



BER Performance Improvement of Dual Chaotic Maps Based on STBC Communication System

Lwaa Faisal Abdulameer *

U. Sripati**

Muralidhar Kulkarni***

*Department of Information and Communication/ Al-khwarizmi College of Engineering/ University of Baghdad/ Iraq

** ,***Electronics and Communication Engineering Department/ NITK. Mangalore/ India

*Email: lwaa@kecbu.uobaghdad.edu.iq

**Email: sripati_achary@yahoo.co.in

***Email: mkuldc@gmail.com

(Received 15 May 2022; Accepted 4 October 2022)

<https://doi.org/10.22153/kej.2022.10.001>

Abstract

Sensitive information of any multimedia must be encrypted before transmission. The dual chaotic algorithm is a good option to encrypt sensitive information by using different parameters and different initial conditions for two chaotic maps. A dual chaotic framework creates a complex chaotic trajectory to prevent the illegal use of information from eavesdroppers. Limited precisions of a single chaotic map cause a degradation in the dynamical behavior of the communication system. To overcome this degradation issue in, a novel form of dual chaos map algorithm is analyzed. To maintain the stability of the dynamical system, the Lyapunov Exponent (LE) is determined for the single and dual maps. In this paper, the LE of the single and dual maps have been computed numerically. Increasing the dynamical behavior of the system by using more complex chaotic maps leads to inferiority in the overall system performance. So, in this work, the BER performance for the dual and single chaotic maps by exploiting the benefits of a hybrid Chaos Shift Keying-Multiple-Input-Multiple-Output (CSK-MIMO) communication system has been investigated. The results show that the dual tent map has more randomness, whereas the single logistic map has the least randomness. As well as the CSK-MIMO gives an outstanding BER performance when it compared with the SISO system which helps in reducing the system's inferiority.

Keywords: Chaotic technique, dual, Lyapunov Exponent, STBC.

1. Introduction

A chaotic waveform is characterized as being deterministic, non-periodic, and very sensitive to any change in initial conditions, i.e., initializing the system with a slight difference in initial conditions generates a new sequence completely different from the original signal [1]. So, to encrypt sensitive data, a chaotic technique can be utilized to produce a key stream with high randomness. In any case, a single chaotic map is attackable to be descended by chaotic reconstruction since it has a simple structure and weak control boundaries. Dual

dimensional chaos has a complicated structure and more parameters [2,3].

To adjust these two factors, a dual chaotic system can be considered [4]. In this paper, dual-chaotic systems that consist of two one-dimensional tent and logistic maps have been designed.

The chaotic attractor can be characterized by measuring the degree of sensitivity to initial conditions. Lyapunov Exponents (LEs) describe the increase of very small perturbations in different directions of the state space on a logarithmic scale, when at least one LE is positive, the attractor under

This is an open access article under the [CC BY](https://creativecommons.org/licenses/by/4.0/) license:



realization characterize by sensitive dependence on initial conditions property and this is termed chaotic [5].

Chaos is utilized in many research areas, such as engineering, mathematics, chemistry, and biology. In communication engineering, chaos introduces important aspects in security as well as multiuser applications in cellular communications. Therefore, chaotic communications is a promising technique in the next wireless generation.

A compound of two 1-D chaotic maps suggests by I. Aouissaoui et al. [6] for information security. Which achieved a logistic-sine map based on a tent chaotic map as well as a cubic-tent map but for SISO channel. The analysis of LE for the proposed maps has been achieved. The bifurcation diagram was plotted to measure the chaotic range but the authors did not calculate the BER for the proposed system.

J. Pedro et al. [7] propose a compound of two 1-D chaotic maps; logistic and tent maps for the deep zoom technique. They found that the random quality of chaos improved with PRNG when the chaotic parameter and a are increased for SISO communication systems. But also they did not compute the BER to ensure the system performance is not affected by the changing in chaotic behavior. M. Lawnik et al. [8] suggest M-map chaotic system for cryptography applications. They measured the LE and plotted the bifurcation diagram. They showed that the minimum value for LE for the proposed analysis was 2 and the maximum value was 12.

A dual map is suggested to resolve the problem of dynamical degradation. A significant advantage in the dynamical systems analysis is the stability of the system, which can be satisfied by using the LE.

In this paper, the LEs for dual tent and logistic maps have been derived. This paper realizes the feasibility of using MIMO to improve the performance of the communication system due to chaotic degradation. We have studied the performance of CSK with the Alamouti scheme for these dual chaotic maps under the AWGN channel. The use of these schemes allows us to enhance security without degrading the BER performance. An exact method to compute the BER has been utilized and analyzed. This method considers the aperiodicity nature of the chaotic signals [9]. The simulation results refer to the combination of STBC and a single chaotic map can degrade the BER when compared to a dual chaotic map in cost of reducing the information protection.

2. Iteration of Chaotic Map

2.1 Tent Map Iteration

Consider the tent map trajectory $x: [0,1]$ is expressed as [10]

$$x_{n+1} = \begin{cases} \frac{x_n}{a} & , 0 \leq x_n < a \\ \frac{1-x_n}{1-a} & , a \leq x_n < 1 \end{cases} \quad \dots(1)$$

The dynamical system trajectory $x(x)$ is obtained by iterating the chaotic map, i.e.,

$$x(k) = f^k[x(0)] = f(\{ \dots f[x(0)] \dots \}), \quad k=0,1,2,\dots \quad \dots(2)$$

2.2 Logistic Map Iteration

The non-linear paradigm of the logistic map is given in equation (3) [11]

$$x_{n+1} = \mu x_n (1 - x_n), \quad \mu \in [0,4], x_n \in (0,1) \quad \dots(3)$$

The sequence $\{x_1, x_2, \dots, x_n\}$ is generated by initializing the initial value $x_0 \in (0,1)$ depending on the value of a parameter μ . A new sequence generates when a small change in the initial value occurs and changes in the value μ . The chaos state behavior occurs with the increase of μ values and achieving a chaos state ultimately. When $\mu > 3.75$, movement from the sequence $\{x_n\}$ appears chaotic behavior.

3. Dual Chaotic Iteration

As mentioned above, a single chaotic system is attackable to be attacked by chaotic reconstruction since it has a simple structure and weak control boundaries. A 2-D chaotic map has more parameters and a complex form, but it has a more complex load. To balance these two factors, a dual chaotic map may be utilized. A dual-maps that consists of two 1-D maps has been implemented.

3.1 Dual-Logistic Map

Chaos may be appeared by LOGISTIC 1 and LOGISTIC 2 such as,

$$\text{LOGISTIC 1: } x_{n+1} = \mu x_n (1 - x_n), \quad \mu \in [3.757,4], x_n \in (0,1) \quad \dots (4)$$

$$\text{LOG2: } x_{n+1} = \eta x_n (1 - x_n), \quad \eta \in [3.57,4], x_n \in (0,1) \quad \dots (5)$$

where μ and η represent the control parameters. In this case, x_{n+1} represents the output sequence of LOGISTIC 1, while y_{n+1} represents the output sequence of LOGISTIC 2 considering $y_0 = x_{n+1}$. So, $\{y_n\}$ is the last output of those two sequences.

