Engineering and Technology Journal
Journal homepage: https://etj.uotechnology.edu.iq

Image encryption based on s-box and 3D chaotic maps and secure image transmission through ofdm in rayleigh fading channel

Jenan A. Namuq[a*], Fadhil S. Hasan[b], Alaa H. Ali[a]

[a] Electrical Engineering Dept., University of Technology-Iraq, Alsina'a street, 10066 Baghdad, Iraq
[b] Electrical Engineering Dept., College of Engineering, Mustansiriyah University, Iraq
*Corresponding author Email: eee.19.13@grad.uotechnology.edu.iq

HIGHLIGHTS

- This paper proposes a new multistage system for image encryption and decryption
- The system enables secure image transmission through an OFDM system
- The system achieved a UACI of around 34, NPCR over 99.4, and CC under 0.05
- Statistical analysis demonstrated the encryption system is secure and robust.

ARTICLE INFO

Handling editor: Ivan A. Hashim

Keywords:
Image encryption; S-box; Chaotic; Fading channel; OFDM; Secure; Transmission.

ABSTRACT

Data security is vital if transferred over a wireless network or stored on a personal computer. The essential properties of chaos, such as initial state sensitivity and unpredictability, make it a crucial candidate for encryption applications. This paper proposes a 3D chaotic map and a cascaded S-Box that can be combined to get a high-efficiency and complex cryptographic algorithm. The first stage is ciphering using a 3D cat map, the second stage is an S-box based on a 3D Henon map, and the third stage is another ciphering stage using a 3D Henon map. This study combines various encryption techniques, including cipher algorithms and substitution boxes, with the OFDM system to establish a secure image transmission over a Rayleigh fading channel. BPSK modulation is used to ensure the simplicity of the proposed system. Three grey images are used, Lena, the camera-man, and Pepper, for testing and comparing with previous works. Security analysis is performed to evaluate the quality and security of the encryption process. For image transmission evaluation, the PSNR and BER are utilized. According to the statistical results, the proposed image encryption scheme is secure and efficient. The comparison with the previous studies shows that this system is competitive with previous works.

1. Introduction

Technology in processing images and communication networks has significantly developed in recent years. Safeguarding sensitive data in both wired and wireless communications is of utmost importance due to real-time data transfer [1]. Multimedia and visual content have 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 developing 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, control sensitivity, and 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. Additional experiments into chaos-based encryption have been done using these features [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]. OFDM has become the norm in modern communication 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 using more 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

http://doi.org/10.30684/etj.2024.141722.1508
Received 11 July 2023; Received in revised form 08 January 2024; Accepted 16 January 2024; Available online 06 February 2024
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Transforms were all reported in prior research and can be used to construct this method [12-14]. 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 Laiphrakpam et al. [15] tried to produce a chaotic sequence, a sine map was utilized; 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 Lai et al., [16], which uses a 2D Logistic-Gaussian hyperchaotic map. Benaissi et al., [17], proposed a novel image encryption algorithm employing a combination of three distinct modified and enhanced chaotic 1D maps.

Dharavathu and Mosa [13], the OFDM system is suggested for transmitting encrypted imagery. The Rubik's cube ciphering technique via Additive white Gaussian noise (AWGN) has been used. They compared these modulations BPSK, PSK, QAM, 16-PSK, and 16-QAM, and FFT techniques to other existing systems. The conclusion was that using Discrete Cosine Transform (DCT) to implement crypto-OFDM improved performance; it was simple to implement and exhibited strong security. Helmy et al., [18] proposed image encryption with a chaotic baker map, and the RC6 algorithm could be efficiently transmitted through the OFDM system and then re-encrypted with a Rubik's cube. The performance of this encryption method was superior to that of the other methods used in that investigation. Eldin [19] used 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, 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 contains three encryption stages 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. The remaining sections of this paper are organized as shown below. During phase two, the methodology of the secure-OFDM system was discussed. Key generation is mentioned in section three. The results are presented in section four, and the conclusions are discussed in section five.

2. Methodology

Three-stage encryption algorithms that are backward-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.

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 Equation (1):

$$c_j = u_j \oplus k_j \quad , j = 0, \ldots, 8MN-1 \tag{1}$$

where $\oplus$ in the equation represents the XOR operator [5].

