be observed.

## 5.1 Images Database

The main database of color images that has been used for our simulation is listed in table (1) observing the name, the type, the extension, the size, and the entropy of each plain image. Original Color images as well as their histogram are obtained in the Fig. 3 and Fig. 4.

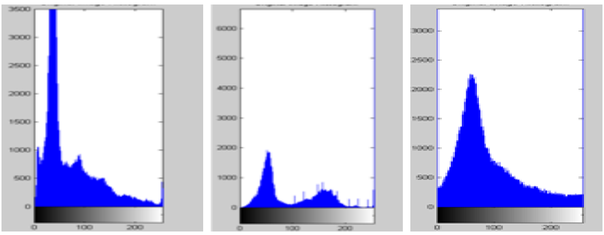
**Table 1. Color Images Database**

| Image | Name | Type | Extension | Size | Entropy |
|---|---|---|---|---|---|
| 1 | Peppers | Original | .png | 384×512 | 7.3785 |
| 2 | My Picture | Original | .JPEG | 450×300 | 6.0302 |
| 3 | Board | Host | .tif | 648×306 | 7.2368 |



(a) (b) (c)

**Fig. 3 Color Images; (a) Original Image (1), (b) Original Image (2), and (c) Host Image**



(a) (b) (c)

**Fig. 4 Image Histogram for; (a) Original Image (1), (b) Original Image (2), and (c) Host Image**

## 5.2 Performance Metrics

We have used six performance metrics to measure the performance of all of three techniques stated in the previous section; elapsed time, entropy analysis, Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), cross correlation coefficient between original and decrypted images, and the histogram analysis for both plain and resulted decrypted images. Besides all of the above performance metrics, the simulation results for original, encrypted, and decrypted images for each technique will be observed. First we must present for the basic definitions for all the above performance metrics as follows.

### *5.2.1 Entropy Analysis*

The entropy of a message source could be defined as in Eq. (1):

$$H(m) = - \sum_{i=0}^{2^N-1} p(m_i)\, log_2(p(m_i)) \qquad (1)$$

Where, $p(m_i)$ is the probability of symbol $m_i$, and N represents the number of bits for each symbol. The entropy represents the most outstanding feature of randomness [38]. For our techniques we concentrate on the difference between the entropy of original images listed in table (1) and the entropy of decrypted images that will be presented for each technique.

### *5.2.2Peak Signal-to-Noise Ratio (PSNR)*

The Peak Signal-to-Noise Ratio is used to measure the degradation between the plain and decrypted images. It can be computed as in Eq. (2):

$$PSNR = 10log_{10}\left(\frac{{Max_{OI}}^2}{MSE}\right) dB \qquad (2)$$

Where, $Max_{OI}$ represents the maximum possible pixel value of the original image [38].

### *5.2.3 Mean Square Error (MSE)*

The Mean Square Error between the original and decrypted images could be computed as in Eq. (2):

$$MSE = \frac{1}{MxNxf} \sum_{k=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} [OI(i,j,k) - DI(i,j,k)]^2 \qquad (3)$$

Where, M is the number of rows, N is the number of columns, f is the number of image frames, OI is the original image, and DI is the decrypted image [38].

### *5.2.4 Cross Correlation Coefficient (R)*

The cross correlation between the original and decrypted images can be defined as in Eq. (4):

$$R = \frac{\sum_m \sum_n (OI_{mn} - \overline{OI})(DI_{mn} - \overline{DI})}{\sqrt{(\sum_m \sum_n (OI_{mn} - \overline{OI})^2)(\sum_m \sum_n (DI_{mn} - \overline{DI})^2)}} \qquad (4)$$

Where, m is the row number, n is the column number, $\overline{OI}$ is the mean value of the pixels of original image, and $\overline{DI}$ is the mean value of the pixels of decrypted image.

### *5.2.5 Histogram Analysis*

The histogram analysis clarifies that, how the pixel values of original or decrypted image are distributed. For good encryption technique, the histogram of decrypted image must be similar to the histogram of original image with slightly little difference [38]. The main equation of histogram of an image is obtained as follows;

$$P_n = \frac{Number\ of\ pixels\ with\ intensity\ n}{Total\ number\ of\ pixels},\ n = 0,\ 1,\ \ldots,\ L - 1 \qquad (5)$$

Where, for f is a given image represented as a r by c matrix of integer pixel intensities ranging from 0 to L − 1. L is the number of possible intensity values, usually 256, and pn denote the normalized histogram of image f [39].

