A Proposed Hybrid Encryption & Watermarking Algorithm for Digital Color Image

M.A. MOHAMED¹, M.I. FATH ALLAH², L.W. ELBON³

¹ The Dean of the Faculty of Engineering, Mansoura University, Mansoura, Egypt
² Assistant Professor at Delta Higher Institute for Engineering & Technology, Mansoura, Egypt
³ Engineer in communication labs of the Faculty of Engineering, Mansoura University, Mansoura, Egypt

Corresponding author: Third Author (e-mail: lobna.elbon1992@hotmail.com).

Abstract— Nowadays, increasing use and distribution of the digital images through multimedia and communication system have been increased. Therefore, the transmitted data can be attacked by unauthorized people. The main considerable challenge in the digital world is maintaining information security. The traditional techniques are unsuitable for the image encryption. Therefore it is necessary to develop the techniques that be able to secure the color images. This paper introduce a hybrid encryption and watermarking for digital color image against the composite attacks. The discrete cosine transform (DCT) and discrete wavelet transform (DWT) transforms have been extensively used in many digital signal processing applications, so DCT and DWT have been applied for image transformation by two methods. Six chaotic maps have been used with different parameters to establish a relation between the data encryption key and watermark. After extensive studies it has been found that the proposed technique has achieved the best performance than that of the traditional ones.

Keywords— Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Inverse Discrete Cosine Transform (IDCT), Inverse Discrete Wavelet Transform (IDWT)

I. INTRODUCTION

Nowadays, the great spreading and growing of data through the multimedia and communication systems is causing several problematic facets against securing the data. Distribution or sharing data become very easy and does not required complex operations. Therefore it is essential to improve the techniques that protected the data from the unauthorized users[1]. Moreover, encryption and watermarking represent powerful techniques in securing the content. Encryption makes the content indecipherable through a reversible mathematical transformation based on a secret key. Watermarking is a technique of embedding data into a multimedia component such as image, audio or video[2]. In this paper Encryption and watermarking techniques will be presented in which the original color image has been multiplied by two chaotic maps of the same type and with different parameters and initial conditions. After that, DWT or DCT has been utilized to get the encrypted image. The argue is getting high robustness against composite attack. That merged three various attacks together; noise, cropping and rotation. The composite attack could be obliged to encrypted image in two different forms which are; friendly form and hard form. Six chaotic maps have been used; (i) Chirikov (ii)Chirikovtan (iii) Henon (iv) Ikeda (v) Logistic and (vi) quadratic. The performance of these scheme maps have been studied with comparative of the traditional ones. The next of this paper is organized as follows; section-2 presents survey and related work, section-3 introduces the proposed techniques, section-4 illustrates the simulation results and discussions, and section-5 demonstrates the conclusions.

II. RELATED WORKS

In 2015 Bennrhouma et al. presented a first virgin of an idea of an semi fragile watermarking and encryption scheme for digital images [3]. In 2016 AlShaikh, Muath, et al. proposed an innovative hybrid encryption watermarking scheme to improve the security and ensure the integrity of medical image content[4]. In 2016 Zear et al. concentrated a novel method for multiple watermarking based on DWT, DCT and SVD has been presented using Back Propagation Neural Network[5]. In 2017 Kang, Xiao-bing, et al. provided a new robust and invisible blind watermarking scheme based on a combination of DCT and SVD in DWT domain has been to improve the imperceptibility and the robustness[6]. In 2018 Loan, Nazir A., et al. reviwed watermark embedding algorithm has been examined for different grayscale and color images[7]. In 2018 Wu, Q. et al. proposed An adaptive and blind audio watermarking algorithm based on chaotic encryption in a hybrid domain to combat various conventional signal-processing attacks[8]. In 2019 Thanki, Rohit M., and Ashish M. Kothari proposed a novel hybrid domain image watermarking technique using watermark speech signal[9]. In 2019 Abdulrahman, Ahmed Khaleel et al. provided an efficient DCT-DWT based hybrid image watermarking method for copyright protection of color images[10]. In 2019 Joshi, M. Tech Scholar Namrata proposed novel computerized water checking strategy dependent on whole number wavelet change with quality based order procedure. For the choice of highlight quality utilized RBF work [11].