As 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 an S-box to get a stage two ciphered image. Converting this image to a binary stream and xored with the second ciphering key generated using a Henon chaotic map, as will be seen later. Using the BPSK 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, $q_\ell, \ell = 0, \ldots, N_{fft}-1$, 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 Equation (2):

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

where $s_{ifft}(v)$ is the v-the OFDM modulated sequence [23, 24].

In 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. Then a P/S takes place, and the BPSK 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 the 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 Equation (3):

$$\tilde{u}_j = \tilde{c}_j \oplus k_j \quad , \mathrm{j} = 0, \ldots, 8\mathrm{MN}-1 \tag{3}$$

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.

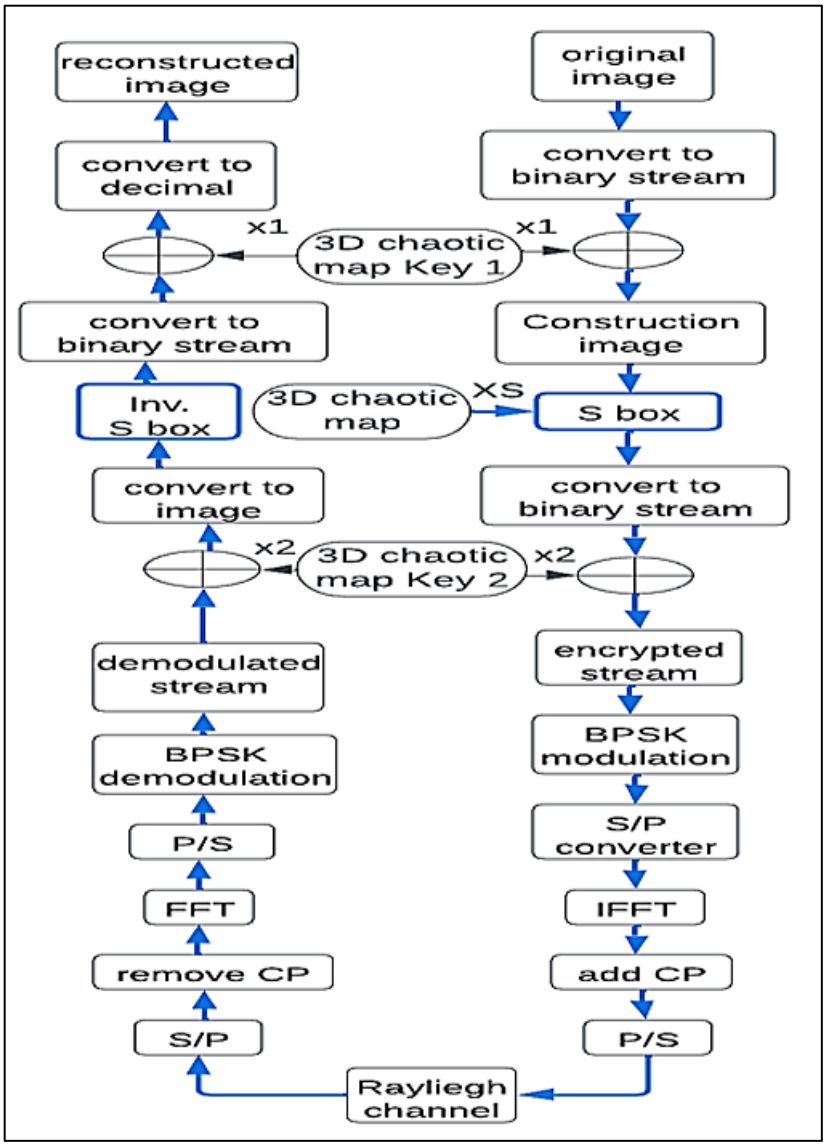


Figure 1: Scheme of secure image transmission over OFDM system

3. Key generator algorithm

Two 3D chaotic maps are used because 3D maps are needed in this work and because of their simplicity and algebraic equation.

