Received: September 28, 2022. Revised: October 25, 2022. 154

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

High Level Security of Image Transmission through STBC-COFDM System

Ahmed Kamil Hasan Al-Ali[1]* **Fadhil Sahib Hasan[2]**

[1] *Department of Electromechanical Engineering, University of Technology, Baghdad, Iraq*
[2] *Department of Electrical Engineering, Mustansiriyah University, Baghdad Iraq*
* Corresponding author's Email: ahmed.k.alali@uotechnology.edu.iq

Abstract: In this paper, the security of image transmission through space time block coding (STBC)-coded orthogonal frequency division multiplexing (COFDM) is enhanced using two stage algorithms. In the first-stage, the samples scrambling algorithm using one dimensional (1D) chaotic map is proposed. In the second stage, the bits scrambling algorithm using chaotic map is proposed. The sample scrambling algorithm is designed depending on three types of 1D chaotic maps that are logistic-sine-cosine (LSC), sine-tent-cosine (STC), and tent-logistic-cosine (TLC) maps. In the bit scrambling algorithm, the stream bits are XORed with a pseudo-random bit generator (PRBG) produced by these chaotic maps using threshold method. Simulation results demonstrate that the image is retrieved with high quality for STBC-COFDM system and low signal to noise ratio (SNR). The image is unrecovered when the correct key is unavailable. For one level of security, the system using TLC chaotic map has the best performance compared with other chaotic maps. The bit error rate (BER) performance of the suggested system achieved 10^{-4} at SNR=1, and 2 dB for (TLC, LSC) and STC, respectively. For two stages of security, the proposed system using STC chaotic map improves the BER performance with a gain of about 2 dB at BER=10^{-4} compared with one stage of security.

Keywords: Image encryption, Low-density parity check coded, One dimensional chaotic map, Orthogonal frequency division multiplexing, Space time block code.

1. Introduction

The space time block coding (STBC) is a famous system to represent multiple input multiple output diversity techniques, it was first proposed by Alamouti [1], with a simple decoder design [2]. STBCs have been used in various applications, such as wireless digital communications [3] and wireless local area networks [4]. Various wireless transmission systems use orthogonal frequency division multiplexing (OFDM) system, such as image processing, and digital video broadcasting [5–7]. OFDM system is widely used in wireless transmission systems because it provides high resistance to noise and multipath fading channel. Also, it has efficient modulation/demodulation and high spectral efficiency by using inverse fast Fourier transform (IFFT) and fast Fourier transform (FFT). The quality of the image signal is degraded when it is transmitted through a multipath fading channel. The OFDM solves this issue by splitting frequency selective channel into various multiple frequency band channels and improves the bit error rate and quality performance of the system [8]. The Combination of STBC and OFDM systems achieved a significant improvement in the BER performance under the multipath fading channel [9].

To increase the improvement of the BER performance of the STBC-OFDM system, Low-density parity check coded (LDPC) is used [10]. The LDPC is a linear block code that achieves better BER performance compared with turbo code [5]. Furthermore, LDPC can be used to decode the signal in parallel and make short-length LDPC codes which have advantages in a modern communication system with high performance in real-time applications [11]. Different algorithms are suggested in previous works for combining OFDM modulation and LDPC to enhance the BER

performance [12], [13]. While all of these above proposed systems are not included the transmitted image on their corresponding system.

Nowadays, various image signals are generated and sent via different network systems [14]. Among the images sent across networks, security techniques are required to prevent the third party to access the transmitted image [15]. Image encryption is a significant method that changes unsecure image into a noise-like image [16], [17]. Confusion diffusion algorithms are well-known encryption algorithms [18], [19]. In the confusion technique, the adjacent image pixels are randomly separated, while in the diffusion technique small change in the original image is spreading [20]. In [21], combined compressive sensing (CS) and fractional wavelet transform (FrWT) for private image transmission is proposed. In [22], 2D Zaslavsky Chaotic Map is proposed for confusion and diffusion the image signal for IOT devices. In [23], 3D coupled map lattice is proposed to generate pseudo random bit generator and used it to encrypt the image signal for IOT applications. All these above systems are not included the transmission of encrypted image through wireless communication channel. We need to select the high security methods and compatible connections with COFDM system.

Various papers have studied the combination of a secure image with OFDM system. In [24], a compressive sensing technique is used to encrypt the image signal and transmitted through BPSK-OFDM system. The limitations of this paper are the complexity of detection the compressed signal using greedy algorithm and transformation of spare signal. Furthermore, the BER of the proposed system under Rayleigh fading channel required high signal to noise ratio (SNR) greater than 25 dB to achieve BER about 10^{-4}. In [25], DES, AES, and Rubik's encryption algorithms were used to scramble the image signal and sent through MIMO OFDM system. In this paper, one level of security was included and AWGN channel was considered to test the secure image transmission system. Furthermore, channel coding was not considered here to increase the reliability under Rayleigh fading channel. In [26], robust image transmission through interleaved LDPC OFDM system was proposed. In this system, the PAPR reduction is enhanced using chaotic interleaver and LDPC code.

