Iraqi Journal of Industrial Research (IJOIR)

Journal homepage: http://ijoir.gov.iq

OFDM Transmission in Rayleigh Fading Channel for S-Box and 3D Chaotic Maps Based Encrypted Image

[1]Jenan Ayad*, [2]Fadhil Sahib Hasan, [1]Alaa H. Ali

[1]Department of Electrical Engineering, University of Technology, Iraq

[2]Department of Electrical Engineering, College of Engineering, Mustansiriyah University, Iraq

Article information

Article history:
Received: November, 09, 2023
Accepted: January, 27, 2024
Available online: October, 20, 2024

Keywords:
Image encryption,
S-box,
Chaotic,
Fading channel,
OFDM

Corresponding Author:
Jenan Ayad
eee.19.13@grad.uotechnology.edu.iq

DOI:
https://doi.org/10.53523/ijoirVol11I2ID410

Abstract

Data encryption is an important part of the communication system. The Chaos essential properties, make it a crucial candidate for encryption applications. There is a compromise between complexity and security in previous studies. In this study, high security was achieved with low complexity. This paper proposed a 3D chaotic map and S-Box has been cascaded to get a high efficiency as complex algorithms or multi-iteration schemes. The first stage is ciphering using 3D cat-map, the second stage is S-box based on 3D henon map, while the third stage is another ciphering stage using 3D henon map. In this study, various encryption techniques, including cipher algorithms and substitution box, are combined with the OFDM system to establish a secure image transmission over a Rayleigh fading channel. QPSK modulation is used to ensure the simplicity of the proposed system. Six gray images are used, Lena, the cameraman, Barbara, Baboon, pepper and Elaine for testing and comparing with previous works. Security analysis is performed to evaluate the quality and security of the encryption process, the entropy value reach 7.99, correlation coefficient is around zero and the histogram is uniform. In addition, the key size is 2^{630}. For image transmission evaluation, the PSNR and BER are utilized and it reached 10^{-5} for BER. According to the statistical results, the proposed image encryption scheme is secure and efficient.

1. Introduction

In recent years, technology in processing images and communication networks has undergone significant development. The safeguarding of sensitive data in both wired and wireless communications is of utmost importance due to real-time data transfer [1]. The use of multimedia and visual content has become commonplace in many fields, including transferring military and medical personal data. Formerly, traditional encryption techniques were used to encrypt images, but their performance was insufficient when encrypting bigger images [2]. For this reason, research has been conducted into the development of several image encryption techniques. Chaos-based encryption research is one of these subjects [3, 4].

There is a close association between chaotic systems and cryptology [5,6]. Randomness, initial parameters, and control sensitivity, ergodicity are features of chaotic systems that satisfy the essential requirements of cryptology [7]. The fact that these values generated by chaotic systems are deterministic and highly unpredictable is a significant advantage for encryption systems. Using these features, additional experiments into chaos-based encryption have been done [8]. Random number sequences are generated by random number generators for use in encryption. The strength of encryption is proportional to the randomness of the generated numbers. The design of random number generators based on chaos is one of the most common encryption applications of chaotic systems [9]. In modern communication, OFDM has become the norm due to its efficacy and dependability in transmitting data over a multipath wireless communication channel [10]. Orthogonal frequency division multiplexing is one form of block modulation algorithm; in this method, symbols are organized into blocks and sent in parallel over a set of subcarriers. As opposed to a single frequency-selective wideband channel, OFDM permits the use of a greater number of frequency-selective narrowband channels [11]. In addition to being easy to install, it has exceptional resistance to the effects of multipath fading. Fast Fourier Transforms, Discrete Wavelet Transforms, and Discrete Cosine Transforms were all reported in prior research and can be used to construct this method [12, 13]. Several wireless communication systems and devices, including 4G LTE generation mobile technologies, have incorporated OFDM technology [10].

Encryption studies based on chaotic systems are incredibly prevalent in the academic literature, some of these studies: In [14], in order to produce a chaotic sequence, a sine map was utilized; in order to strengthen the safety of the system, an elliptic curve point and dynamic permutation table were utilized. This approach makes use of 3D logistic maps. A new method of encryption for medical images is presented in reference [15], which makes use of a 2D Logistic-Gaussian hyperchaotic map. In [16], a novel image encryption algorithm employing a combination of three distinct modified and enhanced chaotic 1D maps has been proposed.

In this paper [13], the OFDM system is suggested for the transmission of encrypted imagery. They employed the Rubik's cube ciphering technique via AWGN. This study compared BPSK, PSK, QAM, 16-PSK, and 16-QAM as well as FFT techniques. Comparing it to other existing systems, They found that using DCT to implement crypto-OFDM improved performance; it was simple to implement and exhibited strong secure. In [18], they proposed encrypted images with chaotic baker map and RC6 algorithm could be efficiently transmitted through the OFDM system, and then re-encrypted with Rubik's cube. The performance of this encryption method was superior to that of the other methods used in that investigation. In [19], they utilized AES, DES, and RC6 through Rayleigh fading and AWGN channels for an OFDM system with multiple encryption techniques. According to the results, FFT-OFDM modulation with erratic encryption provided a superior representation.

According to the results in previous studies, FFT-OFDM modulation with erratic encryption provided a superior representation [20-22]. The challenge is to compromise between complexity and efficiency and try to get as high as possible efficiency with as low as possible complexity. The proposed scheme is contained three encryption stages by using a cipher technique based on the 3D chaotic map, and S-box, to ensure high complexity. These methods outperform other security algorithms due to their simplicity, superior security, and capacity to protect images from differential and statistical assaults. This paper proposed image encryption using two methods of encryption algorithms (ciphering and substitution) and then transmitting these images through an OFDM system over a Rayleigh fading channel. OFDM systems were analyzed using BER.