3.1 Cat map

The equation of a 3D chaotic cat map (3D-CM) is written according to Equations (4),(5), and (6) [26]:

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

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

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

3.2 Henon chaotic map

The equation of a 3D chaotic Henon map (3D-HM) is written as according to Equations (7),(8), and (9) [27]:

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

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

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

where a=1.3,76 and b = 0.1 in this work

4. 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 constructing 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 an 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 discussions

A secure method of picture encryption should be effective against various threats [28, 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 well as 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 implementing 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	BPSK/2	16	64/52	Rayleigh	0 dB to +45 dB

5.1 Statistical analysis tests

5.1.1 Histogram

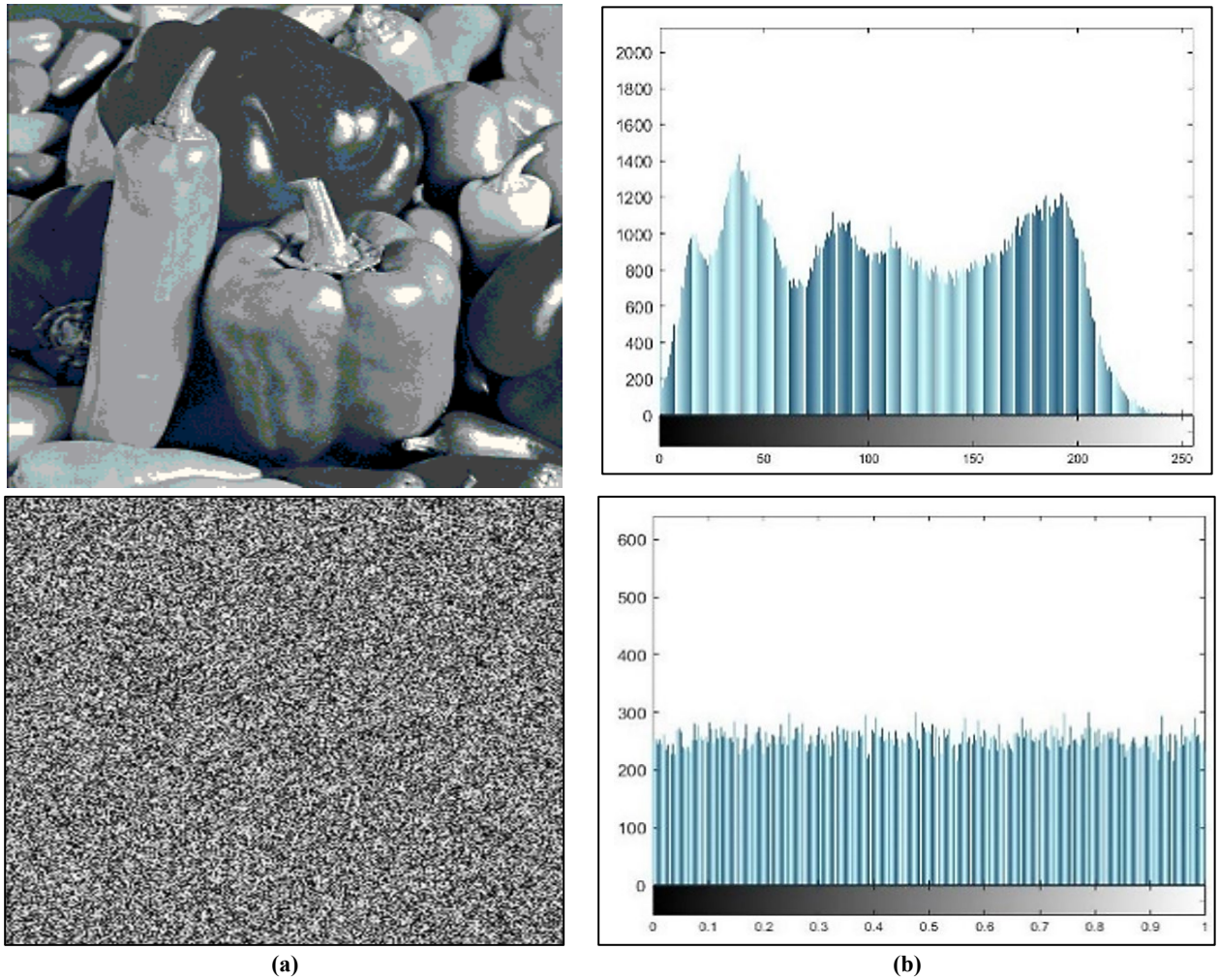
Histograms reveal the distribution of the pixels inside a picture by displaying how many pixels are in each grey level. By studying this data, the cryptanalyst can get a significant deal of understanding regarding the image. To preserve picture integrity, the final image should have a uniformly distributed histogram and must be wholly unlike the histogram of a plain text image. Figure (2.a) shows the testing images (the original and encrypted image of a grey pepper image), while Figure (2.b) shows their histogram representation. 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.

