Received: 25 January 2024 | *Revised:* 4 April 2024 | *Accepted:* 23 May 2024
DOI: 10.37917/ijeee.22.1.17 *Vol. 22 | Issue 1 | June 2026*

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access
IJEEE University of Basrah College of Engineering

Securing Image Transmission Over AWGN Channels Using OFDM Techniques and Hybrid Chaotic Based Cryptography

Hussein Y. Radhi*[1], Ali J. Abboud[1], Sura F. Yousif[2]
[1]Department of Computer Engineering, College of Engineering, University of Diyala, Diyala 00964, Iraq
[2]Department of Chemical Engineering, College of Engineering, University of Diyala, Diyala 00964, Iraq

Correspondance
*Ali J. Abboud
Department of Computer Engineering, College of Engineering,
University of Diyala, Diyala 00964, Iraq
Email: ali.j.abboud@gmail.com

Abstract
The security of communications in various transmitted information's forms such as video, audio, image, and even text and preserving them from attackers has become of great importance in the age of the Internet and cellular networks. Perhaps one of the most important media used to transmit information is digital images. They are distinguished from video and audio by their lack of complexity, and at the same time they are distinguished from text by the possibility of containing more information. Due to the necessity of transmitting huge amounts of information via digital images through additive white Gaussian noise (AWGN) channels for various applications. This transmission of images over unsecured channels is vulnerable to many attacks that must be protected by information security tools. In this research, a hybrid chaos-based system was developed to encrypt and secure images and send them via an orthogonal frequency division multiplexing (OFDM) channel, which leads to transferring large amounts of transmitted information in a short time, with very little interference between the data, and maintaining the transfer rate. Two chaotic techniques, Rossler and Modified Chau system, are used together to create a secret encryption key. This combination of chaotic systems provides highly random sensitive keys with amplitude of 10^{252} that are difficult to predict by the attacker and which makes restoring the original image very difficult in the event of a very small change in the chaotic parameters. Many tests were conducted to determine the strength of the proposed system, including statistical and differential analysis and entropy to verify the strength of the image security approach, in addition to applying some types of attacks to the encrypted image, such as noise and cropping different parts of the image. It is clear that the proposed scheme has strong immunity to these attacks. This was proven by the comparative experimental results. The entropy ratio was very excellent compared to the rest of the results obtained in the rest of the research. This was also the case with the values of (NPCR), (UACI), (NPCR), and Mean Square Error (MSE) was also very good as compared with other researches in the literature. The proposed security approach for OFDM gave a low link and a low bit error rate. And a higher signal-to-noise ratio (PSNR).

Keywords
Cryptography, Chau System, Rossler System, OFDM, AWGN.

I. Introduction

With the great developments in the various means of communication systems in the world and the availability of the Internet widely, it is become necessary to look for ways to protect the information that is transmitted through the available communication channels. This information may have

different forms like text, image, audio or video that necessitate not to be changed by third parties especially military and financial sensitive information. Thus, it needs a high degree of security whenever transmitted from the sender to the recipient [1–4]. Cryptography is crucial technique to achieve the aim of cybersecurity. In the literature, there are plethora of methods proposed by the researchers to secure digital images using different cryptographic algorithms. Basically, images represent one the most used multimedia signals transmitted over communications networks especially for the medical and military applications [5, 6]. Many known cryptographic algorithms are used to protect images such as (DES) data encryption standard, (AES) advanced encryption standard, (RSA) rivest – shamir – adleman, etc. These algorithms differ in the way of using cryptographic keys and their security strength. However, by combining these algorithms together with chaos-based systems will produce strong image security [7]. Chaos systems are unpredictable behavior and responsive to the initially conditions. Hence, each modification in the parameters of chaotic system will change shape of the system characteristics. These systems are used in many applications such as, geology, mathematics, microbiology, biology and encryption, etc. It recently utilized heavily in the field of multimedia security because of their strength in encrypting text, image, audio, and video [8–10]. Images have unique characteristics that distinguish them, which makes them very important in information security applications, whether in civil or military communications. the main characteristic that distinguishes images from text is their large size, and thus the attacker needs a longer time to decrypt them. Since image encryption depends on changing the pixel values and their location, this make the encrypted image is not hackable by the attacker and therefore it is difficult to access the information easily [9]. Chaos based system is used in cryptography to generating the cryptographic key for encryption and decryption processes. This key may be a symmetrical shared secret key or an asymmetric private and public key for public key cryptographic algorithms. The stronger the key, the safer and stronger encryption and cannot be easily broken. The chaos has the ability to generate key space that reaches 10^{90} or 10^{270}, which makes Chaos based systems are very important for cryptography [11, 12]. The Chaotic system is characterized by complex chaos and, at the same time, dynamism, extreme sensitivity to initial conditions, nonlinearity, and no periodicity, and thus it is difficult to predict or control the behavior of these systems. this makes it very important in various fields of information security, and it has other unique characteristics, such as its high ability to withstand external attacks of various kinds, which is very important in image encryption [12]. chaotic system is used in several forms and ways to encrypt data. It depends on the ability to generate large numbers of a random nature that have the ability to be used as a key that is very difficult to know. It is used to encrypt data by changing the values and locations of pixels by converting a single bit cycle or relying on two-dimensional chaos maps, spreading the pixels in a new and chaotic way to obtain high resistance to attacks when transmitted over the Internet, in the case of decryption, the same sequence of random numbers is relied upon [8]. More than one system may be combined to make the general behavior more chaotic and thus retrieving it is very difficult, as it makes a large and random change in the locations of the pixels and is very sensitive to the initial conditions, so that any slight deviation in the initial conditions leads to a large change in the sequence, which makes chaotic systems highly triangular and suitable for encryption [9, 10]. In order to improve many important factors in the cryptography process as compared with others we used a hybrid chaotic system, and noticed from the results that the histogram of Image, and correlation of adjacent pixels are clearly enhanced, beside that the Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI) values became better than other researches, also the values of entropy, mean square error, key space and key sensitivity, Chi-Square Analysis. The hybrid system provides a combination of more than one encryption systems in building a very strong and secure system which has high efficiency, great speed in encryption, and the ability to generate very large encryption keys compared to regular systems, which makes hacking and knowing them very much more difficult, and it has the ability to be applied in a safe and effective manner. It is also possible to increase the strength of encryption by using more than one type of chaos system to generating one or more encryption key(s) that needed by image security system. To obtain perfect transmission in addition to the perfect security, it is possible to use OFDM technology to increase PSNR (peak signal to noise ratio) and decrease BER (bit error rate) [13]. There is a rich literature on digital image security [14–16]. OFDM significantly reduces (BER) and increases (PSNR) in addition to the possibility of transferring large amounts of data on the same channel and has nothing to do with information security, and information security in this research depends on the hybrid system that was built in the research. The term ((AWGN) contains three basic parts: being additive, which means that the signal received by the receiver consists of two parts, which are the original signal in addition to the statistically independent noise signal, being white, which means that the spectral power density is flat in shape, which makes the correlation of the parts of the noise signal in a field of time is zero for all time shifts except zero, and finally the sampling distribution for this signal is a Gaussian distribution [15, 16]. The carrier medium that transmits the signal and which adds this type of noise is called (AWGN) channel and the signal coming out

of it is a mixture of the transmitted data in addition to the noise [14].