2. Theoretical Part

Three-stage encryption algorithms that are backwards-compatible with the OFDM communication system are offered as a way to make the system more secure, efficient, and straightforward. This section provides a comprehensive breakdown of the suggested method for ensuring the safety of image transmissions while using an OFDM-based communication system. The scheme's block diagram is depicted in Figure (1).

3. Experimental Procedure

The first step is to transform the u8 grayscale image $I_{m,n} \in \mathbb{R}^{M\times N}$, m= 0, ..., M-1, n=0, ..., N-1, into jth stream bits, $u_j \in \{0,1\}, j = 0, \ldots, 8MN-1,$ when passing through parallel to serial converter (P/S) [17]. These stream bits are then XORed with the k_j, which represents the jth first ciphering key, to generate c_j, the ciphering sequence, which is the first stage of this system, according to the:

$$c_j = u_j \oplus k_j \quad , j = 0, .., 8MN - 1 \qquad (1)$$

where: $\oplus$ in the equation represents the XOR operator [5]. As will be demonstrated in the subsequent section, the ciphering key is generated using a 3D cat map. The resulting stream is converted to a decimal sequence and then reconstructed to produce a stage one ciphered image. This ciphered image is mapped using S-box to get a stage two ciphered image. Converting this image to a binary stream and xored with the second ciphering key that was generated using a henon chaotic map as will see later.

Using the QPSK modulation method, the encrypted sequence is modulated, and then the serial to parallel converter (S/P) is used to frame the transformed sequence into N_{fft} parallel samples, $q_\ell, \ell = 0, .., N_{fft} - 1$, the number of FFT subcarriers, denoted by N_{fft}. Inverse Fast Fourier Transform (IFFT) is applied to s_ℓ sequences, resulting in the OFDM modulated signal according to:

$$s_{ifft}(v) = \frac{1}{\sqrt{N_{fft}}} \sum_{\ell=0}^{N_{fft}-1} s_\ell \, e^{i2\pi\ell v/N_{fft}} \quad , 0 \le v \le N_{fft} - 1 \qquad (2)$$

where: $s_{ifft}(v)$ is the v-the OFDM modulated sequence [23, 24]. At the end, Cyclic Prefix (CP) is added between OFDM signals to decrease the effect of Inter Symbol Interference (ISI), then serially transmitting these symbols over a Rayleigh fading channel. At the receiver side, firstly removing CP from the v-th received signal, r_v. The OFDM demodulated sequence $\tilde{s}_\ell$ is created by applying the FFT function to the vth received sequence r_v.

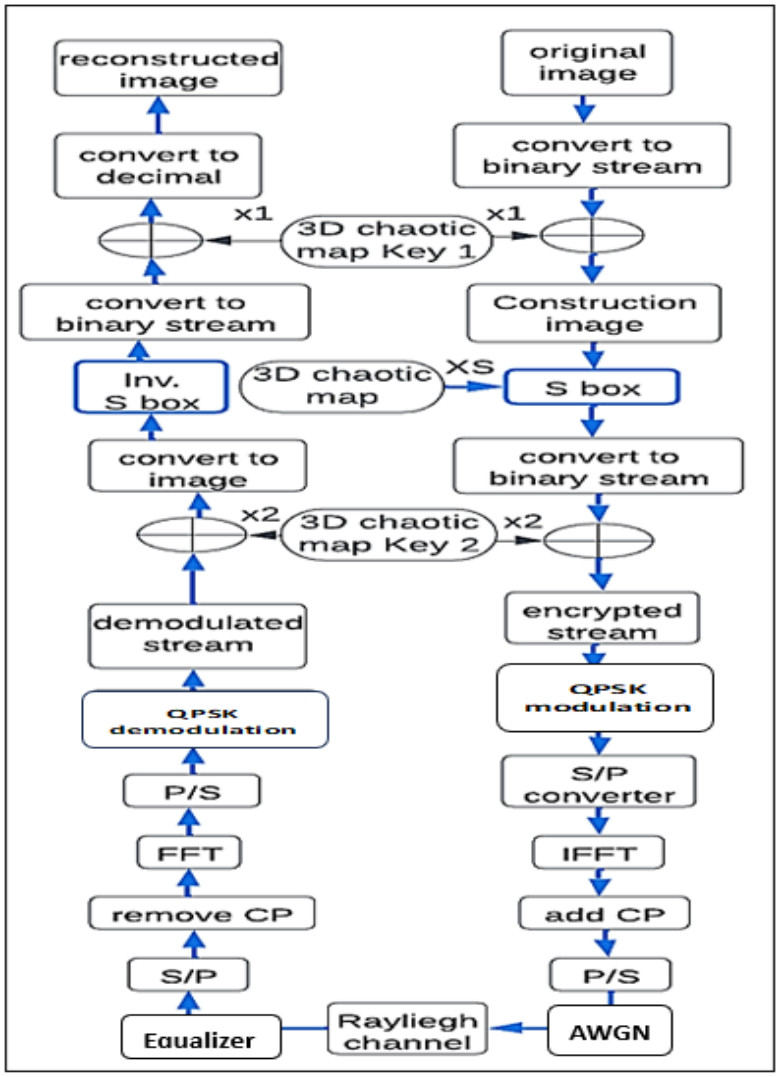


Figure (1): Scheme of secure image transmission over OFDM system.