It is produced by composing the sequences of LOGISTIC 1 and LOGISTIC 2 [4,12].

3.2 Dual-Tent Map

TENT MAP 1 and TENT MAP 2 are represented as follows,

TENT MAP 1:

$$x_{n+1} = \begin{cases} \frac{x_n}{a} & , 0 \leq x_n < a \\ \frac{1-x_n}{1-a} & , a \leq x_n < 1 \end{cases} \dots (6)$$

TENT MAP 2:

$$y_{n+1} = \begin{cases} \frac{y_n}{b} & , 0 \leq x_n < b \\ \frac{1-y_n}{1-b} & , b \leq x_n < 1 \end{cases} \dots(7)$$

where a and b are the control parameter, x_0 and y_0 are initial values, x_{n+1} is the output sequence of TENT MAP 1, and y_{n+1} is the output sequence of TENT MAP 2 considering $y_0 = x_{n+1}$.

So, $\{y_n\}$ is the last output of these two sequences. It is produced by composing the two sequences of TENT MAP 1 and TENT MAP 2 leading to increasing the complexity of chaotic behavior.

4. Lyapunov Exponent

Consider $|\delta_n| = f^n(x_0 + \delta_0) - f^n(x_0)$ being the n iteration number of the chaotic sequence, x_0 denotes the initial condition, and δ_0 be the small random number. However, LE formula can be given as,

$$\lambda = \frac{1}{n} \ln \left| \frac{\delta_n}{\delta_0} \right| = \frac{1}{n} \ln |(f_n)'(x_0)| \dots (8)$$

By expanding the term within algorithm, the approximation value of the LE can be given as,

$$\lambda = \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \dots(9)$$

If the equation (10) have limit when $n \rightarrow \infty$, then the LE for the orbit that begins in x_0 is

$$\lambda = \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \right\} \dots(10)$$

Note that λ depends on x_0 . For points and cycles stable, λ is negative and for chaotic attractors, λ is positive [13].

4.1 LE of Single Logistic [14]

According to equations (3 and 10),

$$\lambda = \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} \ln(\mu) - \ln(2\mu x_i) \right\} \dots (11)$$

4.2 LE of Single Tent [15-17]

According to Eqs. (3) and (10),

$$\lambda = \int_0^a \ln \left| \frac{1}{a} \right| dx + \int_a^1 \ln \left| \frac{1}{1-a} \right| dx \dots (12)$$

4.3 LE of Dual Logistic

LEs of a x_n sequence denoted by,

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{2n} \ln [D_n^T D_n] \dots (13)$$

whenever D_n is the limit exists. Uppercase T represents the transpose.

From Eqs. (10, 11 and 13), a dual logistic map can be expressed as,

$$\text{Let , } x_{n+1} = \mu x_n(1 - x_n), x_{n+1}' = \mu - 2\mu x_n$$

For Dual;

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{2n} \sum_{i=1}^{n-1} \ln \{ [\mu - 2\mu x_n]^T [\mu - 2\mu x_n] - d \} = \lim_{n \rightarrow \infty} \frac{1}{2n} \sum_{i=1}^{n-1} \ln \{ \mu(1 - 2x_n) \}^T [\mu(1 - 2x_n)] - d \} \dots (14)$$

where d is the change in initial value.

4.4 LE of Dual Tent

According to equations (10,12 and 13), a dual tent map can be derived as,

$$\text{Let, } x_{n+1} = \begin{cases} \frac{x_n}{a} & , 0 \leq x_n < a \\ \frac{1-x_n}{1-a} & , a \leq x_n < 1 \end{cases}$$

For dual;

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{2n} \left\{ \left[\int_0^a \ln \left| \frac{1}{a} \right| dx + \int_a^1 \ln \left| \frac{1}{1-a} \right| dx \right]^T \left[\int_0^a \ln \left| \frac{1}{a} \right| dx + \int_a^1 \ln \left| \frac{1}{1-a} \right| dx \right] - d \right\} \dots(15)$$

5. CSK-MIMO Communication System

Let us consider $x(t)$ as the signal that is generated by any chaotic map and defined in the previous section. In CSK, the chaotic signal will occur If $a' + 1'$ is transmitted and an inverted copy of the chaotic signal will appear If $' - 1'$ is transmitted. Therefore, the transmitted signal can be denoted as [18-20,24],

$$s(t) = \begin{cases} x(t), & \text{if '+1' is transmitted} \\ -x(t), & \text{otherwise} \end{cases} \dots(16)$$

Let us consider the time interval of the data symbols ($s_1 = \pm 1$) denoted by T_s , then the chip interval of the chaotic sequence will be T_c ($x_k = x(kT_c)$). However, The transmitted signal is expressed as,

$$u(t) = \sum_{l=0}^{\infty} \sum_{k=0}^{\beta-1} s_l x_{l\beta+k} \dots(17)$$

where β represents the spreading factor ($\beta = \frac{T_s}{T_c}$).

Then, the signal received at the receiver side is denoted as,

$$r(t) = u(t) + n(t) \dots(18)$$

where $n(t)$ represents the AWGN with zero mean and variance σ_n^2 . At the receiver, the received signal is first despreading by generating an exact replica of the chaotic signal that is generated at the transmitter, after that the symbols are integrated over symbol duration T_s . at last, the sign of the decision variable will be computed [9,21], such as,

$$Ds_1 = \text{sign} (s_1 T_c \sum_{k=0}^{\beta-1} (x_{1\beta+k})^2 + w_1) = \text{sign}(s_1 E_b^{(1)} + w_1) \dots(19)$$

Where $\text{sign}(\cdot)$ represents the sign operator, $E_b^{(1)}$ denotes l^{th} bit energy and w_1 is the AWGN computed after despreading processing.

2×2 Space Time Block Code (STBC)

Fig. 1 shows the block diagram of CSK-MIMO transmitter with two antennas and two receive antenna.