### *5.2.6 Elapsed Time*

Elapsed time has represented the total computational time for encryption as well as decryption processes in seconds for each trial of experiments. All of our experiments have been done using the same computer and the same version of MATLAB Program. Our device was connected to internet most of time. All experiments have been applied more than one time and hence the elapsed time has represented the average simulation time for all trials for each experiment.

## 5.3 Simulation Results for Real Channel Techniques

Besides all of the above performance metrics, the simulation results for original, encrypted, and decrypted images for each technique will be depicted. The simulation results will be observed for various types of attacks; (i) noise, (ii) Rotation, and (iii) cropping as will be observed in the following subsections.

### *5.3.1 Noise Attacks*

In this subsection the simulation results as well as performance metrics measurements will be demonstrated for both techniques in the case of three different types of noise; salt & pepper noise, Gaussian noise, and speckle noise. The effect of all of these types will be studied with and without using filters.

### *A. Salt & Pepper Noise without Using Filter*

The simulation results as well as histogram analysis for original, encrypted and decrypted versions of image (1) for our proposed technique with new proposed chaotic map in case of salt and pepper noise without using filters are shown in Fig. 5. The chaotic maps and their parameters have been as follows; (1) our proposed map with K=0.9 for two random keys, (2) Chirikov map with K=0.9 for both random keys, (3) Hénon map with a=1.4 and b=0.3 for both random keys, (4) Logistic map with k=4 for both random keys, (5) Quadratic map with c=1.95 for both random keys, (6) Ikeda map with m=0.9 for both random keys, (7) Baker map with a=0.5 for both random keys, (8) CAT map, and (9) Open CAT (Op-CAT) map with K=0.9 for both random keys. For all the above chaotic maps the initial values have been x0=0.1 and y0=0.1 as initial conditions for the first random key, and x0=0.2 and y0=0.2 for the second random key for all 2D maps. In the case of one dimensional maps (Logistic and Quadratic maps), the initial conditions are; x0=0.1 for the first random key and x0=0.2 for the second random key.

The uniform distribution of the histogram of the encrypted image is obviously shown in case of our proposed technique as in Fig. 6. Other performance metrics values for both traditional and proposed techniques will be introduced in the following table. The measurements of our proposed technique with all nine chaotic maps will be provided for image (1) for brief presentation. From this table we get that our proposed technique with our new chaotic map has given better performance than that of traditional one. Also one can note that our proposed map gave better performance than other eight maps. It is obvious that our proposed technique with new map has given smaller elapsed time than traditional technique; hence it can consider being more suitable for real time applications. A comparison between our proposed map based novel technique and traditional scheme is illustrated obviously through the some graphs for both original images in Fig. 7 to Fig. 9. We have chosen three performance metrics to show the comparison between traditional and proposed techniques graphically. It is found from these graphs that the proposed technique gave smaller elapsed time, MSE, and slightly larger correlation coefficient between plain and decrypted images.

### *B. Salt & Pepper Noise after Using Filter*

In this subsection, the simulation results as well as performance measurements in case of salt & pepper noise after using median filter will be observed as follows. The simulation results and histogram analysis will be presented for image (1) as an example.

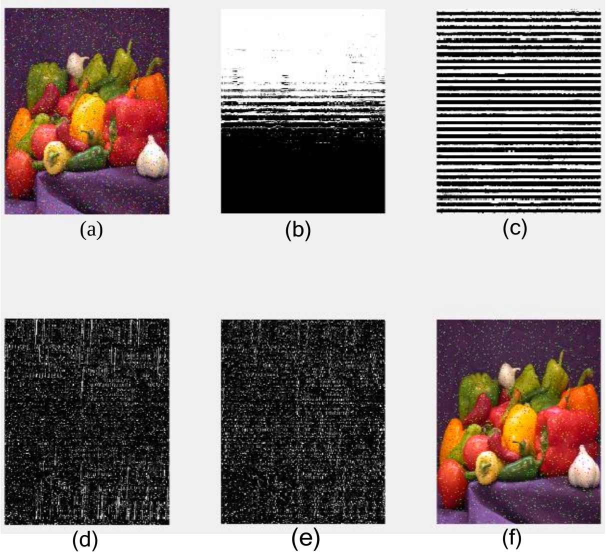


**Fig. 5 The Simulation Results for; (a) Original, (b) LL Component, (c) LH Component, (d) HL Component, (e) HH Component of Encrypted, and (f) Decrypted Versions of Image (1) for Proposed Technique with Proposed Map against Salt & Pepper Noise without Using Filters**