III. THE PROPOSED TECHNIQUE

The main steps of the proposed algorithm will be discussed and illustrated in flow charts in figures (1, 2). First, the original image has been multiplied by the first chaotic map followed by the second one with different initial conditions. More variations have been given by chaotic maps to enhance the performance by varying its parameters and initial conditions. In the second step the DWT as well as DCT has been applied to obtain the encrypted image at the
end of encryption process. The last step is embedding the watermark to obtain watermarking encrypted image. Decryption process the inverse of pervious encryption steps that represented in Fig. (1) and Fig. (2). first extract the watermark from the watermarked image. And then inverse Discrete Wavelet Transform (IDWT) or Inverse Discrete Cosine Transform (IDCT) has been applied to the encrypted image. Then it has been divided by second chaotic map after that dividing by the first one. The last step was to get the resulted decrypted color image. The main equations of six chaotic maps; Chirikov, Chirikovtan, Logistic, Quadratic, Henon, Ikeda will be represented in the next subsection in details. [12, 13]

3.1 Chaotic maps

1. Chirikov Map; [13]
   It is a 2D map and represented by the following equations;

   \[ x_{n+1} = x_n - k \sin y_n \]  \hspace{1cm} (1.a)
   \[ y_{n+1} = y_n + x_{n+1} \]  \hspace{1cm} (1.b)

   Where, K represents the external control parameter.

2. Chirikovtan Map; [13]
   It is a 2D map and represented by the following equations;

   \[ x_{n+1} = x_n - k \tan(y_n) \]  \hspace{1cm} (2.a)
   \[ y_{n+1} = y_n + x_{n+1} \]  \hspace{1cm} (2.b)

3. Logistic Map; [13]
   This is a one-dimensional quadratic map defined by the following equation;

   \[ x_{n+1} = K x_n (1 - x_n) \]  \hspace{1cm} (3)

   Where, K represents the external control parameter.

4. Quadratic Map; [13]
   This map is one dimensional and represented by the following equation;

   \[ x_{n+1} = c - x_n^2 \]  \hspace{1cm} (4)

   Where, C is the external parameter.

5. Henon Map; [13]
   This can be considered as a 2D extension of the logistic map and represented by the following equations;

   \[ x_{n+1} = 1 - a x_n^2 + y_n \]  \hspace{1cm} (5.a)
   \[ y_{n+1} = b x_n \]  \hspace{1cm} (5.b)

   Where, a and b represent external control parameters.

6. Ikeda Map; [13]
   Ikeda map is a 2D chaotic map and represented by the following equations;

   \[ x_{n+1} = 1 + m (x_n \cos(t) - y_n \sin(t)) \]  \hspace{1cm} (6.a)
   \[ y_{n+1} = m (x_n \sin(t) + y_n \cos(t)) \]  \hspace{1cm} (6.b)

   Where, m is the external parameter.

IV. RESULTS AND DISCUSSION

This section will demonstrate the image database, the performance metrics, the simulation results and discussions of these results of the proposed techniques against hard as well as friendly composite attacks compared to some traditional ones.

4.1 Images database

Table 1 observes the name, type, extension, size, and entropy of each plain color image. The original images are observed in Fig. (3) and their histograms are detected in Fig. (4).

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Type</th>
<th>Extension</th>
<th>Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peppers</td>
<td>True color</td>
<td>.png</td>
<td>384x384</td>
<td>512</td>
</tr>
<tr>
<td>Rice</td>
<td>True color</td>
<td>.png</td>
<td>256x256</td>
<td>256</td>
</tr>
</tbody>
</table>

Fig. 3 The Image (a) Original Image (1), (b) watermark Image (2)

Fig. 4 Image Histogram for; (a) Original Image (1), (b) watermark Image (2)
Fig. 1 Flow chart of DWT based proposed technique

Fig. 2 Flow chart of DCT based proposed technique
4.2 Performance Metrics:

Eight performance metrics have been used to test the performance of the proposed technique and make a comparison with the traditional ones; elapsed time, entropy analysis, mean square error (MSE), Peak Signal-to-Noise Ratio (PSNR), cross correlation coefficient between original and decrypted images (R), histogram analysis, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI).[14, 15]