II. Related Works

The image security is affected by major elements. They are proposed and discussed in [17]. It is shown that image scrabbling has strong confusion and regarded as best way to ensure of image security and privacy during communication and saving. In addition, 4 dissimilar keys are used in deciphering operation and moving pixels using XOR in several closed loops. The result of this research is done by regarding entropy and connection coefficients, with few changes in entropy. Such a rapid method to secure transferring digital signals via Internet is presented in [18]. This solution has used RSA to produce key pair for enciphering and deciphering. The key of enciphering is enciphered using RSA. This key is used by RSA as input to the convolutional neural network to produce 6-dimensional chaotic chains. A wheel-switch chaotic system is proposed in [19] to enciphering the image. A confusion and diffusion network are used by this approach to provide high security for digital images. Furthermore, an effective method to secure images has been developed using a group of chaotic sequences. It is made of three main process which are diffusion, shuffling and confusion. Likewise, a novel security technique to encipher the image is suggested [20]. It is an easy in programming to obtain the digital data for image security enhance storage capacity and speed. On other hand, two parameters performance of OFDM are calculated which are BER and PSNR and effect of their change on the transmitted images through OFDM channel are investigated [21]. Eventually, the value of SNR is calculated over modified OFDM which consist of two closed together symbols with the same construction [22]. Based on the limitations of above works, a hybrid cryptography algorithm is developed in this paper using the 3-dimensional Rossler and modified Chua chaotic cryptography schemes to transmit the resulted image using OFDM technique. The article is structured along these lines: section 2 is used to describe related works and section 3 introduces developed approach and section 4 is dedicated for experimental results and analysis and section 5 is committed to explain the robustness of suggested approach in opposition to the attacks and ultimately section 6 is summarizing the conclusions. In this research is of great importance in providing a security system for transferring images from the sender to the recipient through the user's hybrid encryption system, which is very difficult to penetrate by attackers. In addition, sending images via (AWGN) OFDM channel has a very major role in sending data significantly and improving the signal power ratio. To the noise power ratio, which is considered one of the very important factors in communications systems.

III. Proposed Works

A hybrid cryptography method is designed in this research to secure images transmitted in the AWGN channels. It can process both grayscale and color images as shown in Fig. 1 while Fig. 2. shows the flowchart of the proposed work in details. The encryption process is performed by two chaotic systems, Rossler and modified Chau chaotic schemes. They are employed together to create a strong secret key. These systems have following differential equations [23].

1- Encryption Part

a) Rossler Chaotic System

$$\begin{aligned} \dot{x}_R &= -y - x \\ \dot{y}_R &= x + ay \\ \dot{z}_R &= b + z(x - c) \end{aligned} \tag{1}$$

b) Modified Chau System

$$\begin{aligned} \dot{x}_C &= \alpha(y - h) \\ \dot{y}_C &= x - y + z \\ \dot{z}_C &= -\beta z \end{aligned} \tag{2}$$

Where (a, b, c, α, β) are a control parameter while $h = -b\sin(\frac{-\pi x}{2a} + d)$

to optimize the chaotic system, the following functions can be used,

$$\begin{aligned} x(i) &= \text{floor}(x(i) \times 100m) \\ y(i) &= \text{floor}(y(i) \times 100m) \\ z(i) &= \text{floor}(z(i) \times 100m) \end{aligned} \tag{3}$$

random sequence is generated by above equations is leveraged in the enciphering and deciphering operations while chaotic (3) represents the rounded down function. To obtain a mixed key from the equations of Rossler system, the X-OR gate is used as shown in (4) to obtain a new random key to make the image encryption more rigged and secret [23].

$$\begin{aligned} x &= \text{bitxor}(x_C, y_R) \\ y &= \text{bitxor}(y_C, z_R) \\ z &= \text{bitxor}(z_C, x_R) \end{aligned} \tag{4}$$

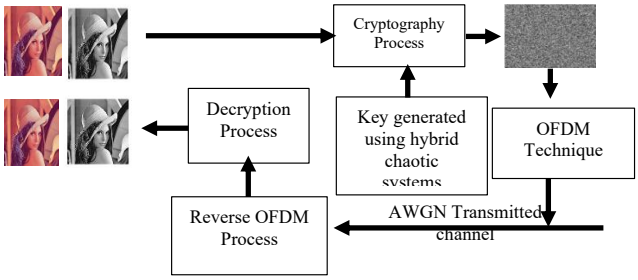


Fig. 1. Framework of proposed method

Now, the pixel's locations in the image are changed, then following keys are used to obtain the final key to be used to perform the substitution operation [23]. The keys schedule process as shown below:

$$\begin{aligned} x &= \text{bitxor}(x_C, y_R) \\ y &= \text{bitxor}(y_C, z_R) \\ z &= \text{bitxor}(z_C, x_R) \end{aligned} \tag{5}$$

2- OFDM Process

The data of the encrypted image is divided using OFDM technology in order to be ready for transmission through AWGN channels. At the recipient side, all operations are executed by the same key to restore the original image. The information of the enciphered digital images is converted into a complex series of numbers with multiple levels by using several signal transforms. They include (IFFT) inverse fast Fourier transform, (DCT) discrete cosine transforms, and (DWT) discrete Wavelet transform. The equation of the signal after applying IFFT is given by [21, 22].

$$x(i) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x(k) e^{-\frac{i\omega ik}{T_s}}, \quad 0 \le i \le N-1 \tag{6}$$

Note that N is count of subcarriers, and x(k) is Kth modulated symbol. DCT technique is used to reduce the inter symbol interference ISI because it compresses the spectral energy well, which composes majority of the samples near zero, and there is another important advantage as compared to FFT, which is to perform the real calculation instead of the complex calculations performed by the FFT, which reduces the complexity of signal processing [21, 22]. FFT transforms is a fast arithmetic transformation from the time domain to the frequency domain and is a very efficient algorithm. Likewise,

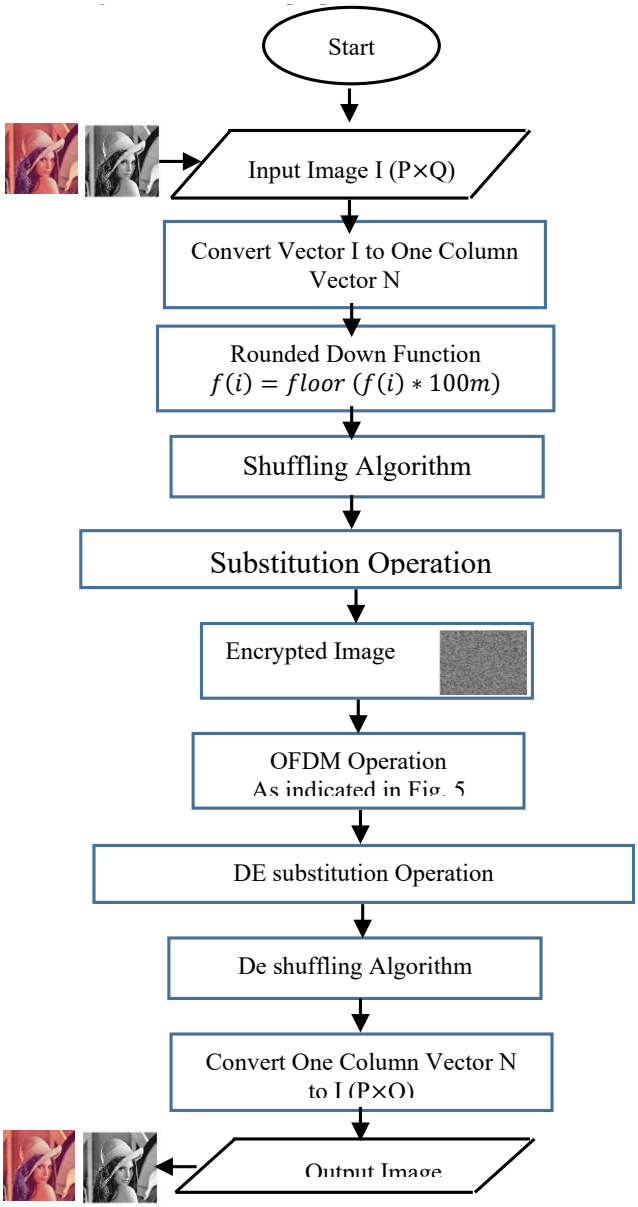


Fig. 2. Flowchart of proposed work

the discrete cosine transform (DCT) is a technique for converting the signal into a primary frequency component which expresses a highly multiplexed sequence data points in terms of the sum of cosine functions, it is more efficient in concentrating energy to less. The ordering coefficients are more than what DFT does for image data [24]. These conversions provide appropriate compression for images before sending them, and thus a well-encrypted and compressed image is obtained without losing any part of the main image features [25]. The transmitted signal using this technique is given by [23].