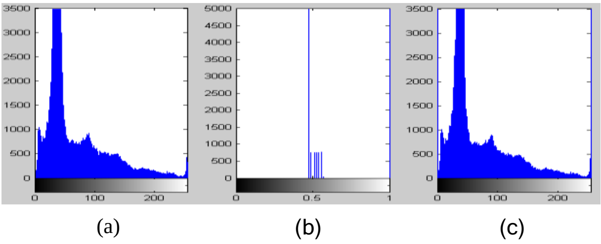


**Fig. 6 The Histogram Analysis for; (a) Original, (b) Encrypted, and (c) Decrypted Versions of Image (1) for Proposed Technique with Proposed Map against Salt & Pepper Noise without Using Filters**

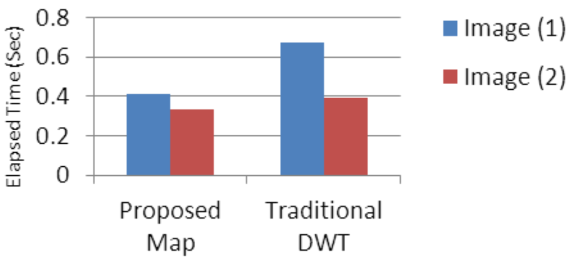


**Fig. 7 Elapsed Time (Sec) for both Traditional and Proposed Techniques**

**Table 2. Performance Metrics in Case of 10 % Salt & Pepper Noise (without Filters) for Image (1)**

| Metrics | Proposed Map | Map (2) | Map (3) | Map (4) | Map (5) | Map (6) | Map (7) | Map (8) | Map (9) | Traditional DWT |
|---|---|---|---|---|---|---|---|---|---|---|
| Elapsed Time (Sec) | 0.4131 | 0.6318 | 0.4502 | 0.4185 | 0.4729 | 0.4615 | 0.4585 | 1.7622 | 1.8026 | 0.6744 |
| UACI | -1.2053 | -1.1963 | -1.219 | -1.258 | -1.257 | -1.253 | -1.121 | 26.0381 | 26.0381 | -1.1947 |
| MSE | 1119.6 | 1139.8 | 1142.9 | 1161 | 1152.2 | 1157.1 | 1173.4 | 7029.7 | 7029.7 | 1153.1 |
| PSNR (dB) | 17.6401 | 17.5625 | 17.5506 | 17.4826 | 17.5155 | 17.4971 | 17.4363 | 9.6615 | 9.6615 | 17.5121 |
| R | 0.8263 | 0.8228 | 0.8231 | 0.8207 | 0.8221 | 0.8210 | 0.8186 | 0 | 0 | 0.8206 |

