A Multiplicative-Additive Chaotic-Address Steganography

Haneen H. Alwan **Faculty of Computer Science and Mathematics** University of Kufa, Najaf 54001, Iraq

Zahir M. Hussain Faculty of Computer Science and Mathematics University of Kufa, Najaf 54001, Iraq

Received Aug..27, 2019. Accepted for publication Jul.15, 2020

DOI :http://dx.doi.org/10.31642/JoKMC/2018/070204

Abstract— In this study, Multiple-Chaotic maps were merged by using multiplicative-additive form to generate the chaotic sequences which are used to track the addresses of shuffled bits in steganography. Three techniques are introduced for image steganography in the spatial domain. The first system is based on the well-known LSB technique, the second system is based on looking for the identical bits between the secret message and the cover image and the third system is based on the concept of LSB substitution, it is employed the mapping of secret data bits with cover pixel bits. It was tested and evaluated security levels for the proposed techniques by using the Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), histogram analysis and correlative analysis and tested the Chaotic sequences generated by using correlation, Lypaunov exponents, Poincaré section and 0-1Test. The results show that the proposed methods perform better than existed systems.

Keywords— Chaos theory, Chaotic maps, Lyapunov exponents, Steganography, Data Security.

INTRODUCTION I.

The digitization is becoming unusually energetic in everything; Digital data is appearing everywhere at the present time [1]. In the secure communications, steganography is playing important role. As result, it is becoming one of interesting research in the data hiding. Digital data can be transmitted by communications media, but the communications media may not secure, data may be manipulated and detected that is dangerous impact on social and personal life [2].

Therefore, it should add a concept that increases the security of data as an additional security dimension, because security and integrity of data are important [3]. For the security of digital data, the existed proposed methods must have developed to protect and secure the digital data.

Chaos theory is considered a hot topic in the recent decades because it has the following unique characteristics: Deterministic, sensitivity to initial conditions and parameters and ergodicity. It is used to provide a high level of security in steganography [4].

II. **RELATED WORKS**

Many researchers have used chaos theory to increase the level of security. It was hidden a grayscale image in a colored cover image in the two least significant bits of the red channel [5]. Secret data is embedded by using the Tent map or Baker's map for determining the locations in the cover image. In [2] the proposed method showed that the secret data has hidden by using the 3D chaotic map (LCA map). It is selected random couple elements (c,d) and selected pixel at (ic, jc, kc),(id, jd, kd). The selected pixel divides into MSB and LSB, then it hides the LSB of secret data in LSB of (ic, jc, kc) and MSB of secret data in LSB of (id , jd , kd). In this proposed algorithm [6], it uses the LSB method to embed secret data, where the cover image divide into two parts: upper and lower. It employs the chaotic maps to determine the locations in two part for hiding the secret data, row number is determined by the TDERCS map, whereas the column number is determined by the NCA and logistic map is used to determine a frame number. In above proposed methods, a number of chaotic maps have been used to increase the security against the attacks especially if there is a suspicion of the secret data.

III. CHAOTIC MAPS

Chaotic systems are characterized the sensitive to change the initial conditions or parameters, a small changing of the initial condition can cause a large effect in the results. Chaotic maps can be employed in the steganography due to the fact that they have statistically powerful features. There are many maps that generating chaotic behaviors such as the Logistic map, Tent map and Quadratic map [7] [4] [5]. The Logistic map defined by:

$$x_{n+1} = \alpha x_n (1 - x_n)$$
 (1)

Where $x_n \in (0, 1)$ and $3.5699 < \alpha \le 4$, it is chaotic behavior. The Tent map where $0 < x_n$ and parameter $\alpha < 1$ (all positive) defined by:

$$x_{n+1} = \frac{x_n}{\alpha} \quad if \ 0 < x_n \le \alpha \qquad (2)$$

$$x_{n+1} = \frac{1-x_n}{1-\alpha} \ if \ \alpha < x_n < 1 \ (3)$$

The Quadratic map is defined as follows:

 $x_n = \alpha - x_n^2$ (4) where α is the chaotic parameter and *n* is a number of iterations; $\alpha \in [1.5, 2]$.