$$x(i)=\frac{\sqrt{2}}{N}\sum_{k=0}^{N-1}x(k)\beta(k)\cos\left(\frac{2k(2i+1)}{2N}\right),\quad i=0,\ldots,N-1 \tag{7}$$

Where $\beta(k)$ is given by [6]:

$$\beta(k)=\begin{cases}\frac{1}{\sqrt{2}} & \text{if } k=0\\ 1 & \text{if } k=1,2,\ldots,N-1\end{cases} \tag{8}$$

DWT is considered one of the most common tools in most signal processing applications in communication systems, which can be considered equivalent to a package of filters, whose number is usually reduced to the maximum extent possible, hence the count of output filters is similar to the count of input filters [23], The equation of transmitted signal using DWT is given by [26].

$$x(i)=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}x(k)\phi(t-kT) \tag{9}$$

Note that $\phi(t)$ represents the wavelet basis function. Fig. 3 views the chart of developed system. Bit error rate (BER) is one the most important measures to test the performance of OFDM system. It represents the error ratio between the transmitted and received bits [21, 23]. Mean square error (MSE) is an important measure to quantify the goodness of restoring or reconstructing the image at recipient side cite24. Whenever the value of MSE is high, the image restoration at receiver side resulted bad quality image [24, 27]. In contrast, the low value of MSE metric represents reconstructing high-quality image at the other end. (PSNR) Peak signal-to-noise ratio is the ratio between the maximum amount of the image pixels and MSE as shown in (10) [25, 27].

$$\text{PSNR}=10\log_{10}\left(\frac{\text{MAX}}{\text{MSE}}\right) \quad (10) \tag{10}$$

IV. Experimental Results and Analysis

Numerous experiments were done to test the strength of the developed hybrid cryptography method. The results are obtained using MATLAB 2021b for Lena, Cameraman, peppers, and Barbara images. Fig. 4 below shows an example for the enciphering and deciphering processes for the developed approach.

The following proof investigations are directed to check the strength and security of the suggested method against several known attacks as follows:

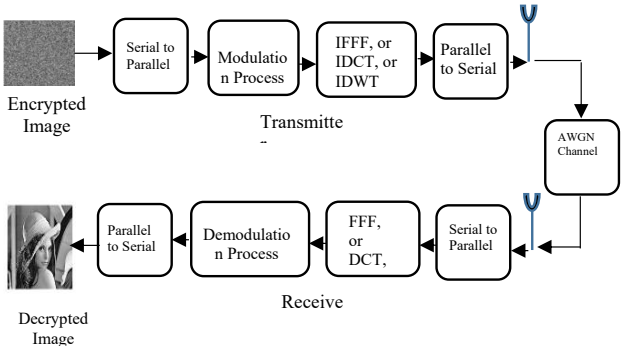


Fig. 3. OFDM crypto system

Fig. 4. Example of encryption and decryption processes

1. Statistical Analysis

This analysis consists of important tests which are:

1.1 Histogram of Image

The image histogram represents the pixel's distribution within image. It supposed to be nearly uniform to protect image from mathematical attacks [26]. Fig. 5 shows the histogram for proposed gray scale images in this work for the original and encrypted images. It is obvious from the results that the histogram of encrypted images is uniformly distributed. Hence, this testing proves that our approach is secure and rigged against such kind of attacks.

Fig. 6f displays the histogram of color images of RGB channels. The histograms of color channels are uniformly distributed and these results insert another evidence about capability our proposed approach to confront statically attacks against color images.

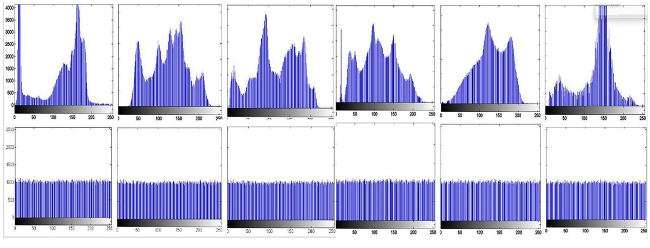
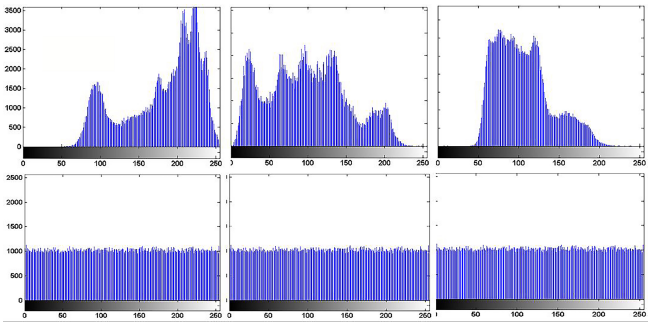
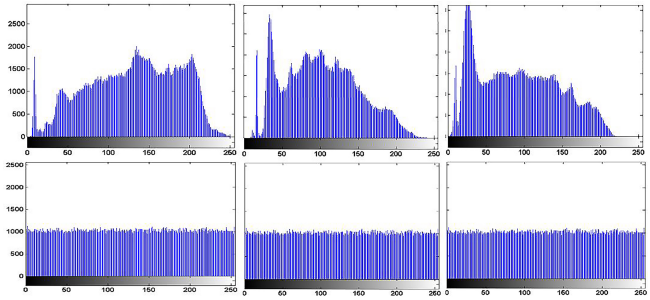


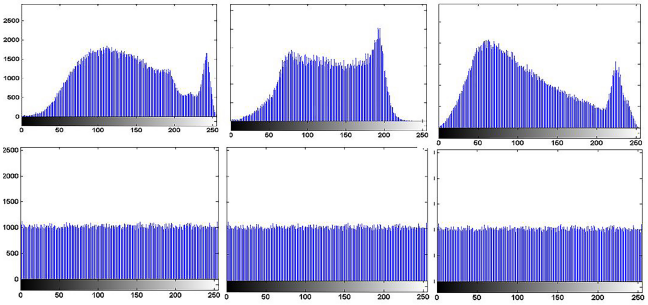
Fig. 5. Histogram of original and encrypted gray-scale images



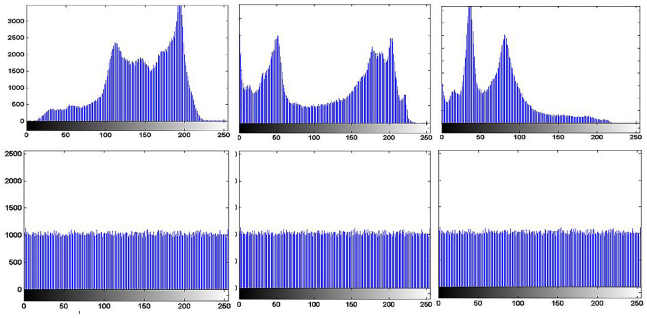
(a) Enciphered Lena image



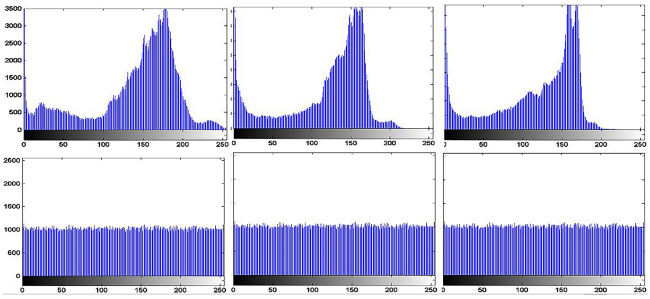
(b) Enciphered Barbara image



(c) Enciphered Baboon image



(d) Enciphered Peppers image



(e) Enciphered Bout image

(f) Color channels Histograms

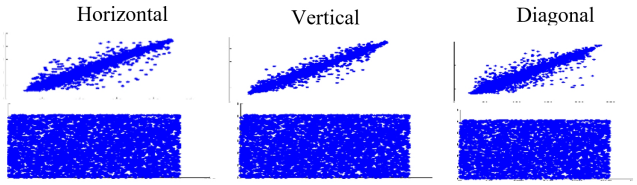


Fig. 7. Correlation of initial and enciphered gray scale Lena image.