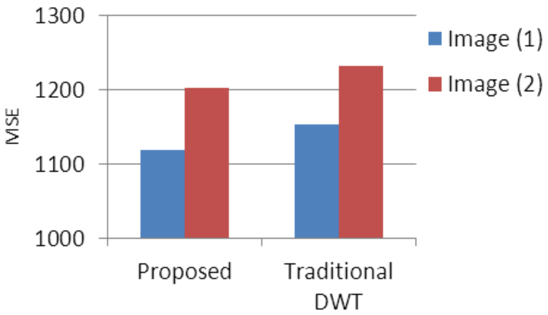


**Fig. 8 MSE for both Traditional and Proposed Techniques**

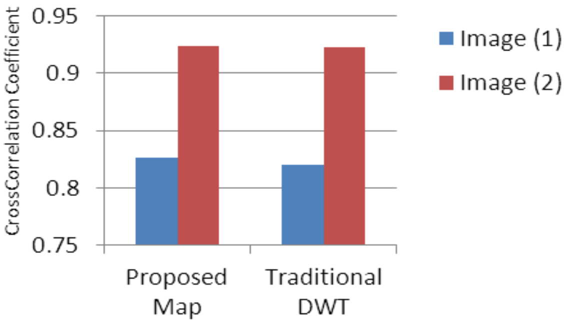
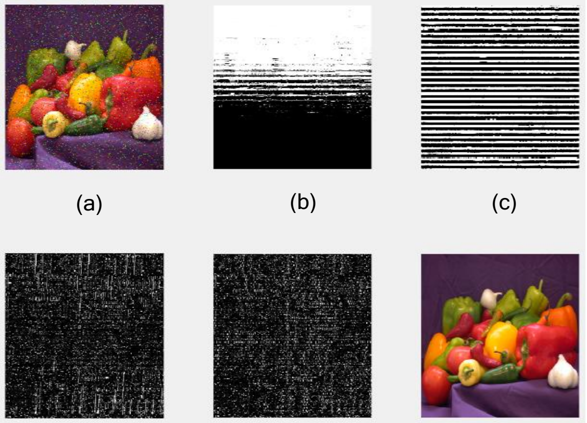


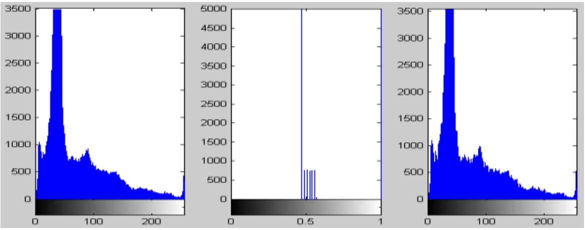
**Fig. 9 Cross Correlation Coefficient for both Traditional and Proposed Techniques**



(a) (b) (c)

(d) (e) (f)

**Fig. 10 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (1) for proposed DWT based technique with our proposed map against salt & pepper noise after using median filter**



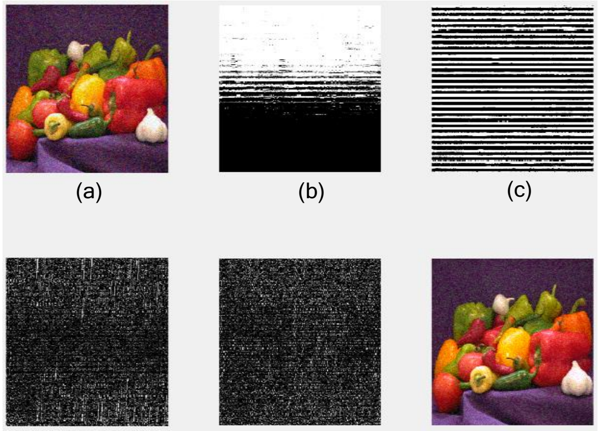
(a) (b) (c)

**Fig. 11 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (1) for proposed DWT based technique with our proposed map against salt & pepper noise after using median filter**

From the previous figures, it is noticed that median filter could be used to approximately get rid of the effect of this type of noise on the decrypted image. Other performance metrics will be listed in the Table 3. It is noticed that from this table that the performance has been enhanced after using median filter. Again we get that our technique with proposed map has given the best performance measurements.

## *C. Gaussian Noise without Using Filter*

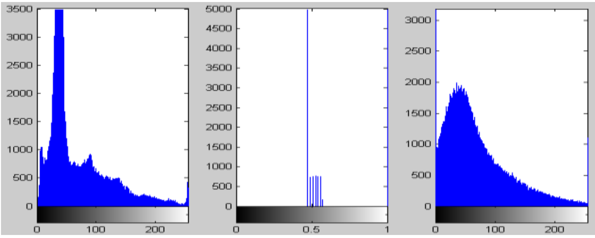
The simulation results for image (1) as an example will be illustrated in this subsection in case of Gaussian noise with mean = 0 and variance = 0.01 without using any type of filters.



(a) (b) (c)

(d) (e (f)

**Fig. 12 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (1) for proposed DWT based technique with our proposed map against Gaussian noise without using filters**

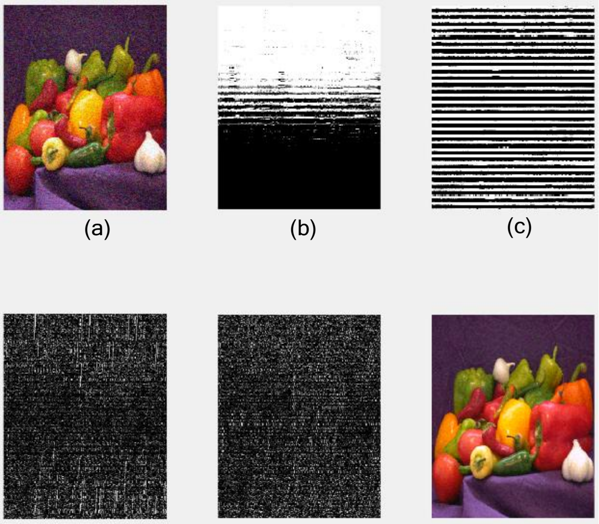


(a) (b) (c)

