Journal of Computer Science

Original Research Paper

A Multiple-Chaotic Approach for Steganography

Haneen H. Alwan and Zahir M. Hussain

Faculty of Computer Science and Mathematics, University of Kufa, Najaf 54001, Iraq

Article history
Received: 08-07-2019
Revised: 01-10-2019
Accepted: 16-10-2019

Corresponding Author:
Zahir M. Hussain
Faculty of Computer Science and Mathematics, University of Kufa, Najaf 54001, Iraq
Email: zahir.hussain@uokufa.edu.iq
zmhussain@ieee.org

Abstract: In a recent work, chaos has been utilized to modify addresses of message bits while hidden in a cover image. In this study, we extend the above technique to include multiple chaotic maps for increased security. Three systems have been modified using chaotic-address mapping for image steganography in the spatial domain. The first system, the well-known LSB technique, is based on the selection of pixels and then hides secret message in the Least Significant Bits LSBs of the given pixel. The second system is based on searching for the identical bits between the secret message and the cover image. The third system is based on the concept of LSB substitution. It employs mapping of secret data bits onto the cover pixel bits. To increase the security performance of the above chaos-based steganographic techniques, multiple-chaotic maps are introduced in this study by using multiple formulas to generate chaotic sequences used to track the addresses of shuffled bits. The generated chaotic sequences were evaluated to determine the randomness (using correlation tests) and the chaotic characteristics of a nonlinear system (using Lyapunov exponent, Poincaré section and 0-1 test). The performance and security levels of the proposed techniques were evaluated by using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), histogram analysis and correlative analysis. The results show that the proposed method performs existing systems.

Keywords: Chaos Theory, Chaotic Maps, Lyapunov Exponents, Steganography, Data Security

Introduction

Data-Hiding is a fundamental part of computer and communication security, data is saved and exchanged through computer and communication devices. Therefore, it is necessary to provide high security for data to prevent unauthorized users from using or manipulating data. Cryptography and steganography, the two parts have the same goal to protect secret data from hackers, But the two parts differ in the way how data is protected. Cryptography provides security by changing content of the message, but steganography is hidden the message without changing its content. In steganography, which information is hidden in an image or other files. Image Steganography is one of the methods that have been developed for secret communication (Li *et al.*, 2011). Image steganography algorithms are classified into two fields: Spatial domain and transform domain-based algorithms. Spatial-based algorithms depend on modify pixel intensities of cover image for data hiding (Vigila and Muneeswaran, 2015). One of the most popular algorithms used in the spatial domain is Least Significant Bits LSB, LSB is implemented by changing least significant bit values in sequential order and this may reduce the security level. Transform domain-based algorithms, the algorithms are based on converting the cover image to the frequency domain where the secret data is embedded in the transform coefficients that can change to hide the data (Wu and Noonan, 2012). Several approaches have been proposed, mostly based on hiding information in least significant bits LSBs of image pixels. As the attacker knows about these famous approaches, the hidden information could be at risk, where the sequential selection especially in LSB approach of the pixels in the cover image causes a decrease in the security level so the random selection will be provided high security. Chaos theory has been used since 1970s, where it has attracted the interest of different scientific research areas, such as physics, mathematics, engineering and biology, etc. (Zhang *et al.*, 2005). Chaos is deterministic, nonlinear, dynamic systems and sensitivity to initial conditions that means any change in the initial condition will result in a quick change in the output, also it has random-like properties, so chaos is used to generate random numbers (Ramadan *et al.*, 2016). Chaos is can be found in nature, through the research and development of chaos theory researchers have found many similar dynamic models of disorder behavior (Sun, 2016). Due of the random behavior of chaos, it can be used to provide a high level of security in steganography (Kadhim and Hussain, 2018).

Related Works

Many researchers have developed LSB method to increase the level of security or hidden data capacity while maintaining image resolution. In this method (Bai *et al*., 2017) is based on combing between LSB substitution mechanism and edge detection where the pixels of cover image are divided into edge areas and non-edge areas. The edge image can be determined by the last 5 LSBs to the original image called MSB image. The method is achieved high embedding capacity while keeping visual quality. This proposed method (Elkamchouchi *et al*., 2017) looks at several alternative schemes to hide a grayscale image in a colored cover image in a spatial area. First, we consider the use of one-dimensional chaotic maps (tent map) against a two-dimensional map (baker map) to select the pixel group where the secret message bits are embedded. The red color channel of the cover image for predefined pixels is affected by the embedding because the eye is not too sensitive to minor changes in this color channel. Then, two systems are examined to embed the LSB; they embed one bit per pixel and embed two bits per pixel. The method is achieved PSNR is high and MSE is low. This proposed method (Tutuncu and Demirci, 2018), An algorithm depends on the LBS embedded method, whose indicators are determined by proposing chaotic number generators. Chaotic number generators generate random and unexpected numbers. The algorithm depends on two main things. firstly, selecting the bits to be embedded as chaotic, secondly, disability to select the data that is embedded in color channel by distorting the other channels. In this proposed method (Sharif *et al*., 2016), a robust image steganography by 3D chaotic map (LCA map). In the proposed method chaotic map is used to generate random numbers for selection with length of 2 L. it is used both LSBs and MSBs with 3D chaotic maps to select of coveted pairs for hiding the secret message. This method has achieved good results in sensitive keys, Quality index, PSNR, MSE and hiding capacity. In this proposed method (Dogan, 2018), the data is hidden by applying the modulo function to the pixel pairs. Random number can be generated from chaotic maps because data-hiding coefficients are selected by random number. If a coefficient of 0 is used, the subtraction factor is used between pixel pairs. If the parameter is 1, the summary operator for the specified pixel pairs is used. In proposed method going to incorporate multiple chaos sequences from different generators as additional dimensions in data hiding. The proposed algorithm (Anees *et al*., 2014) employs in spatial domain and embeds the information in LSBs of carrier image. The carrier image is first broken into two parts, upper and lower, respectively. The information signal is converted into binary of eight bits and split into four MSBs and four LSBs. The information MSBs is embedded into upper part of carrier signal and LSBs are in its lower part. The chaotic maps engaged in proposed algorithm define the exact positions in upper and lower part for embedding of information bits, that is, TDERCS map defines the row number, NCA map defines the column number and the logistic map defines the frame number. After selecting the specific pixel of carrier image for embedding information, it is converted into binary and split into MSBs and LSBs. Its LSBs are then replaced with respective information bits. After embedding each symbol of information, upper and lower parts of the carrier join and makes the steganography image. The LSBs are replaced of the carrier image and are considered as a loss of information or regarded as an addition of noise in it. This method has shown good results against various differential attacks. In this proposed method (Zaghbani and Rhouma, 2013), the insertion stage divides the image into blocks (3 × 3). The blocks that are added to the confidential message are selected through random numbers that are accomplished by the logistic map. We add into each given block three different bits of secret message. The three pixels can be found by estimated values relative to their adjacent. The results show that algorithm provides higher embedding capacity and well image quality. In this proposed method (Tayel *et al*., 2012), It begins by increasing the original pixels of the image from bytes to the color of the word color and then randomly distributes the hidden image pixels within the lower byte of the cover image pixels by distributing the chaos. The original image is isolated from the stego image received in the first phase of the receiver. The initial state of the random chaotic sequence is used to collect a stego image from the lower byte of pixels. The hidden image is then reconstructed. The results show a good hiding of the data tested in the original images with high security if the stego analysis is performed on the original image. In the proposed method (Yu *et al*., 2010) improved adaptive LSB: First, the number of bits to be included in a particular segment is adjusted. With proper parameters, we can get high capacity while maintaining a high degree of security. Second, a Lower Modification Rule (LMR) is used to reduce the modification. Shuffle Message Bits based on Chaos and Genetic Algorithm: use the logistic map for shuffling and use GA to find parameters for the logistic map. The results show that our algorithm realizes high ability of embedding while maintaining good image quality and high degree of security.

In the above proposed methods, the LSB mechanism and other mechanisms were combined to increase the embedding capacity while maintaining the visual quality. Other proposed Methods, LSB mechanism has been integrated with chaos theory for providing high level of security, which characterized by random behavior and sensitive to any change in the initial condition.

Chaotic Maps

A chaotic map used to generate chaotic sequences that are used to hide data. The Chaos sequences are created by using various chaotic maps (Sathishkumar *et al*., 2011). Chaotic maps which have statistically powerful features are used in steganography methods for providing privacy of secret data (Dogan, 2018). There are several different chaotic maps used to generate chaos sequence.

Logistic Map

The logistic map is the most commonly used, where you generate a chaotic sequence, it is described by equation:

$$x_{n+1} = ax_n\left(1 - x_n\right) \tag{1}$$

where, the parameter $\alpha \in (0, 4]$ and $x_n \in (0, 1)$. When 3.5699 < α ≤ 4, it is chaotic behavior (Sun, 2016).

Tent Mapx

It is implemented in the domain of chaotic spread spectrum communication, chaotic encryption system and chaotic optimum algorithm. It is sometimes called the hat map, the x auto-correlation function for the tent map is delta correlated (Sun, 2016). In mathematics, it is a repetitive function and tent-shaped, take *x* (*n*) point on the real line and put it at another point (Sathishkumar *et al*., 2011). The equation of tent map where $0 < x_n$ and parameter $\alpha < 1$ (all positive) is:

$$x_{n+1} = \frac{x_n}{\alpha}\ if\ 0 < x_n \le \alpha \tag{3}$$

$$x_{n+1} = \frac{1 - x_n}{1 - \alpha}\ if\ \alpha < x_n < 1 \tag{4}$$

If α = 0.5 gives the Symmetric Tent Map, which exhibits chaotic behavior; But α ≠ 0.5, gives asymmetric tent maps, which exhibit noise-like data.

Quadratic Map

The quadratic map is chaotic, because it is non-linear. Since contains an equation that determines the behavior of the system so it is deterministic. When initial value x_0 change, it results in a totally different behavior for the map. It can be described by equation (Ramadan *et al*., 2016):

$$x_n = \alpha - x_n^2 \tag{5}$$

where, α is the chaotic parameter and *n* the number of iterations; $\alpha \in [1.5,2]$.

Chaotic Sequences Generation by Using Multiple Chaotic Maps

Chaotic maps are combined for increasing security level instead of using a one chaotic map to generate chaotic sequence for hiding data. The following cases illustrate how chaotic maps will be integrated and generate a new chaotic sequence:

Input: N number of samples, C_1 first Chaotic Sequence of specific chaotic map, C_2 Second Chaotic sequence of specific chaotic map, C_3 chaotic sequence of same first chaotic map but different initial condition and *d* constant.

Output: C_n new chaotic sequence by merging chaotic maps:

Case 1: Using same chaotic map, but different initial condition in two periods:

$$C_n\left(1 : N/2\right) = C_1\left(1 : N/2\right)$$
$$C_n\left(N/2+1 : N\right) = C_3\left(N/2+1 : N\right)$$

Case 2: Using same chaotic map, but different initial conditions in multiplicative form:

$$C_n = C_1 * C_3$$

Case 3: Using same chaotic map, but different initial conditions in additive form:

$$C_n = dC_1 + \left(1 - d\right)C_3$$

Case 4: Using different chaotic maps in multiplicative form:

$$C_n = C_1 * C_2$$

Case 5: Using different chaotic maps in additive form:

$$C_n = dC_1 + \left(1 - d\right)C_2$$

After multiple chaotic maps were merged. For knowing there is randomness in sequences generated or no, then it is generated Gaussian noise (For testing) to compare correlation of chaotic sequences generated with correlation of Gaussian noise as shown Fig. 1. The correlation shape of chaotic sequences generated should be a delta function for better security. Hence, not all chaotic maps give noise-like chaos such as in case, using same map but with slightly different initial condition as shown in Fig. 2. if a delta spike exists within a symmetric shape correlation, then randomness is there as shown in Fig. 3 to 7.