5.1.2 Number of pixel change rate(NPCR) and unified average changing intensity (UACI)

The resistance of this method against differential attacks is measured using the two most prevalent metrics. The first is 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 in Equation (10):

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

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 $D_{a.b} \in B^{M\times N}$.



(a) **(b)**

Figure 2: (a,b) Histogram representation of the original and encrypted image of a grey pepper image: a) the original images, b) the histogram representation of the images

The other parameter is 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. The mathematical expression for the UACI is in Equation (11):

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

The higher the UACI values, the better, and the optimal NPCR value is 99.6094 [30], to obtain satisfactory performance from the image encryption method. The UACI and NPCR values of the encrypted testing grey images with the proposed algorithm are shown in Table 2. Regarding 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. This table shows that compared to systems employed in past studies, the NPCR and UACI values of the suggested systems in this paper are considered good values to avoid UACI and NPCR attacks and have a better image transmission that is more efficient and safer.

Table 2: NPCR and UACI Tests

Image Name		Scheme	[4]	[13]	[24]
UACI	Lena	34.4418	33.4974	-----	33.06
	C-man	34.6395	33.4974	31.1276	33.06
	Peper	34.5999	----	----	----
NPCR	Lena	99.9846	99.6037	----	99.46
	C-man	99.6125	99.6038	99.6063	99.46
	Peper	99.5755	----	----	----

5.1.3 Entropy

One of the essential parameters of statistical tests 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 in Equation (12):

$$H(X) = -\sum_{j=1}^{K} P_r(\chi_j) \log_2 P_r(\chi_j) \quad (12)$$

$$P_r(X = \chi_j) = \frac{1}{IS} \quad (13)$$

where X is the original image, $\Pr(\chi_j)$ *in eq* (13) 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.Table 3 shows the entropy values for encrypted test images of the encryption scheme. 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 pepper and Lena grey images utilized in an earlier study and described in Table 3.

Table 3: Entropy tests

Image Name	Encrypted Image				
	Original	Scheme	[4]	[13]	[24]
Lena	7.4808	7.9973	7.9973	7.9974	7.716
C-man	7.0097	7.9974	7.9971	7.9957	7.7
Peper	7.2260	7.99736			

5.1.4 Correlation coefficient analysis

A correlation coefficient (CC) is important for examining the three-dimensional relationship between two adjacent pixels. The pixels comprising the plain text picture 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. Equation (14) is the equation of CC as follows:

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

where E(.) represents the mean value function and $\alpha.$, $\beta.$ represents the two neighboring pixels.

The test results for the three-directions 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 pepper plaintext images and their encrypted image. Figure (3. a) shows the horizontal direction, Figure (3. b) shows the vertical direction, Figure (3. c) shows diagonal direction of Pepper's original image; while Figure (3. d) shows the horizontal direction, Figure (3. e) shows the vertical direction, Figure (3. f) shows the diagonal of the encrypted version of Pepper's image.

Table 4: Correlation coefficient test

Image Name		Encrypted image				
		original	Scheme	[4]	[13]	[5]
Lena	H	0.95348	-0.0182	−0.0031	----	0.00047
	V	0.98917	-0.0364	0.0084	----	−0.0391
	D	0.82862	0.0479	0.0108	----	0.00305
Camera man	H	0.9261	-0.0482	-0.0017	−0.0047	0.0021
	V	0.9781	-0.0579	-0.0143	0.0411	0.0019
	D	0.8956	-0.0876	0.0086	−0.066	-0.0002
Peper	H	0.8654	-0.0315	----	----	----
	V	0.7949	0.0567	----	----	----
	D	0.8967	-0.0623	----	----	----

5.1.5 Key analysis

The secure encryption system must employ key sensitivity 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 of 10^{-15}, the resulting cipher images, considered unrecognizable, when using different testing images such as Figure (4. a) pepper, Figure (4. b) camera-man and Figure (4. c) Lena.

The key space is the number of keys 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]. The proposed scheme has three parameters for the first ciphering stage: initial values of 3D-CM. Three of the initial values and two control parameters for 3D-HM, which are 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 be approximately $(10^{15})^{13} \approx 2^{630}$. Consequently, our system has sufficient key space to defend itself against exhaustive attacks. In Table 5, we can see how our scheme compares to others regarding key space.