**Fig. 13 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (1) for proposed DWT based technique with our proposed map against Gaussian noise without using filters**

## *D. Gaussian Noise after Using Filter*

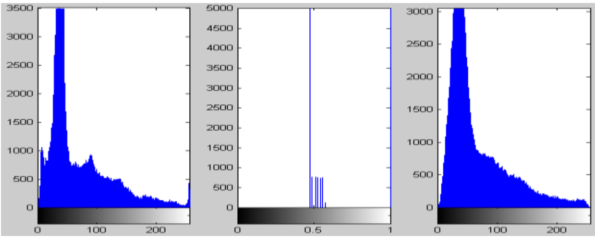
It has been found that the wiener filter is the most suitable one to reduce the effect of Gaussian noise on the decrypted image. The simulation results as well as histogram analysis after using this type of filter for image (1) will be demonstrated in the following figures.



(a) (b) (c)

(d) (e (f)

**Fig. 14 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (1) for proposed DWT based technique with our proposed map against Gaussian noise after using wiener filter**

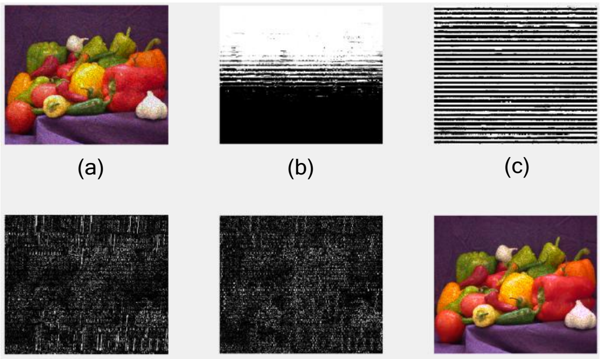


(a) (b) (c)

**Fig. 15 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (1) for proposed DWT based technique with our proposed map against Gaussian noise after using wiener filter**

## *E. Speckle Noise without Using Filter*

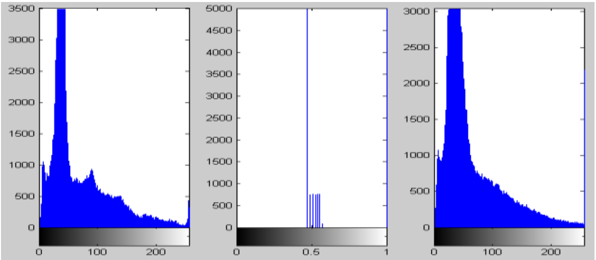
The simulation results and histogram analysis for image (1) will be presented in this subsection in case of speckle noise with mean = 0 and variance = 0.4 without using any type of filters.



(a) (b) (c)

(d) (e (f)

**Fig. 16 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (1) for proposed DWT based technique with our proposed map against speckle noise without using filters**



(a) (b) (c)

**Fig. 17 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (1) for proposed DWT based technique with our proposed map against speckle noise without using filters**

### *F. Speckle Noise after Using Filter*

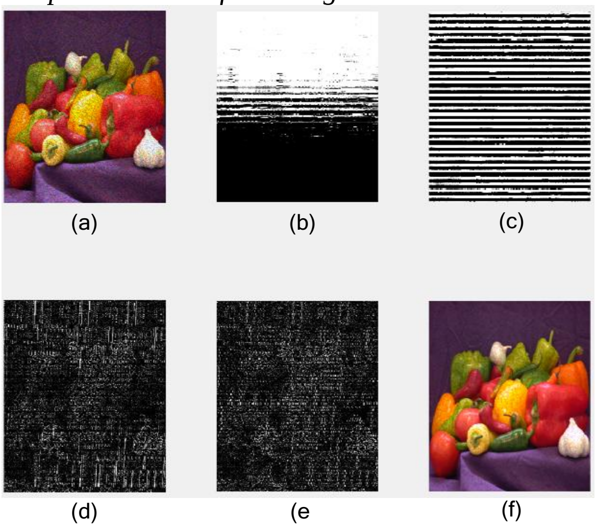


**Fig. 18 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (1) for proposed DWT based technique with our proposed map against speckle noise after using median filter**

The simulation results as well as histogram analysis for image (1) in case of speckle noise after using median filter; which has been found the most suitable type to minimize the effect of this type of noise, will be obtained in this subsection through the Fig. 18 and Fig. 19.