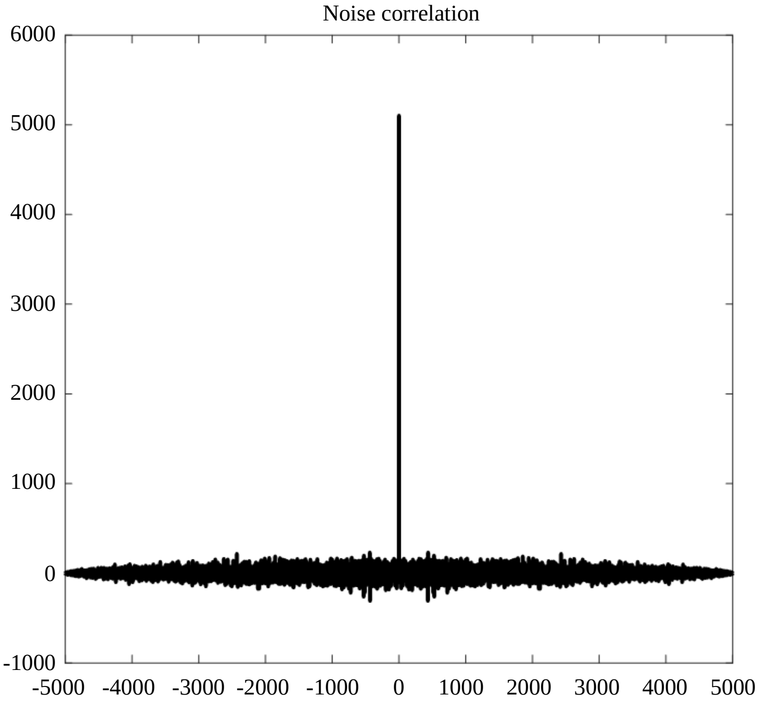


Fig. 1: Correlation of the Gaussian noise

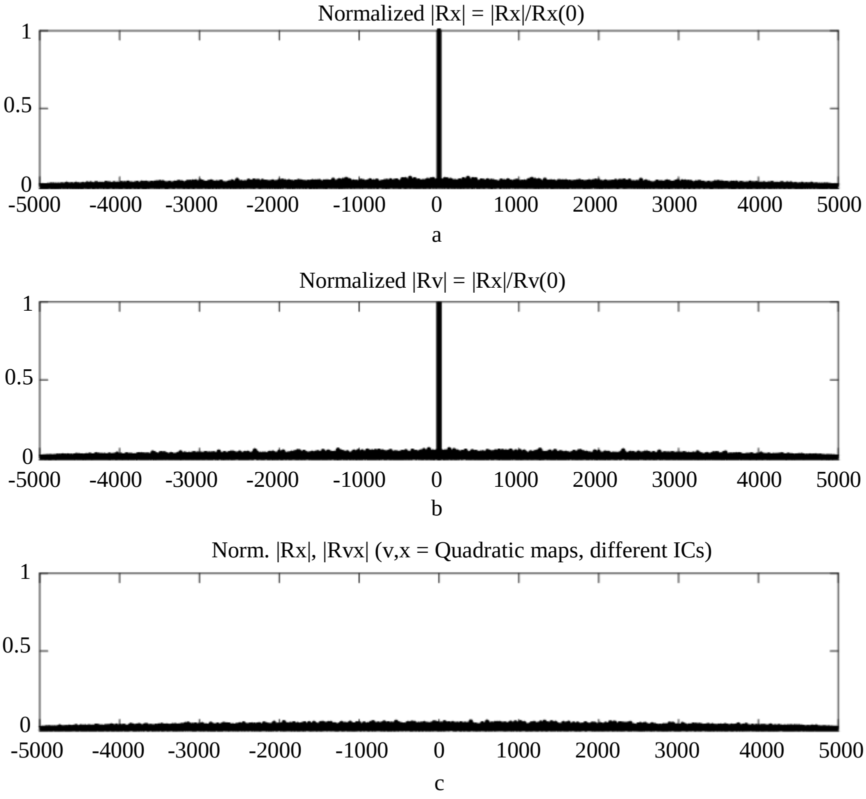


Fig. 2: Using same map but with slightly different initial condition: (a). Correlation of the quadratic map (α = 2 and xn = 0.7). (b). Correlation of the quadratic map (α = 2 and xn = 0.7+ 0.00000001). (c). Correlation of a and b

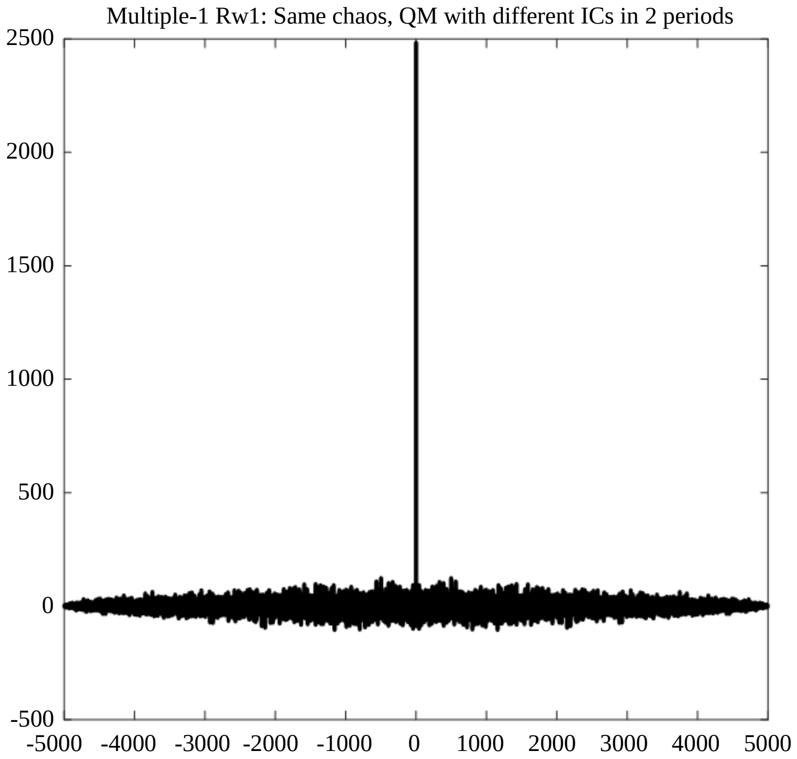


Fig. 3: Correlation of the two quadratic map chaotic sequences but different initial condition in two periods as case 1

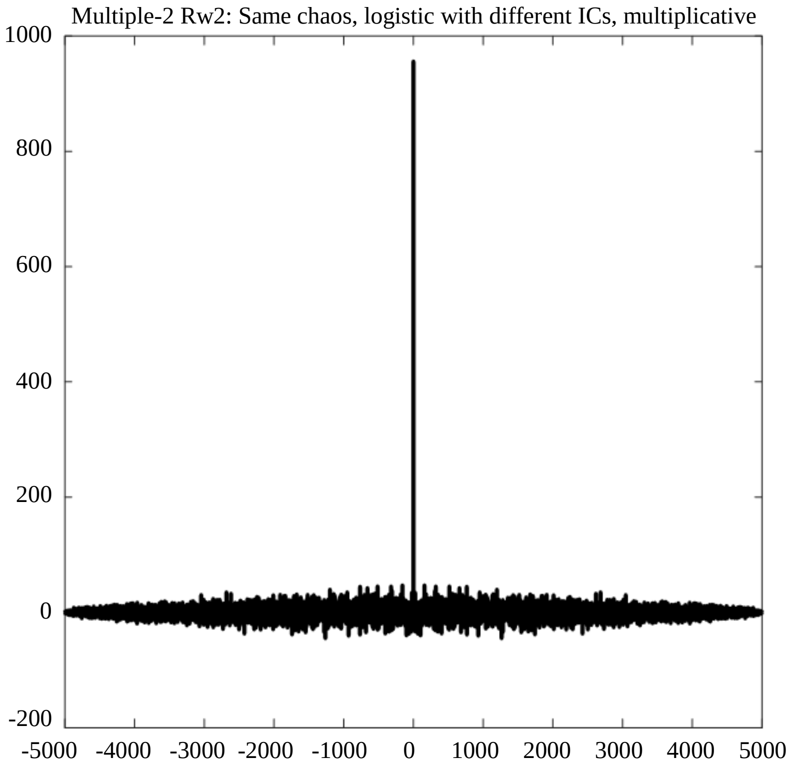


Fig. 4: Correlation of the two logistic chaotic sequences but different initial condition in multiplicative form as case 2

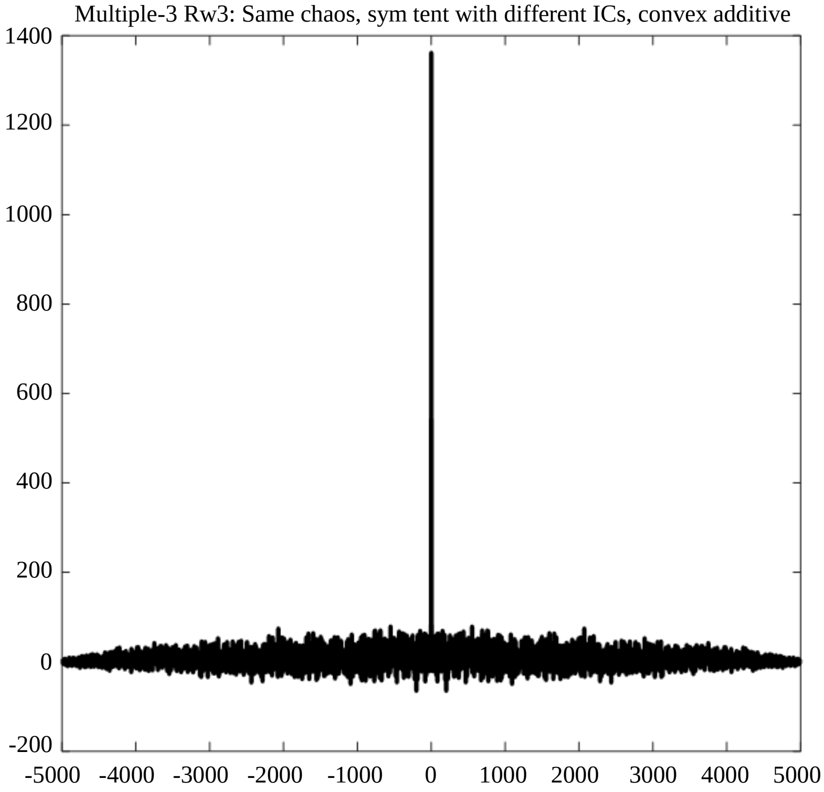


Fig. 5: Correlation of the two tent chaotic sequences but different initial condition in additive form as case 3

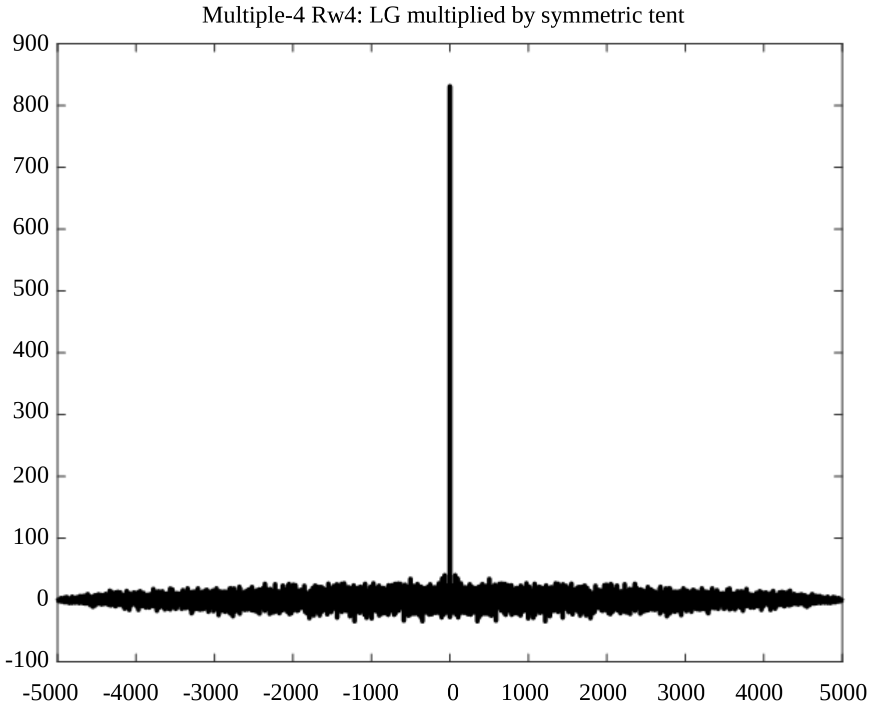


Fig. 6: Correlation of the logistic chaotic sequence multiplied by Tent chaotic sequence with different initial condition as case 4

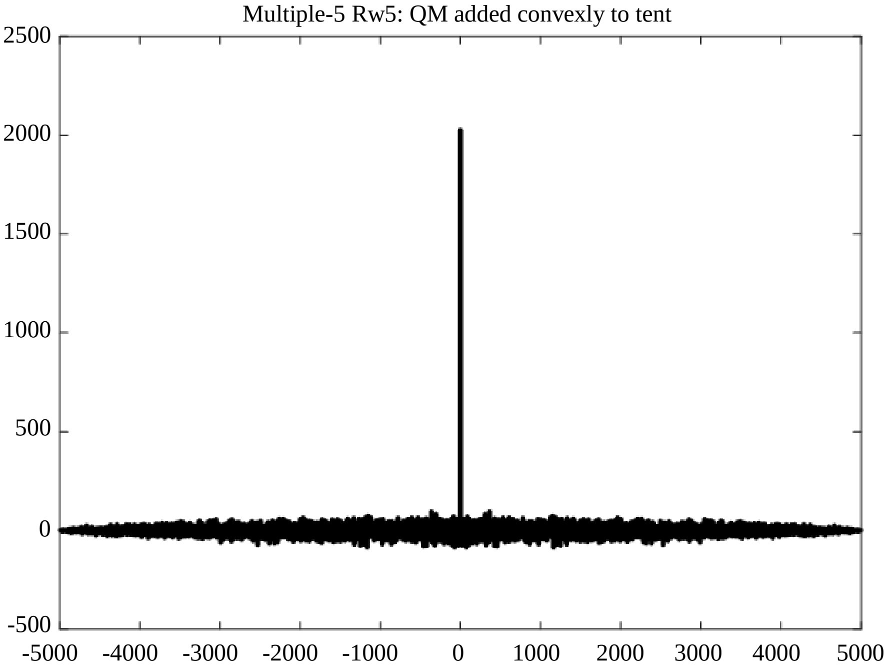


Fig. 7: Correlation of the quadratic chaotic sequence added with tent chaotic sequence with different initial condition as case 5

Characteristic Analysis Methods for Chaotic Sequences

Lyapunov Exponent has been calculated that describes the dynamics of path evolution that gives the average rate of convergence or distance between two adjacent paths in the phase space. Its value is either negative, positive or zero. In the case of negative values means that the two paths are close to each other This means that the system is not chaotic, Positive values mean that the two paths are separated from each other, this means that a chaotic system which is sensitive to the initial conditions and zero means that the stable system as shown in Fig. 8 to 10 (Sun, 2016; Ramadan *et al*., 2016). Lyapunov exponent in one dimensional maps can be defined as follows:

$$\lambda_{x_0} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{\infty} \ln \left| f'(x_i) \right| \quad (6)$$

where, *f*' is the derivative of the function *f*.