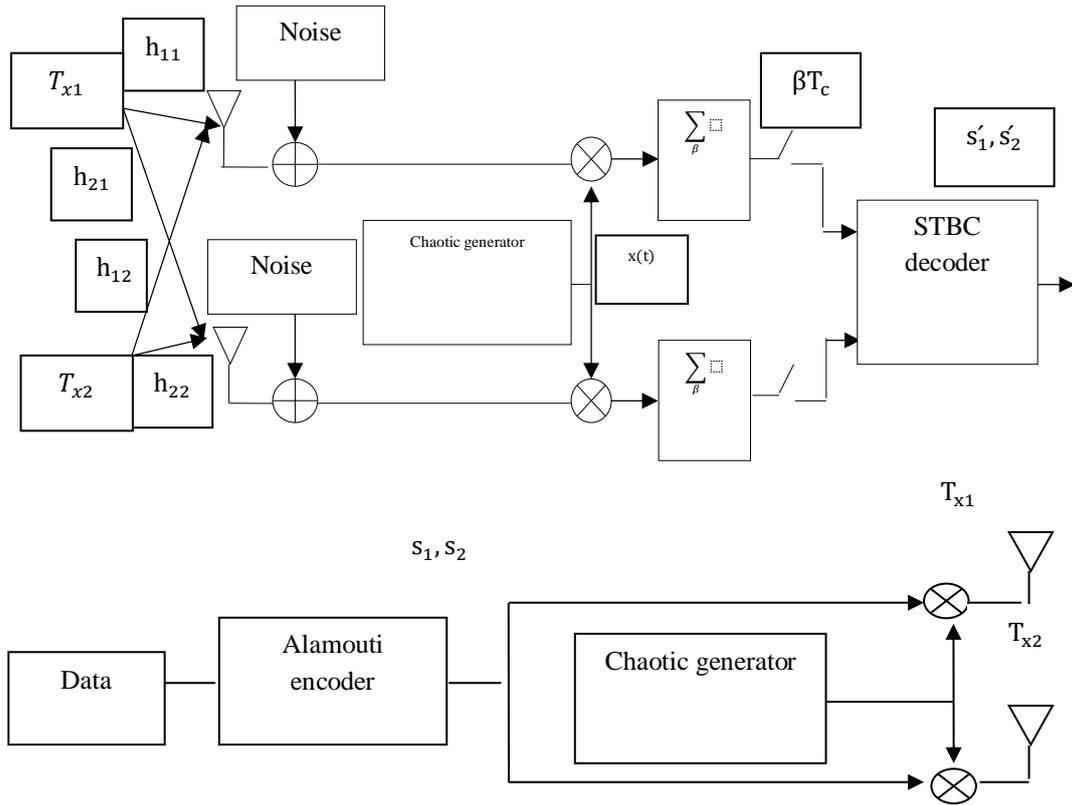


Fig. 1 2 × 2 MIMO-CSK communication scheme.

The designed symbols for STBC denoted by,

$$S = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} \dots (20)$$

Table. 1, The transmitted signa

Time interval	$s_1(t)$ from first transmitter	$s_2(t)$ from second transmitter
$[0, \beta T_c]$	$s_1 x_k$	$s_2 x_k$
$[\beta T_c, 2\beta T_c]$	$-s_2^* x_{k+\beta}$	$s_1^* x_{k+\beta}$

Table. 2, The signal received by the first receiving antenna

Time	Received signal on first receiving antenna
$[0, \beta T_c]$	$h_{11} s_1 x_k + h_{21} s_2 x_k + n_k^1$
$[\beta T_c, 2\beta T_c]$	$-h_{11} s_2^* x_{k+\beta} + h_{21} s_1^* x_{k+\beta} + n_k^2$

Table. 3,**The signal received by the second receiving antenna**

Time	Received signal on second receiving antenna
$[0, \beta T_c]$	$h_{12}S_1X_k + h_{22}S_2X_k + n_k^1$
$[\beta T_c, 2\beta T_c]$	$-h_{12}S_2^*X_{k+\beta} + h_{22}S_1^*X_{k+\beta} + n_k^2$

The t^{th} bit energy is denoted by $E_b^{(l)} = \sum_{k=1}^{\beta} x_k^{(l)2}$.

Table. 4,**The equivalent baseband of the symbol at R_{x1}**

Time	The equivalent baseband of the symbol at R_{x1}
$[0, \beta T_c]$	$Y_{11} = E_b(h_{11}S_1 + h_{21}S_2) + N_{11}$
$[\beta T_c, 2\beta T_c]$	$Y_{21} = E_b(-h_{11}S_2^* + h_{21}S_1^*) + N_{21}$

Where, $N_{11} = \sum_{k=1}^{\beta} n_k^1 x_k$ and $N_{21} = \sum_{k=1}^{\beta} n_k^2 x_{k+\beta}$ represent AWGN components.

Table .5,**The equivalent baseband of the symbol at R_{x2}**

Time	The equivalent baseband of the symbol at R_{x2}
$[0, \beta T_c]$	$Y_{12} = E_b(h_{12}S_1 + h_{22}S_2) + N_{12}$
$[\beta T_c, 2\beta T_c]$	$Y_{22} = E_b(-h_{12}S_2^* + h_{22}S_1^*) + N_{22}$

$N_{12} = N_{11}$ and $N_{22} = N_{21}$ represent AWGN components and h_{11}, h_{21}, h_{12} and h_{22} are the channel coefficients for 2×2 scheme. The above formulas are derived in [6].

The received vector is expressed as,

$$Y = E_b HS + N \quad \dots (21)$$

The data are estimated by multiplying the vector Y by the conjugate transpose of H (equation 22) and then computed by the decision variable (equation 23);

$$\begin{pmatrix} D_{s1} \\ D_{s2} \end{pmatrix} = H^* Y \quad \dots (22)$$

The estimated bits are computed from the sign of the decision variables,

$$s'_1 = \text{sign } D_{s1}; \quad s'_2 = \text{sign } D_{s2} \quad \dots (23)$$

5.1 Performance Analysis

Let us consider the channel coefficient is constant for 2×2 STBC under the assumption of AWGN. The BER formula of the proposed scheme is expressed in (24) [21,22,24].

$$P_e(E_b^{(l)}) = \frac{1}{2} \text{erfc} \left(\sqrt{\frac{(h_{11}^2 + h_{21}^2 + h_{12}^2 + h_{22}^2) E_b^{(l)}}{N_0}} \right)$$

Now,

$$E_{xi}[Q\{E(x)/\sqrt{\text{Var}(x)}\}]$$

where

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} \exp(-u^2/2)$$

$$\begin{aligned} BER &= \sum_{n,p=1}^2 h_{n,p}^2 \sum_{l=0}^{\beta-1} E_{xi} \left(\sum_{i=0}^{\beta-1} \frac{x_i^2}{N_0} \right)^2 \\ &= \sum_{l=0}^{\beta-1} E_{xi} \left(\sum_{i=0}^{\beta-1} \frac{x_i^2}{N_0} \right)^{\frac{1}{2}} (h_{11}^2 \\ &\quad + h_{21}^2 + h_{12}^2 + h_{22}^2) E_b^{(l)} \end{aligned}$$

$\sum_{i=0}^{\beta-1} x_i^2 = E_b^{(l)}$ is the chaotic symbol energy, and $E_{xi} = \int_0^{\infty} p(E_b^{(l)}) dE_b^{(l)}$,

The BER formula for 2×2 STBC is formulated as,

BER =

$$\int_0^{\infty} \frac{1}{2} \text{erfc} \left(\sqrt{\frac{(h_{11}^2 + h_{12}^2 + h_{21}^2 + h_{22}^2) E_b^{(l)}}{N_0}} \right) p(E_b^{(l)}) dE_b^{(l)} \quad \dots (24)$$

Where $p(E_b^{(l)})$ is the PDF of the $E_b^{(l)}$. The BER formula resulted from integration given in equation (24). To compute the integral in equation (24), the distributed energy must be considered. Because of the PDF consider to be intractable, the method to compute the BER is evaluating the histogram of $E_b^{(l)}$ followed by a numerical integration [18,19,18]. Fig. (2) presents the histogram of the $E_b^{(l)}$, for 50000 samples obtained by simulation and $\beta=4$.