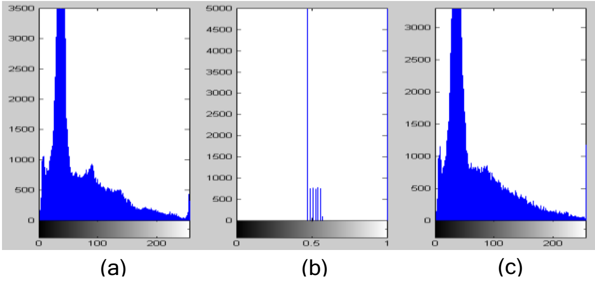


**Fig. 19 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (1) for proposed DWT based technique with our proposed map against speckle noise after using median filter**

From all the previous results we could get that the proposed algorithm with new map gave the best performance either in case of existence or absence of filters.

### *5.3.2 Rotation Attacks*

In this subsection, the simulation results as well as performance metrics for our novel technique will be introduced in case of rotation attack. Rotation by different degrees has been studied and we will choose rotation by 5 degrees as an example. All simulation results as well as performance metrics will be provided for image (2) as an example as follows.

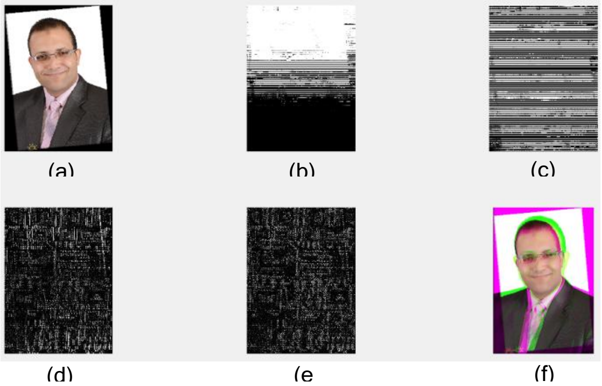


**Fig. 20 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (3) for proposed DWT based technique with our new map against rotation attack by 5 degrees**

Only the elapsed time has been differed in case of rotation attacks for both images using either traditional or proposed technique; hence it will be depicted in the graph in Fig. 22. All other measurements have been the same for both techniques in this case.

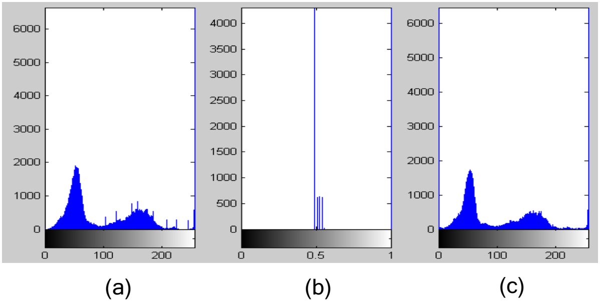


**Fig. 21 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (3) for proposed DWT based technique with our new map against rotation attack by 5 degrees**

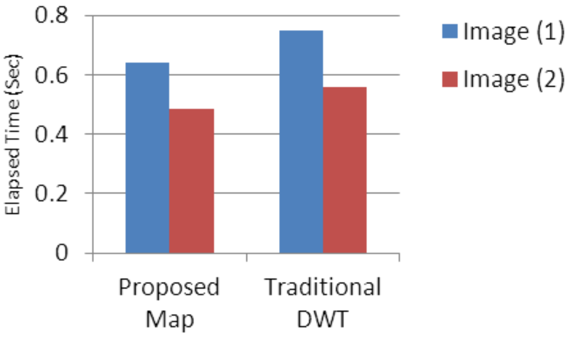


**Fig. 22 the Elapsed Time for both Techniques in case of Rotation Attack with 5 Degrees**

### *5.3.3 Cropping Attacks*

In this subsection, the simulation results as well as performance metrics for our proposed techniques will be depicted in case of cropping attack. The simulation results and histogram analysis for image (2) as an example will be illustrated in the following figures. The original image has been imposed to centralized cropping with block of size 100×100.