Poincaré section is also used for testing of chaotic dynamics. when dynamic system has only one fixed point or a small number of discrete points, the motion of dynamic system is periodic. when dynamic system has closed curve, the motion of dynamic system is quasi-periodic. when dynamic system has pieces of dense points that which are characterized a fractal structure, the motion of dynamic system is chaotic as shown in Fig. 11 to 13 (Sun, 2016; Bag and Ganguli, 2015).

The 0 - 1 Test is also used for distinguishing between regular and chaotic dynamics in deterministic dynamical systems. If trajectories are bounded, Dynamical systems are regular dynamics. But if trajectories are Brownian, Dynamical systems are chaotic dynamics as shown in Fig. 14 to 16 (Sun, 2016; Gottwald and Melbourne, 2016). After chaotic maps were merged and chaotic sequences were produced, it was shown some methods to determine the chaotic characteristics of a nonlinear system as Lyapunov exponent, Poincaré section and 0-1 test. It has been shown that all the generated sequences that have been merged have chaotic characteristics.

Duplicate Addresses Processing of Chaotic Sequence

Chaotic sequences generated real numbers within range [0,1]. These sequences must be modified to get integers that will be used to specify the new pixel addresses in the cover image. When the chaotic sequence was converted into integer numbers, there is a problem that will appear is the duplicate addresses. This problem can be solved by adding one to the following addresses to avoid duplication, the autocorrelation of the real chaos signal and the autocorrelation of an integer chaos signal to determine whether the attributes of the correlation have changed or not, (Kadhim and Hussain, 2018) as shown in Fig. 17.

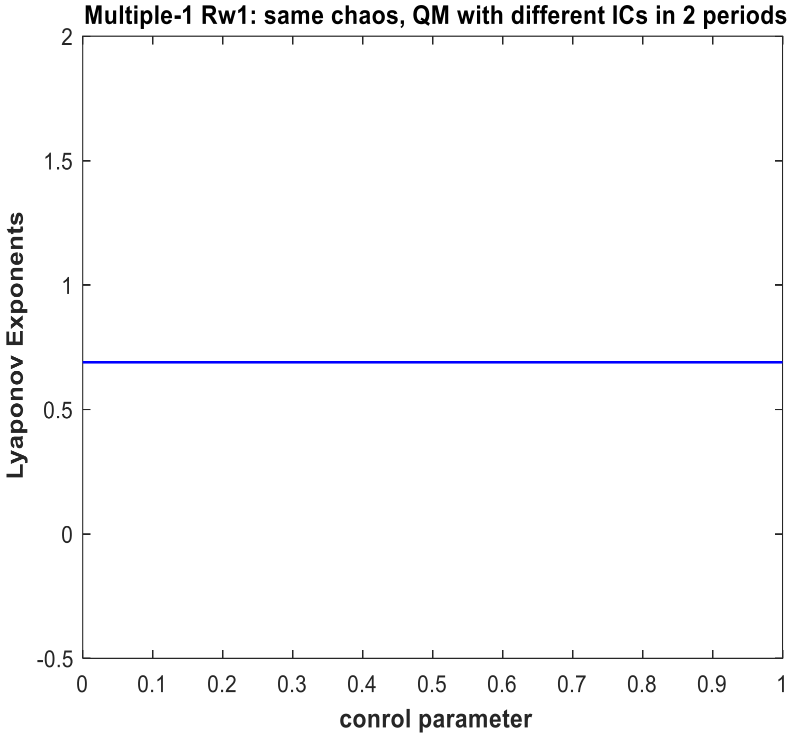


Fig. 8: Lyapunov exponents of the case 1 by using same quadratic map, but different initial condition in multiple periods

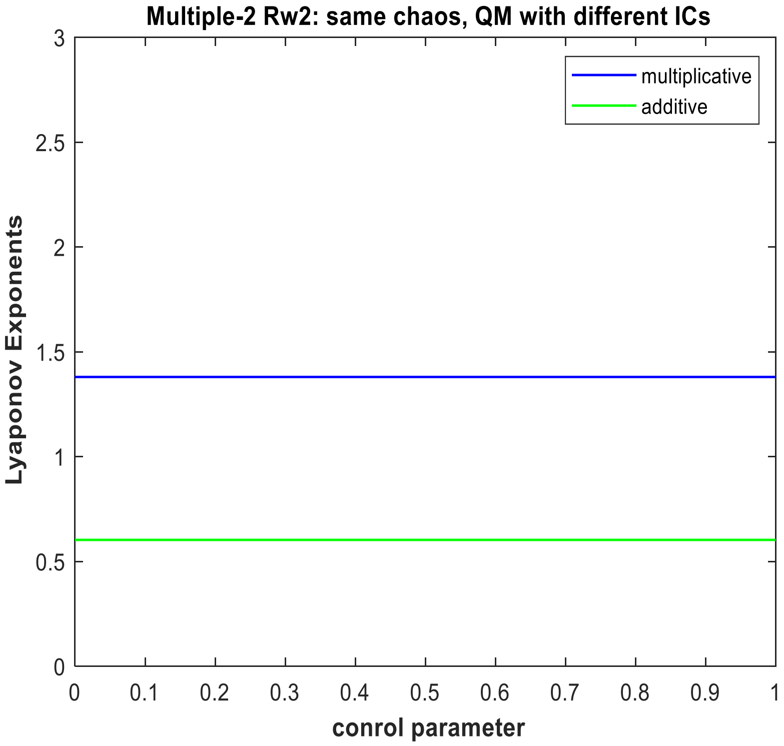


Fig. 9: Lyapunov exponents of the case 2 and case 3 by using same quadratic map, but different initial conditions in multiplicative and additive form

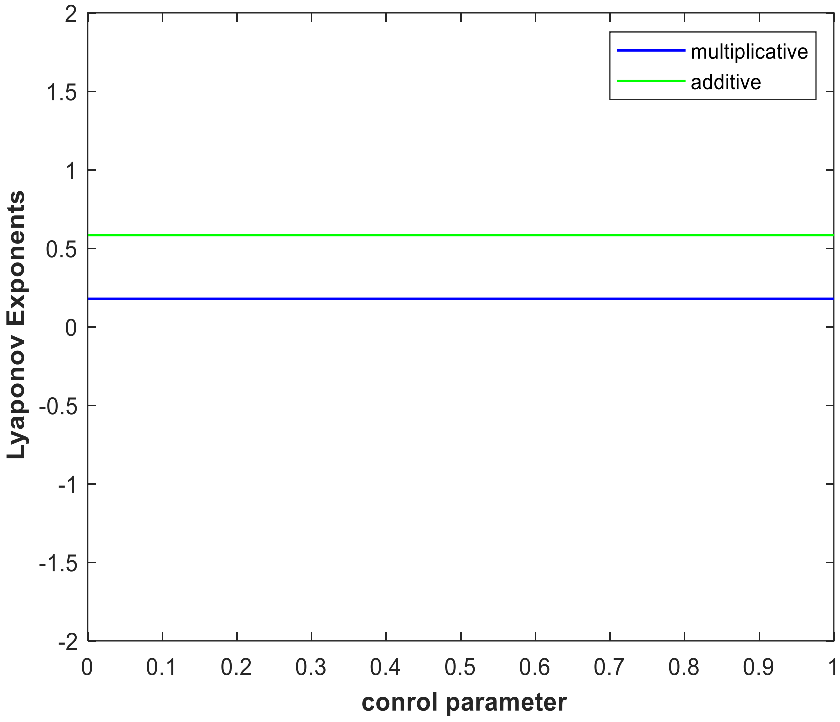


Fig. 10: Lyapunov exponents of the case 4 and case 5, logistic chaotic sequence multiplied and added by tent chaotic sequence with different initial condition

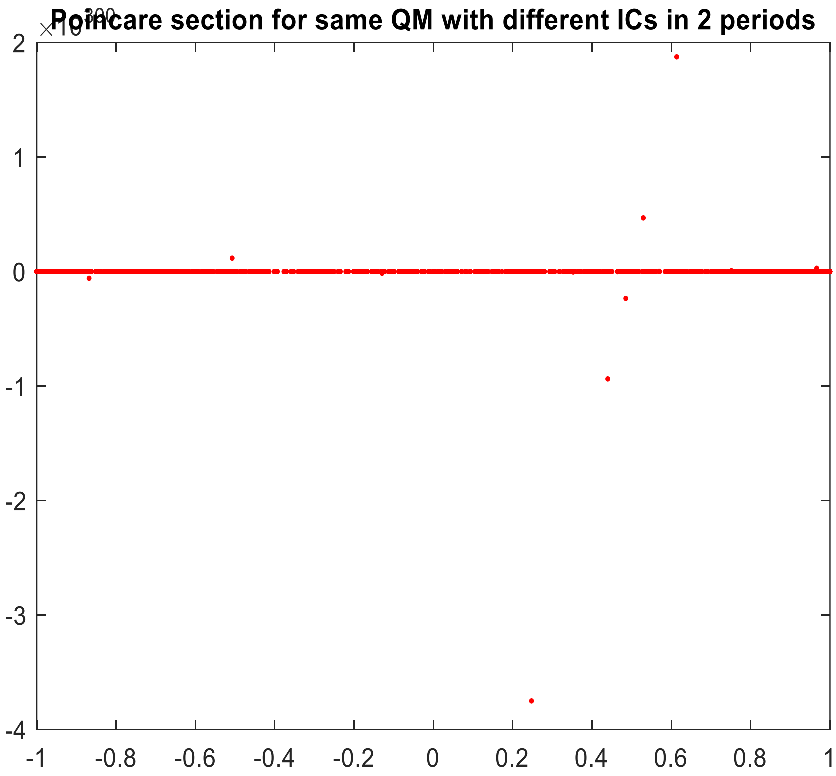


Fig. 11: Poincaré section of the case 1 by using same quadratic map, but different initial condition in multiple periods

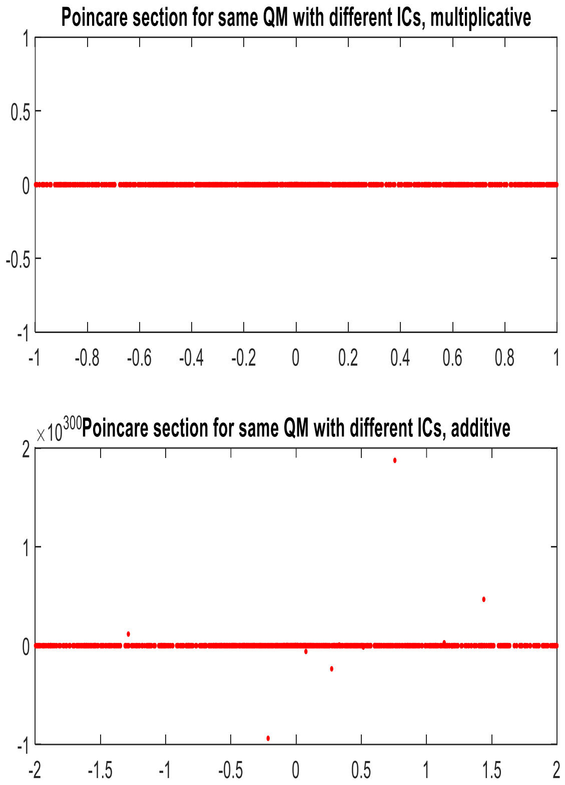


Fig. 12: Poincaré section of the case 2 and case 3 by using same tent map, but different initial conditions in multiplicative and additive form

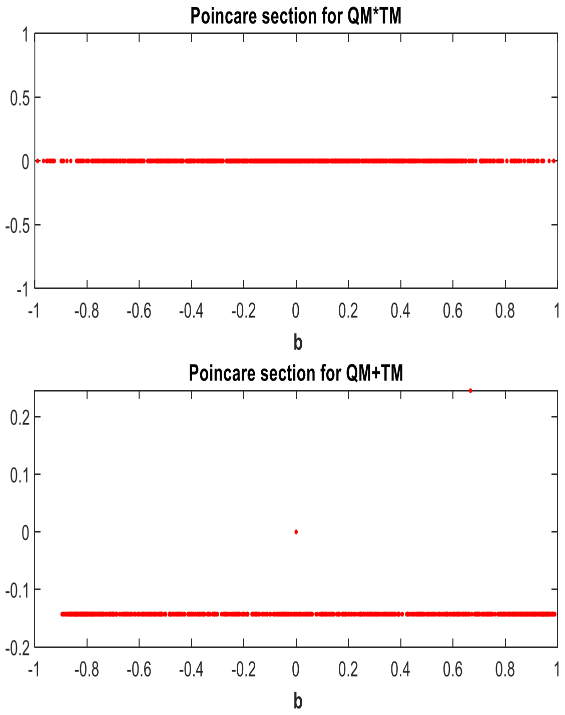


Fig. 13: Poincaré section of the case 4 and case 5, quadratic chaotic sequence multiplied and added by tent chaotic sequence with different initial condition