The main contribution of this paper is to propose a novel secure image transmission system based on STBC coded OFDM and LDPC. To improve the security of the proposed image transmission system, two levels of sample and bit scrambling techniques based on a chaotic system are used to encrypt the image. In the sample scrambling stage, three types of chaotic maps, including logistic-sine-cosine (LSC), sine-tent-cosine (STC), and tent-logistic-cosine (TLC), are examined in the proposed scrambling algorithm. In the bit scrambling stage, the pseudo random bit generator is produced using first order dynamic system. The encrypted image is passed through LDPC coding to improve the burst error of the channel and increase the reliability of the system. After that, the information is sent through the STBC-OFDM system.

This paper is organized as follows. Sample and bit scrambling techniques using chaotic system are presented in section 2. The system model is described in section 3. The simulation results are discussed in section 4. Section 5 presents a comparison with conventional image secure over MIMO OFDM system. Sections 6 and 7 describe the key space and key randomness analysis, respectively. Finally, the conclusion and future work are depicted in section 8.

2. Sample and bit scrambling techniques using chaotic system

2.1 Sample scrambling technique

The following procedure is used to scramble the plain image P of size N × M [15]:

Step 1: The chaotic sequence G is generated using one of the following chaotic maps
A. LSC map
The LSC map can be defined as

$$x_{i+1} = cos\,(\pi(4s\,x_i(1-x_i) + (1-s)\gamma - 0.5)) \quad (1)$$

where $\gamma = \sin(\pi x_i)$
B. STC map
The STC map can be represented as

$$x_{i+1} = \begin{cases} cos\big(\pi(\rho + 2(1-s)x_i - 0.5)\big), \\ \qquad x_i < 0.5; \\ cos\big(\pi(\rho + 2(1-s)(1-x_i) - 0.5)\big), \\ \qquad x_i \geq 0.5 \end{cases} \quad (2)$$

where $\rho = s\sin(\pi x_i)$.
C. TLC map
The TLC can be represented as

$$x_{i+1} = \begin{cases} cos\big(\pi(2sx_i + \theta)\big), & x_i < 0.5 \\ cos\big(\pi(2s(1-x_i) + \theta)\big), & x_i \geq 0.5 \end{cases} \quad (3)$$

where $\theta = 4(1 - s)x_i(1 - x_i) - 0.5$, the parameter s∈[0,1], G∈ $\mathbb{R}^{4L^2+1}$, and the value of L can be computed as:

$$L = min\{\lfloor\sqrt{M}\rfloor, \lfloor\sqrt{N}\rfloor\} \quad (4)$$

where $\lfloor . \rfloor$ is the largest integer value.

Step 2: The A, B, C, and D matrices are calculated according to the following equations:

$$A = G_{1:L^2}, B = G_{L^2+1:2\,L^2}, C = G_{2\,L^2+1:3\,L^2}, D = G_{3\,L^2+1:4\,L^2} \quad (5)$$

Step 3: The A, B, C, and D matrices are sorted using sort fuction as following:

$$[A', IA] = sort(A), [B', IB] = sort(B), [C', IC] = sort\,(C),\ [D', ID] = sort(D) \quad (6)$$

where A′, B′, C′ and D′ are A_{IA}, B_{IB}, C_{IC} and D_{ID}, respectively.

Step 4: finding the matrices O∈ $N^{L^2\times L^2}$ and Q∈ $N^{L^2\times L^2}$according to

$$O_{i,j} = IA_m\,, \qquad (i, j = 1{:}\,L^2)$$

where $m = \big((i + IB(j) - 1) mod\ L^2\big) + 1$

$$Q_{i,j} = IC_n \quad (7)$$

where $n = \big((i + ID(j) - 1)\ mod\ L^2\big) + 1$

Step 5: the scrambled matrix T can be computed as

$$T\big(\alpha(i,j), \beta(i,j)\big) = p(i,j),\ i,j = 1{:}\,L^2 \quad (8)$$

where

$$\alpha(i,j) = \left(\left\lfloor\frac{O_{i,j} - 1}{L}\right\rfloor \times L\right) + \left(\left\lfloor\frac{Q_{O_{i,j},j} - 1}{L}\right\rfloor + 1\right)$$

$$\beta(i,j) = ((O_{i,j} - 1) mod L) \times L + ((Q_{O_{i,j},j} - 1)\ mod\ L + 1))$$

2.2 Bit scrambling algorithm

The pseudo-random bit generator (PRBG) is generated from a first-order dynamic system with one dimension using the following procedure.