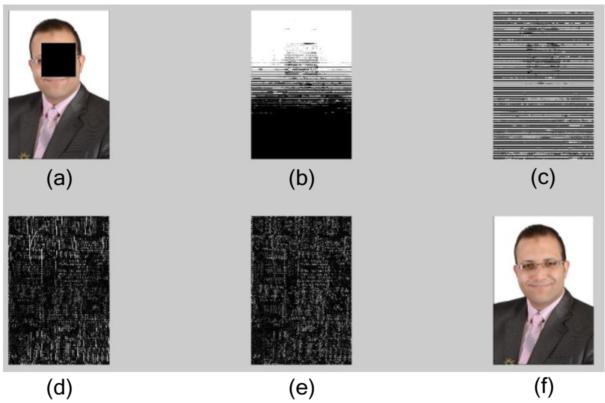


**Fig. 23 The simulation results for; (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted versions of image (3) for proposed DWT based technique with our new map against centralized cropping attack**

As a result of extensive comparative study we could found that CAT and Open-CAT maps based techniques have given the worst performance. Except that all other maps based novel technique as well as traditional one gave the same performance measurements except elapsed time in which our proposed map has given smallest values for that time than traditional scheme as more clearly observed from the next graph in Fig. 25.

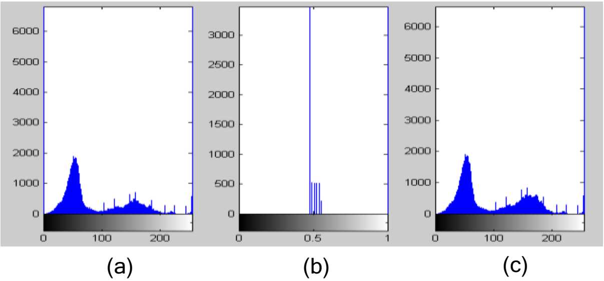


**Fig. 24 The histogram analysis for; (a) original, (b) encrypted, and (c) decrypted versions of image (3) for proposed DWT based technique with our new map against centralized cropping attack**

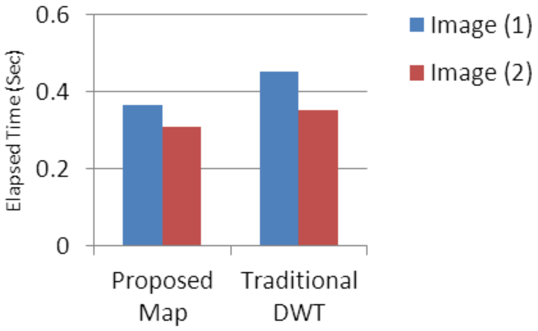


**Fig. 25 the Elapsed Time for both Techniques in case of Cropping Attack**

**Table 3. Performance Metrics in Case of 10 % Salt & Pepper Noise (after Using Median Filter) for Image (1)**

| Metrics | Proposed Map | Map (2) | Map (3) | Map (4) | Map (5) | Map (6) | Map (7) | Map (8) | Map (9) | Traditional DWT |
|---|---|---|---|---|---|---|---|---|---|---|
| Elapsed Time (Sec) | 0.4418 | 0.4342 | 0.4326 | 0.4440 | 0.4275 | 0.4394 | 0.4870 | 1.8105 | 1.8021 | 0.5470 |
| UACI | 0.0365 | 0.0338 | 0.0405 | 0.0441 | 0.0408 | 0.0375 | 0.1474 | 26.0381 | 26.0381 | 0.0428 |
| MSE | 9.7810 | 10.1059 | 9.8753 | 10.3506 | 9.8944 | 10.3858 | 29.1264 | 7029.7 | 7029.7 | 10.5400 |
| PSNR (dB) | 38.2270 | 38.0851 | 38.1853 | 37.9811 | 38.1769 | 37.9664 | 33.4879 | 9.6615 | 9.6615 | 37.9024 |
| R | 0.9981 | 0.9981 | 0.9981 | 0.9980 | 0.9981 | 0.9980 | 0.9945 | 0 | 0 | 0.9980 |