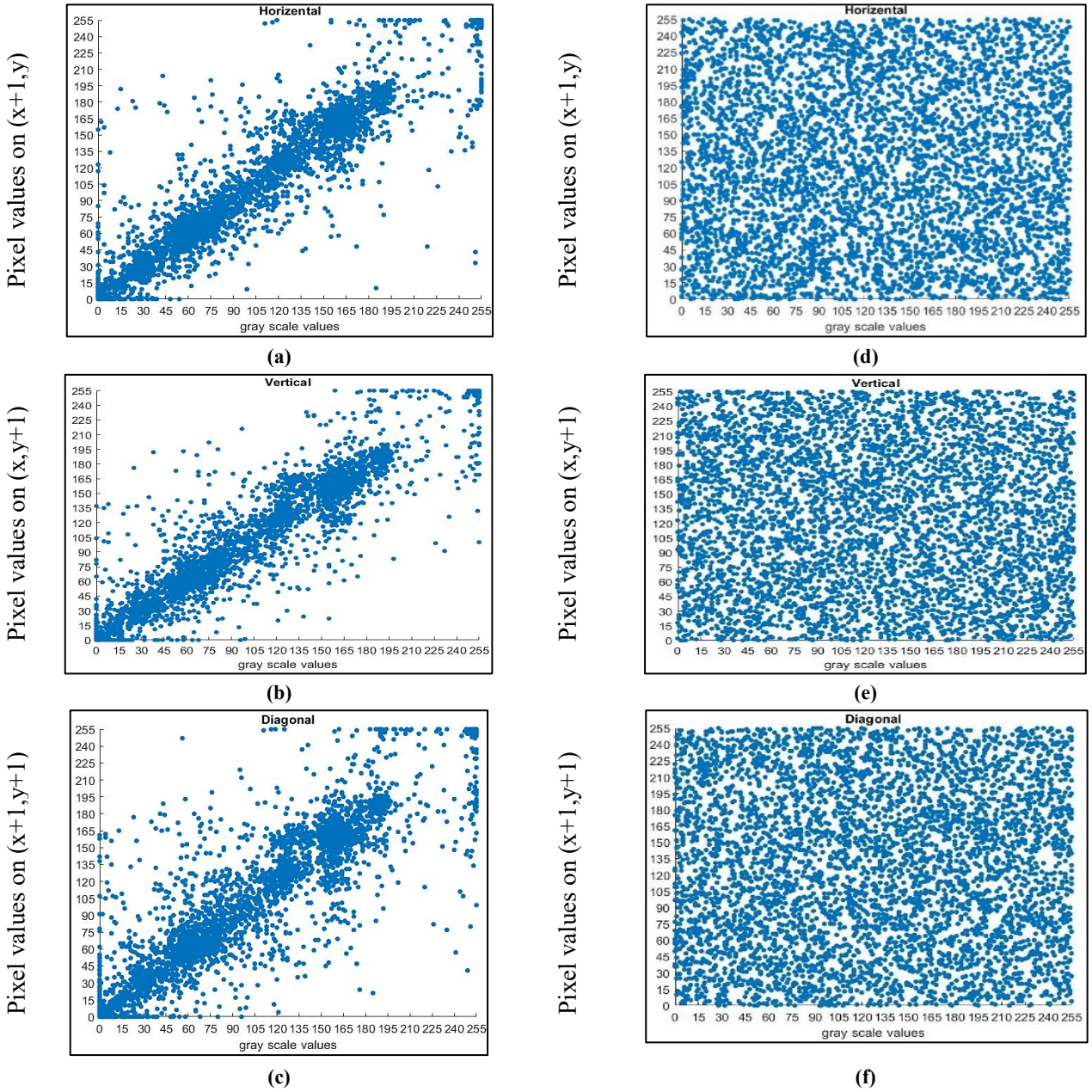


Figure 3: (a-f) Adjacent pixels correlation: a) horizontal direction, b) vertical direction, c) diagonal direction of Pepper's original image; d) horizontal direction, e) vertical direction, f) diagonal of the encrypted image