1. Generate one dimension chaotic sequence using the following equations [27].

$$x_{n+1} = \begin{cases} \frac{h}{p_1} x_n & x_n \in (0, p_1] \\ \frac{h}{L_1 - p_1}(L_1 - x_n) & x_n \in (p_1, L_1] \\ \frac{h}{p_2 - L_1}(x_n - L_1) & x_n \in (L_1, p_2] \\ \frac{h}{L_2 - p_2}(L_2 - x_n) & x_n \in (p_2, L_2] \end{cases} \quad (9)$$

where L_1, L_2, p_1, p_2, h ∈ $\mathbb{R}^+$ are the setting parameters of the dynamic system.

2. The PRBG is generated by the thresholding method according to the following equation

$$PRBG_n = x_n > Threshold \quad (10)$$

Where

$$Threshold = \frac{(max\ (x_n) - min\ (x_n))}{2} \quad (11)$$

3. The stream bit un is XORed with PRBGn to produce the ciphered message according to the following equation

$$\acute{u_n} = u_n \oplus PRBG_n \quad (12)$$

where ⊕ is XOR operation.

3. System model

Fig. 1 describes the proposed transmitter model of secure image transmission through the STBC-COFDM system. Firstly, the color image is encrypted for first level security using the chaotic scrambling technique as explained in section 2. The message is converted to stream bits and encrypted by the second level security using a stream cipher system with a chaotic PRBG system. The binary streams are decomposed into two binary sequences using a serial to parallel (S/P) converter. Each sequence is applied to half-rated irregular LDPC codes with LDPC matrix of size 696×1392. Each output of the LDPC encoders (S_1, S_2) is 1392 bits. After that, the messages are passed through binary phase shift keying (BPSK) digital modulation. The IFFT is applied to each BPSK modulated signal to produce OFDM modulated signals (s_1,s_2). According to Table 1, the two sequences are encoded by

Table 1. The transmitted STBC sequences

Time	Antenna 1	Antenna 2
T	s_1	s_2
t+T	$-s_2^*$	s_1^*

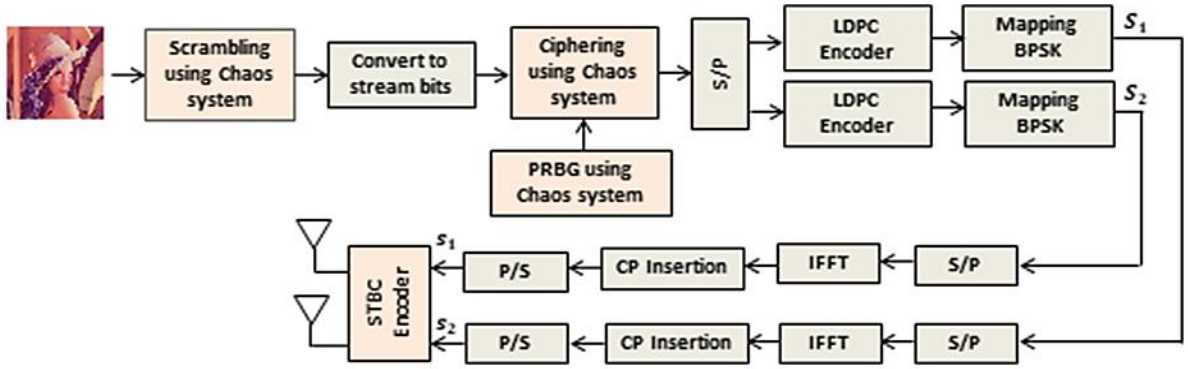

Figure. 1 The proposed transmitter model of secure image transmission through the STBC-COFDM system

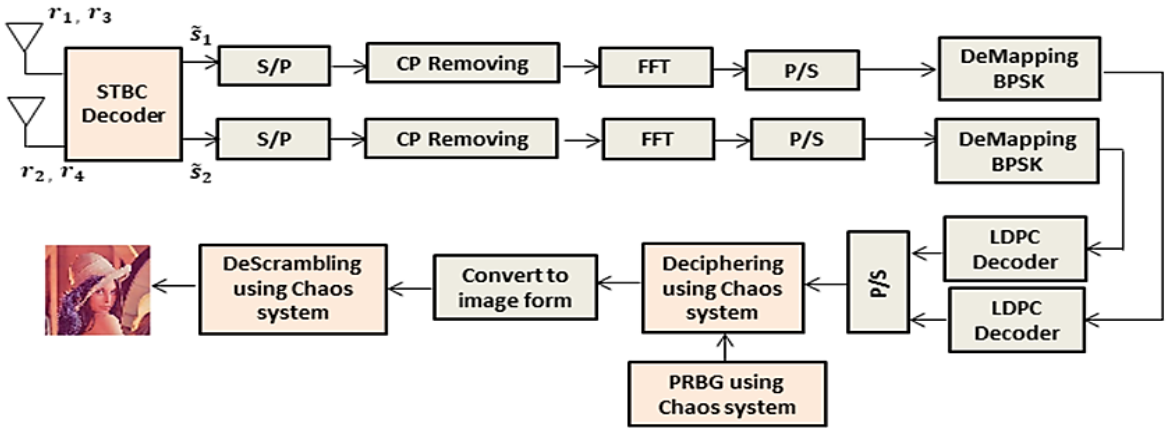

Figure. 1 The proposed receiver model of secure image transmission through the STBC-COFDM system

applying Alamouti encoder [1] to the modulated signals (s_1, s_2).