Then a P/S is take place, and QPSK demodulator generates stream bits $\tilde{c}_j$, where j=0,..8MN-1. Xoring $\tilde{c}_j$ with the second ciphering stage key x2, and convert the resulting stream to image which is mapped by inverse S-box and convert the resulting image to binary stream, By XORing $\tilde{c}_j$ with the first ciphering stage key x1, k_j, the j-th set of decrypted stream bits, $\tilde{u}_j$, can be determined [25], according to:

$$\tilde{u}_j = \tilde{c}_j \oplus k_j \quad , \mathbf{j = 0, \ldots, 8MN - 1} \qquad (3)$$

By transforming the serial data into a 2D unit 8 matrix, the image is retrieved, $\tilde{I}_{m,n}$, m=0,..M-1,n=0,..,N-1.

4. Key Generator Algorithm

4.1. Cat Map

The equation of a 3D chaotic cat map (3D-CM) is written as [26]:

$$x_{n+1} = (3x_n + y_n + 4z_n) mod\ 1 \qquad (4)$$

$$y_{n+1} = (6x_n + 3y_n + 11z_n) mod\ 1 \qquad (5)$$

$$z_{n+1} = (6x_n + 2y_n + 9z_n) mod\ 1 \qquad (6)$$

Wher x,y and z are the three dimensions of the cat map.

4.2. Henon Chaotic Map

The equation of a 3D chaotic henon map (3D-HM) is written as [27]:

$$x_{n+1} = a - y_n^2 - bz_n \qquad (7)$$

$$y_{n+1} = x_n \qquad (8)$$

$$z_{n+1} = y_n \qquad (9)$$

where: x,y and z are the three dimensions, and (a, b) are the control parameters of the henon map.

4.3. S-Box

To describe the nonlinear transformation of the pixel value p using the S-box matrix s, the substitution function sb (s, p) is defined. The function value is the transformed ciphertext pixel value. Based on the previous chaotic maps (3D-CM, 3D-HM), a new algorithm for the construction of dependable S-boxes has been proposed. The (i, j) element in the original image, P (k1, k2), is shuffled to a new position based on the index defined before as S-box. Imag_sb is the ciphertext pixel value obtained.

The detailed steps of generating an S-box based on chaotic sequences are shown in Algorithm 1.

Algorithm 1 Sbox with chaotic map

input Image of size m×n and chaotic sequence (xi, yi, zi).
output substitute image Imag_sb.
[xs]=sort (x) by its index.
sb_matrix← generating matrix (16*16) from the index vector.
for k1=1:n
or k2=1:m **do**
Imag_sb ← index of the image pixel value +1;
end for
end for

5. Results and Discussion

A secure method of picture encryption should be effective against a variety of threats [29]. Many statistical studies are addressed, including differential attack analysis (uniform average change intensity and the number of pixel change rates) and key analysis (key sensitivity and key space), as also correlation coefficient, information entropy, and histogram. In this part, we also analyze our proposed technique in light of existing methods. Using 256x256 grey images transmitted over a Rayleigh fading channel, this section demonstrates the scheme's efficacy in transmitting the encrypted image via the OFDM system. The parameters that will be utilized in the implementation of the proposed system are detailed in Table (1). The visual quality of the received images is evaluated using various SNRs, whereas the efficacy of the OFDM communication system is measured by BER.

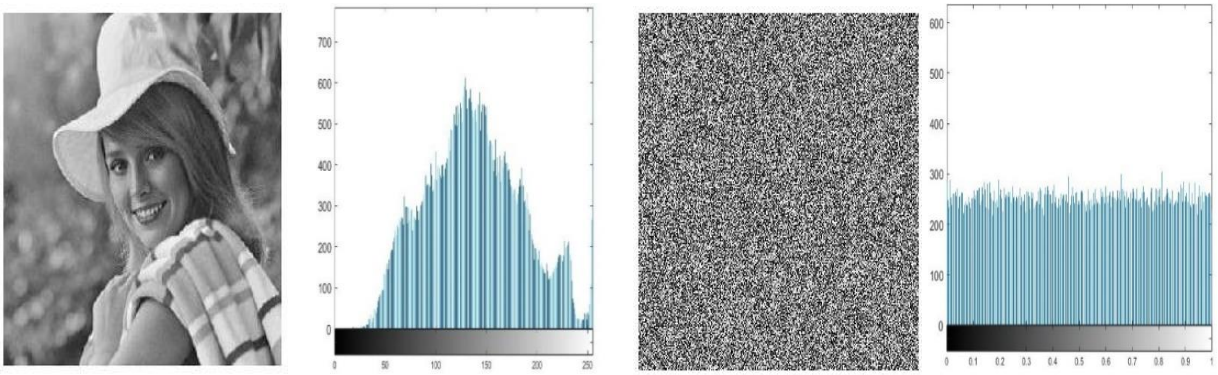
Table (1): The Parameters of the Simulation Program.

Factors	Type of modulation/ order	Length Of CP	The subcarriers number / (n_{fft})	Channel Type	Range of SNR
Values	QPSK/ 4	9	64/52	Rayleigh	0 dB to +40 dB

5.1. Statistical Analysis Tests

5.1.1. Histogram

Histograms reveal the distribution of the pixel inside a picture by displaying how many pixels are in each gray level. Through the study of this data, the cryptanalyst can get a significant deal of understanding regarding the image. To preserve picture integrity, the final image should have a uniformly distributed histogram and must be a wholly unlike the histogram of a plain text image. Figure (2) shows the testing gray images with their histogram and the encrypted versions with their histogram, using the Elaine image. Figure (2) demonstrates that the encrypted image's histogram provides no helpful information. The suggested approach can effectively conceal the original image's content since the resulting scrambled image has a drastically different appearance and an even distribution of intensity values. Consequently, the suggested system is impervious to statistical attacks and possesses an efficient attribute of confusion.