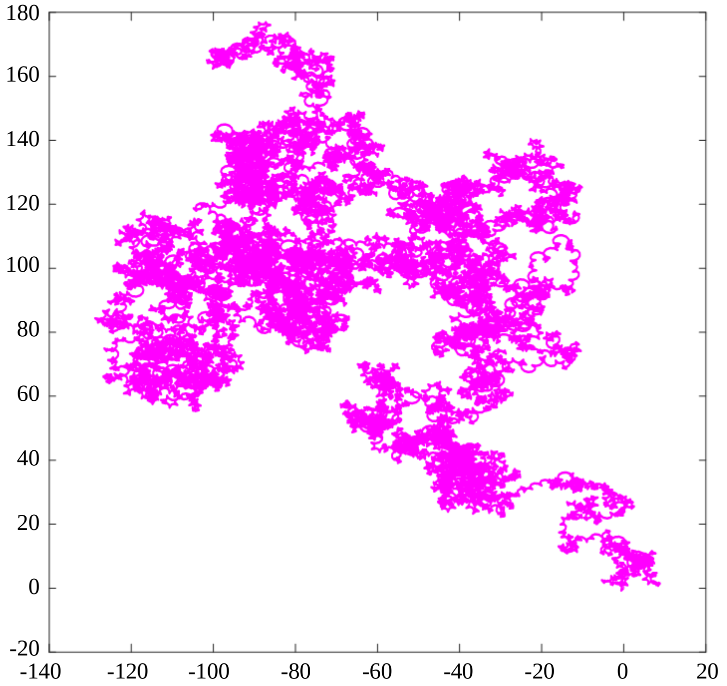


Fig. 14: 0-1 Test of the case 1 by using same quadratic chaotic sequence, but different initial condition in multiple periods

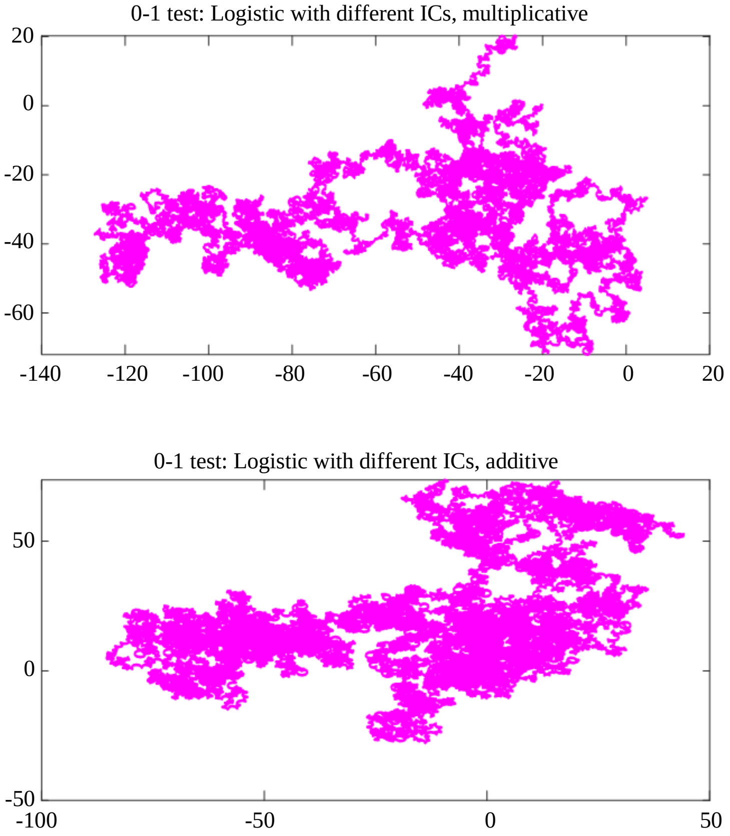


Fig. 15: 0-1 Test of the case 2 and case 3 by using same logistic map, but different initial conditions in multiplicative and additive form

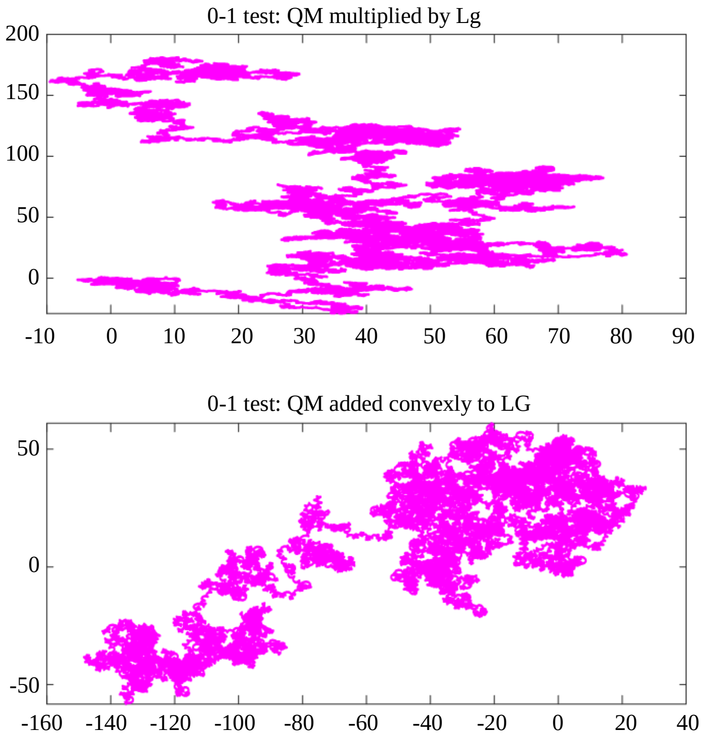


Fig. 16: 0-1 Test of the case 4 and case 5, quadratic chaotic sequence multiplied and added by logistic chaotic sequence with different initial condition

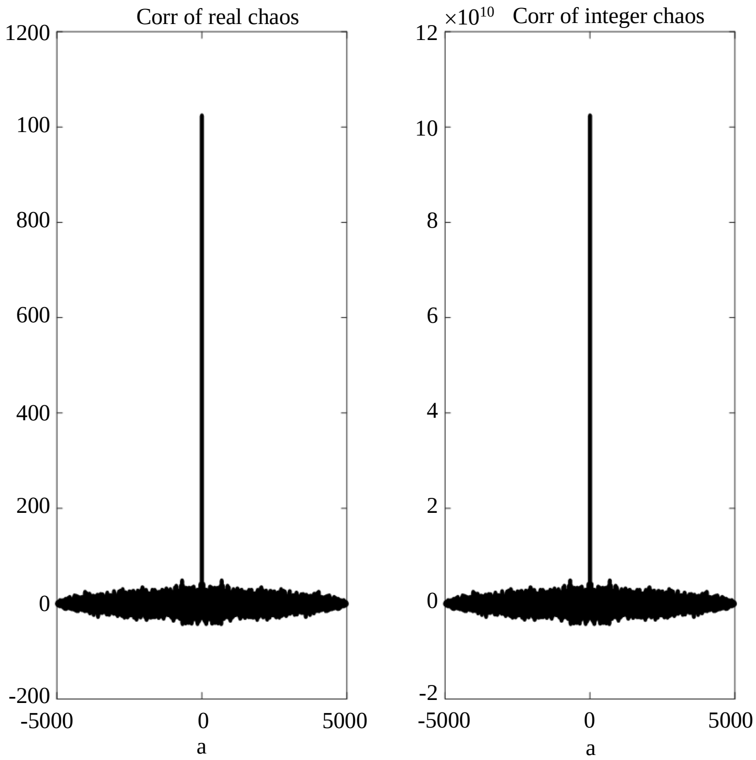


Fig. 17: The autocorrelation of the quadratic chaotic sequence added with Logistic chaotic sequence with different initiaconditionof Case 5 (a) correlation of real chaos (b) correlation of integer chaos

LSB Steganography Technique

LSB steganography is one of the most widely used methods in spatial domain, it replaces the least significant bits of the chosen pixel (The choice is either sequential or random) of the cover image with the bits of the secret message. The changing in least significant bits has less impact on image. This method embeds the fixed-length secret bits in the same fixed-length LSBs of pixels. This technique is simple and fast. It is preferable to use grayscale images because during the process of embedding secret data the correlation between color components will change. There are two types of LSB steganography technique: LSB substitution and LSB-matching. In LSB-substitution method, a secret data is embedded of cover image by substituting the LSBs of cover image pixels with secret data bits. The LSB-substitution increases and decreases or leave without changing (the bit of secret data is matching the LSB of cover image) of pixels value. In LSB-matching method, a secret data is embedded of cover image if the LSB of the cover image pixel matches the bit of secret data, no occurred changing, otherwise increases and decreases of pixels value (Ker, 2005; Hiary *et al*., 2016).

The Proposed System

According to the addresses were generated by merging multiple chaotic maps, three expanded systems are proposed from the chaotic LSB method and the chaotic Identical Bits Method and Data Mapping and LSB Substitution method.

Multiple-Chaotic LSB Steganography

In this study, 1, 2 and 4 LSBs (Kadhim and Hussain, 2018) were used to hide the secret message. it is increasing the capacity, but the increase leads to a clear distortion of the stego image especially when used Statistical measurements, thus it will reduce the security level. Therefore, one chaotic map was used to generate chaotic sequence. The proposed system uses multiple chaotic maps merged to generate integer chaotic to select 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; the Multiple-Chaos-LSB embedding and the Multiple-Chaos-LSB retrieving.

Multiple-Chaotic-LSB Embedding

Firstly, the cover image and secret message are converted into binary and a secret key is created by merging multiple chaotic maps and then processed to randomly select the pixel image address pixels.

The output of the encoding process represents the stego image.

Multiple-Chaotic-LSB Retrieving

Firstly, the stego image converted into binary, then the random pixels of the stego image is selected by the same secret key was used in embedded algorithm to extract the pixels and retrieve secret message bits according to binary table.

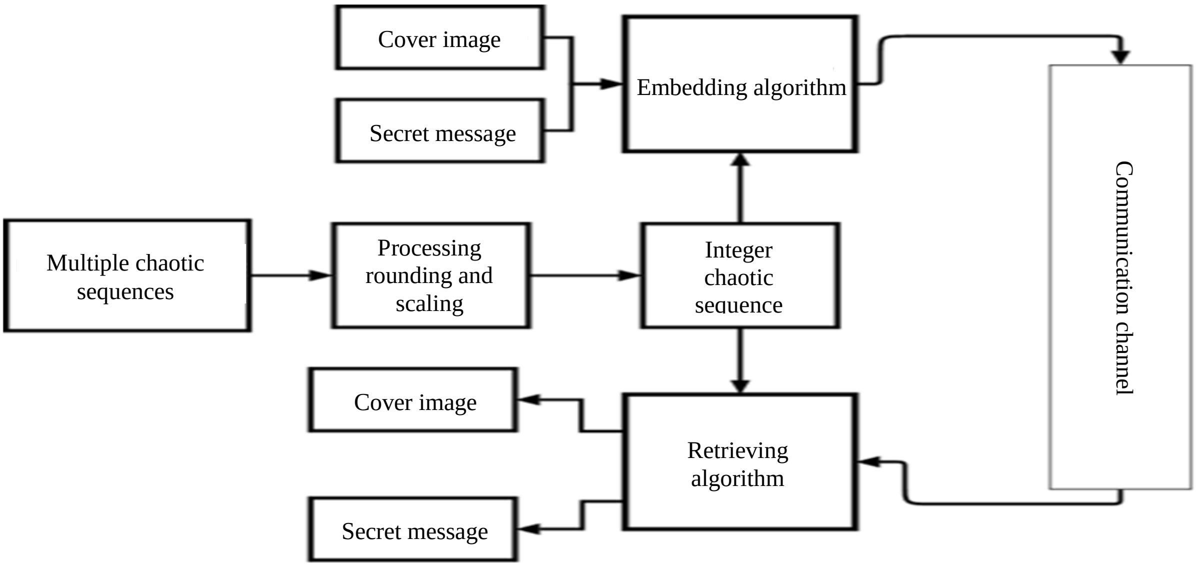


Fig. 18: Block diagram of the proposed system

Multiple-Chaotic-Identical-Bits Steganography

This technique (Al-Shatnawi, 2012) 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. Therefore, one chaotic map was used to generate chaotic sequence, to select pixel addresses of the cover image for embedding the secret message (Kadhim and Hussain, 2018). The proposed system uses multiple chaotic maps merged to generate chaotic sequences, to select pixel addresses of the cover image for embedding the secret message.

The proposed system is divided into two processes; the Multiple-Chaotic image is selected by the same secret key was used in embedded algorithm to extract the secret message.

Multiple-Chaotic-Identical-Bits Embedding

First, the cover image and secret message are converted into binary and a secret key is created by merging multiple chaotic maps and then processed to randomly identical bits will be searched, where 2 bits of the secret message are hidden in the select the pixel image address pixels. After the pixel has been selected at random, the 2-bit image cover and saved the bits locations in binary table. The output of the encoding process represents the stego image.

Multiple-Chaotic-Identical-Bits Retrieving

Firstly, the stego image converted into binary, then the random pixels of the stego image is selected by the same secret key was used in embedded algorithm to extract the pixels and retrieve secret message bits according to binary table.