Fig. 2 shows the proposed receiver model of secure image transmission through the STBC-COFDM system. The channel matrix $H \in \mathbb{C}^{2\times 2}$ ($H = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix}$) is generated by an i.i.d. Gaussian sources with zero-mean and half σ^2. The received sequences at the two receiver antennas can be expressed as:

$$\begin{aligned} r_1 &= h_{11}s_1 + h_{12}s_2 + n_1 \\ r_2 &= -h_{11}s_2^* + h_{12}s_1^* + n_2 \\ r_3 &= h_{21}s_1 + h_{22}s_2 + n_3 \\ r_4 &= -h_{21}s_2^* + h_{22}s_1^* + n_4 \end{aligned} \tag{13}$$

where n_1,n_2, n_3 and n_4 are Additive white Gaussian noise sequences with zero mean and σ^2 variance. The maximum likelihood (ML) detector [1] is applied to the received sequences to recover the original transmitted sequences:

$$\begin{aligned} \tilde{s}_1 &= h_{11}^* r_1 + h_{12} r_2^* + h_{21}^* r_3 + h_{22} r_4^* \\ \tilde{s}_2 &= h_{12}^* r_1 - h_{11} r_2^* + h_{22}^* r_3 - h_{21} r_4^* \end{aligned} \tag{14}$$

The FFT is applied to each STBC decoded signal ($\tilde{s}_1, \tilde{s}_2$) to produce OFDM demodulated signals ($\tilde{S}_1, \tilde{S}_2$). The recovered binary sequences are produced by taking BPSK demapping and each sequence is passed through the minimum sum LDPC decoder algorithm [28] to recover the secure binary sequence. The two level decryption algorithms are applied to LDPC decoded sequence to recover the original transmitted image signal.

4. Simulation results

In these experimental results, the 256×256 color Lenna image is applied to the STBC-COFDM system with number of transmitter and receiver antennas are 2×2. The FFT size is 256 with 25% cyclic prefix guard. LDPC is used as channel coding with rate=1/2. Three types of chaotic maps, including (LSC, STC, and TLC) are used in scrambling techniques. Also, these chaotic maps are used to generate the PRBG. MATLAB program version R2019a is used to simulate the proposed system. Table 2 shows experimental parameters.

Figs. 3 to 5 illustrate the root mean square error (RMSE), peak signal to noise ratio (PSNR), and BER of scrambling techniques only with correct and incorrect keys, respectively. From these figures, they can be concluded that the image is undetected when the incorrect key is used. The TLC chaotic map achieved the best performance results

Received: September 28, 2022. Revised: October 25, 2022.

Table 2. Experimental parameters.

Lenna image	256×256×3
Modulation /Order	BPSK/2
Channel coding	LDPC with rate= ½
No. of transmitting and receiving antennas	2×2
Channel model	2×2 STBC channel, AWGN
FFT size	256 with 25% cyclic prefix guard
Types of chaotic maps used	LSC, STC, and TLC
Quality measures	PSNR, RMSE
Language of program	MATLAB version R2019a

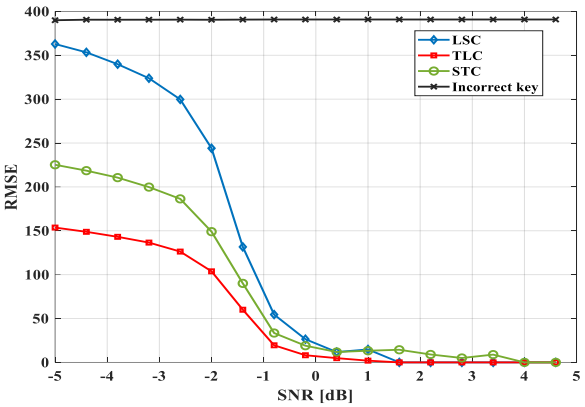

Figure. 3 RMSE comparisons for three chaotic maps versus SNR with correct and incorrect keys