1.2. Correlation of Adjacent Pixels

The correlation among neighboring pixels represents the link among near pixels in diagonal, horizontal and vertical directions. It is known that this correlation is too large for adjacent pixels and small for far pixels. Hence, when encoding an image in a certain encryption algorithm, this correlation between adjacent pixels should be minimized as much as possible [28,29]. The correlation between any two pixels is given in (11) [29–31].

$$C_{ab} = \frac{|\mathrm{cov}(a,b)|}{\sqrt{D(a)} \times \sqrt{D(b)}} \tag{11}$$

Where (a and b) are the values of two neighbor's pixels, while convolution (.,.) and D(.) are computed, as follows:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - \bar{x})^2 \tag{13}$$

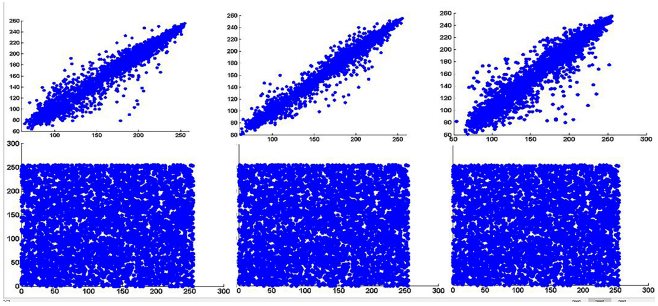
$$\mathrm{cov}(a,b) = \frac{1}{N}\sum_{i=1}^{N} (a_i - \bar{a})(b_i - \bar{b}) \tag{14}$$

Fig. 7 and Fig. 8 show the correlation of gray scale and color Lena images respectively.

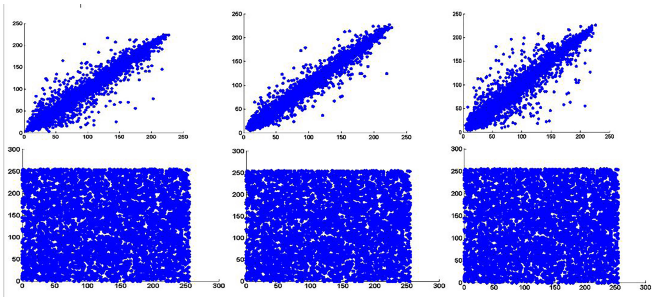
Table I presents the correlation among plain and enciphered grayscale images while Tables II, III, and IV are used to show the correlation among plain and enciphered color images in three directions (i.e., H, V and D).

2. Differential Analysis

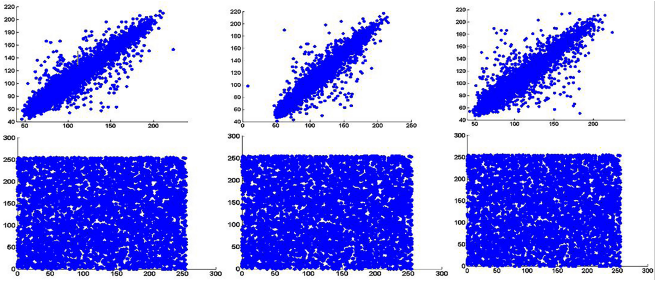
Differential analysis consists of two parameters:



(a) Correlation of original and encrypted color Lena original image (Green channel) in the H, V, D



(b) Correlation of original and encrypted color Lena original image (Green channel) in the H, V, D directions



(c) Correlation of original and encrypted color Lena original image (Blue channel) in the H, V, D

Fig. 8. Correlation of plain and enciphered color Lena image

2.1. Number of Pixel Change Rate (NPCR)

NPCR means the portion of modification in the pixels of the encrypted image in event of any change in pixels of the plain image [32]. It is an important tool for measuring the quality and strength of encryption as shown in (15) [33–35].

$$\mathrm{cov}(a,b) = \frac{1}{N}\sum_{i=1}^{N}(a_i-\bar{a})(b_i-\bar{b}) \tag{15}$$

Where W is the image width and H is the image height and D (i, j) is the difference between two images

$$D(i,j) = \begin{cases} 1 & \text{if } E_1(i,j) \neq E_2(i,j) \\ 0 & \text{if } E_1(i,j) = E_2(i,j) \end{cases} \tag{16}$$

E1 is the original image encoding of the and E2 is the encoding of the original image after change in one pixel.

2.2. Unified Average Changing Intensity (UACI)

This testing represents the mean difference among the original and the enciphered images [29]. It can be calculated as given in 17) [36–38].

$$\mathrm{UACI} = \frac{1}{H\times W}\left[\sum_{i,j}\frac{|E_1(i,j)-E_2(i,j)|}{255}\right]\times 100\% \tag{17}$$

Table V displays the scores of NPCR and UACI metrics on grayscale image compared with references [26, 28, 39], Tables VI and VII below present the scores of NPCR and UACI analyses for color images and Lena image compared with references [31, 38, 40] respectively Note that outcomes pertaining to the schemes are compared with those derived from the same study.

The data in these tables confirm that the developed approach is secure and the encryption operation is rigid against the differential attack.

3. Entropy Analysis

Entropy is defined as a mathematical measure of randomness. It is employed to distinguish the internal texture of images and to calculate the confusion of encrypted images [39]. The entropy is defined as in (18) [40]:

$$\sum_{i=0}^{2^{n-1}} P_i \log_2(P_i) \tag{18}$$

P is the pixel's values probability. Tables VIII and IX show the results of entropy values for grayscale and color images compared with references [26, 28, 40], and [31, 37, 38, 41] respectively. The results in these tables are near to the standard value (8), which demonstrates that the encrypted image is random enough and secure and robustness against information entropy attacks.

4. Mean Square Error (MSE)

Mean square error is the dissimilarity among the pixels of the plain image and the pixels of enciphered image [31]. It is an essential metric to specify the quality of the processed images. The various image processing operations including

TABLE I.
CORRELATION COEFFICIENT SCORES OF THE GRAYSCALE IMAGES

Image	H		V		D	
	Plain	Enciphered	Plain	Enciphered	Plain	Enciphered
Barbara	0.9161	0.000616	0.9682	-0.000895	0.8968	0.003200
Baboon	0.8665	-0.001000	0.7588	-0.000621	0.7262	-0.003300
Boat	0.9381	0.000371	0.9713	0.001800	0.9222	-0.000152
Lena	0.9719	-0.002100	0.9850	-0.000436	0.9593	-0.000639
Peppers	0.9728	0.000821	0.9709	-0.001100	0.9471	-0.001400

TABLE II.
CORRELATION COEFFICIENT SCORES OF THE RED COLOR CHANNEL

Image	H		V		D	
	Original(R)	Encrypted(R)	Original(R)	Encrypted(R)	Original(R)	Encrypted(R)
Barbara	0.9264	0.000918	0.9699	-0.000854	0.9080	0.001700
Baboon	0.9231	-0.00150	0.8660	-0.000935	0.8543	0.000242
Boat	0.9624	0.000262	0.9706	0.000735	0.9348	0.000504
Lena	0.9798	0.002700	0.9893	-0.002000	0.9697	-0.000309
Peppers	0.9620	0.000342	0.9572	-0.000956	0.9230	-0.003600