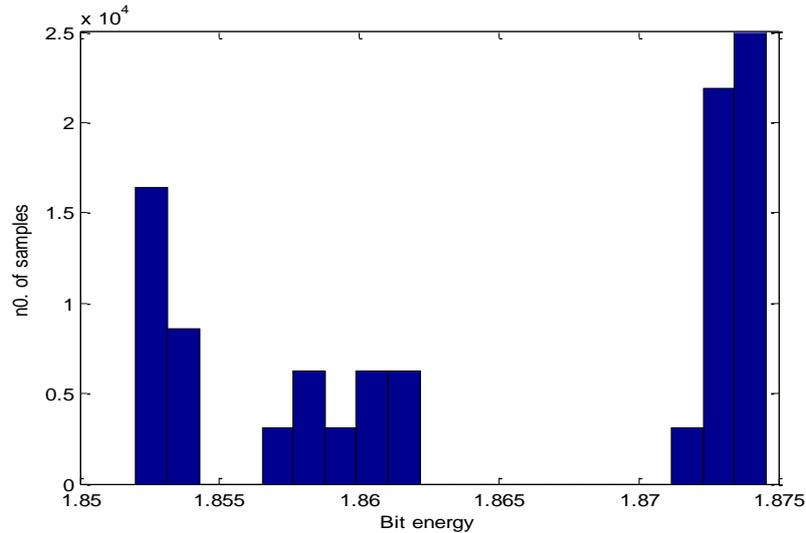


Fig. 2 $E_b^{(1)}$ histogram.

Applying numerical integration, the BER formula is expressed as,
 BER =

$$\sum_{l=1}^m \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{(h_{11}^2 + h_{12}^2 + h_{21}^2 + h_{22}^2) E_b^{(l)}}{N_0}} \right) p(E_b^{(l)}) \dots (25)$$

In the above equations, m denotes the number of histogram classes and $p(E_b^{(l)})$ is the probability of the energy in interval centered on $E_b^{(l)}$.

6. Results and Discussions

Fig.3 shows the single logistic map providing the chaotic behavior beyond $\mu = 3.57$. This map has more randomness $\mu = 3.8$ and LE equals 0.5. Fig.4 presents the single tent map. It is observed that this map has chaotic properties within the range (0,1) of a control parameter (a). It has more randomness when the value of (a) is greater than 0.5 and LE equals 0.85. A dual logistic is provided in Fig.5. It has more randomness when $\mu > 2.35$ and $\mu < 4$. More randomness appeared at $\mu = 4$ and LE equals 0.81.

Fig.6 presents the dual tent which has chaos properties in the range (0,1) of a . It has more randomness when $a = 0.5$ and LE at equals 1.2. We observed from Fig. 3 and Fig. 4 that when a very small change in initial values say 10^{-16} , a new chaotic sequence is generated completely different from the current state. Therefore, with increasing the time of iteration more than 20 times, the difference exponentially increases. For the dual logistic map in Fig. 5, this difference appears with

increasing the iteration time more than 40 times, after this value, the difference exponentially increases.

In Fig.6, the dual tent map has the difference between two sequences is very sensitive to a very small change in initial conditions. However, this map shows better sensitivity to initial conditions. Whereas, the single tent map provides the best sensitivity than dual single and logistic maps according to results obtained from LE.

Table (6) summarizes the values of LEs for presented chaotic maps

Table 6, values of LE

Chaotic map	LE
Single logistic	0.5
Single tent	.0.85
Dual logistic	0.81
Dual tent	1.2

From the above table, it is observed that the dual tent has the most randomness whereas the single logistic map has the least randomness.

In Fig.7, the BER is degraded for single map when a 2×2 is considered for the system. Also, for a dual tent, when the system is compensated with 2×2 STBC, the SNR will gain 0.5 dB as compared to 2×2 single logistic for the same BER under the AWGN assumption. It is noted that there is a tradeoff between the randomness and BER performance. So, the BER performance can be achieved by implementing 2×2 single tent map at the cost of reducing randomness.

From Figs. 3,4, 5, and 6, we observed that chaotic maps give highly distinct sequences as

compared to the PN sequence generator. The degree of distinctness is more for the dual chaotic map as compared to the single chaotic map.

Now, let us suppose that x_n and y_n are two-sequence with length N . The auto-correlation and the cross-correlation are defined in equations (26 and 27) respectively [4].

$$R_x(j) = \frac{1}{N} \sum_{i=1}^N x_i x_{i+j} \quad \dots(26)$$

$$R_{xy}(j) = \frac{1}{N} \sum_{i=1}^N x_i y_{i+j} \quad \dots(27)$$

where N is the sequence's length and j is the distance between two chaotic elements.

Fig.8 shows the auto-correlation of dual tent. The auto-correlation is maximum at zero time shift. Fig. 9 presents that the single tent map provides a cross correlation function near zero (maximum value 0.0085) when compared to dual tent (highest value 0.028). However, the two sequences of single tent satisfy the orthogonality property more than dual tent map