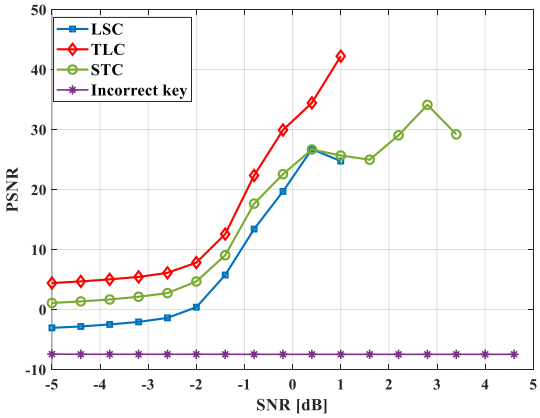

Figure. 4 PSNR comparisons for three chaotic maps versus SNR with correct and incorrect keys

compared with other chaotic maps when the correct key is used. The LSC chaotic map achieved the worst performance results compared with other chaotic maps when the correct key is used. Also, the BER performance of the proposed system achieved 10^{-4} at SNR=1, and 2 dB for (TLC, LSC) and STC, respectively.

Figs. 6 to 8 illustrate the RMSE, PSNR, and BER comparisons between one and two levels of security, respectively. From these figures, they can

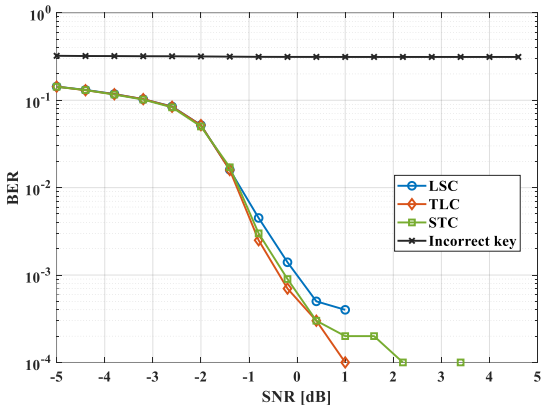

Figure 5. BER comparisons for three chaotic maps versus SNR with correct and incorrect keys

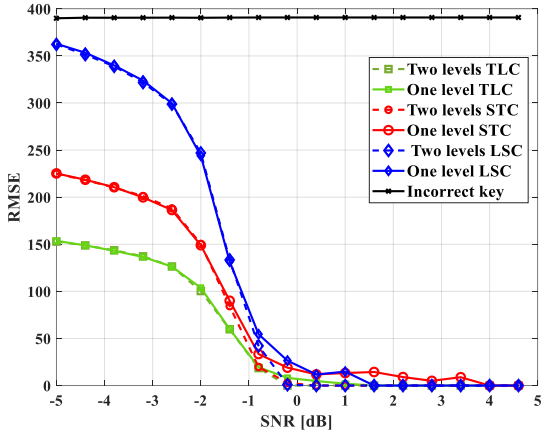

Figure. 6 RMSE comparisons between one and two levels of security for three chaotic maps versus SNR with correct and incorrect keys

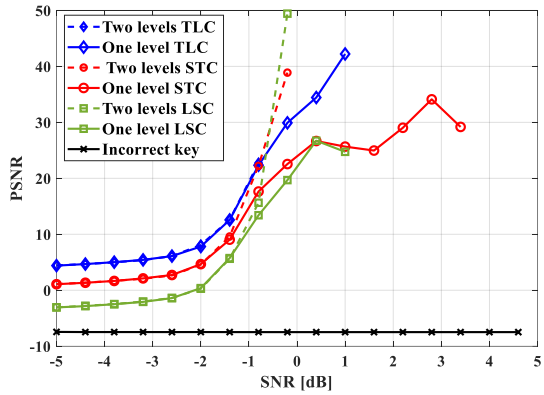

Figure. 7 PSNR comparisons between one and two levels of security for three chaotic maps versus SNR with correct and incorrect keys

be concluded that the image is undetected when the incorrect key is used. In general, the results of two levels of security have the best performance compared with one level of security for the same chaotic map. The two levels of security of STC

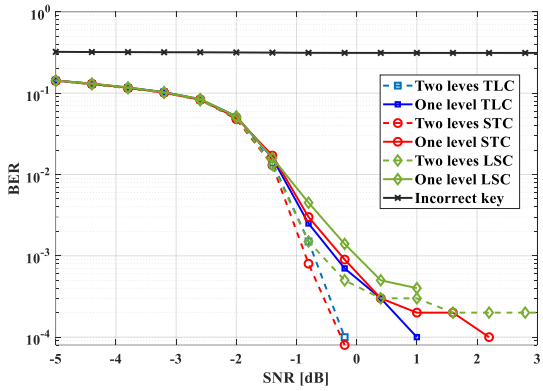

Figure. 8 BER comparisons between one and two levels of security for three chaotic maps versus SNR with correct and incorrect keys