(a) (b)

Figure (2): Histogram representation of the original and encrypted image of Elaine gray image: (a) the original image, (b) the proposed scheme.

5.1.2. NPCR and UACI

The resistance of this method against differential attacks is measured using the two most prevalent metrics. The first is referred to as Number of Pixel Change Rate (NPCR), which defines the percentage of pixel differences between two photographs. Suppose $I_1(a,b)$ and $I_2(a,b)$, a=0, .., M-1, b=0, .., N-1, are two different encrypted images, each of which differs from its related plaintext image by a single pixel. The formula for calculating the % NPCR is as follows:

$$\mathbf{NPCR}=\frac{\sum_{a=0}^{M-1}\sum_{b=0}^{N-1} D_{a,b}}{M*N} * \mathbf{100}\% \qquad (10)$$

where: $D_{a.b}$ is a (0, 1) matrix calculated by $I_1(a,b)$ and $I_2(a,b)$. If $I_1(a,b)$=$I_2(a,b)$, then $D_{a.b}$ = 0; otherwise, $D_{a.b}$= 1, and $D_{a.b} \in B^{M\times N}$.

The other parameter is Unified Average Changing Intensity (UACI), when there is a tiny difference (ex. one or two pixels), between two plain text images, then UACI is utilized to determine the average intensity of disparities in pixels between these images. The mathematical expression for the UACI is:

$$\mathbf{UACI} = \left[\sum_{a=0}^{M-1}\sum_{b=0}^{N-1}\frac{|I_1(a,b)-I_2(a,b)|}{255}\right] * \frac{100\%}{M*N} \qquad (11)$$

The higher UACI values the better, and the optimal NPCR value is 99.6094 [30], in order to obtain satisfactory performance from the image encryption method. The UACI and NPCR values of the encrypted testing gray images with the proposed algorithm are shown in Table (2). In terms of NPCR, the provided methods exhibit superior or competitive values, whereas higher values suggest more secure images. NPCR and UACI values were decided by the image's format and dimensions. Table (2) shows a comparison with previous works. From this table, it is evident that in comparison with systems employed in past studies, the NPCR and UACI values of the suggested systems in this paper are considered good values in order to avoid UACI and NPCR attacks and have a better image transmission that is also more efficient and safer.

Table (2): NPCR and UACI Tests

Image Name		Scheme	[4]	[13]	[24]
UACI	**Lena**	34.6253	33.4974	-----	33.06
	Cameraman	34.630	33.4974	31.1276	33.06
	Peper	34.3948	----	----	----
	Barbara	34.6365	----	----	----
	Baboon	34.6030	----	----	----
	Elaine	34.1588	----	----	----
NPCR	**lena**	99.6429	99.6037	----	99.46
	Cameraman	99.6521	99.6038	99.6063	99.46
	Peper	99.5941	----	----	----
	Barbara	99.5712	----	----	----
	Baboon	99.5834	----	----	----
	Elaine	99.6033	----	----	----

5.1.3. Entropy

One of the statistical tests' essential parameters is information entropy. It is used to calculate the randomness of the image. When the grayscale image size is 256 by 256 there are 256 levels; assuming each level has the same probability, the entropy value is 8 bits. Its mathematical expression is:

$$\boldsymbol{H(X)} = -\sum_{j=1}^{K} \boldsymbol{P_r(\chi_j)}\,\mathbf{log_2}\,\boldsymbol{P_r(\chi_j)} \qquad (12)$$

$$\boldsymbol{P_r(X=\chi_j)} = \frac{\mathbf{1}}{\boldsymbol{IS}} \qquad (13)$$

where: X is the original image, $\Pr(\chi_j)$ is the probability of

$X = \chi_j$, χ_j is j-th possible value in X, K indicates the number of levels present in an image, and S stands for intensity sequence number, which is related to the format of the image. In Table (3), the entropy values for encrypted test images of the encryption scheme are shown. The entropy value measured in this study is marginally different from the value expected by theory. This approach exhibits an increase in entropy compared to the Elaine and Lena gray images utilized in an earlier study and described in Table (3).

5.2. Correlation Coefficient Analysis

A correlation coefficient (CC) is an important parameter for examining the three-dimension relationship between two adjacent pixels. The pixels that comprise the picture of plain text have a solid association in all directions. In a secure system, the data are uncorrelated and random; thus, the value tends toward zero, and the encrypted plaintext image preserves all of its original features. If Q random pairings of the surrounding pixels of an image with the values (α_j, β_j), where j might vary from 1 to Q, are chosen. The equation of CC is:

$$CC = \frac{\sum_{j=1}^{Q}(\alpha_j - E(\alpha))(\beta_j - E(\beta))}{\sqrt{\sum_{j=1}^{Q}(\alpha_j - E(\alpha))^2}\sqrt{\sum_{j=1}^{Q}(\beta_j - E(\beta))^2}} \quad (14)$$

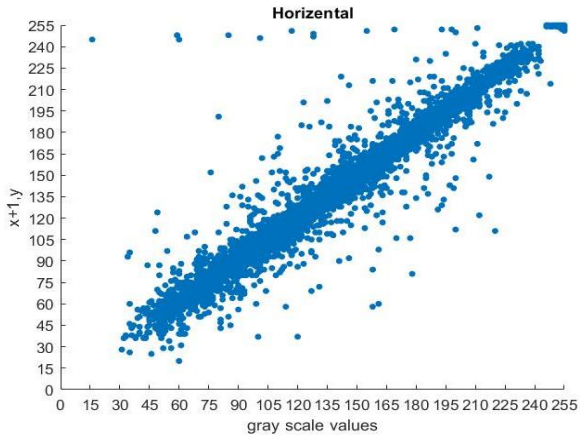
where: E(.) represents the mean value function and $(\alpha \ , \beta)$ represents the two neighboring pixels. The test results for the three-direction CC of encrypted images and the proposed system are presented in Table (4). The CC values of the suggested methods are superior to those found in the table, which covers earlier studies. Figure (3) depicts the three correlation directions for the Elaine plaintext images and their encrypted image.