IV. CHAOTIC SEQUENCES GENERATION BY USING MULTIPLE CHAOTIC MAPS

For increasing security level, Multiple Chaotic maps are used by merging each other instead of using a one chaotic map to generate chaotic sequence for hiding data. Three chaotic maps are used in multiplicative-additive form as given below.

$$C_n = (dC_1 + (1 - d)C_2) * C_2$$

where C_1 chaotic sequence of specific chaotic map, C_2 chaotic sequence of specific chaotic map, C_3 chaotic sequence of specific chaotic map, C_n new chaotic sequence by merging chaotic maps and *d* constant to increase the complex the equation and the value 0 < d < 1.

After it was generating sequences, it must be tested to know the sequences generated either chaotic or not. For knowing randomness in sequences generated or no, it is generated Gaussian noise to compare correlation of sequences generated with correlation of Gaussian noise as shown Fig (1). For better security, the shape of chaotic maps correlation should be a delta function. Hence, not all chaotic maps give noise-like chaos. There is randomness if a delta spike exists within a symmetric shape correlation as shown in Fig (2).

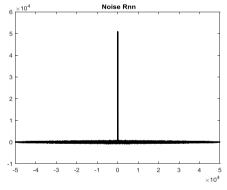


Fig. 1 Correlation of the Gaussian Noise

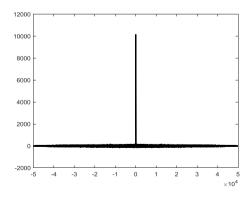


Fig. 2 Correlation of Quadratic chaotic sequence added with Tent chaotic sequence then multiplied by Logistic chaotic sequence with different initial condition in multiplicative-additive form.

V. THE CHARACTERISTIC ANALYSIS METHODS FOR CHAOTIC SEQUENCES

Chaotic characteristics of a nonlinear system can be determined by many methods such as Lyapunov exponent, Poincaré section and 0–1 test.

Lyapunov exponent value is either negative, positive or zero. In the case of negative values, the system is not chaotic. Positive values, the system is chaotic which is sensitive to the initial conditions and zero means that the stable system [8] [9]. Lyapunov exponent defined is:

$$\lambda_{x_o} = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{\infty} \ln|f'(x_i)| \quad (5)$$

where f' is the derivative of the function f.

Poincaré section of dynamic system is chaotic when dynamic system has pieces of dense points which are characterized a fractal structure [10] [11].

The 0-1Test of dynamical system is chaotic if trajectories are Brownian, otherwise it is regular dynamics [10] [12].

It has been shown that all the sequences that have been merged have chaotic characteristics as shown Fig (3), Fig (4) and Fig (5).

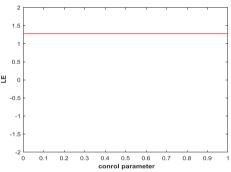


Fig. 3 Lyapunov exponents of Quadratic chaotic sequence added with the Tent chaotic sequence then multiplied by the Logistic chaotic sequence with different initial condition in a multiplicative-additive form.

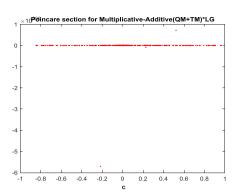


Fig. 4 Poincaré section of Quadratic chaotic sequence added with the Tent chaotic sequence then multiplied by the Logistic chaotic sequence with different initial condition in a multiplicative-additive form.

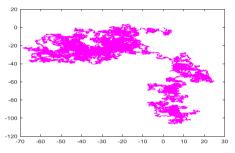


Fig. 5 0-1 Test of Quadratic chaotic sequence added with the Tent chaotic sequence then multiplied by the Logistic chaotic sequence with different initial condition in a multiplicative-additive form.

VI. DUPLICATE ADDRESSES PROCESSING OF CHAOTIC SEQUENCE

when it is modified chaotic sequences generated (real numbers) to get integers that will be used to specify the new pixel addresses in the cover image, there will be a problem which is the duplicate addresses and it can be solved by adding one to the following addresses to avoid duplication. To determine whether the attributes of the sequences have changed or not after modified and removed duplication, it is tested by the autocorrelation of the real chaos signal and the autocorrelation of an integer chaos signal. it can be shown in Fig (6) how the attributes of correlation have unchanged [4].