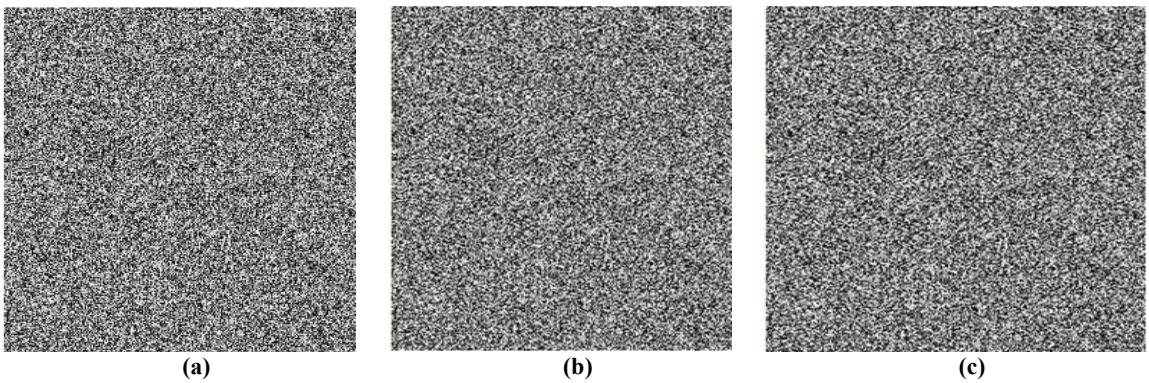


Figure 4: (a-c) Decrypted image at FFT-OFDM system with an incorrect key: a) pepper, b) camera-man and c) Lena

Table 5: Keyspace comparison

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

5.2 OFDM system analysis

Figure 5 illustrates variations of the proposed method's BER versus SNR variation plots for Figure (5.a) Pepper, Figure (5.b) camera-man, and Figure (5.c) Lena images in both Rayleigh and AWGN channels. According to the diagrams, the BER of the system has a fast slope down when using AWGN; it achieved high accuracy when SNR is lower than 10 dB, while for Rayleigh fading channel, the reconstructed image became accurate after 30 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 performs marginally better in situations with higher noise levels. When recovering the original images, the PSNR values increase 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 pepper image at the receiver side after passing through the communication channel. Figure (6.a) when SNR=20 dB, Figure (6.b) when SNR=30 dB; and Figure (6.c) when SNR=40 dB. This scheme demonstrates excellent efficiency; it can achieve high PSNR values at low and high SNRs. From this figure, the pepper image can be recognized and gets clear at SNR=10 dB.