Table (3): Entropy tests.

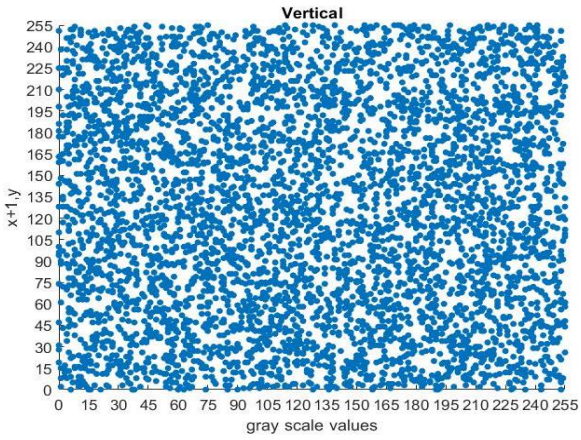
Image Name	Encrypted Image				
	Original	Scheme	[4]	[13]	[24]
Lena	7.9971	7.9973	7.9973	7.9974	7.716
Cameraman	7.9973	7.9974	7.9971	7.9957	7.7
Peper	7.9969	7.99736	----	----	----
Barbara	7.9973	----	----	----	----
Baboon	7.9974	----	----	----	----
Elaine	7.9973	----	----	----	----

Table (4): Correlation Coefficient Test.

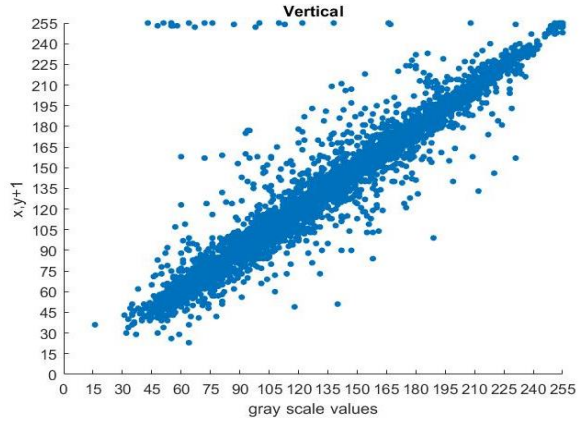
Image Name			Encrypted image			
		original	Scheme	[4]	[13]	[5]
Lena	H	0.9534	-0.0619	−0.003	----	0.0004
	V	0.9891	-0.0780	0.0084	----	−0.039
	D	0.8286	0.0259	0.0108	----	0.0030
Camera man	H	0.9261	0.0174	-0.0017	−0.004	0.0021
	V	0.9781	-0.0791	-0.0143	0.0411	0.0019
	D	0.8956	-0.0990	0.0086	−0.066	-0.0002
Peper	H	0.8654	-0.0266	----	----	----
	V	0.7949	-0.1176	----	----	----
	D	0.8967	-0.111	----	----	----
Barbara	H	0.8858	0.0666	----	----	----
	V	0.9350	0.0945	----	----	----
	D	0.9271	0.0173	----	----	----
Baboon	H	0.2042	-0.1005	----	----	----
	V	0.4055	0.0154	----	----	----
	D	0.6140	-0.0742	----	----	----
Elaine	H	0.9454	-0.0051	----	----	----
	V	0.9200	-0.078	----	----	----
	D	0.8966	-0.017	----	----	----



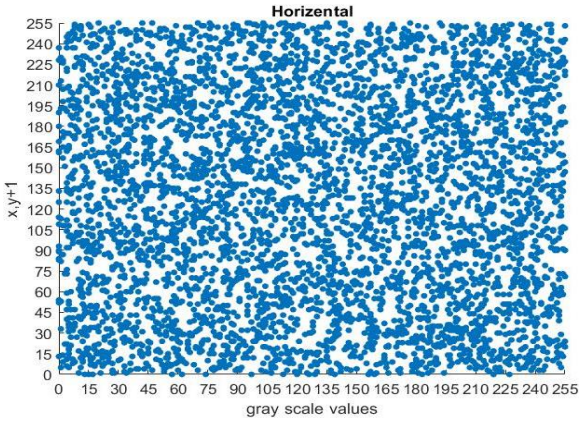
(a)



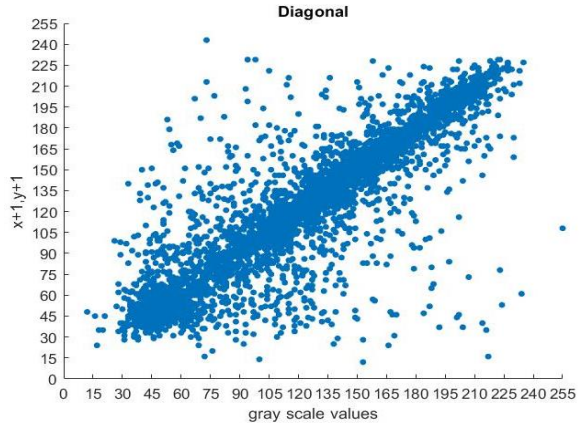
(d)