I. THE LSB STEGANOGRAPHY TECHNIQUE

The LSB steganography is one of the methods in spatial domain. Least significant bits (LSBs) of cover image are replaced with bits of the secret data. It is selected pixel of cover image either sequential or random, where the sequential selection of the pixels in the cover image causes a decrease in the security level, as result the random selection is preferred due to provide high security. There are two types of LSB steganography technique: the LSB substitution and LSB-matching. In the LSB-substitution, the pixel value can be increased and decreased or left without changing. In the LSB-matching method, a bit of secret data is the matched the LSBs of the cover image pixel. If it is matching so no occurred

changing, otherwise a pixel value is increased and decreased. [13], [14].

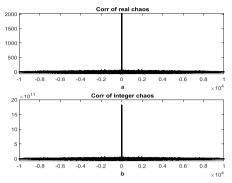


Fig. 6 The autocorrelation of Quadratic chaotic sequence added with Tent chaotic sequence then multiplied by Logistic chaotic sequence with different initial condition in multiplicative-additive form. (a) correlation of real chaos (b) correlation of integer chaos.

II. THE PROPOSED SYSTEM

According to the addresses which were generated by merging multiple chaotic maps, three expanded systems are proposed a Multiplicative-Additive Chaotic LSB method, a Multiplicative-Additive Chaotic Identical Bits Method, and a Multiplicative-Additive Chaotic Data Mapping and LSB Substitution method.

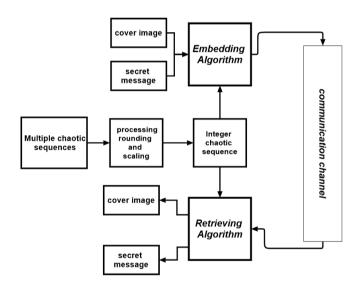


Fig. 7 Block diagram of the proposed system

III. A MULTIPLICATIVE-ADDITIVE CHAOTIC LSB STEGANOGRAPHY

The proposed system uses multiple chaotic maps merged to generate integer chaotic to select the pixel addresses of the cover image for embedding the secret message. The parameters of the chaotic maps and the method of integrating chaotic sequences are secret keys known only to the sender and receiver. The attacker cannot detect the existence of a secret message without knowing these secret keys. The proposed system is divided into two processes; a Multiplicative-Additive Chaotic -LSB embedding and a Multiplicative-Additive Chaotic -LSB retrieving.

IV. A MULTIPLICATIVE-ADDITIVE CHAOTIC -IDENTICAL-BITS STEGANOGRAPHY

This technique [15] is based on searching the identical bits between the cover image bits and the secret message bits. If there are not identical bits, secret message bits are hidden in 2LSBs of the cover image. This provides a security level more than traditional LSB technique. The proposed system uses multiple chaotic maps merged to generate chaotic addresses, to select the pixel addresses of the cover image for embedding the secret message. The proposed system is divided into two processes; a Multiplicative-Additive Chaotic -Identical-Bits embedding and a Multiplicative-Additive Chaotic -Identical-Bits Retrieving.

V. A MULTIPLICATIVE-ADDITIVE CHAOTIC DATA MAPPING AND LSB SUBSTITUTION

In the method which is discussed in [16], the first cover pixel bits and secret data bits were divided into pairs. Next, in the embedding process, these pairs of four secret data bits were mapped with the 4-MSBs of cover pixel bits. The 2LSB substitution is employed to maintain the mapping status between the cover and secret data. The proposed system uses multiple chaotic maps merged to generate integer chaotic to select the pixel addresses of the cover image for embedding the secret message.

VI. QUALITY MEASURES

There are different types of measurements to measure the visual quality for steganography (ex. MSE, PSNR) [17]. The MSE illustrates the square of error between cover image and stego image, MSE measures the distortion in image. The PSNR is a ratio of the extreme signal to noise power between the stego image and the cover image, PSNR measures the quality of the image. The MSE and PSNR define by:

$$MSE = \frac{1}{H*W} \sum_{i=1}^{H*W} (C_i - S_i)^2$$
(6)
$$PSNR = 10 * \log_{10} \frac{Max^2}{MSE}$$
(7)

Where C_i represents cover pixel value; S_i represents stego pixel value, H * W: represent the height and width of cover the image, Max = maximum pixel intensity value that is 255. According to the results in Table (1) and Table (2), the two proposed systems are better quality and higher security than chaotic LSBs and chaotic identical bits techniques in [4] due to provide a balance between quality and security. We note that the proposed a Multiplicative-Additive Chaotic IdenticalBits technique is better than the proposed a Multiplicative-Additive Chaotic -Data Mapping and LSB Substitution and a Multiplicative-Additive Chaotic -LSB technique.