4.2.1 Elapsed Time

Elapsed time can be defined as the total calculation time for encryption as well as decryption processes in second for all experiments.[14]

4.2.2 Entropy Analysis

The entropy could be defined as in Eq. (7):

$$H(m) = -\sum_{i=0}^{n-1} p(m_i) \log_2(p(m_i))$$

(7)

Where, p(mi) is the probability of symbol mi, and N represents the number of bits for each symbol.[14]

4.2.3 Mean Square Error (MSE)

The Mean Square Error between the original and decrypted images could be computed as in Eq. (9):

$$MSE = \frac{1}{MNf} \sum_{l=1}^{M} \sum_{i=1}^{N} (O_I(i,j,k) - D_I(i,j,k))^2$$

(8)

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.[14]

4.2.4 Peak 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. (8):

$$PSNR = 10 \log_{10} \left( \frac{max_{oi}}{MSE} \right) \text{ dB}$$

(9)

Where, maxoi represents the maximum possible pixel value of the original image.[14]

4.2.5 Cross Correlation Coefficient (R)

The cross correlation between the original and decrypted images can be defined as in Eq. (10):

$$R = \frac{\sum_{m=0}^{M} \sum_{n=0}^{N} (O_{m,n} - O_{m,n}) (D_{m,n} - D_{m,n})}{\sqrt{\sum_{m=0}^{M} \sum_{n=0}^{N} (O_{m,n} - O_{m,n})^2 \sum_{m=0}^{M} \sum_{n=0}^{N} (D_{m,n} - D_{m,n})^2}}$$

(10)

Where, m is the row number, n is the column number, OI is the mean value of the pixels of original image, and DI is the mean value of the pixels of decrypted image.[14]

4.2.6 Histogram Analysis

The histogram analysis shows the distribution of the pixel values in encrypted and decrypted images. To obtain an effective encryption technique, the histogram of the decrypted image must be close to that of the original one. The main equation of the histogram of an image is obtained in Eq. (11):

$$P_n = \frac{\text{Number of pixel with intensity } n}{\text{Total number of pixels}}, \quad n = 0, 1, \ldots, L - 1$$

(11)

Where (f) is a given image represented as a matrix of size r by c 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.[14]

4.2.7 Number of Pixels Change Rate (NPCR)

NPCR measures the percentage of different pixel numbers between the two images and is defined as

$$NPCR = \frac{\frac{1}{M \times N \times f} \sum_{k=1}^{M} \sum_{l=1}^{N} \sum_{j=1}^{f} |O_I(i,j,k) - D_I(i,j,k)| \times 100\%}{128}$$

(12)

Where, M is the number of rows, N is the number of columns, f is the number of image frames.

The practical value for 1-NPCR should be about 0.99[15]

4.2.8 Unified Average Changing Intensity (UACI)

UACI measures the average intensity of differences between the two images and is defined as

$$UACI = \frac{\frac{1}{M \times N \times f} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{f} |O_I(i,j,k) - D_I(i,j,k)|}{2^{l-1}} \times 100\%$$

(13)

Where, M is the number of rows, N is the number of columns, f is the number of image frames. The practical value for UACI should be 0.33.[15]

4.3 Simulation Results & Discussions

In this section the proposed hybrid encryption and watermarking technique will be discussed on a personal computer with the following qualifications; (i) Intel corei5-8250U CPU @ 1.60GHz 1.08GHz; (ii) 8 GB RAM; (iii) SATA hard disk 1TB.

The simulation results as well as performance metrics measurements will be illustrated. The performance of each technique has been measured against friendly as well as hard composite attacks.

4.3.1 Friendly Attacks

Friendly composite attacks means that the composite type of attacks has been imposed to the encrypted image whose uniform histogram distribution. In this section the simulation results as well as the performance metrics measurements will be explained.

The chaotic maps and their parameters have been as follows; (1) Chirikov map with K=0.9 for two random keys, (2) Chirikovtan map with K=0.9 for both random keys, (3) Logistic map with k=4 for both random keys, and (4) Quadratic map with c=1.95 for both random keys, (5) Hénon map with a=1.4 and b=0.3 for both random keys, (6) Ikeda map with m=0.9 for both random keys.