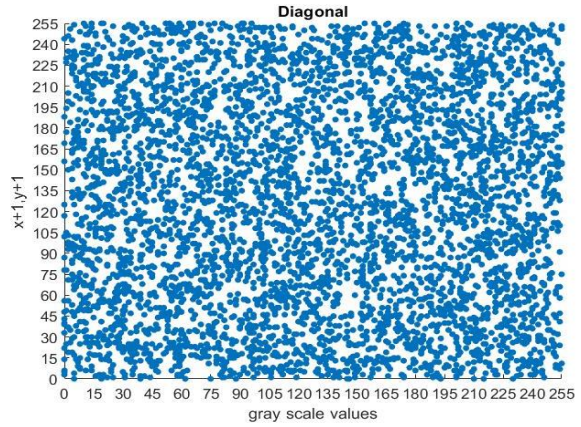
(b)



(e)



(c)



(f)

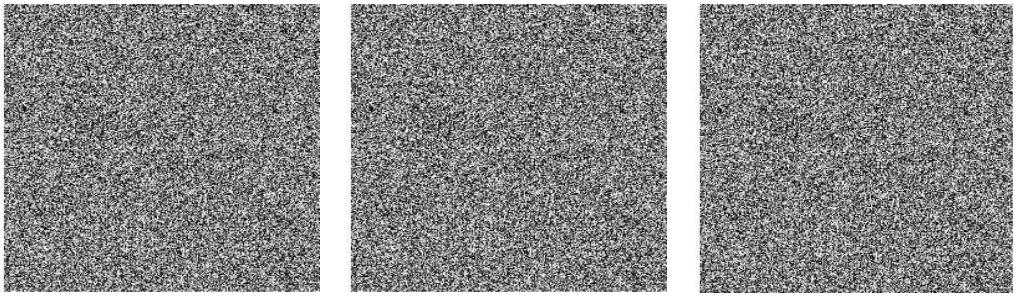
Figure (3): Adjacent pixels correlation: (a)horizontal direction, (b) vertical direction, (c) diagonal direction of Elaine original image; (d)horizontal direction, (e) vertical direction, (f) diagonal of the encrypted image.

5.3. Key Analysis

The secure system of encryption must employ key sensitivity in order to resist any thorough attack. When there is just a slight variation between the encryption and decryption keys, yet the original data remains unrecoverable, the encryption technique is said to have "key sensitivity" even When the difference between the two initial values is only 10^{-15} points, the final sequence will be entirely distinct [31, 32]. When the initial values of PRBG differ by a factor of10−15, the resulting cipher images are depicted in Figure (4), which are considered unrecognizable images. The key space is the total number of keys that can be used within a specific cryptographic technique. For protection against brute-force attacks, it is advised that the total key search space be more than 2^{100} [33]. In the proposed scheme, there are three parameters for the first ciphering stage; initial values of 3D-CM. Three initial values and two control parameters for 3D-HM, which is used with the second ciphering stage and S-box stage, suppose the accuracy of these parameters is set to 10^{-15}, therefore the corresponding key space size will approximately about $(10^{15})^{13} \approx 2^{630}$. Consequently, our system has sufficient key space to defend itself against any exhaustive attack. In Table (5), we can see how our scheme compares to others regarding key space.

Table (5): Key space comparison.

	Proposed Scheme	**[6]**	**[25]**	**[32]**	**[34]**
Key space	$10^{195}=2^{630}$	2^{256}	2^{256}	2^{232}	10^{30}



(a) (b) (c)

Figure (4): Decrypted image at FFT-OFDM system with an incorrect key: (a) Elaine, (b) camera-man and (c) Lena