Multiple-Chaotic Data Mapping and LSB Substitution

In this proposed method (Zakaria *et al*., 2018), 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. 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 pixel addresses of the cover image for embedding the secret message.

Multiple-Chaotic Data Mapping and LSB Substitution (Embedding Algorithm)

First, the cover image and secret message are converted into binary and a secret key is created by merging multiple chaotic maps and then processed to randomly select the pixel image address pixels. The secret message divides into pairs, the MSBs of cover image divide into two pairs, then:

- If match the first pair of MSB of cover image with the first pair of secret data, then replace the second bit of LSB with ‘1’ otherwise ‘0’
- If match the second pair of MSB of cover image with the second pair of secret data, then replace the first bit of LSB with ‘1’ otherwise ‘0’
- If either LSB1 or LSB2 is ‘0’, then the 2-LSBs of next pixel would be replaced with the previous unmatched bit pair of message
- If there is no matching between two pairs of MSB of cover image with the two pairs of secret data, the situation is ignored.

Multiple-Chaotic Data Mapping and LSB Substitution (Retrieving Algorithm)

First, the stego image is converted into binary and a secret key is created by merging multiple chaotic maps and then processed to randomly select the pixel image address pixels. The pixel of stego image divide MSBS into two pairs and the last 2LSB, then:

- If LSB2 is ‘1’ and LSB1 is ‘0’ of stego image, restore MSB1 as a first secret pair and restore the 2-LSBs of the next pixel as a second secret pair
- If LSB1 is ‘0’ and LSB2 is ‘1’, restore MSB2 as a second secret pair and restore the 2-LSBs of the next pixel with a first secret pair
- If both LSB1 and LSB2 are ‘1’, then restore the first secret pair from MSB1 and restore the second secret pair from MSB2
- If both LSB1 and LSB2 are ‘0’, it is ignored

Experimental Results and Discussion

In this study, the chaotic-2LSBs technique, the Chaotic-Identical-Bits technique (Kadhim and Hussain, 2018) and Data Mapping and LSB Substitution (Zakaria *et al*., 2018) and the three proposed systems have been implemented using grey-scale images on MATLAB (R2018a), windows 10. All techniques are applied to hide the secret messages (text: The science of today is the technology of tomorrow) and (image: MATLAB cell image 100*100) as shown in Fig. 19. The performance of these techniques has been evaluated using different experiments. Four MATLAB grayscale images with different sizes (toysnoflash.png 912*684, lighthouse.png 480×640, yellowlily.jpg 1224×1632 and flamingos.jpg 1296×972) are used as cover images shown in Fig. 20.

Performance Measures

The evaluation of steganographic methods is requested to determine if the method is better than others. Therefore, there are some criteria used to evaluate steganographic methods (Tayel *et al*., 2012). There are different types of measurements to measure the visual quality for steganography (ex. MSE, PSNR). MSE illustrates the square of error between cover image and stego image, MSE measures the distortion in image.

PSNR is the ratio of the extreme signal to noise power between the stego image and the cover image, PSNR measures the quality of the image. MSE and PSNR can be calculated based on the following Equations (7) and (8):

$$MSE = \frac{1}{H*W}\sum H \underset{i=1}{*} W\left(C_i - S_i\right)^2 \quad (7)$$

$$PSNR = 10*\log_{10}\frac{Max^2}{MSE} \quad (8)$$

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 to 3, where a secret message (grayscale image) is hidden over grayscale image, the three proposed systems exhibit better quality and higher security than chaotic-LSBs, chaotic-identical bits and Chaotic-Data Mapping and LSB Substitution; they provide a balance between quality and security. It is noted that the proposed Multiple-Chaotic Identical-Bits technique is better than the proposed Multiple-Chaos-Data Mapping and LSB Substitution and Multiple-Chaos-LSB technique.

In Table 4 to 6 where a secret message (text: The science of today is the technology of tomorrow) is hidden over grayscale image, the three proposed systems have better quality and higher security than chaotic-LSBs, chaotic-identical bits and Chaotic-Data Mapping and LSB Substitution techniques. It is noted that the proposed Multiple-Chaotic LSB technique is better than the proposed Multiple-Chaotic-Data Mapping and LSB Substitution and Multiple-Chaotic identical bits technique.

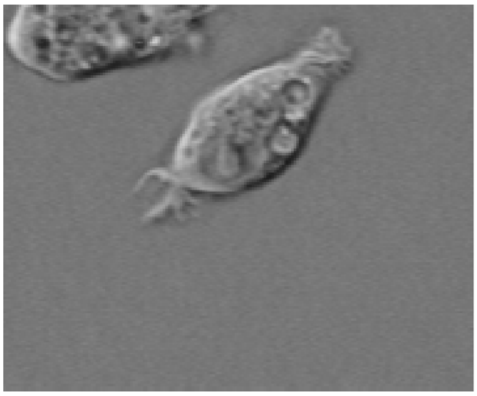
The size ratio R_m between message size and cover size can be calculated on various sizes of the secret image (cell.tif image 5*5, 10*10, 20*20, 30*30) by the following Equation (9):

$$R_m = \frac{Message\,Size}{Cover\,Image\,Size} \quad (9)$$

The relationship between the size ratio R_m and the PSNR is the reverse, that is meaning the size ratio Rm increases, PSNR decreases but the size ratio R_m increases, MSE increases as shown in Fig. 21 and 22.

The section of today is the technology of tomorrow

(a)



(b)

Fig. 19: The secret message (a) text (b) cameraman image

(a)

(b)

(c) (d)

Fig. 20: The cover MATLAB images: (a) toysnoflash.png (b) lighthouse.png (c) yellowlily.jpg (d) flamingos.jpg

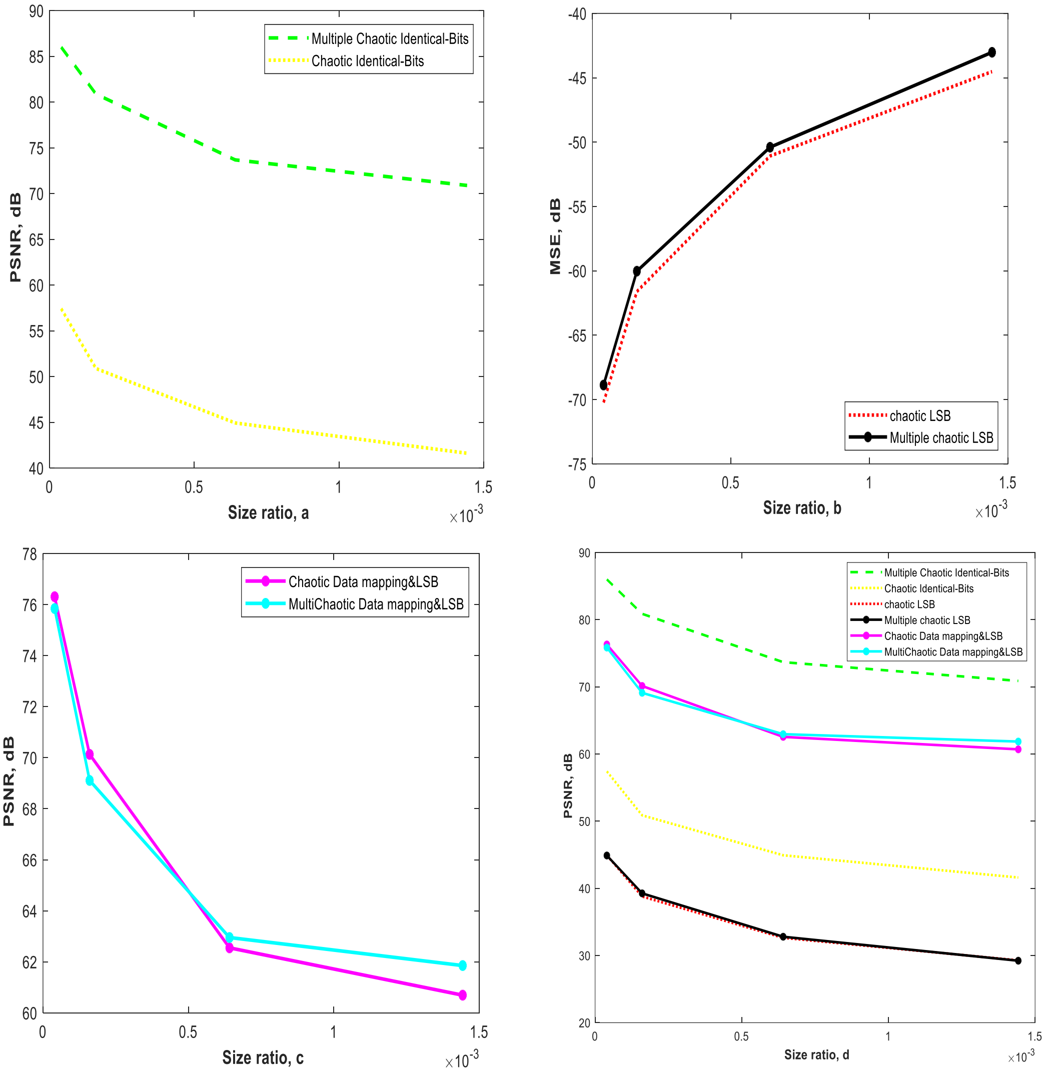
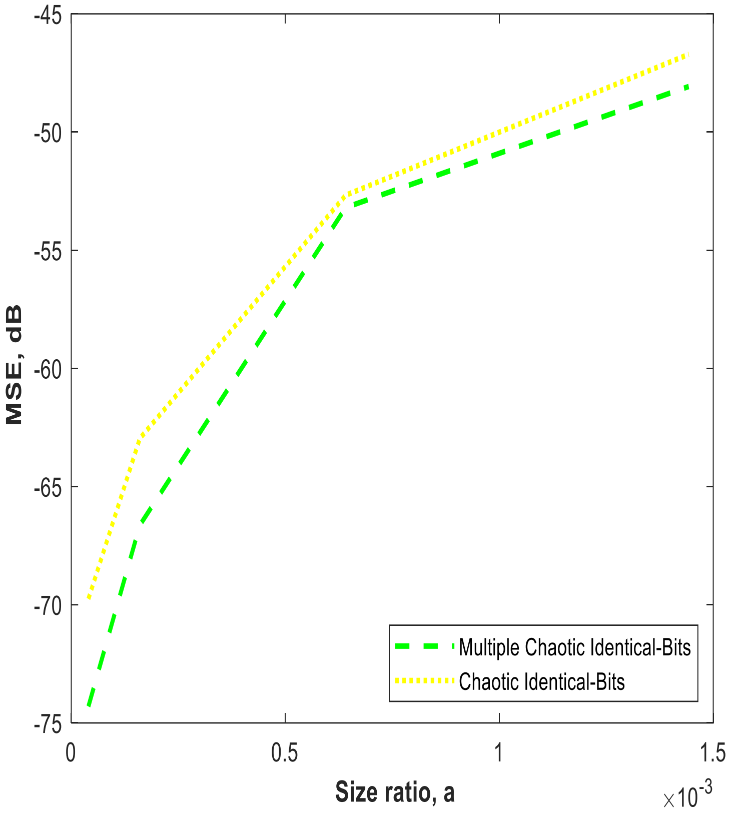
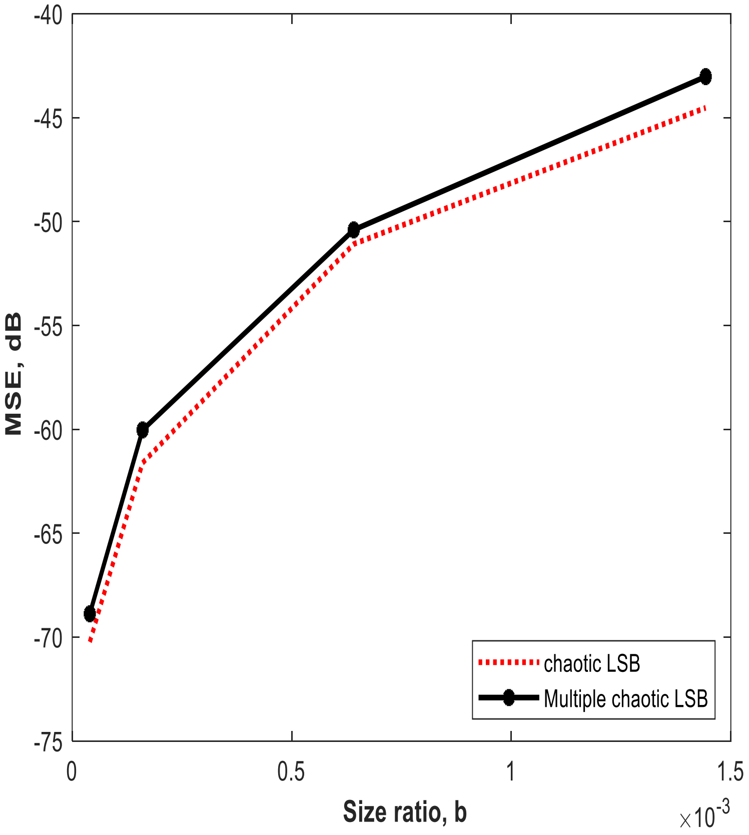


Fig. 21: The size ratio Vs. PSNR by applying (a) Chaotic LSB and Multiple-chaotic LSB. (b) Chaotic identical-bits and Multiple-chaotic identical-bits. (c) Multiple-chaotic- Data Mapping and LSB Substitution and Chaotic Data Mapping and LSB Substitution technique. (d) all proposed method