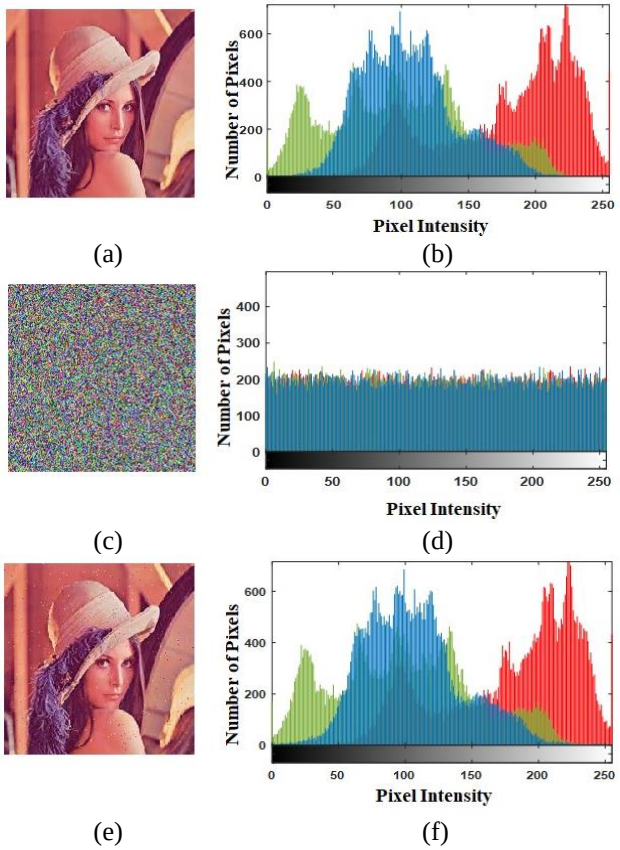

Figure. 9 Image histogram results: (a) original image, (b) original image histogram, (c) encrypted image, (d) encrypted image histogram, (e) recovered image at SNR=-1 dB, and (f) histogram of the recovered image

chaotic map enhanced the BER performance with a gain about 2 dB at BER=10^{-4} compared with one level of security of STC. The two levels of security based on LSC chaotic map achieved the worst performance results compared with other chaotic maps when the correct key is used. The eavesdropper with incorrect keys cannot be detected the information bits. The best RMSE result is achieved for TLC chaotic map.

Fig. 9 shows the original encrypted image histogram, and recovered image at SNR= -1 dB, respectively. Fig. 9(a) shows original image. The histogram of the original image is shown in Fig. 9(b). Fig. 9(c) shows the encrypted image. The encrypted histogram image is shown in Fig. 9(d). Figs. 9(e) and 9(f) show the recovered image and the histogram of the recovered image, respectively.

It can be noted that the histogram of the encrypted image has a uniform distribution which proved security of the system. The original image can be recovered with the same histogram and distribution of pixels.

5. Comparison with conventional secure image over MIMO-OFDM system

The comparisons of BER and PSNR for the proposed two levels of image encryption over STBC-COFDM system and CryptoMIMO–OFDM (2×2) systems [25] with corresponding SNRs for grey cameraman image of size 256 × 256 are illustrated in Tables 3 and 4, respectively. From these tables, we concluded that the proposed system improved the performance of secure image over the crypto MIMO-OFDM system for different values of SNR. At SNR=1 dB, the BER performance of the proposed system approaches zero and the value of PSNR is infinity, while the conventional MIMO-OFDM systems [25] have BER=0.042 and PSNR= 8 or 10 dB, respectively at SNR=1 dB. This is proved that the proposed systems have faster convergent to the desired performance. Table 5 shows another comparison of PSNR and BER of the proposed method with references [21], [23], and [24]. From this table, it is clear that the proposed method outperforms to [24] in both BER and PSNR, where achieves SNR gain about 24 dB at BER = 10^{-4} and PSNR gain about 16. For [21] and [23] the comparison is made only on PSNR since these references using only image encryption without transmission. The proposed system shows good performance of image transmission.

6. Key space

Key space is crucial for a cryptosystem. It needs to be large enough to resist a brute-force attack. In this system, we have two secret keys (k_1 and k_2) which contain the parameters of the employed chaotic maps (CMs), i.e., $k_1 = (x_0, s)$ for LSC, STC, TLC maps and k2 = (x_0, L_1, L_2, p_1, p_2, h) for one-dimensional chaotic system. According to IEEE floating-point precision [29], the precision of each

Table 3 Comparison of BER versus SNR for cameraman image

SNR	Two levels security of STBC-COFDM System with LSC	Two levels security of STBC-COFDM System with STC	Two levels security of STBC-COFDM System with TLC	2× 2 MIMO-OFDM AES [25]	2× 2 MIMO-OFDM DES [25]	2× 2 MIMO-OFDM Rubik's Cube [25]
-2	0.0498	0.0479	0.0491	-	-	-
-1	0.0015	0.013	0.014	-	-	-
0	0.0003	0.0008	0.0001	0.0453	0.0484	0.0493
1	0.0002	0.00008	0	0.0422	0.0426	0.0423