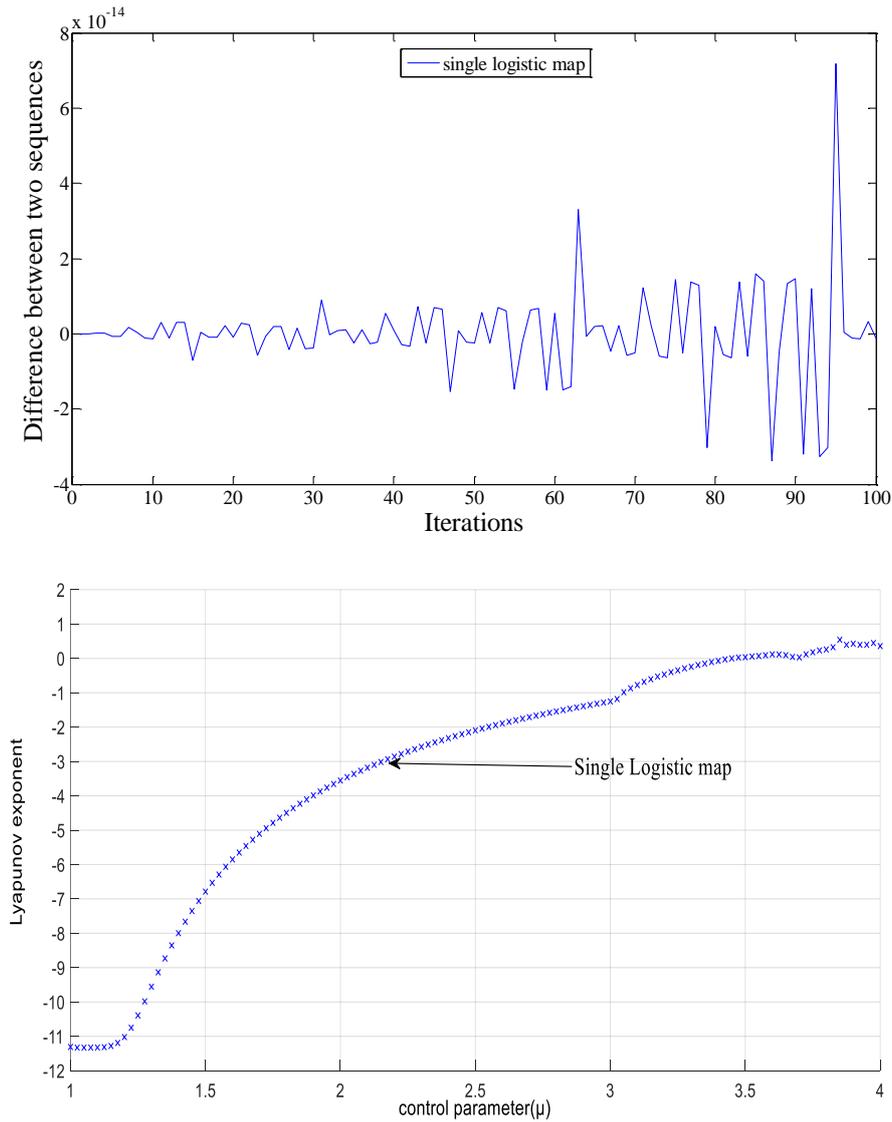


Fig. 3. The difference between two single logistic and its LE.

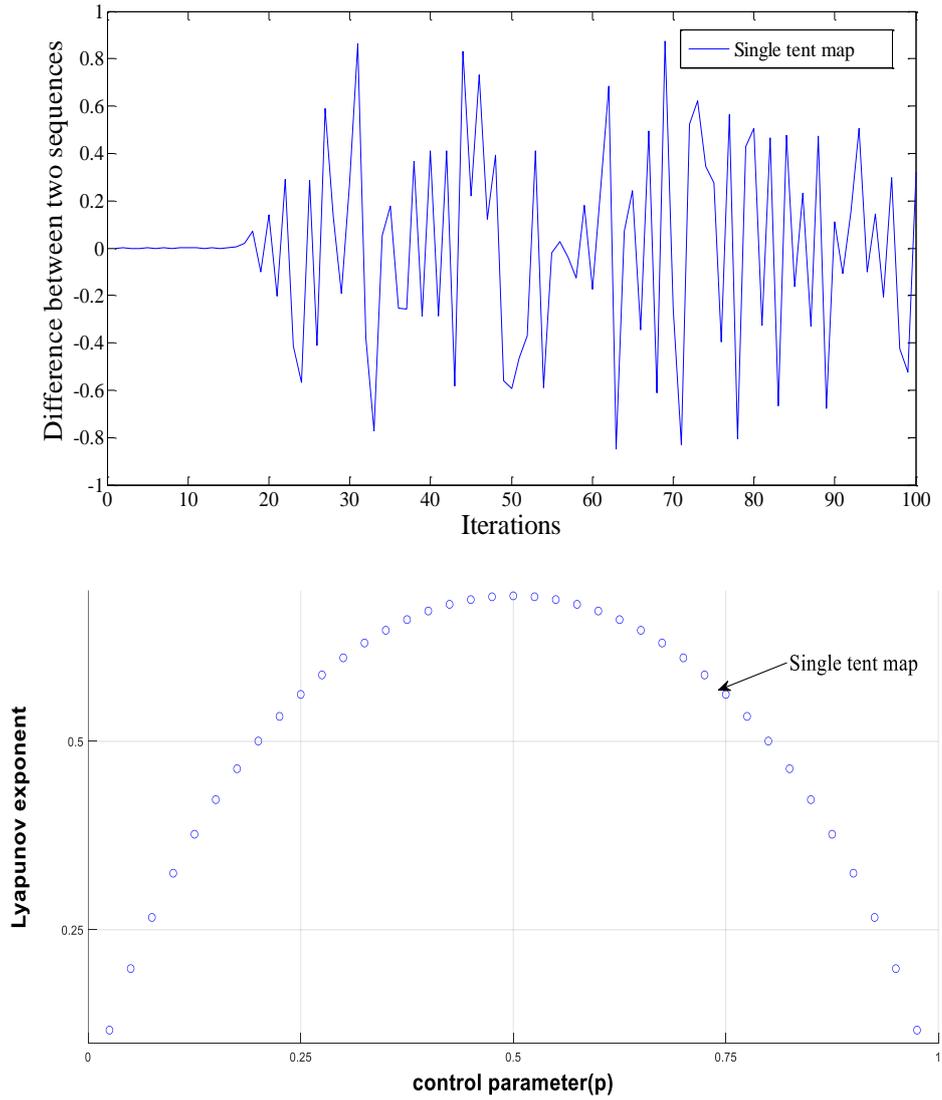
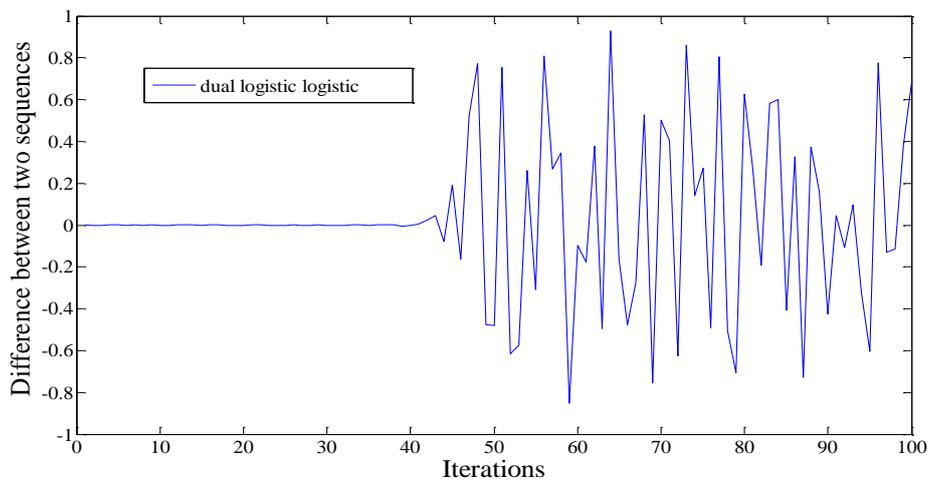


Fig. 4. a) The difference between two single tent and its LE.