-45
-50
-55
-60
-65
-70
-75
MSE, dB
0
0.5
1
1.5
Size ratio, a
×10^-3
Multiple Chaotic Identical-Bits
Chaotic Identical-Bits


-40
-45
-50
-55
-60
-65
-70
-75
MSE, dB
0
0.5
1
1.5
Size ratio, b
×10^-3
chaotic LSB
Multiple chaotic LSB

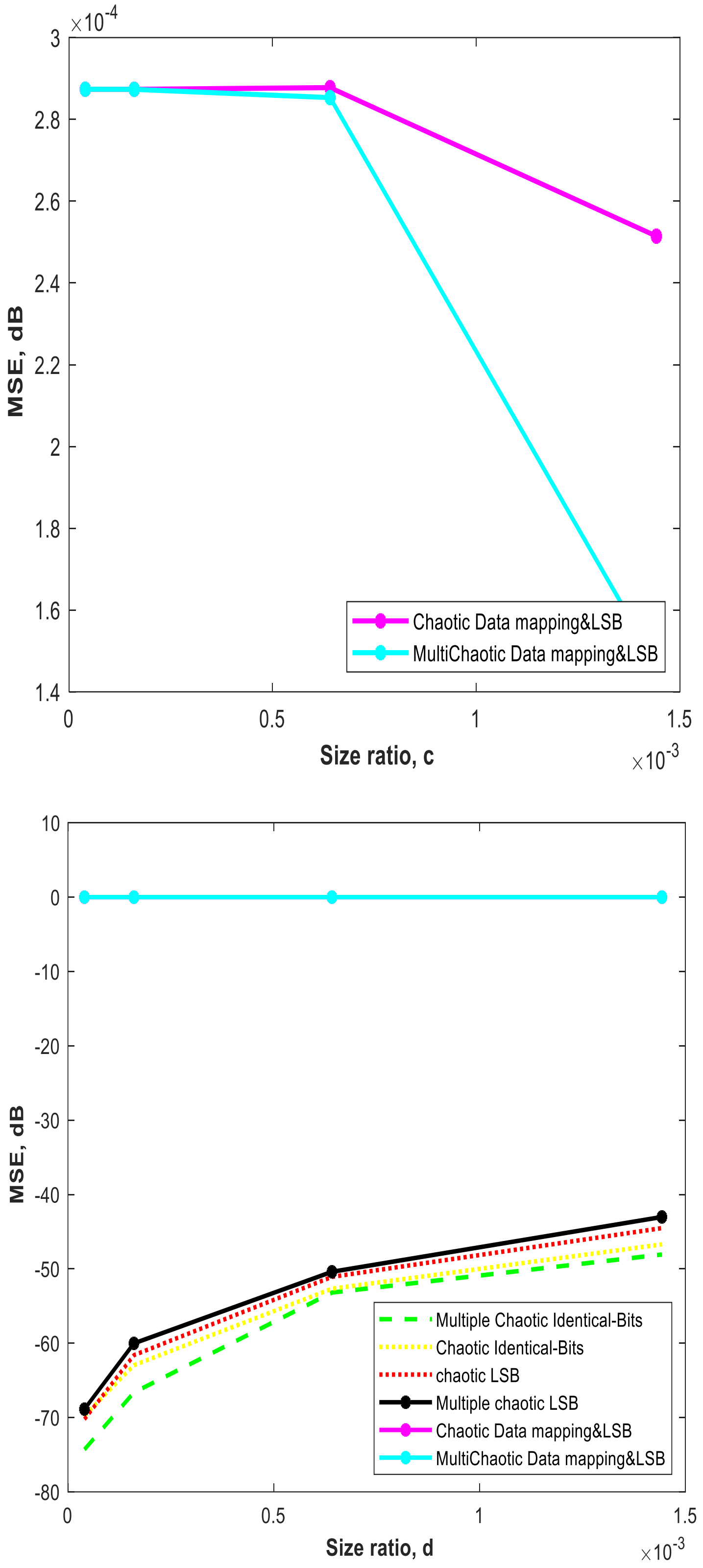


Fig. 22: The size ratio Vs. MSE by applying (a) Chaotic LSB and Multiple-chaotic LSB. (b) Chaotic identical-bits and Multiple-chaotic identical-bits. (c) Multiple-chaotic- Data Mapping and LSB Substitution and Chaotic Data Mapping and LSB Substitution technique. (d) all proposed method

Table 1: Comparison the value of PSNR and MSE between chaotic identical-bits technique in (Kadhim and Hussain, 2018) and Proposed multiple chaotic identical-bits technique implemented in this work when hiding an image of size (100*100)

		Chaotic identical-bits technique in (Kadhim and Hussain, 2018)		Proposed Multiple chaotic identical-bits	
Cover image	Cover image size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912×684	31.0867	50.6302	60.0241	0.0647
Lighthouse.png	480×640	27.1865	124.2897	57.2813	0.1216
Yellowlily.jpg	1224×1632	34.9057	21.0142	64.9654	0.0207
Flamingos.jpg	1296×972	34.3944	23.6394	64.1635	0.0249

Table 2: Comparison the value of PSNR and MSE between Chaotic-2LSB technique in (Kadhim and Hussain, 2018) and Proposed multiple chaotic-2LSB technique implemented in this work when hiding an image of size (100*100)

		Chaotic-2LSB technique in (Kadhim and Hussain, 2018)		Proposed Multiple chaotic-2LSB	
Cover image	Cover image size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912×684	55.9020	0.1671	55.9044	0.1670
Lighthouse.png	480×640	52.8613	0.3365	52.8347	0.3385
Yellowlily.jpg	1224×1632	60.9381	0.0524	60.9572	0.0522
Flamingos.jpg	1296×972	58.9762	0.0823	58.9852	0.0821

Table 3: Comparison the value of PSNR and MSE between proposed data mapping and LSB Substitution (Zakaria *et al*., 2018), chaotic data mapping and LSB substitution and proposed multiple chaotic- data mapping and LSB substitution technique implemented in this work when hiding an image of size (100*100)

		Data Mapping and LSB Substitution (Zakaria *et al*., 2018)		chaotic - Data Mapping LSB Substitution		Proposed Multiple chaotic - Data Mapping and LSB Substitution	
Cover image	Cover image size	PSNR	MSE	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912×684	46.6930	1.3925	50.4663	0.5840	52.2267	0.3894
Lighthouse.png	480×640	44.1992	2.4726	50.6059	0.5656	50.7869	0.5425
Yellowlily.jpg	1224×1632	53.0142	0.3248	58.1773	0.0989	58.1832	0.0988
Flamingos.jpg	1296×972	54.4672	0.2325	55.7706	0.1722	55.8763	0.1681

Table 4: Comparison the value of PSNR and MSE between chaotic identical-bits technique in (Kadhim and Hussain, 2018) and proposed multiple chaotic identical-bits technique implemented in this work when hiding a text: (The science of today is the technology of tomorrow)

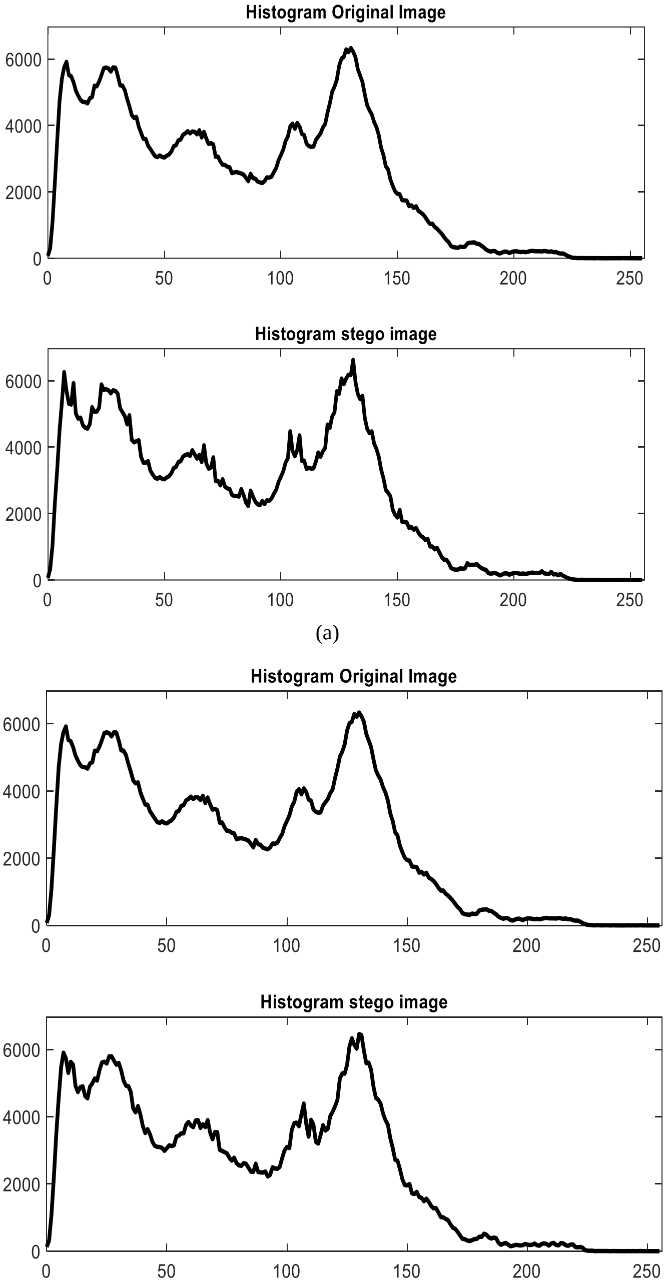
		Chaotic identical-bits technique in (Kadhim and Hussain, 2018)		Proposed Multiple chaotic identical-bits	
Cover image	Cover image size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912×684	49.2389	0.7748	50.8729	0.5319
Lighthouse.png	480×640	46.8382	1.3467	48.4929	0.9200
Yellowlily.jpg	1224×1632	50.1692	0.6254	52.0676	0.4039
Flamingos.jpg	1296×972	51.4263	0.4682	52.6757	0.3512

Table 5: Comparison the value of PSNR and MSE between chaotic-2LSB technique in (Kadhim and Hussain, 2018) and proposed multiple chaotic-2LSB technique implemented in this work when hiding a text: (The science of today is the technology of tomorrow)

		Chaotic-2LSB technique in (Kadhim and Hussain, 2018)		Proposed Multiple chaotic-2LSB	
Cover image	Cover image size	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912×684	78.6228	8.9290e-04	79.5588	7.1977e-04
Lighthouse.png	480×640	76.0327	0.0016	76.7007	0.0014
Yellowlily.jpg	1224×1632	83.6077	2.8334e-04	84.4520	2.3328e-04
Flamingos.jpg	1296×972	82.1006	4.0089e-04	82.5439	3.6199e-04

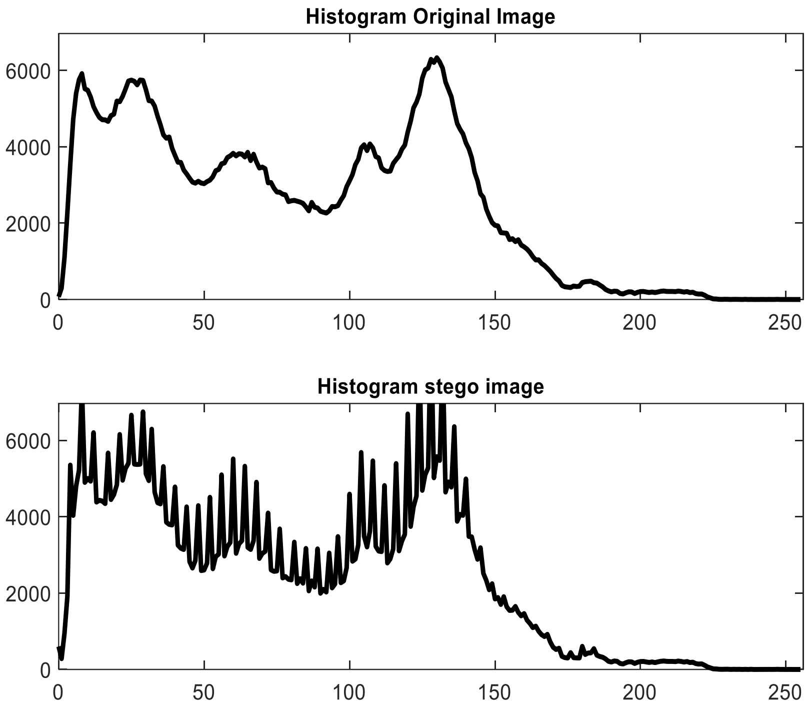
Table 6: Comparison the value of PSNR and MSE between proposed data mapping and LSB substitution (Zakaria *et al*., 2018), chaotic data mapping and LSB substitution and proposed multiple chaotic- data mapping and LSB substitution technique implemented in this work when hiding a text: (The science of today is the technology of tomorrow)