The size ratio Rm between message size and cover size can be calculated on various sizes of the secret image (cell.tif image 5 * 5, 10 * 10, 20 * 20, 30 * 30) by the following equation (8):

$$Rm = \frac{\text{Message Size}}{\text{Cover ImageSize}}$$
(8)

The relationship between the size ratio Rm and the PSNR is the reverse, that is meaning the size ratio Rm increases, PSNR decreases but the size ratio Rm increases, MSE increases as shown in Fig. (8) and Fig. (9).

Table 1 Comparison the value of PSNR and MSE between Chaotic-2LSB technique in [4] and Proposed a Multiplicative-Additive Chaotic -2LSB technique implemented in this work when hiding an image of size (100*100)

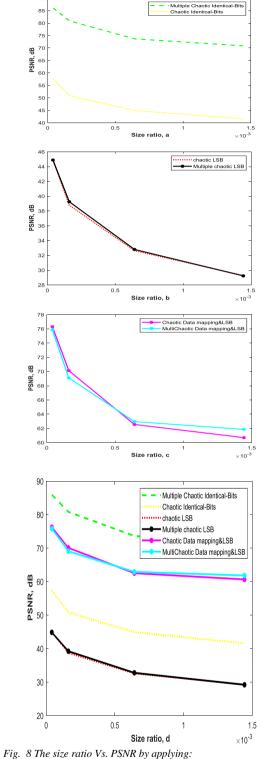
		Chaotic-2LSB technique in [4]		Proposed a Multiplicative- Additive Chaotic -2LSB	
Cover image	Cover size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912x684	55.9020	0.1671	55.9109	0.1667
lighthouse.png	480x640	52.8613	0.3365	52.8554	0.3369
yellowlily.jpg	1224x1632	60.9381	0.0524	60.9703	0.0520
flamingos.jpg	1296x972	58.9762	0.0823	58.9876	0.0821

Table 2 Comparison the value of PSNR and MSE between Chaotic identicalbits technique in [4] and Proposed a Multiplicative-Additive Chaotic identical-bits technique implemented in this work when hiding an image of size (100*100)

		Chaotic identical- bits technique in [4]		Proposed a Multiplicative- Additive Chaotic identical-bits	
Cover image	Cover size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912x684	31.0867	50.6302	60.2564	0.0613
lighthouse.png	480x640	27.1865	124.2897	57.3885	0.1186
yellowlily.jpg	1224x1632	34.9057	21.0142	64.7120	0.0220
flamingos.jpg	1296x972	34.3944	23.6394	64.2851	0.0242

Table 3 Comparison the value of PSNR and MSE between proposed Chaotic Data Mapping and LSB Substitution and Proposed a Multiplicative-Additive Chaotic - Data Mapping and LSB Substitution technique implemented in this work when hiding an image of size (100*100)

work when maing an image of siz		Chaotic-Data Mapping and LSB Substitution		Proposed a Multiplicative- Additive Chaotic - Data Mapping and LSB Substitution	
Cover image	Cover size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912x684	50.4663	0.5840	52.0459	0.4060
lighthouse.png	480x640	50.6059	0.5656	61.1042	0.0504
yellowlily.jpg	1224x1632	58.1773	0.0989	64.3300	0.0240
flamingos.jpg	1296x972	55.7706	0.1722	62.0901	0.0402



(a) Chaotic identical-bits and a Multiplicative-Additive Chaotic identicalbits.

bits.
(b) Chaotic LSB and Multiple-chaotic LSB.
(c) a Multiplicative-Additive Chaotic - Data Mapping and LSB Substitution and Chaotic Data Mapping and LSB Substitution technique. (d) all proposed method

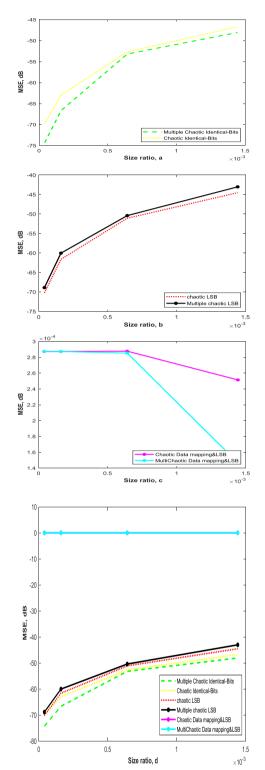


Fig. 9 The size ratio Vs. MSE by applying: (a) Chaotic identical-bits and a Multiplicative-Additive Chaotic identical-bits.