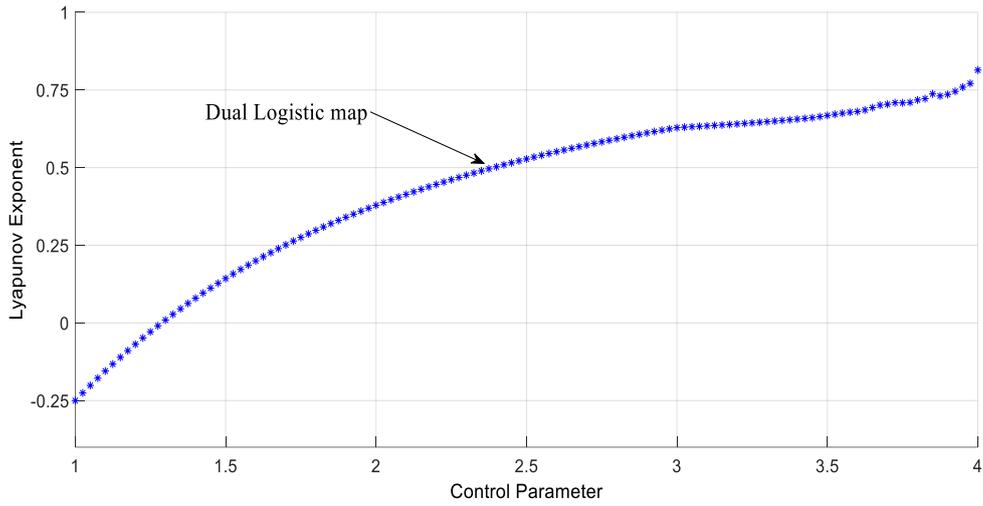


Fig. 5. The difference between two dual logistic and its L.E

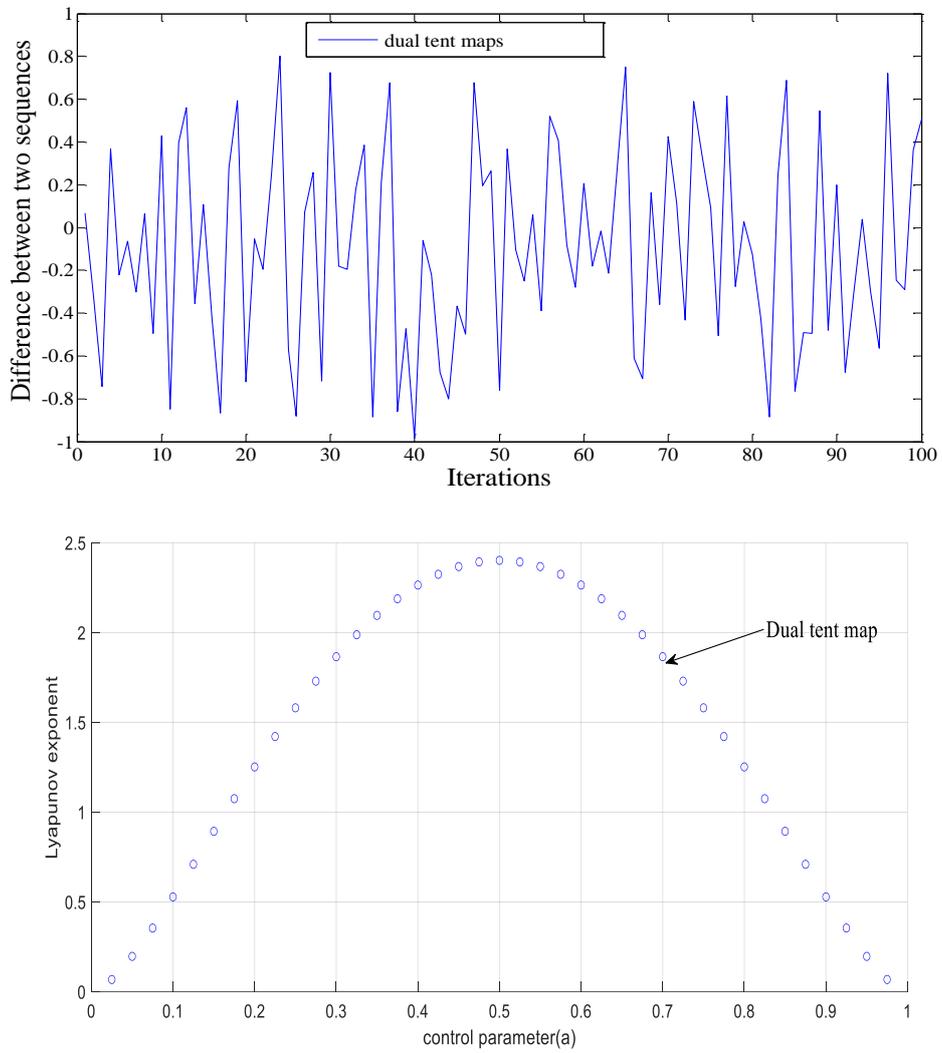


Fig. 6. The difference between two dual tent and its LE.

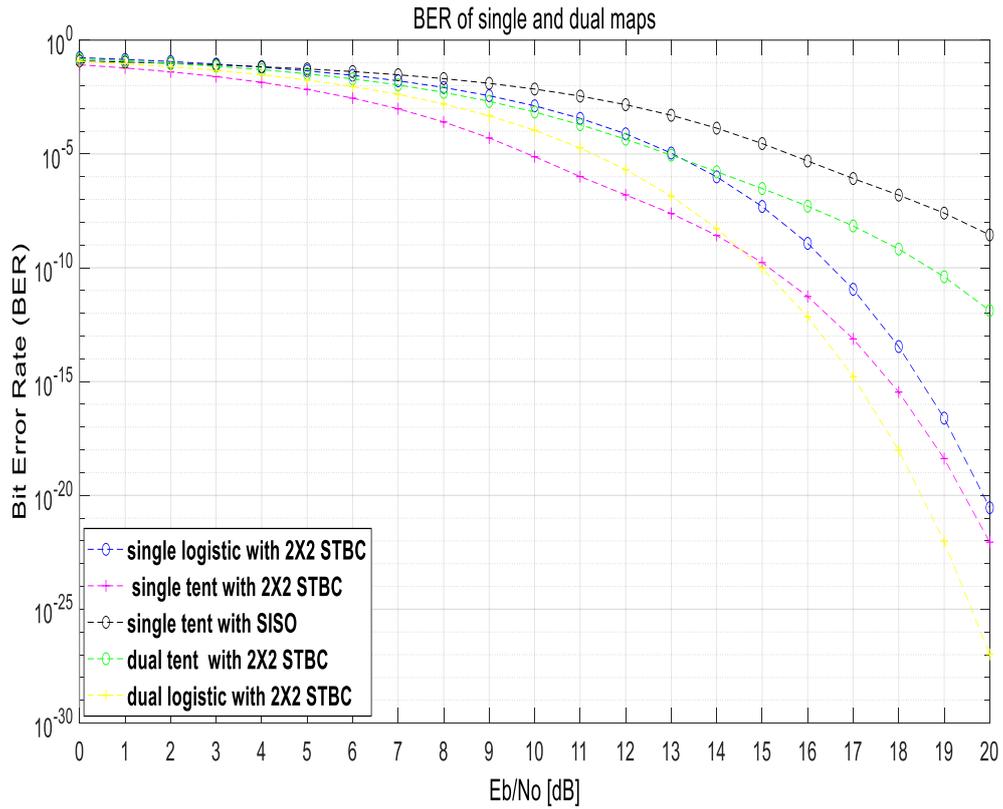


Fig. 7. BER for single and dual maps.