Table 4. Comparisons of PSNR versus SNR for cameraman image

SNR	Two levels security of STBC-COFDM System with LSC	Two levels security of STBC-COFDM System with STC	Two levels security of STBC-COFDM System with TLC	2× 2 MIMO-OFDM AES [25]	2× 2 MIMO-OFDM DES [25]	2× 2 MIMO-OFDM Rubik's Cube [25]
-2	0.2794	4.5866	8.1008	-	-	-
-1	15.6376	9.612	12.597	-	-	-
0	49.4218	38.8846	50	8.38	8.43	10.28
1	Inf	Inf	Inf	8.43	8.63	10.42

Table 5. Comparisons of PSNR and BER

	Two levels security of STBC-COFDM System with STC	Two levels security of STBC-COFDM System with TLC	[24]	[21]	[23]
SNR	-0.2 dB	1 dB	>25 dB	-	-
PSNR	50	45	≈ 29	35.6631	50

Table 6. NIST tests results for $PRBG_n$

NIST Tests	Frequency	Block Frequency M=128	Runs	Longest Runs of Ones	Rank	FFT	Overlapping Templates All One	Nonoverlapping Templates	Universal Statistical	Linear Complexity	Serial	Entropy	Cumulative Sum
$PRBG_n$	0.6531	0.9932	0.0453	0.1230	0.2561	0.6562	0.1542	0.4532	0.2343	0.9731	0.324	0.087	0.542

parameter is larger than 10^{-15}. For CM's parameters, the precision level is about 10^{-15}. Therefore, the key space size can be approximated as $(10^{15})^8 = 10^{120} \approx 2398$. This key space is big enough against brute-force attack. The key space of the proposed system is bigger than a minimal standard [30] of key space 2100.

7. Key randomness analysis

The randomness of the key system is analyzed using the Statistical Randomness Test Suite that is available by National Institute of Standards and Technology (NIST) [31] to decide if either the key generated is a good random key or not. The NIST randomness test suite contains 15 measures as shown in Table 6. All these 15 functions are applied to the PRBG used in the ciphering system. The generated binary bits from the proposed PRBG are exceeding these 15 tests successfully as shown in Table 5, where all test values are greater than the threshold of 0.01.

8. Conclusion

A new two-level image secure transmission system has been proposed in this paper. This system is based on combining sample and bit scrambling techniques to enhance the performance of the image secure system. Three chaotic maps are tested to encrypt the unsecure image, including (STC, TLC, and LSC). In the first security level, the unsecure image is scrambled using three chaotic maps. In the second security level, the scrambled image is

encrypted using three chaotic maps. Experimental results show that two levels of security based on the STC chaotic map improved the performance of the image security transmission system compared with other chaotic maps.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first. The supervision, review of work and project administration, have been done by second author.

Reference

[1] S. M. Alamouti, "A simple transmit diversity technique for wireless communications", *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 8, pp. 1451–1458, 1998.

[2] H. Jafarkhani, "A quasi-orthogonal space-time block code", *IEEE Transactions on Communications*, Vol. 49, No. 1, pp. 1–4, 2001.

[3] Y. Djemamar, S. Ibnyaich, and A. Zeroual, "Full-rate space-time block code for four transmit antennas with linear decoding", *Jordanian Journal of Computers and Information Technology*, Vol. 6, No. 3, pp. 202–214, 2020.

[4] P. Nikhate, A. R. Deshmukh, and S. Choudhari, "Study and analysis in MIMO wireless channel for STBC and equalization techniques by using MATLAB", In: *Proc. of 2021 Third International Conf. on Inventive Research in Computing Applications (ICIRCA)*, pp. 422–429, 2021.

[5] M. Yang, C. Bian, and H. S. Kim, "OFDM-guided deep joint source channel coding for wireless multipath fading channels", *IEEE Transactions on Cognitive Communications and Networking*, Vol. 8, No. 2, pp. 584–599, 2022.

[6] B. Vaseghi, S. S. Hashemi, S. Mobayen, and A. Fekih, "Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems", *IEEE Access*, Vol. 9, pp. 21332–21344, 2021.

[7] J. Patel and M. Seto, "Live RF image transmission using OFDM with RPi and PlutoSDR", In: *Proc. of 2020 IEEE Canadian Conf. on Electrical and Computer Engineering (CCECE)*, pp. 1–5, 2020.

[8] Z. Wang, Y. Hou, and Z. Wang, "Compressed image transmission in precoded OFDM VLC systems", *Research Square*, pp. 1–23, 2022.