		Data Mapping and LSB Substitution (Zakaria *et al*., 2018)		Chaotic-Data Mapping and LSB Substitution		Proposed Multiple chaotic- Data Mapping and LSB Substitution	
Cover image	Cover image size	PSNR	MSE	PSNR	MSE	PSNR	MSE
Toysnoflash.png	912×684	67.5116	0.0115	74.1836	0.0025	75.2000	0.0020
Lighthouse.png	480×640	65.6618	0.0177	72.7356	0.0035	73.4674	0.0029
Yellowlily.jpg	1224×1632	72.5050	0.0037	78.7554	8.6605e-04	80.9864	5.1813e-04
Flamingos.jpg	1296×972	78.1818	9.8832e-04	78.5531	9.0735e-04	79.3335	7.5811e-04



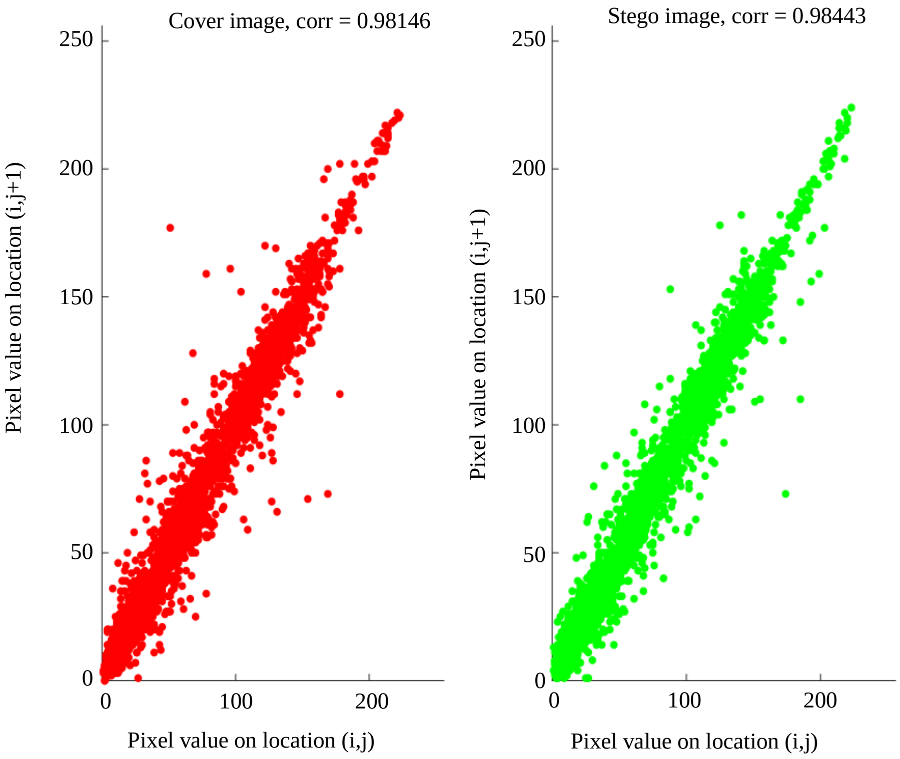
(a)

(b)

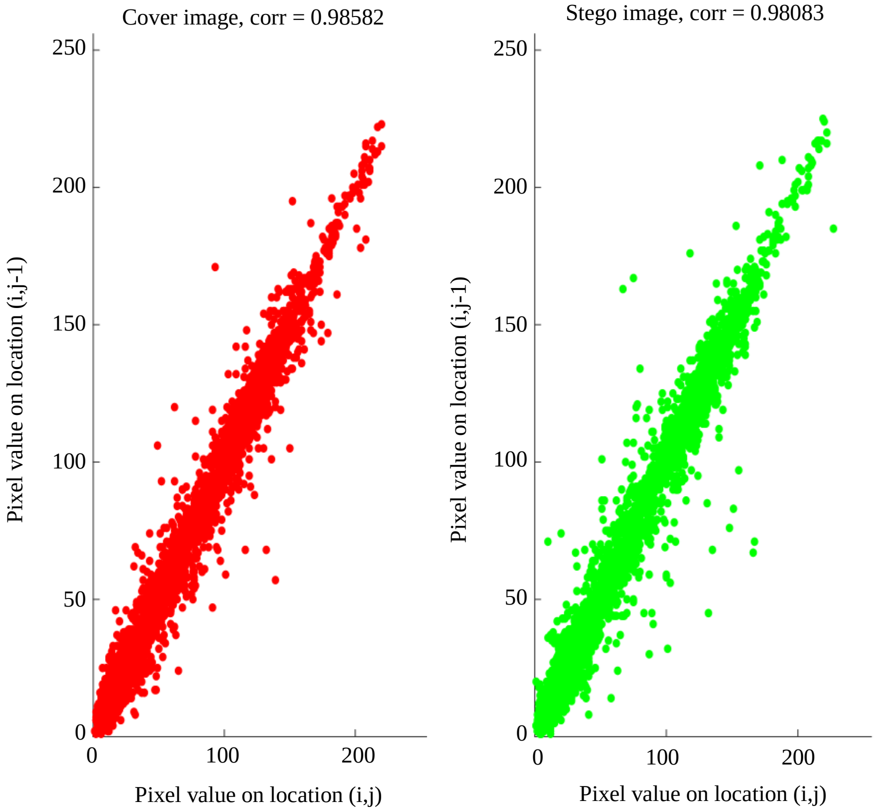


(c)

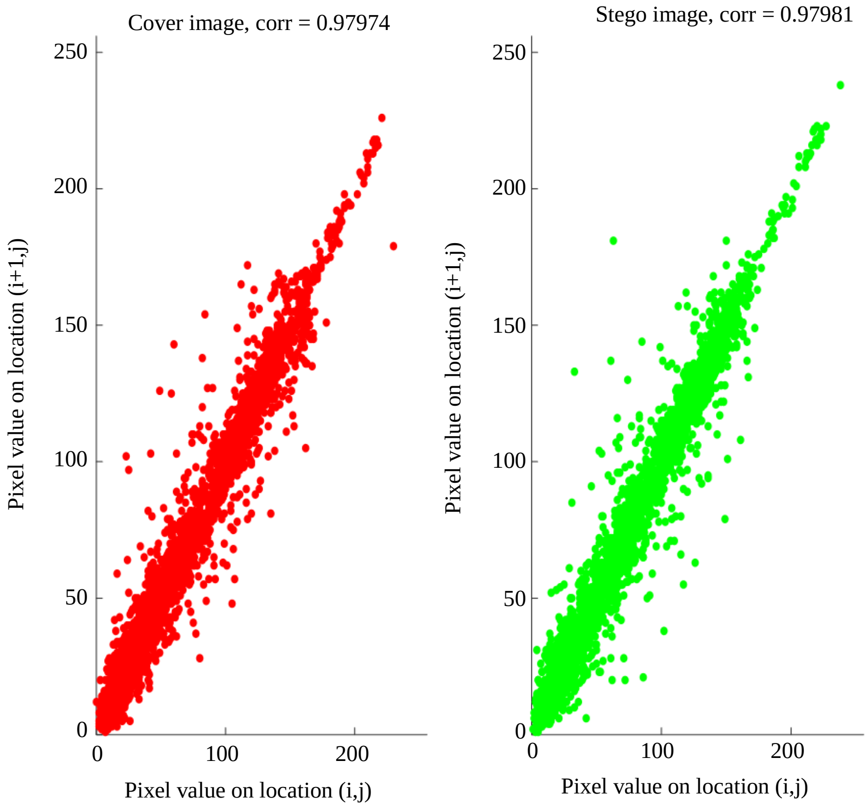
Fig. 23: Histogram analysis for original image (Toysnoflash) and stego image when applying (a) multiple-chaotic identical-bits and multiple-chaotic identical-bits (b) multiple-chaotic LSB and multiple-chaotic LSB. (c) multiple-chaotic- data mapping and LSB substitution technique



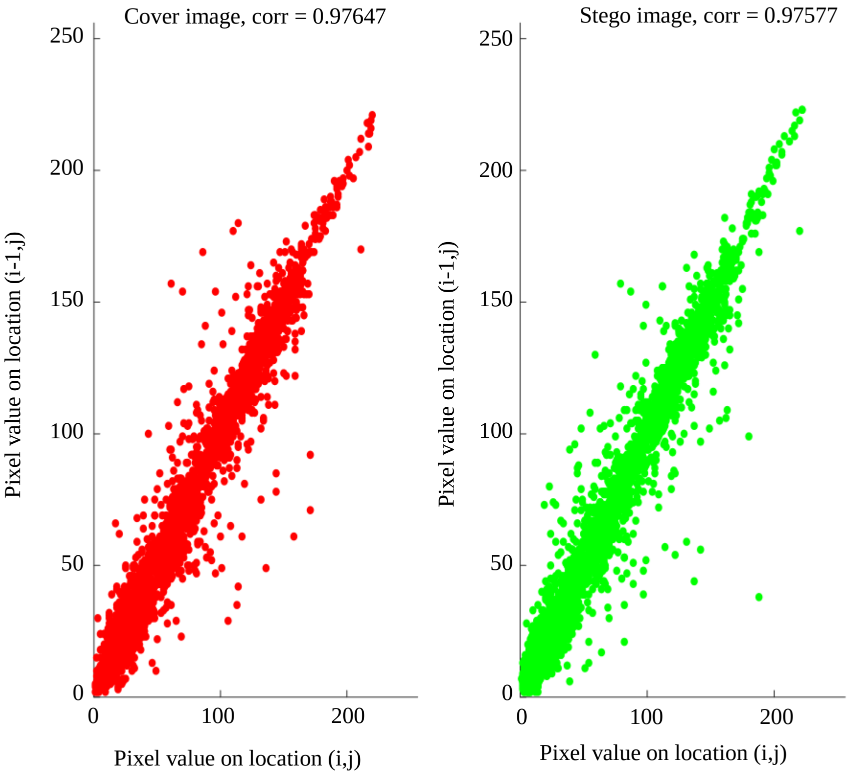
(a)


Cover image, corr = 0.98582
Stego image, corr = 0.98083
Pixel value on location (i,j-1)
Pixel value on location (i,j)
0
50
100
150
200
250

(b)

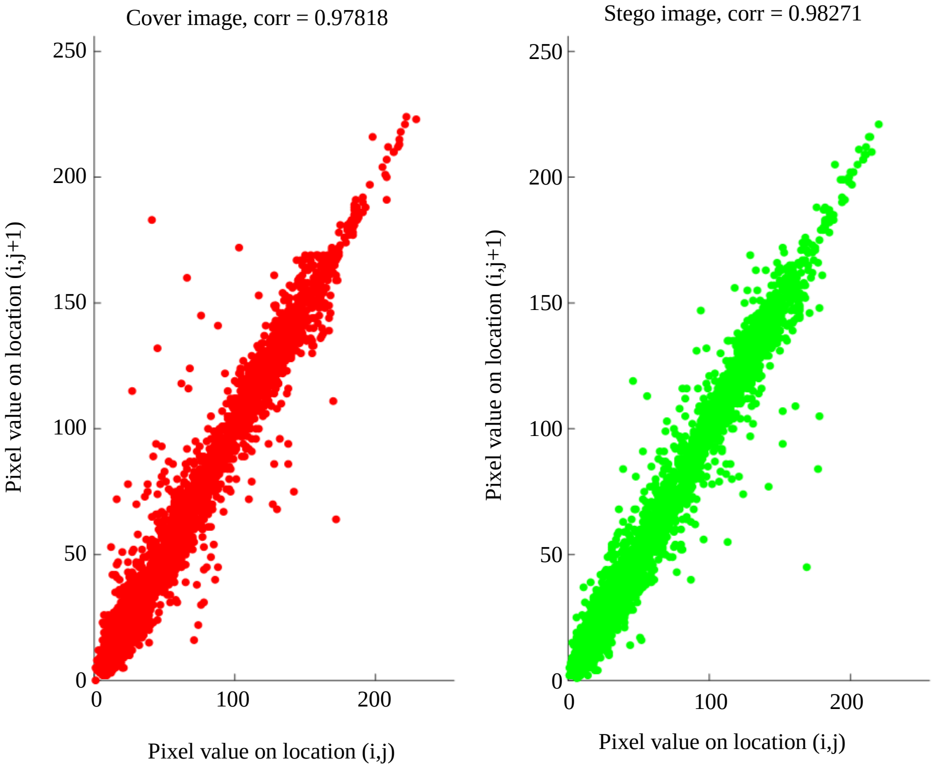

Cover image, corr = 0.97974
Stego image, corr = 0.97981
Pixel value on location (i+1,j)
Pixel value on location (i,j)
0
50
100
150
200
250

(c)