(b) Chaotic LSB and Multiple-chaotic LSB.
(c) a Multiplicative-Additive Chaotic - Data Mapping and LSB Substitution and Chaotic Data Mapping and LSB Substitution technique.

(d) all proposed method

VII. HISTOGRAM ANALYSIS

Histogram can be determined using the distribution of pixels by comparing both stego and cover image. Fig. (10), Fig. (11) and Fig (12) show the histogram of cover and stego images when applying the proposed a Multiplicative-Additive Chaotic -LSB technique, a Multiplicative-Additive Chaotic -identical bits technique and Proposed a Multiplicative-Additive Chaotic - Data Mapping and LSB Substitution technique. We note little distortion after the secret message is embedding into the cover image except a Multiplicative-Additive Chaotic - Data Mapping and LSB Substitution technique.

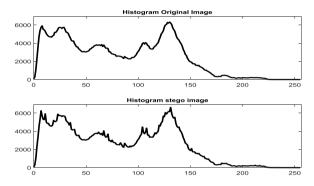


Fig. 10 Histogram analysis for original image (Toysnoflash) and stego image when applying a Multiplicative-Additive Chaotic identical-bits.

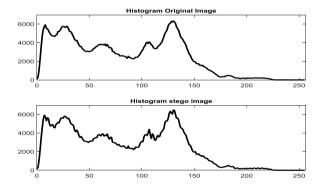


Fig. 11 Histogram analysis for original image (Toysnoflash) and stego image when applying a Multiplicative-Additive Chaotic 2LSB.

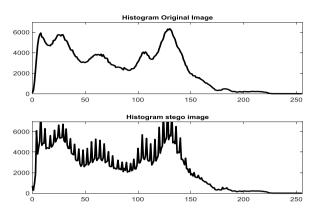


Fig. 12 Histogram analysis for original image (Toysnoflash) and stego image when applying a Multiplicative-Additive Chaotic Data Mapping and LSB Substitution.

VIII. CORRELATIVE ANALYSIS

The correlation between two contiguous pixels (horizontal, vertical and diagonal) is calculated by selecting 5000 pairs of contiguous pixels random from the cover image and the stego images. It can be computed by the following equations:

$$R_{xy} = \frac{\operatorname{cov}_{(x,y)}}{\sqrt{D_{(x)}} * \sqrt{D_{(y)}}}$$
(9)

$$\operatorname{cov}_{(x,y)} = \varepsilon(x - \varepsilon_x)(y - \varepsilon_y) \tag{10}$$

$$\varepsilon_x = \frac{-}{N} \sum_{i=1}^N x_i \tag{11}$$

$$D_{(x)} = \frac{1}{N} \sum_{i=1}^{N} (x_i - \varepsilon_x)^2$$
(12)

$$\operatorname{cov}_{(x,y)} = \frac{1}{N} \sum_{i=1}^{N} (x_i - \varepsilon_x) (y_i - \varepsilon_y)$$
(13)

where, x and y are the intensity values of two adjacent pixels and N is the total number of pixels in the image. Fig. (13), Fig. (14) and Fig. (15) show the correlation between two adjacent pixels of the cover image (Toysnoflash) and stego image after embedding the secret image (cell) by the proposed a Multiplicative-Additive Chaotic -LSB, a Multiplicative-Additive Chaotic identical bits technique and a Multiplicative-Additive Chaotic - Data Mapping and LSB Substitution technique. There is no significant difference in correlation coefficient after embedding. This indicates a high security level.