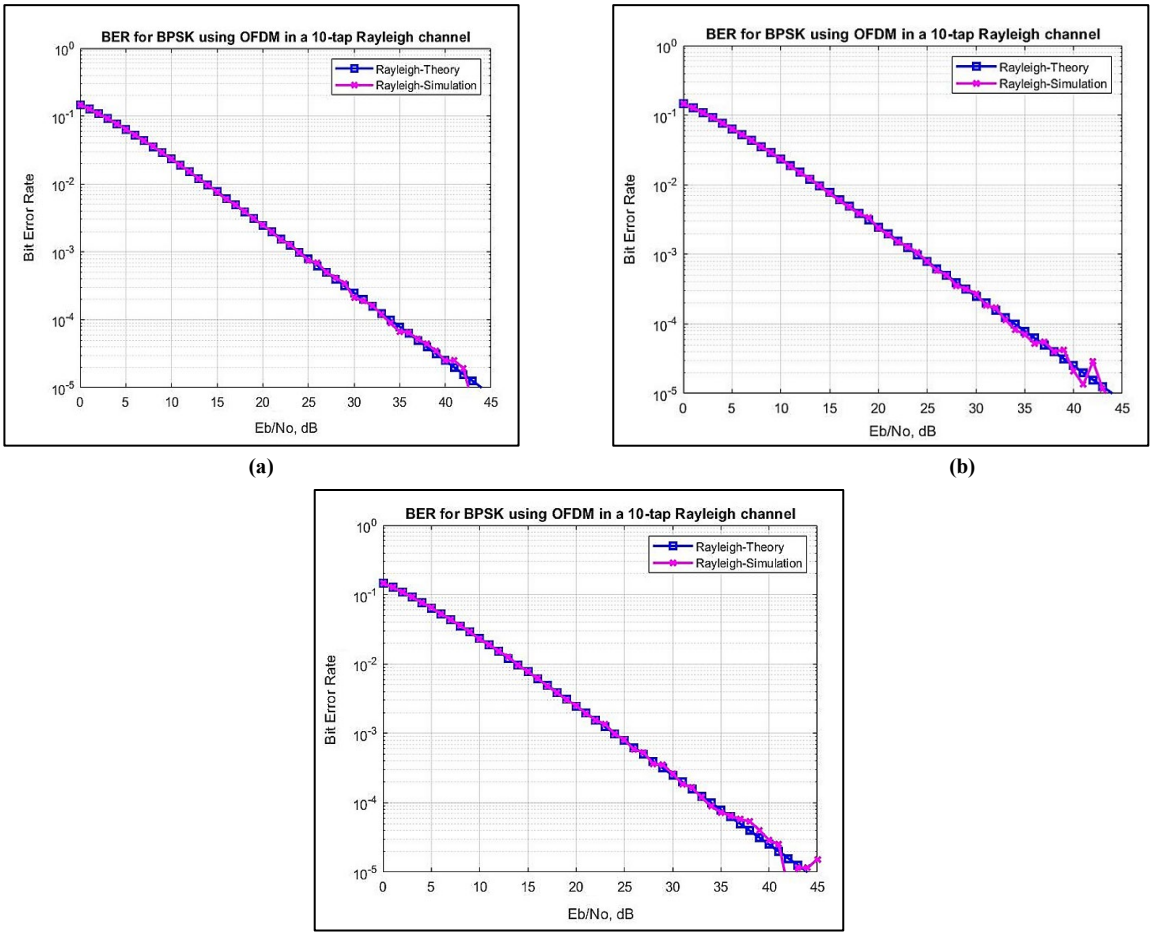


Figure 5: (a-c) BER versus SNR plots of OFDM system for a) a pepper image, b) camera-man, and c) Lena images

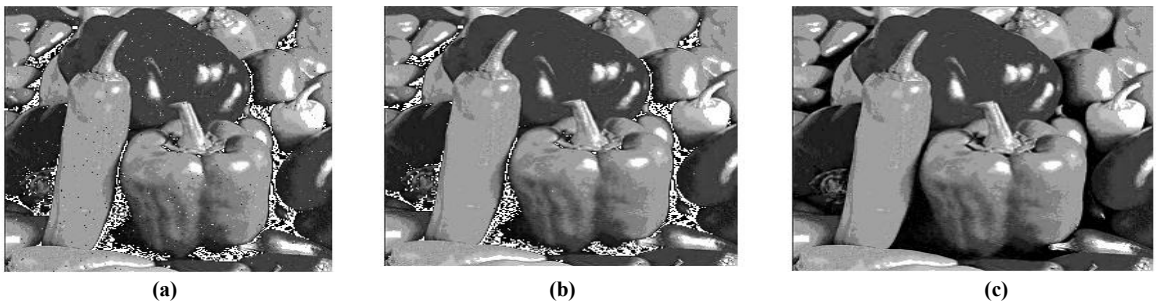


Figure 6: (a-c) The visual inspection quality of the decrypted pepper image at the OFDM system for different SNRs a) SNR=20 dB, b) SNR=30 dB; and c) SNR=40 dB

6. Conclusion

Simple and secure 3D chaotic maps have been proposed for encryption images and transmission with BPSK over the OFDM system communication channel. The proposed system was designed for efficient and safe image transmission through the Rayleigh fading channel. This system is proposed to achieve high security with low complexity and has an accurately 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; 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 be used as 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.

Author contributions

Conceptualization, J. Namuq. F. Hasan. and A. Ali.; methodology, J. Namuq.; software, F. Hasan.; validation, F. Hasan. and A. Ali.; formal analysis, J. Namuq.; investigation, J. Namuq.; resources, J. Namuq.; data curation, J. Namuq.; writing—original draft preparation, J. Namuq.; writing—review and editing, F. Hasan.; visualization, F. Hasan.; supervision, F. Hasan. and A. Ali.; project administration, F. Hasan. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of interest

The authors declare that there is no conflict of interest.