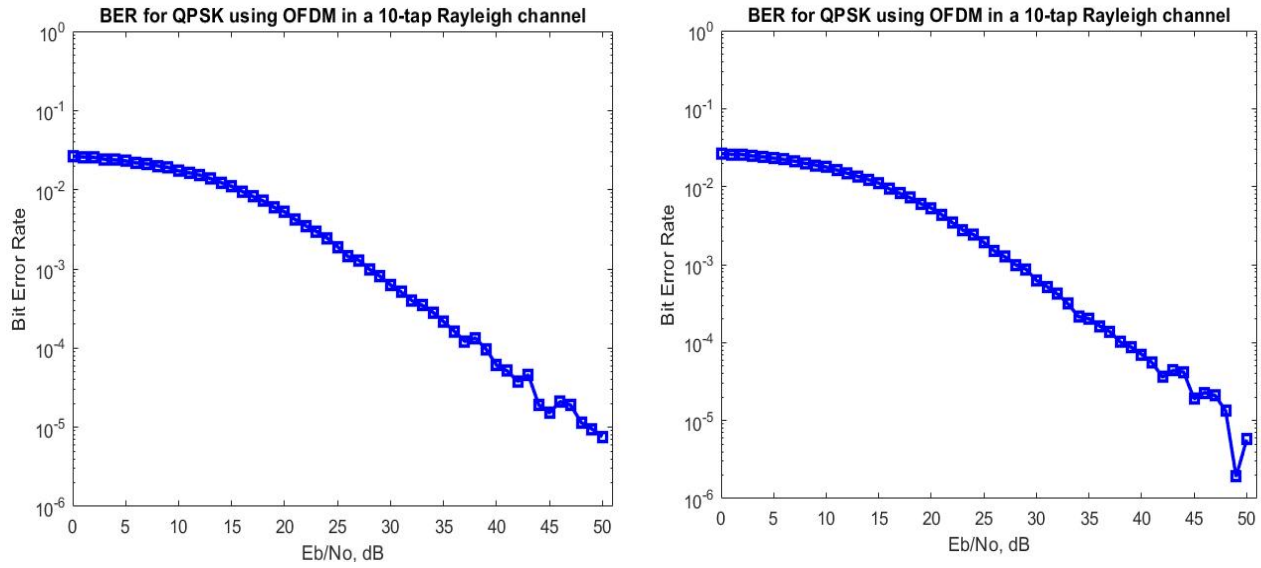
5.4. OFDM System Analysis

Figure (5) illustrates variations of the BER versus SNR variation plots of the different proposed method for Elaine, and, camera man images in Rayleigh channels. According to the diagrams, the BER of the system has a fast slope down, it achieved high accuracy when SNR is lower than 25 dB. Moreover, the eavesdropper cannot decrypt the original image because the BER of the encrypted version is always set to 0.50 [35]. The proposed algorithm is quite robust to noise, and it shows a good performance in situations with higher noise levels. When recovering the original images, the PSNR values increase in tandem with the SNR. Due to the results, the suggested design is one of the most optimal systems. Figure (6) shows the visual inspection quality of the recovered Elaine image at the receiver side after passing through the communication channel. This scheme demonstrates excellent efficiency, it can achieve high PSNR values at both low and high SNRs. From this figure, the Elaine image can be recognized and it gets clear at SNR=10 dB.

6. Conclusions

Simple and secure 3D chaotic maps have been proposed for encryption images and transmission with QPSK over OFDM system communication channel. The proposed system was designed for efficient and safe image transmission through Rayleigh fading channel. This system is proposed to achieve high security with low complexity and also having accurate recovered image quality. Even when the signal-to-noise ratio is set to 10 decibels, the observations, and numerical results demonstrate that the proposed encrypted-OFDM system functions

are acceptable and can understand the message, and that its performance is superior to that of the previous works, where the entropy value reach 7.99, correlation coefficient is around zero and the histogram is uniform, the values of NPCR is more than 99.5 and the values of UACI is more than 34; it is more secure, with key space 10^{195} and more simplicity, by using two stages of XOR ciphering and S-box, thus it is easy to implement. For future work, many chaotic maps can be used instead of the (3D-CM and 3D-HM), and another modulation type can used and also DWT instead of FFT. This technology has the potential to be implemented in numerous contexts, including but not limited to financial transactions, medical images, mobile application development, etc.



(a) (b)

Figure (5): BER versus SNR plots of OFDM system for: (a) Elaine image, and (b) camera-man.

(a) (b) (c)

Figure (6): The visual inspection quality of the decrypted Elaine image at the OFDM system for different SNRs (a) SNR=10 dB, (b)SNR=20 dB; and (c) SNR=30 dB.

Conflict of Interest: The authors declare that there are no conflicts of interest associated with this research project. We have no financial or personal relationships that could potentially bias our work or influence the interpretation of the results.