## 6. CONCLUSIONS

For more secure information transmission; encryption has played vital rule for multimedia transmission. Since images represent a very popular and important form of multimedia; optical encryption techniques have become very effective and important due to optical nature of an image. The main challenge of our research was to get robust optical encryption technique against attacks that have been imposed to original image not to encrypted one. Most researches have interested in the effect of attacks on encrypted image which are considered friendly attacks. On the other hand our paper have concerned on those attacks that affected on original image which gave more powerful technique. Nine chaotic maps have been used with our proposed technique; eight of them were predefined and one has been our proposed one. Six performance metrics have been used to measure the performance of our novel technique as well as to compare the performance of our scheme with traditional DWT based one. After extensive comparative study, it has been found that our proposed technique using new map gave the best performance against various types of attacks; noise with different types, rotation by distinct degrees, and cropping attacks. In the future the proposed technique can be applied on optical images instead of digital images.

## 7. REFERENCES

[1] F. Hartung and M. Kutter, “Multimedia Watermarking Techniques," Proceedings of the IEEE, Vol. 87, No. 7, PP. 1079-1107, July 1999.

[2] A. Alfalou, C. Brosseau, " Optical Image Compression and Encryption Methods," Adv. Opt. Photon 1, hal-00516980, PP: 589-636, Sep 2010.

[3] 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, Issue 4, No. 2, PP: 125-129, July 2014.

[4] N. K. Neshchal, T. J. Naughton, "Flexible Optical Encryption with Multiple Users and Multiple Security Levels," ELSEVIER, Optics Communication 284, PP:735-739, 2011.

[5] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 30 (2005) 1644.

[6] G. Situ, G. Pedrini, W. Osten, Appl. Opt. 49 (2010) 457.

[7] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the Design of Perceptual MPEG Video Encryption Algorithms," CoRR abs/cs/0501014, 2005.Encryption Algorithms, CoRR abs/cs/0501014, 2005.

[8] N. F. Elabady, H. M. Abdalkader, M. I. Mousa, and S. F. Sabbeh, "Image Encryption Based on New One Dimensional Chaotic Map," Technical Report.

[9] C. Fu, Z. Zhang and Y. Cao, “An improved image encryption algorithm based on chaotic maps,” Third International Conference on Natural Computation, Vol. 3, Washington, PP. 24-27, 2007.

[10] P. Refregier, and B. Javidi, "Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding," Optics. Letters., Vol. 20, PP: 767-769, 1995.

[11] N. Debbarma, L. Kumari, and J. L. Raheja, "2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 2, Issue 4, PP. 387-392, July-August 2013.

[12] K. Gupta, and S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map," Journal of Information Security, No. 2, PP. 139-150, October 2011.

[13] A. Alfalou, C. Brosseau, " Optical Image Compression and Encryption Methods," Adv. Opt. Photon 1, hal-00516980, PP: 589-636, Sep 2010.

[14] 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, Issue 7, July 2014.

[15] 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," arXiv: 1501. 04167v1 [cs. CR], PP: 1-18, Jan 2015.

[16] Z. Shao, H. Shu, J. Wu, and Z. Dong, "Double Color Image Encryption using Iterative Phase Retrieval Algorithm in Quaternion Gyrator Domain," Optics Express, inserm-00951570, Version 1, Feb 2014.

[17] Q. A. Kester, "Image Encryption based on The RGB Pixel Transposition and Shuffling," I. J. Computer Network and Information Security DOI: 10.5815/ijcnis.2013.07.05, PP: 43-50, 2013.

[18] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, "Color Image Encryption by using Arnold Transform and Color Blend Operation in Discrete Cosine Transform Domains," Optics Communications (248), ELSEVIER, PP. 123-128, 2011.

[19] X. Deng, and X. Zhu, "A Simple and Practical Color Image Encryption with the Help of QR Code," Optica Applicata, Vol. XLV, No. 4, PP. 513- 521, 2015.

[20] 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 (0975 – 8887), Vol. 128, No. 1, PP: 1:14, September 2015.

[21] H. G. Shuster, and W. Just, "Deterministic Chaos an Introduction," WILEY-VCH Verlag GmbH & Co. KGaA, ISBN:3527-40415-5, 2005.

[22] www.Wikipedia.com\List of Chaotic Maps.

[23] R. C. Gonzalez and R. E.Woods, "Digital Image Processing,” Third Edition, 2008.