TABLE III.
CORRELATION COEFFICIENT SCORES OF GREEN COLOR CHANNEL

Image	H		V		D	
	Original(G)	Enciphered(G)	Original(G)	Enciphered(G)	Original(G)	Enciphered(G)
Barbara	0.9160	0.001600	0.9685	-0.001700	0.8968	0.001800
Baboon	0.8654	-0.002200	0.7650	-0.001900	0.7348	-0.001700
Boat	0.9620	0.000854	0.9704	0.000293	0.9345	0.001100
Lena	0.9689	0.001200	0.9824	-0.001400	0.9554	0.000908
Peppers	0.9840	0.000510	0.9815	0.001500	0.9676	0.001900

TABLE IV.
CORRELATION COEFFICIENT SCORES OF BLUE COLOR CHANNEL

Image	H		V		D	
	Original(B)	Enciphered(B)	Original(B)	Enciphered(B)	Original(B)	Enciphered(B)
Barbara	0.9297	0.000791	0.9723	-0.000696	0.9118	0.002600
Baboon	0.9072	-0.000950	0.8808	0.000332	0.8398	0.001400
Boat	0.9651	0.000734	0.9734	0.000048	0.9407	0.001200
Lena	0.9325	-0.001100	0.9574	-0.000472	0.9181	-0.000867
Peppers	0.9644	0.002500	0.9699	0.000450	0.9400	-0.001100

TABLE V.
NPCR AND UACI FOR GRAYSCALE IMAGES

Methods	Images	Proposed Work	
		NPCR	UACI
Proposed Work	Camera	0.9967	0.3359
	Man	0.9968	0.3358
	Peppers	0.9968	0.3337
	Barbara	0.9968	0.3338
	Baboon	0.9964	0.3331
	Boat	0.9969	0.3355
[26]	Camera	0.9961	0.3356
	Man	0.9968	0.3357
	Peppers	0.9966	0.3337
	Barbara	0.9963	0.3344
	Baboon	0.9961	0.3329
[28]	Camera	0.9961	0.3341
	Man	0.9961	0.3354
	Peppers	0.9963	0.3348
	Barbara	0.9962	0.3346
	Baboon	0.9961	0.3340
[39]	Camera	0.9961	0.3349
	Man	0.9961	0.3341
	Peppers	0.9963	0.3348
	Barbara	0.9961	0.3343
	Baboon	0.9961	0.3352

TABLE VI.
NPCR AND UACI FOR COLOR IMAGES

Methods	NPCR	UACI
Lena	0.9967	0.3359
Peppers	0.9966	0.3386
Barbara	0.9963	0.3367
Baboon	0.9965	0.3387
Boat	0.9964	0.3372
Sail Boat	0.9962	0.3376

TABLE VII.
NPCR AND UACI FOR COLOR IMAGES

Methods	NPCR	UACI
Proposed Work	0.9967000	0.3359000
[31]	0.996287	0.303432
[38]	0.9959000	0.3097000
[40]	0.9961937	0.3344153

TABLE VIII.
ENTROPY OF GRAYSCALE

Images	**Entropy Values**
Proposed Work	
Camera Man	7.998400
Lena	7.999000
Peppers	7.999800
Barbara	7.999800
Baboon	7.998800
Boat	7.998700
[27]	
Camera Man	7.997300
Lena	7.997100
Peppers	7.997000
Barbara	7.997800
Baboon	7.997100
[28]	
Camera Man	7.997400
Lena	7.997300
Peppers	7.997000
Barbara	7.997800
Baboon	7.997600
[40]	
Camera Man	7.997400
Lena	7.997300
Baboon	7.996900

encryption, steganography techniques, or any other changing that images may be exposed to [42]. MSE can be calculated from the following mathematical relationship [28, 31].

$$\mathrm{MSE} = \frac{1}{PQ}\sum_{i=1}^{P}\sum_{j=1}^{Q}\left[f(i,j)-\hat{f}(i,j)\right]^2 \tag{19}$$

Note that Q, P are the image height and width respectively. f (i, j), and $\hat{f}(i,j)$ are the pixel values of a plain image and enciphered image respectively. Tables X, XI and XII shows PSNR, MSE and Correlation values before and after the attacks for the Lena image. The results in these tables refers to the goodness of our developed. Table XIII shows MSE values of gray scale images as compared with other algorithms.

5. KEY SPACE AND KEY SENSITIVITY ANALYSES

Key space is stated as the total number generated keys for crypto system [28, 43]. In this research our key capacity for the developed approach is $(10^{18})^{14} = 10^{252}$, which considered very secret in comparison with other related researches as

TABLE IX.
ENTROPY OF COLOR IMAGES

Images	Entropy Values
Proposed Work	
Lena	7.999400
Peppers	7.999500
Barbara	7.999200
Baboon	7.999300
Boat	7.999300
[38]	
Lena	7.998700
Peppers	7.998700
Barbara	7.998700
Baboon	7.997600
[41]	
Lena	7.994100
Peppers	7.994000
Baboon	7.997600
[31]	
Lena	7.994100
Peppers	7.994000
[37]	
Lena	7.991600

shown in Table 13. In contrast, the key awareness means that any modification in the secret key makes the original image difficult to recover [25,31]. From the programing analysis perspective, it is found that any change in the value of Rossler and Chau parameters at the receiver side by (0.000000000000001) will lead to impossibility of recovering the plain image as displayed in Fig. 9. Perhaps one of the very important factors in the encryption process is the key used in the encryption and decryption process. The larger the area of the encryption key, the more difficult it becomes to break it, which represents a set of keys that can be generated and is more complex and difficult to break and detect by attackers [44].

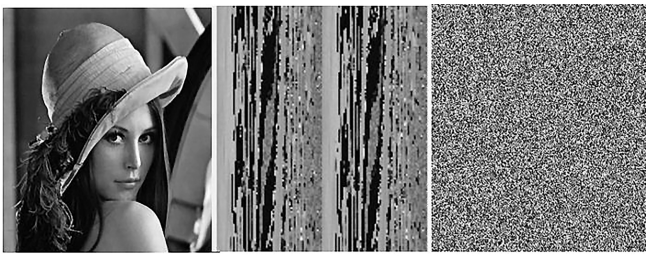


Fig. 9. Kev sensetivity

6. CHI-SQUARE ANALYSIS

It is considered one of the most important tests to know the ability of the developed scheme to resist mathematical attacks [40] [32]. Chi-Square represents the analysis of the pixel dispersion for encrypted image graph. As the lower score of this metric, it will lead to greater consistent and coherent enciphered image [28]. The following equation is used to find the chi-square [25]:

$$x^2 = \frac{\sum_{j=1}^{256} \left((p_j - p)^2\right)}{p} \tag{20}$$

p_j is the observed value of pixel numbers and p being the expected scores of the encrypted images? Table XIV shows different scores of this analysis for the grayscale and colour images which indicates the strength of developed system in preventing threats. This factor is very important because it reveals the difference between the two categorical distributions from each other, where the result is zero for no two identical distributions, and then the difference in the distributions begins. Therefore, it is considered very important for testing samples in search of randomness [32].