References

[1] Chen, Z. and Ye, G. (2022) "An asymmetric image encryption scheme based on hash SHA-3, RSA, and Compressive Sensing," *Optik*, 267, p. 169676. Available at: https://doi.org/10.1016/j.ijleo.2022.169676.
[2] Ali, R.S. *et al.* (2022) "Enhancement of the cast block algorithm based on novel S-box for image encryption," *Sensors*, 22(21), p. 8527. Available at: https://doi.org/10.3390/s22218527.
[3] Imad Mhaibes, H., Hattim Abood, M. and Farhan, A. (2022) "Simple lightweight cryptographic algorithm to secure imbedded IOT devices," International Journal of Interactive Mobile Technologies (iJIM), 16(20), pp. 98–113. Available at: https://doi.org/10.3991/ijim.v16i20.34505.
[4] H. Luo and B. Ge, "Image encryption based on Henon chaotic system with nonlinear term," Multimed. Tools Appl., vol. 78, no. 24, pp. 34323–34352, 2019, doi: 10.1007/s11042-019-08072-4.
[5] A. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimed. Tools Appl.*, vol. 80, no. 2, pp. 2753–2772, 2021, doi: 10.1007/s11042-020-09648-1.
[6] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "An Efficient OFDM-Based Encryption Scheme Using a Dynamic Key Approach," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 361–378, 2019, doi: 10.1109/JIOT.2018.2846578.
[7] J. Ayad, F. S. Hasan and A. H. Ali, "Efficient Transmission of Secure Images with OFDM using Chaotic Encryption," *2022 4th International Conference on Circuits, Control, Communication and Computing (I4C)*, Bangalore, India, 2022, pp. 391-396, doi: 10.1109/I4C57141.2022.10057774.
[8] Elsaid, S.A., Alotaibi, E.R. and Alsaleh, S. (2022) "A robust hybrid cryptosystem based on DNA and hyperchaotic for images encryption," *Multimedia Tools and Applications*, 82(2), pp. 1995–2019. Available at: https://doi.org/10.1007/s11042-022-12641-5.
[9] Naik, R.B. and Singh, U. (2022) "A review on applications of chaotic maps in pseudo-random number generators and encryption," *Annals of Data Science* [Preprint]. Available at: https://doi.org/10.1007/s40745-021-00364-7.
[10] J. Ayad, F. Sahib Hasan and A. H. Ali, "OFDM Transmission for encrypted Images based on 3D Chaotic Map and S-Box through Fading Channel," *2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES)*, Tumakuru, India, 2023, pp. 1-6, doi: 10.1109/ICSSES58299.2023.10199452.
[11] Asha, M., Surekha, T.P. Development of OFDM technique for underwater communication in system on chip. *Int J Syst Assur Eng Manag* (2023). https://doi.org/10.1007/s13198-023-01901-8
[12] M. Jacovic, K. Juretus, N. Kandasamy, I. Savidis, and K. R. Dandekar, "Physical Layer Encryption for Wireless OFDM Communication Systems," *J. Hardw. Syst. Secur.*, vol. 4, no. 3, pp. 230–245, 2020, doi: 10.1007/s41635-020-00097-8.
[13] K. Dharavathu and A. Mosa, "Secure image transmission through crypto-OFDM system using Rubik's cube algorithm over an AWGN channel," *International Journal of Communication Systems*, 33(8), p.e4369
[14] Laiphrakpam, D.S. *et al.* (2022) "Encrypting multiple images with an enhanced chaotic map," *IEEE Access*, 10, pp. 87844–87859. Available at: https://doi.org/10.1109/access.2022.3199738.
[15] Lai, Q. *et al.* (2023) "High-efficiency medical image encryption method based on 2D logistic-gaussian hyperchaotic map," *Applied Mathematics and Computation*, 442, p. 127738. Available at: https://doi.org/10.1016/j.amc.2022.127738.
[16] Benaissi, S., Chikouche, N. and Hamza, R. (2023) "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, 272, p. 170316. Available at: https://doi.org/10.1016/j.ijleo.2022.170316.
[17] Jalil, M. A., Ayad, J., & Abdulkareem, H. J. (2020). Modulation Scheme Identification Based on Artificial Neural Network Algorithms for Optical Communication System. *Journal of ICT Research and Applications*, *14*(1), 69-77. https://doi.org/10.5614/itbj.ict.res.appl.2020.14.1.5
[18] M. Helmy, E. S. M. El-Rabaie, I. M. Eldokany, and F. E. A. El-Samie, "3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm," *3D Res.*, vol. 8, no. 4, 2017,doi: 10.1007/s13319-017-0145-8.
[19] S. Eldin, "Optimized OFDM Transmission of Encrypted Image Over Fading Channel", *Sens. Imaging.*, 2014, doi: 10.1007/s11220-014-0099-3.
[20] H. A. Abdullah and H. N. Abdullah, "Secure image transmission based on a proposed chaotic maps", vol. 884. 2020.

[21] F. Hasan and M. Saffo, "FPGA Hardware Co-Simulation of Image Encryption Using Stream Cipher Based on Chaotic Maps", *Sensing and Imaging*, vol. 21, no. 1, 2020. doi: 10.1007/s11220-020-00301-7.
[22] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM Physical Layer Encryption Scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, 2017, doi: 10.1109/TVT.2016.2571264.
[23] I. Eldokany and E. M. E. S. M. Elhalafawy, "Efficient Transmission of Encrypted Images with OFDM in the Presence of Carrier Frequency Offset," *Wirel. Pers. Commun.*, vol. 84, no. 1, pp. 475–521, 2015, doi: 10.1007/s11277-015-2645-2.
[24] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Adv.*, vol. 10, no. 7, 2020, doi: 10.1063/5.0009225.
[25] Z. Hua, Y. Zhou, and H. Huang, "A novel bit level multiphase-based chaotic system for image encryption," *Inf. Sci. (Ny).*, vol. 480, pp. 403–419, 2019, doi: 10.1016/j.ins.2018.12.048.
[26] Qian, X. *et al.* (2021) "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, 9, pp. 61334–61345. Available at: https://doi.org/10.1109/access.2021.3073514.
[27] Z. A. Abduljabbar *et al.*, "Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.
[28] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.
[29] W. J. Jun and T. S. Fun, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step," *IEEE Access*, vol. 9, pp. 120596–120612, 2021, doi: 10.1109/ACCESS.2021.3108789.
[30] S. F. El-Zoghdy, H. S. El-sayed, and O. S. Faragallah, "Transmission of Chaotic-based Encrypted Audio Through OFDM," *Wirel. Pers. Commun.*, vol. 113, no. 1, pp. 241–261, 2020, doi: 10.1007/s11277-020-07187-4.
[31] J. Arif *et al.*, "A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022, doi: 10.1109/ACCESS.2022.3146792.
[32] B. Arpacı, E. Kurt, K. Çelik, and B. Ciylan, "Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit," *J. Electr. Eng. Technol.*, vol. 15, no. 3, pp. 1413–1429, 2020, doi: 10.1007/s42835-020-00393-x.
[33] B. Ge, X. Chen, G. Chen, and Z. Shen, "Secure and Fast Image Encryption Algorithm Using Hyper-Chaos-Based Key Generator and Vector Operation," *IEEE Access*, vol. 9, pp. 137635–137654, 2021, doi: 10.1109/ACCESS.2021.3118377.
[34] Z. Wang, "Secure Image Transmission in Wireless OFDM Systems Using Secure Block Compression Encryption and Symbol Scrambling," IEEE, vol. 7, 2019, doi:10.1109/ACCESS.2019.2939266
[35] Helmy M, *et al*. "Chaotic encryption with different modes of operation based on Rubik's cube for efficient wireless communication," Multimed Tools Appl. 2018;77:27337-27361. Springer Science+Business Media, LLC, part of Springer Nature 2018.