[9] Y. Djemamar, S. Ibnyaich, and A. Zeroual, "Space-time block coding techniques for MIMO 2× 2 system using walsh-hadamard codes", *Journal of Information and Communication Convergence Engineering*, Vol. 20, No. 1, pp. 1–7, 2022.

[10] N. E. Maammar, S. Bri, and J. Foshi, "Performances concatenated LDPC based STBC-OFDM system and MRC receivers", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 1, pp. 622–630, 2018.

[11] L. Deng, Z. Shi, O. Li, and J. Ji, "Joint coding and adaptive image transmission scheme based on DP-LDPC Codes for IoT scenarios", *IEEE Access*, Vol. 7, pp. 18437–18449, 2019.

[12] A. E. Taleby, Y. Chaibi, M. Boussetta, A. Allouhi, and M. Benslimane, "A novel fault detection technique for PV systems based on the K-means algorithm, coded wireless Orthogonal Frequency Division Multiplexing and thermal image processing techniques", *Solar Energy*, Vol. 237, pp. 365–376, 2022.

[13] O. Muta and Y. Akaiwa, "Peak power reduction method based on structure of parity-check matrix for LDPC coded OFDM transmission", In: *Proc. of 2007 IEEE 65th Vehicular Technology Conf.*, pp. 2841–2845, 2007.

[14] V. M. Schönberger and K. Cukier, *Big data: A revolution that will transform how we live work and think*, Boston, MA, USA: Houghton Mifflin, 2013.

[15] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption", *Information Sciences*, Vol. 480, pp. 403–419, 2019.

[16] C. Li, D. Lin, and J. Lu, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits", *IEEE MultiMedia*, Vol. 24, No. 3, pp. 64–71, 2017.

[17] C. Li, D. Lin, J. Lu, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography", *IEEE MultiMedia*, Vol. 25, No. 4, pp. 46–56, 2018.

[18] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, and B. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption", *Signal*

Processing, Vol. 142, pp. 340–353, 2018.

[19] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion", *Signal Processing*, Vol. 144, pp. 134–144, 2018.

[20] Y. G. Yang, J. Tian, H. Lei, Y. H. Zhou, and W. M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata", *Information Sciences*, Vol. 345, pp. 257–270, 2016.

[21] A. K. Chatamoni, R. N. Bhukya, and P. R. Jeripotula, "A Novel Approach based on Compressive Sensing and Fractional Wavelet Transform for Secure Image Transmission", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 4, pp. 11-21, 2021, doi: 10.22266/ijies2021.0831.02.

[22] A. H. Mohammed, A. K. Shibeeb, and M. H. Ahmed, "Image Cryptosystem for IoT Devices Using 2-D Zaslavsky Chaotic Map", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 2, pp. 543-553, 2022, doi: 10.22266/ijies2022.0430.48.

[23] M. S. Oudah and A. T. Maolood, "New Pseudo-Random Key Generator for IoT-security Model Based on a Novel 3D Coupled Map Lattice", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 5, pp. 139-150, 2022, doi: 10.22266/ijies2022.1031.13.

[24] Z. Wang, "Secure image transmission in wireless OFDM systems using secure block compression-encryption and symbol scrambling", *IEEE Access*, Vol. 7, pp. 126985–126997, 2019.

[25] K. Dharavathu and S. A. Mosa, "Efficient transmission of an encrypted image through a MIMO–OFDM system with different encryption schemes", *Sensing and Imaging*, Vol. 21, No. 1, 2020.

[26] N. F. Soliman, Y. Albagory, M. A. M. Elbendary, W. A. Hanafy, E. S. M. E. Rabaie, S. A. Alshebeili, and F. E. A. E. Samie, "Chaotic interleaving for robust image transmission with LDPC coded OFDM", *Wireless Personal Communications*, Vol. 79, No. 3, pp. 2141–2154, 2014.

[27] R. A. Elmanfaloty and E. A. Bakr, "An image encryption scheme using a 1D chaotic double section skew tent map", *Complexity*, Vol. 2020, pp. 1–18, 2020.

[28] I. W. Yun, H. Lee, and J. T. Kim, "An alternative approach obtaining a normalization factor in normalized min-sum algorithm for low-density parity-check code", *Wireless Communications and Mobile Computing*, Vol. 2018, pp. 1–7, 2018.

[29] N. Whitehead and A. F. Flore, "Precision & performance: Floating point and IEEE 754 compliance for NVIDIA GPUs", 2011. https://developer.download.nvidia.com/assets/cuda/files/NVIDIA-CUDA-Floating-Point.pdf (Accessed Jan. 27, 2017).

[30] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", *International Journal of Bifurcation and Chaos*, Vol. 16, No. 08, pp. 2129–2151, 2006.

[31] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", *National Institute of Standards and Technology, Gaithersburg, MD*, 2010.