7. FDM ANALYSIS

In this research, the image is sent through the ADWGN OFDM channel and then the PSNR value is calculated with and without OFDM for Binary Phase Shift Keying (BPSK), Quadrature phase-shift keying (QPSK), 8 PSK, and 16 PSK as displayed in Table XV. To test the strength of the developed work, the PSNR is calculated for various values of energy to noise ratio (E_b/N_o), where E_b is the bit energy, N_o represents noise energy as shown Table XV. The results in Table XVI is compared with research studies in references [23] and [44], Table XVII illustrate the values of FFT, DCT, and DWT for cameraman image where $E_b/N_o = 10dB$, 1 by 1 antennas. OFDM is one of the important techniques for sending multiple waves carrying the signal through the same channel in parallel and it is studied and analyzed by calculating (BER) in addition to (PSNR) after sending it through the (AWGN) channel, which is very important for studying the behavior of the proposed system, which has proven a decrease in Ratios (BER) In addition to increasing the ratio of (PSNR) which plays a major role in studying the behavior of (OFDM) , through studying it the quality of the received images is known, as the value of (PSNR) is calculated for the received demodulation image and the original image, the results indicate obtaining high values for (PSNR) This confirms the quality of the proposed system [13, 22]. The results in the Tables XV, XVI and XVII above demonstrates that our proposed method is robust against noise due to its low noise ratio

TABLE X.
CROPPING ATTACK FOR COLOR AND GRAY LENA IMAGES

Proposed Image	Correlation Values, MSE, and PSNR of Lena Color Image			PSNR, MSE and Correlation values for gray scale Lena Image		
	MSE	PSNR (dB)	CC	MSE	PSNR (dB)	CC
Cropping 12.5 %	1356.48	16.3915	0.6987	8695.3	15.0785	0.5877
25 % in the top left part	4656.71	11.2801	0.5631	3547.9	12.6311	0.5785
25 % in the bottom right part	4495.82	11.3482	0.5672	3466.9	12.7314	0.5877

TABLE XI.
SPECKLE NOISE ATTACK FOR COLOR AND GRAY LENA IMAGES

Noise Density	Correlation Values, MSE, and PSNR of Lena Color Image			PSNR, MSE and Correlation values for gray scale Lena Image		
	MSE	PSNR (dB)	CC	MSE	PSNR (dB)	CC
0.1	2078.23	12.8721	0.6382	2559.7	14.0488	0.6970
0.2	3717.81	10.1782	0.5987	3238.8	13.0270	0.6262
0.3	4037.39	8.8901	0.5013	3831.0	12.2977	0.5670

in comparison with other related works in case chaos system is exist or not.

V. ROBUSTNESS AGAINST ATTACKS

It is very important to know the strength of the proposed system and the extent of its resistance to attacks carried out by the attacker. There are types of attacks that encrypted media are exposed to, including mathematical attacks carried

out by the attacker against certain types of encryption systems, including (RSA), which includes a number of types Integer Factoring Attacks, Wiener's Attack, Low Public Exponent Attacks, ...etcetera and there are another types of attacks that can be applied to the proposed system [19]. In the following subsections will explain the powerfulness of developed method in combating different kinds of attacks as follows:

1. CROPPING ATTACKS

Cropping attack is a crucial attack on image security systems. It is necessary to test the opposition of the developed scheme this attack and show its effects on the deciphered image if the enciphered image is cropped [41]. Three different cropping locations are used for the encrypted images and then the test is done to check if we can recover the original image or not. The results illustrate that the image is recovered with minimal quality problems in the decrypted image. Eventually these facts mean that the developed hybrid approach is strong in respect to this attack as shown in Fig. 10 and Fig. 11.

Noise is another important attack on the image security systems. There are various types of noise but in this research will explore two kinds of them as explained below:

2. SALT AND PEPPER NOISE ATTACK

This type of noise causes troubles to image and the security system must be tested to prove its resistance against such

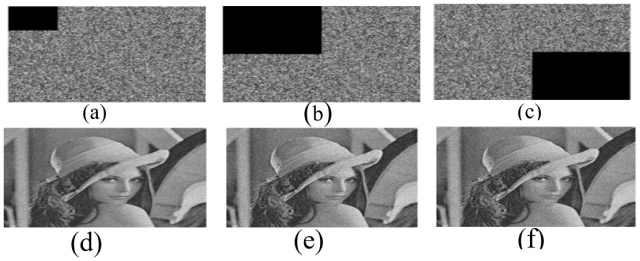


Fig. 10. Cropping results of attack on encrypted image, (a) Encrypted image cropped by 12.5 %, (b) Encrypted image cropped by 25 % in the left top part, (c) Enciphered image cropped by 25 % in the bottom right part, (d) Deciphered image of (a), (e) Deciphered image of (b), (f) Deciphered image of (c).

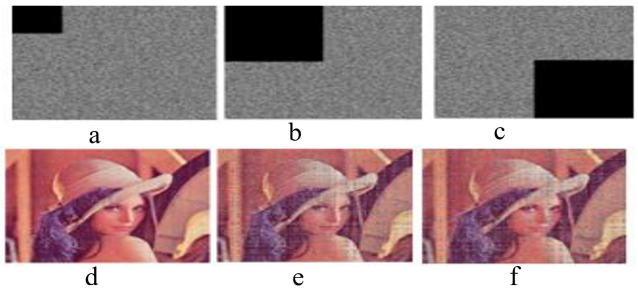


Fig. 11. Cropping attack results on encrypted image, (a) Encrypted image cropped by 12.5 %, (b) Enciphered image cropped by 25 % in the top left part, (c) Enciphered image cropped by 25 % in the bottom right part, (d) Deciphered image of (a), (e) Deciphered image of (b), (f) Deciphered image of (c).

TABLE XII.
SPECKLE NOISE ATTACK FOR COLOR AND GRAY SCALE LENA IMAGES

Noise Density	Correlation Values, MSE, and PSNR of Lena Color Image			PSNR, MSE and Correlation values for gray scale Lena Image		
	MSE	PSNR (dB)	CC	MSE	PSNR (dB)	CC
0.1	2078.23	12.8721	0.6382	2559.7	14.0488	0.6970
0.2	3717.81	10.1782	0.5987	3238.8	13.0270	0.6262
0.3	4037.39	8.8901	0.5013	3831.0	12.2977	0.5670

TABLE XIII.
MSE VALUES

Images	**MSE**
Camera Man	9488.3000
Lena	7968.8000
Peppers	8464.5000
Barbara	8378.8000
Baboon	7234.0000
Boat	8641.2000
[27]	
Camera Man	16178.0000
Lena	8972.0000
Peppers	11967.0000
Baboon	21725.0000
[40]	
Camera Man	9489.7000
Barbara	17997.0000
Baboon	21694.0000
[32]	
Lena	9072.7000
Peppers	8199.6000
Baboon	7188.3000

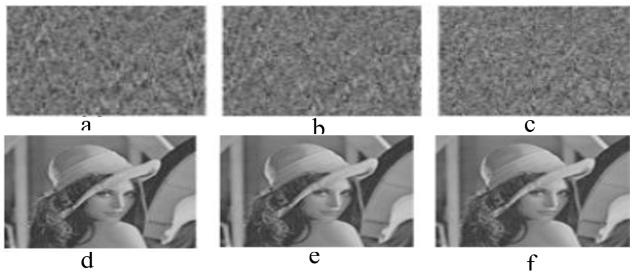


Fig. 12. Salt and pepper noise attack results on encrypted image, (a) (b) Enciphered noisy image with noise density 0.2, (c) Enciphered noisy image with noise density 0.3, (d) Deciphered image of (a), (e) Deciphered image of (b), (f) Deciphered image of (c).

type of noise. Fig.12 shows that the effect of this noise on encrypted gray scale image while Fig.13 displays the influence of this attack for color image

3. SPECKLE NOISE ATTACK

This type of noise has an adverse effect on the image quality. It is a strong noise that can be applied on the enciphered images with different various ratios as displayed in Fig. 14 and Fig. 15 for grayscale and color images respectively.

Tables XVIII, 19 and 20 shows PSNR, MSE and Correlation values before and after the attacks for the Lena image. The results in these tables refers to the goodness of our developed scheme in resisting this kind of attacks.