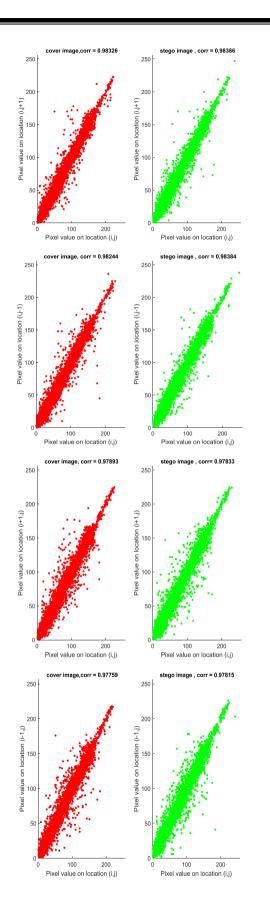
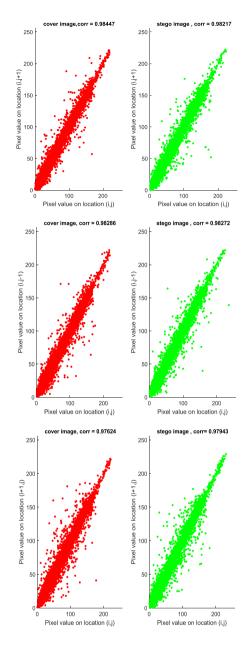


Fig. 13 Correlation of adjacent pixels (vertical and horizontal) in the a Multiplicative-Additive Chaotic Identical-Bits technique



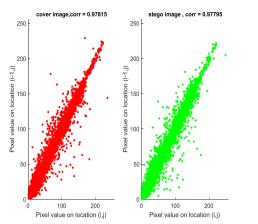
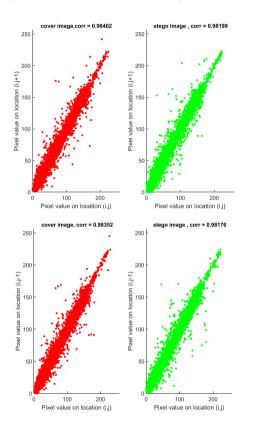


Fig. 14 Correlation of adjacent pixels (vertical and horizontal) in the a Multiplicative-Additive Chaotic 2LSB technique.



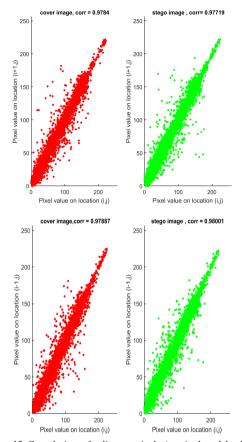


Fig. 15 Correlation of adjacent pixels (vertical and horizontal) in the Multiplicative - Additive Chaotic - Data Mapping and LSB Substitution technique.

IX. FUTURE DIRECTIONS

The approach would be tested under noise and attenuation types, e.g. Rayleigh fading [18]. The approach can also be tested under the conditions of other channels models such as Nakagami or geometrical models as in [18] [19] [20] [21], in addition to testing under the method of OFDM [22] [23] and testing under the integration of chaos with OFDM and space-time coding [24]. Testing the robustness of the approach for compressed data over OFDM could also be handled [25].

X. CONCLUSION

In this paper, three systems are used to hide information in the spatial domain. These systems rely on well-known LSB, the identical bits and data mapping and LSB substitution. The new systems have improved upon the latest approach to applying chaos theory for address shuffling, as they have created a new security dimension by combining multiple chaos maps according to Multiplicative-Additive Chaotic form for generating chaotic sequences with better chaotic properties.

These sequences increase the chaotic range of available parameters and are secure against attacks even if there is a suspicion of a secret message. Several performance measures have been considered to test security levels, such as histogram analysis, PSNR, and correlative analysis. The results show that the proposed systems have a much higher level of security than their conventional counterparts. It can be pointed out that the proposed approach is versatile as it can be added to other steganography systems to improve their security.