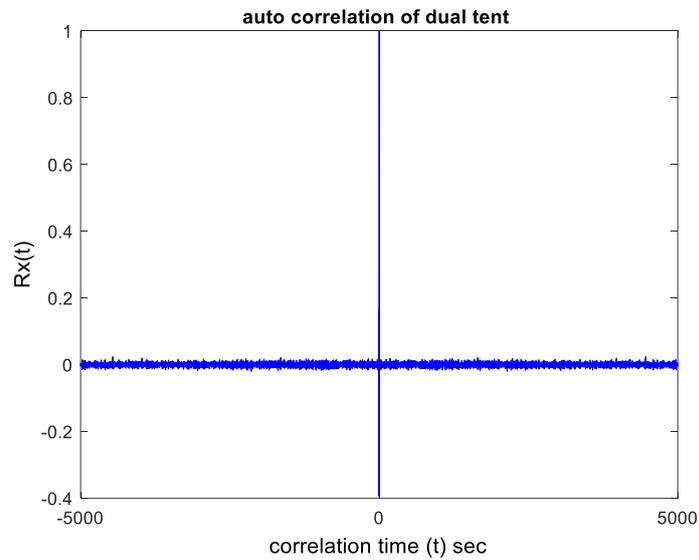


Fig. 8. auto-correlation of dual tent.

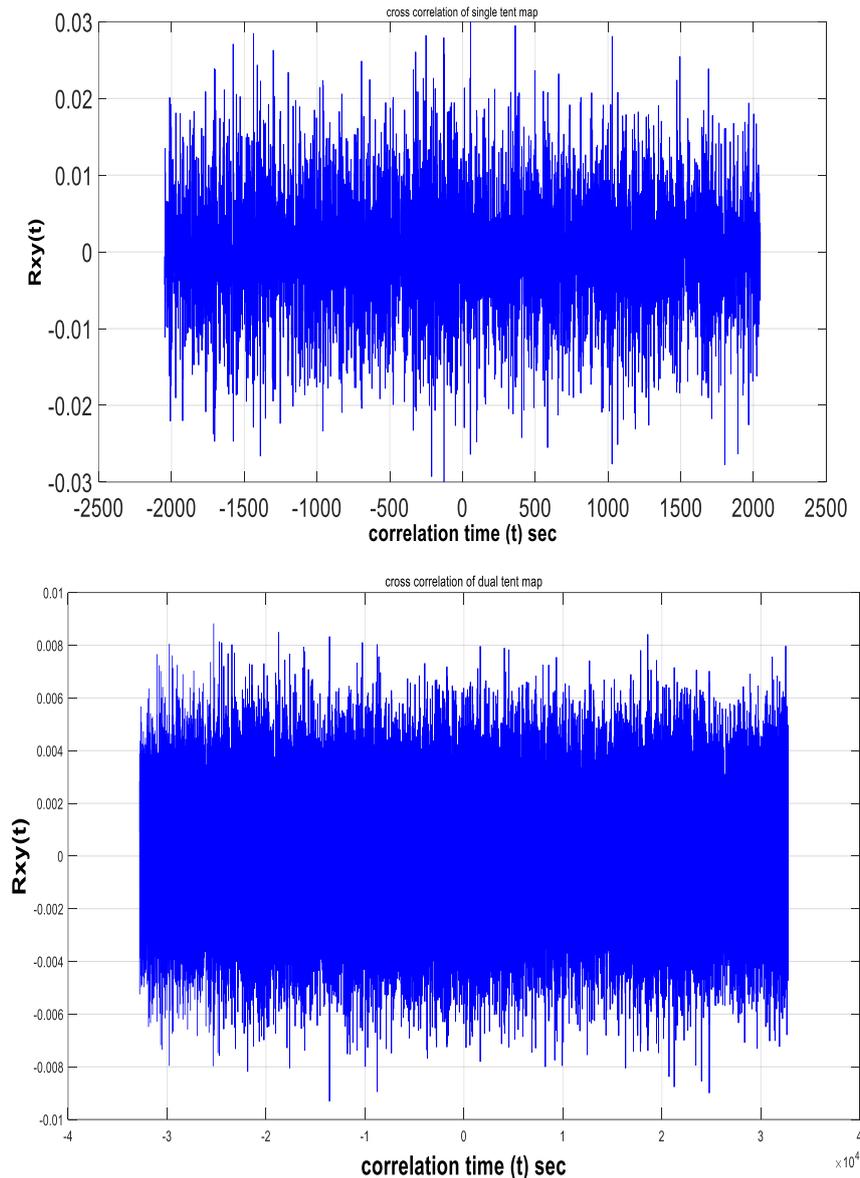


Fig. 9. cross-correlation of single and dual tent.

6. Conclusions

The data encryption based on the dual chaotic presented in this work has excellent randomness. The LEs for the single and dual maps have been computed numerically. In this work, the exact BER for dual and single chaotic maps modulated CSK 2×2 STBC under AWGN has been investigated. The final results show that the randomness of the dual tent map is better than the single tent map, single logistic map, and dual logistic map. As well as the 2×2 CSK-MIMO gives a better BER performance as compared with the SISO system.