![Simulation Results](image-url)

**Fig. 5** The Simulation Results for; (a) Original, (b) Encrypted, and (c) Decrypted Versions of Image (1) for DCT Based Technique with Logistic Map against Friendly Composite Attack in Case of Gaussian Noise
From figures 5-8 it has been found that the proposed technique have been given more uniform distribution histogram for encrypted images in case of Logistic Map although the original image has been affected by encryption and watermarking algorithm, therefore it must be recommended to use Logistic Map against Friendly composite attack in case of Gaussian noise. To obtain more accurate and specific judgment when comparing DCT and DWT based techniques against composite attacks it has been found that the DWT based technique method has given better results in MSE, elapsed time, PSNR, R, NPCR and UACI in case of using Logistic chaotic map against friendly composite attacks with Gaussian noise. All performance metrics for all these techniques will be listed in charts.

While all these results have been shown by Gaussian noise, the research also applied to include different and various type of noise such as; salt & pepper and Speckle. It have been founded from these measurements that the proposed algorithms have given best performance against composite attack.

Fig. 6 The Histogram Analysis for; (a) Original, (b) Encrypted Versions of Image (1) for DCT Based Technique with Logistic map against Friendly Attack in Case of Gaussian Noise

Fig. 7 The Simulation Results for; (a) Original, (b) LL Component, (c) LH Component, (c) HL Component, (d) HH Component of Encrypted, and (d) Decrypted Versions of Image (1) for DWT Based Technique with Logistic Map against Friendly Composite Attack in Case of Gaussian Noise

Fig. 8 The Histogram Analysis for; (a) Original, (b) Encrypted Versions of Image (1) for DWT Based Technique with Logistic map against Friendly Composite Attack in Case of Gaussian Noise

Fig. 9 the Elapsed time and Cross Correlation Coefficient measurements for DCT based technique

Fig. 10 PSNR, NPCR, UACI, Entropy measurements of original image for DCT based technique.

Fig. 11 Mean Square Error measurements for DCT based technique.
From these measurements that demonstrated in Figures from (9–11) it has been found that the Logistic Map has given the minimum elapsed time for DCT based technique, the maximum cross correlation coefficient between original and decrypted images in case of Quadratic Map, Chirikov Map has given the largest PSNR and least MSE. 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.

The Figures from (12–14) that illustrated the performance metrics measurements for DWT based technique it has been found that Ikeda Map has given the minimum elapsed time, Logistic Map has been given maximum cross correlation coefficient between original and decrypted images, Ikeda Map has been given the largest PSNR and least MSE. 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.

After a general examination, it is clearly found that the DCT as well as DWT based techniques have given best performance measurements against composite attack over the traditional one stated in reference [13]. It has been found that there were enhancement ratios in most performance metrics values when using these techniques. DCT based approach in case of Logistic Map has given about 73.9% enhancement in cross correlation coefficient (R), 55% improvement in MSE, 56.6% enhancement in PSNR, about 16.65% improvement in UACI, and about 42.5% enhancement in Elapsed time. On the other hand, DWT based technique in case of Logistic Map has achieved about 89.42% enhancement in cross correlation coefficient (R), 32.57% improvement in MSE, 21.6% enhancement in PSNR, 338% improvement in UACI, and about 23.35% enhancement in Elapsed time.

4.3.2 Hard Attacks
In this section hard attacks will be illustrated where the composite form of attacks imposed to the original image. The simulation results as well as performance metrics will be demonstrated.

![Fig.12 the Elapsed time and Cross Correlation Coefficient measurements for DWT based technique](image)

![Fig.13 PSNR, NPCR, UACI, Entropy measurements of original image for DCT based technique](image)

![Fig.14 Mean Square Error measurements for DWT based technique](image)

![Fig. 15 The Simulation Results for; (a) Original, (b) Encrypted, and (c) Decrypted Versions of Image (1) for DCT Based Technique with Quadratic Map against Hard Composite Attack in Case of Gaussian Noise](image)
From figures 15-18 it has been found that the proposed technique have been given more uniform distribution histogram for encrypted images with Quadratic Map in case of DCT based technique against Hard composite attack but in case of DWT technique the Henon Map has been presented more uniform distribution histogram for encrypted images, so it has been advised to use Quadratic Map against Hard composite attack in case of Gaussian noise for DCT based technique and Henon map for DWT based technique. Also in case of Hard composite attack when comparing DCT and DWT based techniques against composite attacks it has been found that the DWT based technique method has provided better results in MSE, elapsed time, PSNR, R, NPCR and UACI in case of using Logistic chaotic map against friendly composite attacks with Gaussian noise. All performance metrics for all these techniques will be listed in charts.