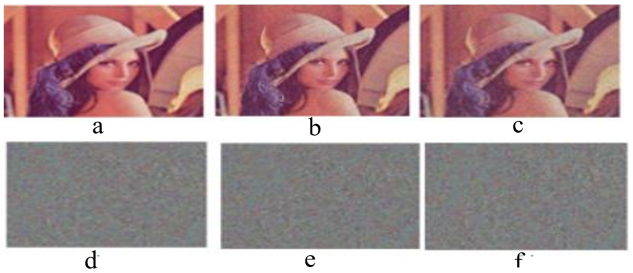


Fig. 13. Noise attack of salt and pepper results on enciphered image, (a) Enciphered noisy image with noise density 0.1, (b) Enciphered noisy image with noise density 0.2, (c) Enciphered noisy image with noise density 0.3, (d) Deciphered image of (a), (e) Deciphered image of (b), (f) Deciphered image of (c).

VI. TIME EXECUTION ANALYSIS

Execution time is one of important factors to consider in evaluating the efficiency of the proposed hybrid cryptography

TABLE XIV.
KEY SPACE VALUES COMPARISON

Encryption Method	Proposed work	[25]	[28]	[29]	[32]	[33]	[36]	[38]	[39]	[40]	[42]	[43]
Key space	10^{252}	10^{152}	10^{150}	10^{144}	10^{75}	10^{120}	10^{70}	$2^{256} \approx 10^{77}$	$2^{430} \approx 10^{129}$	10^{240}	$2^{186} \approx 10^{56}$	10^{98}

TABLE XV.
CHI-SQUARE ANALYSIS

Image	Proposed Work	[28]	[40]	Proposed Work	[18]	[25]	[41]
Lena	240.1484	254.42	246.7578	247.2103	241.0026	253.1934	269.6766
Peppers	223.1484	256.00	-	236.0231	238.2259	241.2647	287.0703
Barbara	220.9531	-	221.0859	228.7325	230.1341	-	-
Baboon	236.0117	-	245.8906	240.3961	235.2350	247.3672	-
Boat	240.0176	-	-	244.5602	-	-	-
Cameraman	243.9863	255.34	240.8906	-	-	-	-

TABLE XVI.
PSNR FOR ADWGN OFDM

SNR at BER=	PSNR (dB)			
	BPSK	QPSK	8 PSK	16 PSK
0 dB	9.5568	9.8817	9.1233	10.6981
5 dB	11.3448	11.6712	10.5924	11.8031
10 dB	15.0112	15.5401	13.0134	17.0235
15 dB	22.6912	23.9001	16.5601	22.1827

TABLE XVII.
PSNR VALUES FOR DIFFERENT E_b/N_o VALUES FOR PROPOSED SYSTEM

System Configuration	PSNR (dB)		
	FFT	DCT	DWT
Proposed Work with Chaotic System	53.8975	30.6882	33.1047
[23] with Chaotic System	53.8881	30.3995	32.7138
[44] without Chaotic System	13.0074	17.4532	-

TABLE XVIII.
PSNR VALUES FOR $\frac{E_b}{N_0} = 10dB$, FOR CAMERAMAN IMAGE BASED ON OFDM

Chaos system with OFDM	$\frac{E_b}{N_0} = 0dB$	$\frac{E_b}{N_0} = 5dB$	$\frac{E_b}{N_0} = 10dB$
FFT	18.8560	30.1982	53.9812
DCT	16.6201	23.0635	30.5116
DWT	16.4875	23.9286	32.8831

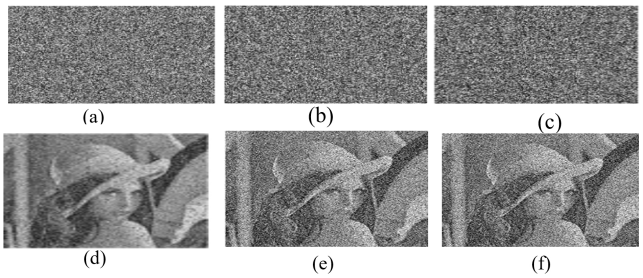


Fig. 14. Speckle noise attack results on encrypted image, (a) Enciphered noisy image with noise density 0.1, (b) Enciphered noisy image with noise density 0.2, (c) Enciphered noisy image with noise density 0.3, (d) Deciphered image of (a), (e) Deciphered image of (b), (f) Deciphered image of (c).

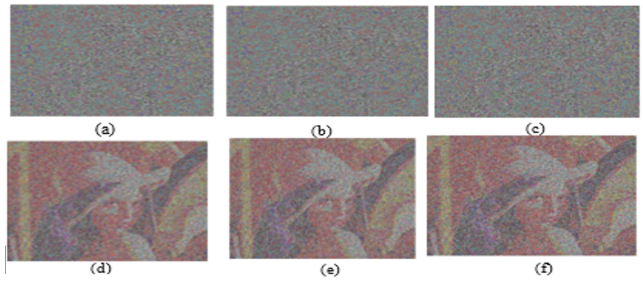


Fig. 15. Speckle noise attack results on encrypted image, (a) Enciphered noisy image with noise density 0.1, (b) Enciphered noisy image with noise density 0.2, (c) Enciphered noisy image with noise density 0.3, (d) Deciphered image of (a), (e) Deciphered image of (b), (f) Deciphered image of (c).

TABLE XIX.
EXECUTION TIME IN SECONDS FOR LENA IMAGE (256*256)

Gray scale Image			
Algorithm	**Proposed Work**	**[23]**	**[45]**
Enciphering Time	1.016710	2.44	-
Deciphering Time	1.230457	2.95	-
Total Execution Time	1.956879	5.39	2.792
Color Image			
Algorithm	**Proposed Work**	**[29]**	**[31]**
Enciphering Time	1.409543	-	2.582389
Deciphering Time	1.230457	-	3.149124
Total Execution Time	2.635887	2.750966	5.731513

system. Its importance is not less than other evaluation criteria including accuracy, complexity, cost, and others. It is sure that the less execution time, the less the complexity of the proposed system is, hence, the cost is as low as possible [37] [44] [45]. The proposed system was accomplished using the Core i5, intel memory is 8.00 GB, 1035G1. Table XIX shows the execution time of the developed method in comparison with other related state of art approaches. It is evident that our method surpasses other compared methods by having the least execution time among them. It is sure that the less execution time the less the complexity of the proposed system is, and therefore the cost is as low as possible [33] [45] [46].

Table XIX shows the importance of quickly completing the processes of encryption, decryption, sending and receiving the signal using the (OFDM) via (AWGN) channel technology, as all researchers seek to reduce the time required for this through the use of accurate algorithms and programs with functions that are quick to execute, accurate, and short at the same time to save the time needed to complete them. The proposed system, which showed a noticeable improvement in the execution times of the encryption and decryption process well compared to previous works. The characteristics of the first computer ref [27] are Intel Core (i3) CPU 1.9 GHz, 4 GB RAM, and the properties of second computer ref [29] is 3.4 GHz Intel R Core TM i7, 8 GB and the properties of the third one [31] are 2.9 GHz Intel® Core TM i9, 32 GB while the final one [45] properties are 3.4 GHz Intel Core i5-3570 CPU and 4.0 GB RAM, the proposed system was accomplished using the Core i5, intel memory is 8.00 GB, 1035G1. Table XIX gives the implementing time as compared with other algorithms. From the results obtained and comparison with previous results, it becomes clear how quickly the algorithms proposed in the system can be completed. Although there are some minor differences in the characteristics of each computer's installation, the results are considered good compared to the rest of the research.

VII. CONCLUSION

A hybrid cryptography approach is proposed in this paper. OFDM technique is used to reduce the interference and the selective bias that may occur in normal transmission. Such interference might happen because the division of the total channel into narrow signals. The simulation results prove that it is hard to restore the plain image by the cryptanalyst since the key sensitivity of the proposed approach is very high. Furthermore, any tiny modification in the key causes a large modification in the deciphered image hence this will result in the attacker's failure to recover original image. To sum up, it is evident that the proposed approach can be used to transfer securely images over AWGN channels.

CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

REFERENCES

[1] M. Haque, S. Ahmad, A. Abboud, M. Hossain, K. Kumar, S. Haque, D. Sonal, M. Rahman, and S. Marisennayya, "6g wireless communication networks: Challenges and potential solution," *International Journal of Business Data Communications and Networking (IJBDCN)*, vol. 19, no. 1, pp. 1–27, 2024.

[2] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust image hashing with ring partition and invariant vector distance," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 200–214, 2015.

[3] A. Abboud, A. Albu-Rghaif, and A. Jassim, "Balancing compression and encryption of satellite imagery," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3568–3586, 2018.

[4] A. Abboud and S. Jassim, "Incremental fusion of partial biometric information," in *Proceedings of Mobile Mul-*

timedia/Image Processing, Security, and Applications, vol. 8406, pp. 169–177, 2012.

[5] A. Abboud and S. Jassim, "Biometric templates selection and update using quality measures," in *Proceedings of Mobile Multimedia/Image Processing, Security, and Applications*, vol. 8406, pp. 74–82, 2012.

[6] C. Singar, J. Bharti, and R. Pateriya, "Image encryption based on cell shuffling and scanning techniques," in *Proceedings of 2017 International Conference on Recent Innovations in Signal Processing and Embedded Systems (RISE)*, pp. 257–263, 2017.

[7] A. Abboud and S. Jassim, "Image quality guided approach for adaptive modelling of biometric intra-class variations," in *Proceedings of Mobile Multimedia/Image Processing, Security, and Applications*, vol. 7708, pp. 189–198, 2010.

[8] M. Salim, A. Abboud, and R. Yildirim, "A visual cryptography-based watermarking approach for the detection and localization of image forgery," *Electronics*, vol. 11, no. 1, p. 136, 2022.

[9] Y. Wu, J. Noonan, and S. Agaian, "A wheel-switch chaotic system for image encryption," in *Proceedings of 2011 International Conference on System Science and Engineering*, pp. 23–27, 2011.

[10] M. Mishra and S. Pandit, "Image encryption technique based on chaotic system and hash function," in *Proceedings of IEEE International Conference on Computer Communication and Systems (ICCCS14)*, pp. 63–67, 2014.

[11] Q. Zhang, W. Li, and Q. Ding, "Discrete design of lorenz chaotic system based on euler method and image encryption," in *Proceedings of Third International Conference on Robot, Vision and Signal Processing (RVSP)*, pp. 176–179, 2015.

[12] P. Chaturvedi and D. Jain, "A hybrid rsa and rc6 based secure image cryptography to minimize entropy and enhance correlation," in *Proceedings of 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 32–37, 2016.

[13] H. Farsi and J. Farid, "Video transmission using new adaptive modulation and coding scheme in ofdm based cognitive radio," *Journal of Communications*, vol. 1, no. 4, pp. 239–249, 2013.

[14] S. Yousif, A. Abboud, and H. Radhi, "Robust image encryption with scanning technology, the el-gamal algorithm and chaos theory," *IEEE Access*, vol. 8, pp. 155184–155209, 2020.

[15] G. Hu, W. Kou, and J. Peng, "A novel image encryption algorithm based on cellular neural networks hyper chaotic system," in *Proceedings of IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 1878–1882, 2018.

[16] S. Yousif, A. Abboud, and R. Alhumaima, "A new image encryption based on bit replacing, chaos and dna coding techniques," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27453–27493, 2022.

[17] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.

[18] B. Y. Irani, P. Ayubi, F. A. Jabalkandi, M. Y. Valandar, and M. J. Barani, "Digital image scrambling based on a new one-dimensional coupled sine map," *Nonlinear Dynamics*, 2024.

[19] J. Nkapkop, J. Effa, A. Toma, F. Cociota, and M. Borda, "Chaos-based image encryption using the rsa keys management for an efficient web communication," in *Proceedings of 12th IEEE International Symposium on Electronics and Telecommunications (ISETC)*, pp. 59–62, 2016.

[20] L. Chen, G. Song, and X. Meng, "Study of sierpinski gasket used in gray image scrambling," in *Proceedings of IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 2298–2302, 2018.

[21] H. Wu, Y. Shao, K. Mikolajczyk, and D. Gündüz, "Channel-adaptive wireless image transmission with ofdm," *IEEE Wireless Communications Letters*, vol. 11, no. 11, pp. 2400–2404, 2022.

[22] K. Dharavathu and A. Mosa, "Secure image transmission through crypto-ofdm system using rubik's cube algorithm over an awgn channel," vol. 33, p. e4369, 2020.

[23] S. Eldin, "Optimized ofdm transmission of encrypted image over fading channel," *Sensing and Imaging*, vol. 15, pp. 1–14, 2014.

[24] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.

[25] P. Andono, "Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption," *IEEE Access*, vol. 10, pp. 115143–115156, 2022.

[26] N. Sharkawy, Y. Afify, W. Gad, and N. Badr, "Gray-scale image encryption using dna operations," *IEEE Access*, vol. 10, pp. 63004–63019, 2022.

[27] Y. Hamza and M. Omer, "An efficient method of image encryption using rossler chaotic system," *Academic Journal of Nawroz University*, vol. 10, no. 2, pp. 11–22, 2021.

[28] A. U. Rehman, D. Xiao, A. Kulsoom, M. Hashmi, and S. Abbas, "Block mode image encryption technique using two-fold operations based on chaos, md5 and dna rules," *Multimedia Tools and Applications*, vol. 78, pp. 9355–9382, 2019.

[29] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and kaa map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023.

[30] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, pp. 26203–26222, 2019.

[31] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Rgb image encryption through cellular automata, s-box and the lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, 2022.

[32] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Image encryption scheme based on newly designed chaotic map and parallel dna coding," *Mathematics*, vol. 11, no. 1, p. 231, 2023.

[33] T. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and s-box," *Multimedia Tools and Applications*, vol. 81, no. 15, pp. 20585–20609, 2022.

[34] M. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3d chaotic map with an application to color image encryption," *Nonlinear Dynamics*, vol. 94, pp. 723–744, 2018.

[35] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.

[36] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools and Applications*, vol. 76, pp. 9907–9927, 2017.

[37] Y. Liu, G. Cen, B. Xu, and X. Wang, "Color image encryption based on deep learning and block embedding," *Security and Communication Networks*, vol. 2022, pp. 1–14, 2022.

[38] I. Q. Abduljaleel, S. A. Abdul-Ghani, and H. Z. Naji, "An image of encryption algorithm using graph theory and speech signal key generation," in *ICMAICT*, 2020.

[39] Z. Abduljabbar, I. Abduljaleel, J. Ma, M. A. Sibahee, V. Nyangaresi, D. Honi, A. Abdulsada, and X. Jiao, "Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022.

[40] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, and W. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.

[41] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020.

[42] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.

[43] S. Zhou, P. He, and N. Kasabov, "A dynamic dna color image encryption method based on sha-512," *Entropy*, vol. 22, no. 10, p. 1091, 2020.

[44] L. Kansal, G. Gaba, N. Chilamkurti, and B. Kim, "Efficient and robust image communication techniques for 5g applications in smart cities," *Energies*, vol. 14, no. 13, p. 3986, 2021.

[45] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image encryption with double spiral scans and chaotic maps," *Security and Communication Networks*, vol. 2019, pp. 1–15, 2019.

[46] I. Eldokany, E. El-Rabaie, S. Elhalafawy, M. Z. Eldin, M. Shahieen, N. Soliman, M. El-Bendary, M. El-Naby, F. Al-Kamali, I. Elashry, and F. A. El-Samie, "Efficient transmission of encrypted images with ofdm in the presence of carrier frequency offset," *Wireless Personal Communications*, vol. 84, pp. 475–521, 2015.