7. References

- [1] K. Daniela and E. Marcio, "On the Power Spectral Density of Chaotic Signals Generated by Skew Tent Maps," IEEE International Symposium on Signals, Circuits and Systems", Vol. 1, pp. 1-4, 2007.
- [2] A. Kathleen, S. Tim and Y. James, Chaos, An Introduction to Dynamical Systems. Springer 1996.
- [3] F. Jiu and T. Chi, Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications. Word Scientific, 2008.
- [4] C. Yi, Li Z. and W. Yifang, A Data Encryption Algorithm based on Dual Chaotic System: proceeding of the 2010 International Conference on Computer Application and

- System Modeling (ICCASM 2010), pp. V4-431V4-435, 2010.
- [5] Parlitz U.: Lyapunov Exponents from Chau's Circuit., *Journal of Circuits, Systems and Computers*, Vol. 3, No. 2, pp. 507-523, 1993.
- [6] I. Aouissaoui, T. Bakir, A. Sakly, and S. Femmam, "Improved One-Dimensional Piecewise Chaotic Maps for Information Security", *Journal of Communications*, Vol. 17, No. 1 P.P. 1-6., January 2022.
- [7] J. Pedro do V. Alvarenga, J. Machicao, and O. M. Bruno, "Chaotical PRNG based on composition of logistic and tent maps using deep-zoom", *Chaos, solitons and fractals-Elsevier*, Vol. 161, 2022.
- [8] M. Lawnik and M. Berezowski, "New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography", *Symmetry- MDPI*, Vol. 14, 2022.
- [9] G. Kaddoum, Mai V. and F. Gagnon, "On the performance of chaos shift keying in MIMO communications systems". *IEEE WCNC-PHY*, pp. 1432-1437, 2011.
- [10] A. Mozsary, L. Azzinari, K. Krol and V. Porra, Theoretical connection between PN-sequences and chaos makes simple FPGA pseudo-chaos sources possible: proceeding of the 8th IEEE International Conference on Electronics, Circuits and Systems, February 2001.
- [11] A. Abir, A. Safwan, Q. Wang, V. Calin and B. Bassem, "Comparative study of 1-D chaotic generator for digital data encryption", *IAENG International Journal of Computer Science*, 2008.
- [12] K. Ljupco, S. Janusz, A. Jose and T. Igor, "Discrete Chaos-I: Theory", *IEEE Transaction of Circuits and Systems-I*, Vol 53, No. 6, pp. 1300-1309, 2006.
- [13] E. Ibarra, R. Vazquez, M. Cruz and J. Rio, Numerical Calculation of the Lyapunov Exponent for the Logistic Map: proceeding of the 12th International Conference on Mathematical Methods in Electromagnetic Theory, pp. 409-411, 2008.
- [14] H. Martin and M. Yuri, "An Introduction to the Synchronization of Chaotic Systems: Coupled Skew Tent Maps", *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 44, No. 10, pp. 856-866, 1997.
- [15] G. Kaddoum, P. Charge and D. Roviras, "A generalized methodology for bit-Error-rate reduction in correlation-based communication schemes using chaos", *IEEE Communication Letters*, Vol. 13, No. 8. , 2009.
- [16] L. Abdulameer., D. Jokhakar, U. Sripathi and M. Kulkarni: BER Performance Enhancement for Secure Wireless Communication Systems based on Chaotic MIMO Techniques., proceeding of the International Conference on Communication and Electronics System Design, 2013.
- [17] R. Sankpal, A. Vijaya, Image Encryption Using Chaotic Maps. A Survey, *Lecture notes in networks and systems*, Springer, p.p. 835-844, 2014.
- [18] S. Das, K. Mandal, and M. Chakraborty, "LMMSE equalized DCSK communication system over a multipath fading channel with AWGN noise", proceeding of the third International Conference on Computer, Communication, Control and Information Technology (C3IT), p.p 1-4, 2015.
- [19] V. Manikandan & Rengarajan Amirtharajan, "On dual encryption with RC6 and combined logistic tent map for grayscale and DICOM", *Multimedia Tools and Applications*, P.P. 1-30, 2021.
- [20] A. Imoize , A. Ibhaze , A. Atayero , and K. Kavitha, "Standard Propagation Channel Models for MIMO Communication Systems", *Hindawi Wireless Communications and Mobile Computing*, PP. 1-36, 2021.
- [21] R. Dhia'a, "Design a Security Network System against Internet Worms", *Al-Khwarizmi Engineering Journal*, Vol. 8, No. 3, PP 40 – 52, p.p. 1-13, 2012.
- [22] R. Yamazaki, Y. Shimada, and T. Ikeguchi, "Chaos MIMO system with efficient use of information of bits", *NOLTA, IEICE*, P.P. 1-15, 2020.
- [23] I. Kadhem, "A New Audio Steganography System Based on Auto-Key Generator", *Al-Khwarizmi Engineering Journal*, Vol. 8, No. 1, p.p. 27 – 36, 2012.
- [24] L. Abdulameer, ANALYSIS AND DESIGN OF RELIABLE AND SECURE CHAOTIC COMMUNICATION SYSTEMS FOR OPTICAL AND WIRELESS LINKS, Dept. of Electronics and Communication Engg., NITK, 2014.

تحسين اداء منظومة الاتصالات الفوضوية الثنائية باستخدام تقنية الهوائيات المتعددة

لواء فيصل عبد الأمير* اودبي سريباتي** مولدير كولكرني***

*قسم هندسة المعلومات والاتصالات/ كلية الهندسة الخوارزمي/ جامعة بغداد/ العراق
المعهد الوطني للتكنولوجيا كارتاكا/ قسم هندسة الالكترونيات والاتصالات/ الهند*البريد الالكتروني: lwa@kecbu.uobaghdad.edu.iq**البريد الالكتروني: sripati_achary@yahoo.co.inالبريد الالكتروني: mkuldc@gmail.com

الخلاصة

ان الحفاظ على سرية المعلومات عند انتقالها خلال الوسط من والى المستخدم تعد من الامور الضرورية جدا. الاشارة الفوضوية تعد من الخيارات الممتازة لتشفير الاشارات وخصوصا انها تمتاز عن الخوارزميات الاخرى بكون الاشارة لا تكرر نفسها بعد مدة من الزمن وان اي تغيير حتى لو كان صغيرا جدا في القيم الابتدائية سوف يولد اشارة جديدة مما يصعب على المتتصتين استراق الاشارة. الاشارة الفوضوية الثنائية تمتاز بكونها أكثر فوضوية من الاحادية مما يولد اشارة معقدة جدا بالنسبة للمتتصت. في هذا البحث، تم تصميم نوعين للاشارات الفوضوية الاحادية ونوعين مماثلين للاشارة الفوضوية الثنائية وقد تم قياس مدى فوضوية كل اشارة من خلال اشتقاق خوارزمية لكل نوع وتمثل بـ (Lyapunov Exponent (LE)). ايضا تم في هذا البحث استخدام تقنية متعددة الهوائيات لتحسين الاداء العام لمنظومة الاتصالات لكون استخدام الاشارات الفوضوية يؤدي الى تقليل الاداء بسبب زيادة سرية المعلومة (العلاقة العكسية بين الانتروبي والاداء). النتائج بينت بأن Dual chaotic map اعطت اعلى قيمة من الـ (LE) مما يعني انها أكثر فوضوية من بقية الانواع المستخدمة في البحث. ايضا من خلال استخدام تقنية الهوائيات المتعددة تبين ان استخدام 2x2 مع single chaotic map يقدم احسن اداء مقارنة بالانواع الاخرى المستخدمة.