References

[1] Z. Chen, and G. Ye, An asymmetric image encryption scheme based on hash SHA-3, RSA, and Compressive Sensing, Optik, 267 (2022) 169676. https://doi.org/10.1016/j.ijleo.2022.169676

[2] R. S. Ali et al., Enhancement of the cast block algorithm based on novel S-box for image encryption, Sensors, 22 (2022) 8527. https://doi.org/10.3390/s22218527

[3] I. Mhaibes, H. Abood, M. and A. Farhan, Simple lightweight cryptographic algorithm to secure imbedded IOT devices, Int. J. Interact. Mobile Technol., (iJIM), 16 (2022) 98–113. 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., 78 (2019) 34323–34352. https://doi.org/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., 80 (2021) 2753–2772. https://doi.org/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., 6 (2019) 361–378. https://doi.org/10.1109/JIOT.2018.2846578

[7] J. Ayad, F. S. Hasan and A. H. Ali, Image encryption using One Dimensional Chaotic Map and transmission Through OFDM system, 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-7. https://doi.org/10.1109/ICCCNT56998.2023.10308260.

[8] S. A. Elsaid, E. R. Alotaibi, and S. Alsaleh, A robust hybrid cryptosystem based on DNA and hyperchaotic for images encryption, Multimedia Tools Appl., 82 (2022) 1995–2019. https://doi.org/10.1007/s11042-022-12641-5

[9] R. B. Naik, and U. A. Singh, A review on applications of chaotic maps in pseudo-random number generators and encryption, Ann. Data Sci., 2022. https://doi.org/10.1007/s40745-021-00364-7

[10] J. Ayad, F. S. 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. https://doi.org/10.1109/ICSSES58299.2023.10199452.

[11] M. Asha, T. P. Surekha, Development of OFDM technique for underwater communication in system on chip, Int. J. Syst. Assur. Eng. Manag., 14 (2023) 977-988. 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., 4 (2022) 230–245. https://doi.org/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, Int. J. Commun. Syst., 33 (2020) e4369. https://doi.org/10.1002/dac.4369

[14] 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. https://doi.org.10.1109/I4C57141.2022.10057774.

[15] D. S., Laiphrakpam, *et al.*, Encrypting multiple images with an enhanced chaotic map, IEEE Access, 10 (2022) 87844–87859. https://doi.org/10.1109/access.2022.3199738

[16] Q. Lai, et al., High-efficiency medical image encryption method based on 2D logistic-gaussian hyperchaotic map, Appl. Math. Comput., 442 (2023) 127738. https://doi.org/10.1016/j.amc.2022.127738

[17] S. Benaissi, N. Chikouche, and R.. Hamza, A novel image encryption algorithm based on hybrid chaotic maps using a key image, Optik, 272 (2023) 170316. https://doi.org/10.1016/j.ijleo.2022.170316

[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., 8 (2017). https://doi.org/10.1007/s13319-017-0145-8

[19] S. Eldin, Optimized OFDM Transmission of Encrypted Image Over Fading Channel, Sens. Imaging, 2014. https://doi.org/10.1007/s11220-014-0099-3

[20] Abdullah, H. A. and Abdullah, H. N., Secure image transmission based on a proposed chaotic maps, 2020.

[21] F. Hasan and M. Saffo, FPGA Hardware Co-Simulation of Image Encryption Using Stream Cipher Based on Chaotic Maps, Sens. Imaging, 21 (2020). https://doi.org/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., 66 (2017) 2114–2127. https://doi.org/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., 84 (2015) 475–521. https://doi.org/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., 10 (2020). https://doi.org/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)., 480 (2019) 403–419. https://doi.org/10.1016/j.ins.2018.12.048

[26] X. Qian et al., A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques, IEEE Access, 9 (2021) 61334–61345. 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, 10 (2022) 26257–26270. https://doi.org/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, 9 (2021) 37855–37865. https://doi.org/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, 9 (2021) 120596–120612. https://doi.org/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., 113 (2020) 241–261. https://doi.org/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, 10 (2022) 12966–12982. https://doi.org/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., 15 (2020) 1413–1429. https://doi.org/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, 9 (2021) 137635–137654. https://doi.org/10.1109/ACCESS.2021.3118377

[34] Z. Wang, Secure Image Transmission in Wireless OFDM Systems Using Secure Block Compression Encryption and Symbol Scrambling, IEEE, 7 (2019) 126985 - 126997. https://doi.org/10.1109/ACCESS.2019.2939266

[35] M. Helmy, et al. Chaotic encryption with different modes of operation based on Rubik's cube for efficient wireless communication, Multimed Tools Appl., 77 (2018) 27337-27361. https://doi.org/10.1007/s11042-018-5923-7