XI. REFERENCES

- S. S. A. K. Singh and S. P. Ghrera, "A Recent Survey On Data Hiding Techniques," International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.
- [2] A. Sharif, M. Mollaeefar and M. Nazari, "A novel method for digital image steganography based on a new three-dimensional chaotic map," Springer Science, Business Media New York, 2016.
- [3] A. Rasmi and M. Mohanapriya, "An Extensiv Survey of Data Hiding Techniques," European Journal of Applied Sciences 9 (3): 133-139, 2017 ISSN 2079-2077 © IDOSI Publications, 2017 DOI: 10.5829/idosi.ejas.2017.133.139, 2017.
- [4] O. N. Kadhim and Z. M. Hussain, "Information Hiding using Chaotic-Address Steganography," Journal of Computer Science, 2018.
- [5] H. Elkamchouchi, W. M. Salama and Y. Abouelseoud, "Data hiding in a digital cover image using chaotic maps and LSB technique,"12th International Conference on Computer Engineering and Systems (ICCES), 2017.
- [6] A. Anees, A. M. Siddiqui, J. Ahmed and I. Hussain, "A technique for digital steganography using chaotic maps," Springer Science, Business Media Dordrecht, 2013.
- [7] S. Dogan, "A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map," I. J. Computer Network and Information Security, 2018.
- [8] G. P. Williams, Chaos Theory Tamed book, JOSEPH HENRY PRESS Washington, 1997.
- [9] N. Ramadan, H. E. H. Ahmed, S. E. Elkhamy and F. E. Abd El-Samie, "Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map," American Journal of Signal Processing, DOI: 10.5923/j.ajsp.20160601.01,

2016.

- [10] S. Kehui, Chaotic Secure Communication, Berlin/Boston: Tsinghua University Press and Walter de Gruyter GmbH., 2016.
- [11] A. BAG and B. GANGULI, "METHODS TO DETECT CHAOS AND BIFURCATION ANALYSIS," Diss. 2015.
- [12] G. A. Gottwald and I. Melbourne, "The 0-1 Test for Chaos: A review," Springerlink, Part of the Lecture Notes in Physics book series (LNP, volume 915), 4 March 2016.
- [13] A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images," IEEE signal processing letters 12.6 (2005): 441-444.
- [14] H. Hiary, K. . E. Sabri, M. S. Mohammed and A. Al-Dhamari, "A Hybrid Steganography System based on LSB Matching and Replacement," (IJACSA) International Journal of Advanced Computer Science and Applications, 2016.
- [15] A. M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality," Applied Mathematical Sciences, Vol. 6, no. 79, 3907 - 3915, 2012.
- [16] A. A. Zakaria , M. Hussain , A. W. Abdul Wahab, M. Y. Idna Idris , N. A. Abdullah and K.-H. Jung, "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution," MDPI, Basel, Switzerland., 2018.
- [17] M. Tayel, H. Shawky and A. E.-D. Sayed Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data," ISBN 978-89-5519-162-2, 2012.
- [18] A. K. Gurung, F. S. AI-Qahtani, . Z. M. Hussain and H. Alnuweiri, "Performance Analysis of Amplify-Forward Relay in Mixed Nakagami-m and Rician Fading Channels," The IEEE International Conference on Advanced Technologies for Communications (ATC), 2010.
- [19] A. K. Gurung, F. S. Al-Qahtani, K. A. Qaraqe, H. Alnuweiri and Z. M. Hussain, "General Order Antenna Selection in MIMO Cooperative Relay Network," International Conference on Signal Processing and Communication Systems (ICSPCS'2010), 2010.

- [20] S. S. Mahmoud, F. S. Al-Qahtani, Z. M. Hussain and A. Gopalakrishnan, "Spatial and temporal statistics for the geometrical-based hyperbolic macrocell channel model," Digital Signal Processing: A Review Journal, 2008.
- [21] S. S. Mahmoud, Z. M. Hussain and P. O'Shea, "A Geometrical-Based Microcell Mobile Radio Channel Model," Wireless Networks, 2006.
- [22] A. K. Gurung, F. S. Al-Qahtani, A. Z. Sadik and Z. M. Hussain, "Power Savings Analysis of Clipping and Filtering Method in OFDM Systems," The Australasian Telecommunication Networks and Applications Conference (ATNAC), 2008.
- [23] K. Abdullah and Z. M. Hussain, "Simulation of Models and BER Performances of DWT-OFDM versus FFT-OFDM," in Algorithms and Applications, InTech Publishers, 2011.

- [24] Y.-S. Lau, K. H. Lin and Z. M. Hussain, "Space-Time Encoded Secure Chaos Communications with Transmit Beamforming," IEEE TENCON, 2007.
- [25] N. Al-Hinai, . A. Z. Sadik and Z. M. Hussain,"Transmission of Compressed Image over PLC Channel: A Comparative Study," IEEE GCC Conference and Exhibition, 2009.