From performance metrics measurements that presented through Figures (19 -21) for DCT based technique it has been found that the Logistic Map has been given least MSE, the largest PSNR, the maximum cross correlation coefficient between original and decrypted images, and the least value for UACI, except the elapsed time Ikeda map has been given the minimum Elapsed time. 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.
Also in case of Hard attack, after a general analysis, it is visibly found that the proposed techniques have given higher performance measurements against composite attack over the traditional one stated in reference [13]. It has been found that there were enhancement ratios in most performance metrics values when using these techniques. DCT based approach in case of Quadratic Map has given about 81.94% enhancement in cross correlation coefficient (R), 55.9% improvement in MSE, 57.92% enhancement in PSNR, about 8.166% improvement in UACI, and about 30.29% enhancement in Elapsed time. On the other hand, DWT based technique in case of Henon Map has achieved these enhancement ratios as follows: 92.62% in (R), 33.35% in MSE, 22.61% in PSNR, 359.23% in UACI, and 12.76% in Elapsed time.

V. CONCLUSION

This paper proposes a hybrid encryption-watermarking technique for digital color image. The watermarking phase is based on DWT that has been applied for image transformation in one method and DCT has been applied in the other one, while the encryption phase is based on using six chaotic maps of different dimensions and also based on DCT in one method and DWT in other one. The proposed encryption algorithm showed better performance than traditional ones with respect to the security level and the encryption speed. It also showed better performance as compared with some of the most recent existing techniques.

Finally, experimental results proved that the proposed hybrid encryption-watermarking technique achieved high security performance against composite-severe attacks and it also achieved high degree of imperceptibility and robustness.

VI. REFERENCES


1Mohamed Abdel-Azim Mohamed received the Ph.D. degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the electronics & communications engineering department, then awarded the associate professor degree in 2012 until now. He has 91 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and field programmable gate array (FPGA) applications. I had awarded the best Ph.D. thesis at Mansoura University at 2006. He is the Dean of Faculty of Engineering in Mansoura University. 

E-mail: mazim12@yahoo.com

2M. I. Fath Allah was born in Mansoura, Dakahlia, Egypt in 1985. He received the B.S. degree in Electronics & Communications Engineering from the Faculty of Engineering-Mansoura University, Mansoura, Egypt, in 2007, M. S. degree in optical communications (Implementation of Optical OFDM System using FPGA) from the Faculty of Engineering-Mansoura University, Mansoura, Egypt, in 2012, and the Ph.D. degree in optical encryption of images (Development of Optical Encryption Techniques) from the Faculty of Engineering-Mansoura University, Mansoura, Egypt, in 2017. From 2007 to 2010, he was a demonstrator in Communications & Electronics Department at the Faculty of Engineering-Mansoura University, Mansoura, Egypt. From 2010 to 2012, he works as an Assistant Lecturer in Communications & Electronics Department at Delta Higher Institute for Engineering & Technology, Mansoura, Egypt. Since 2017 till now, he has been an Assistant Professor in Communications & Electronics Department at Delta Higher Institute for Engineering & Technology, Mansoura, Egypt. He has 12 publications in various international journals and conferences. His current research interests include multimedia processing, encryption, wireless communication systems, and Field Programmable Gate Array (FPGA) applications.

E-mail: mismail1885@yahoo.com

3Lobna Wael Elbon (corresponding author) was born in Mansoura, Dakahlia, Egypt in 1992. She graduated from faculty of engineer in 2014. She worked in communication labs of the Faculty of Engineering as an engineer in 2016. My current research interests are in image processing, Encryption, Watermarking and Steganography.

E-mail: lobna.elbon1992@hotmail.com