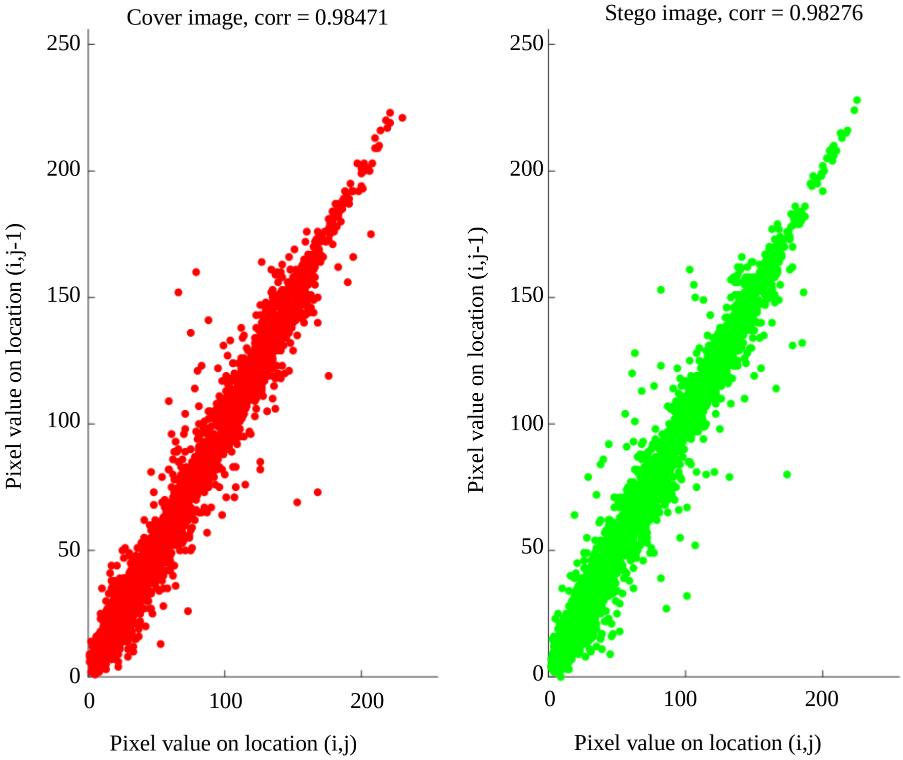


(d)

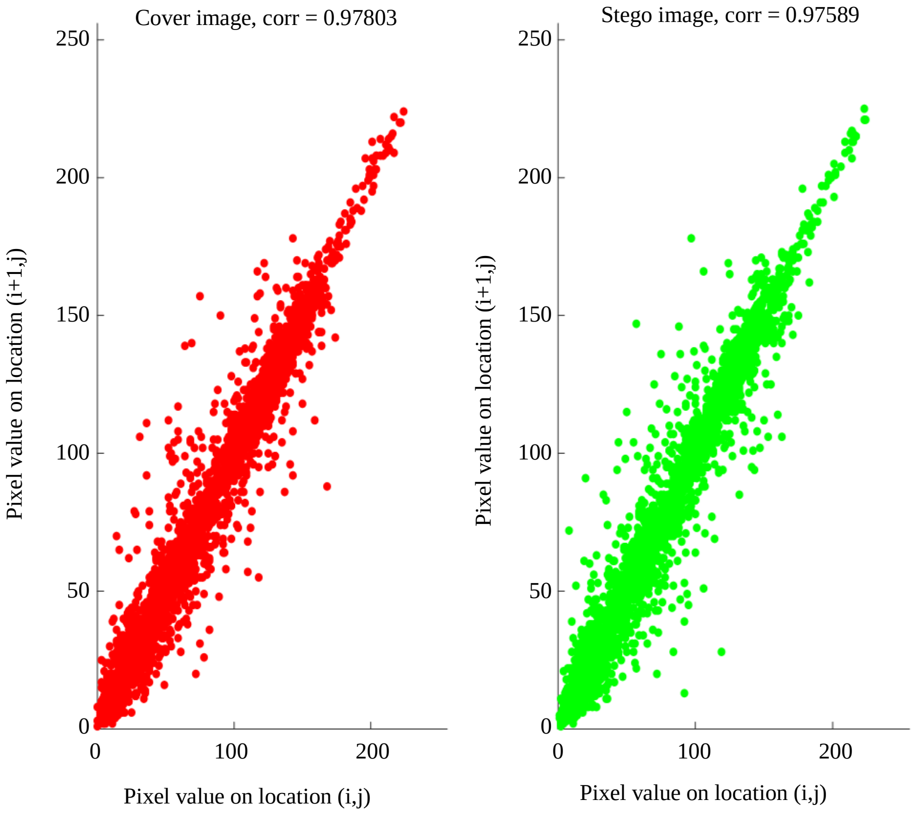
Fig. 24: Correlation of adjacent pixels (vertical and horizontal) in the multiple-chaotic-LSB technique



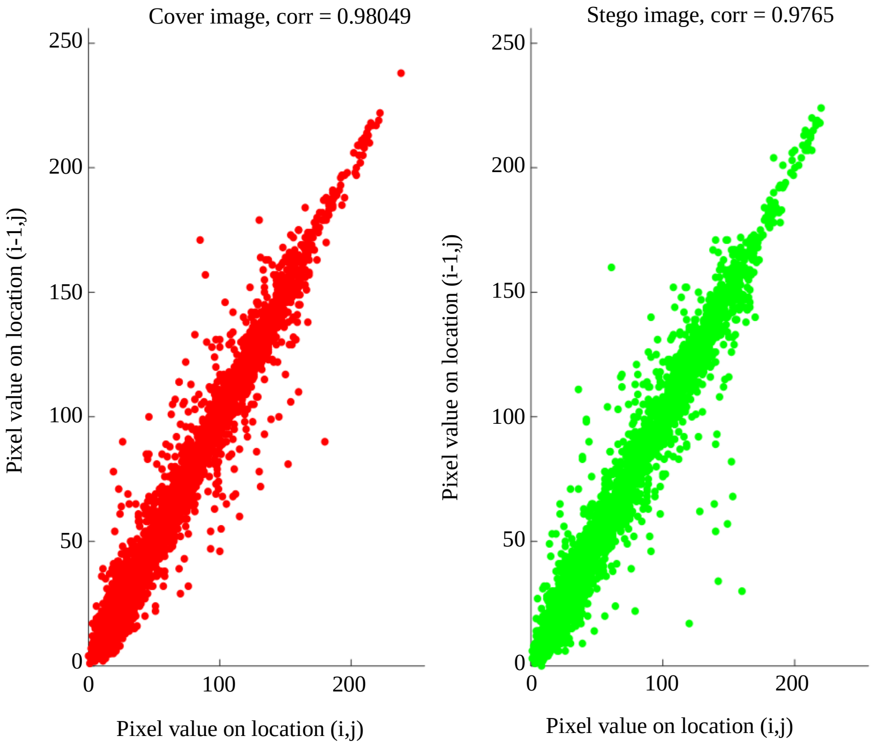
(a)


Cover image, corr = 0.98471
Stego image, corr = 0.98276
Pixel value on location (i,j-1)
Pixel value on location (i,j)
0
50
100
150
200
250

(b)

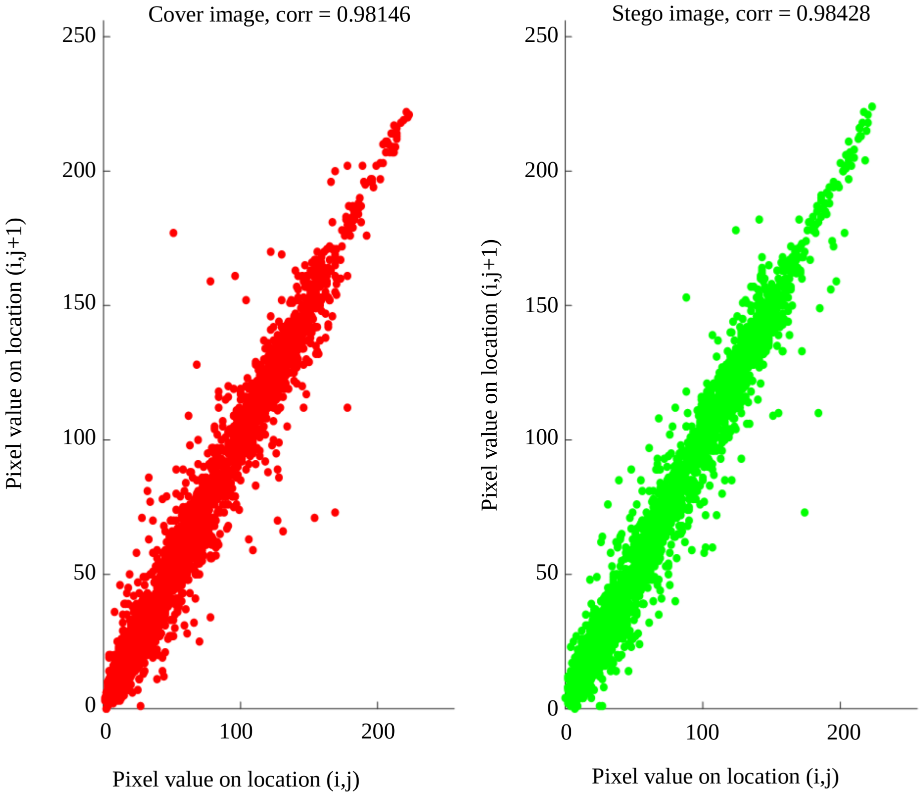

Cover image, corr = 0.97803
Stego image, corr = 0.97589
Pixel value on location (i+1,j)
Pixel value on location (i,j)
0
50
100
150
200
250

(c)

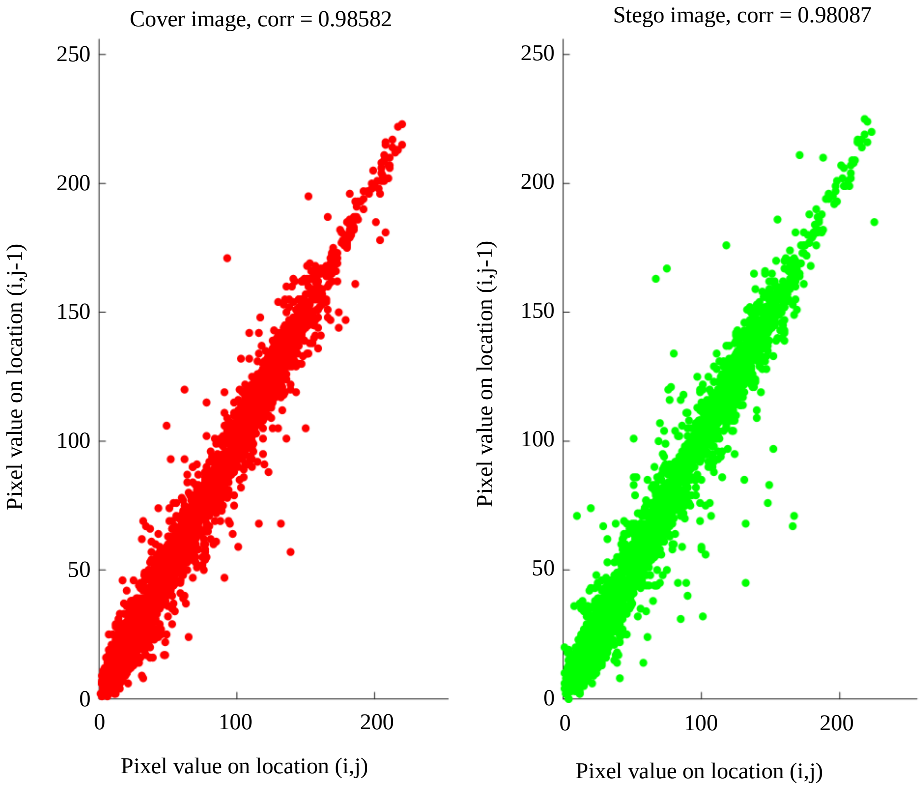


(d)

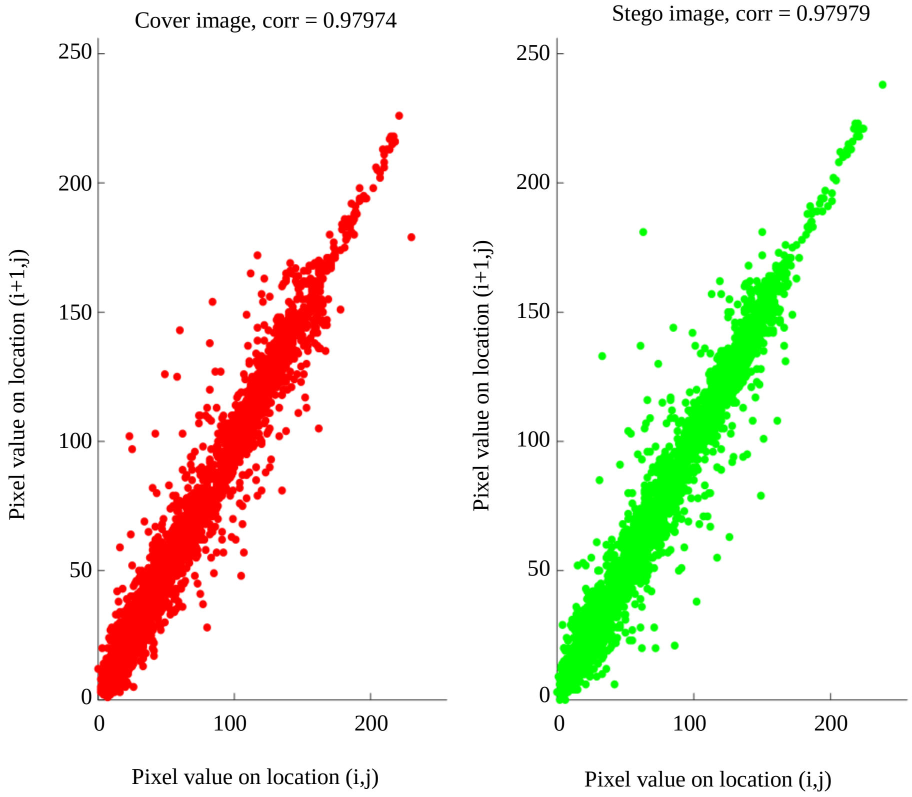
Fig. 25: Correlation of adjacent pixels (vertical and horizontal) in the multiple-chaotic identical-bits technique



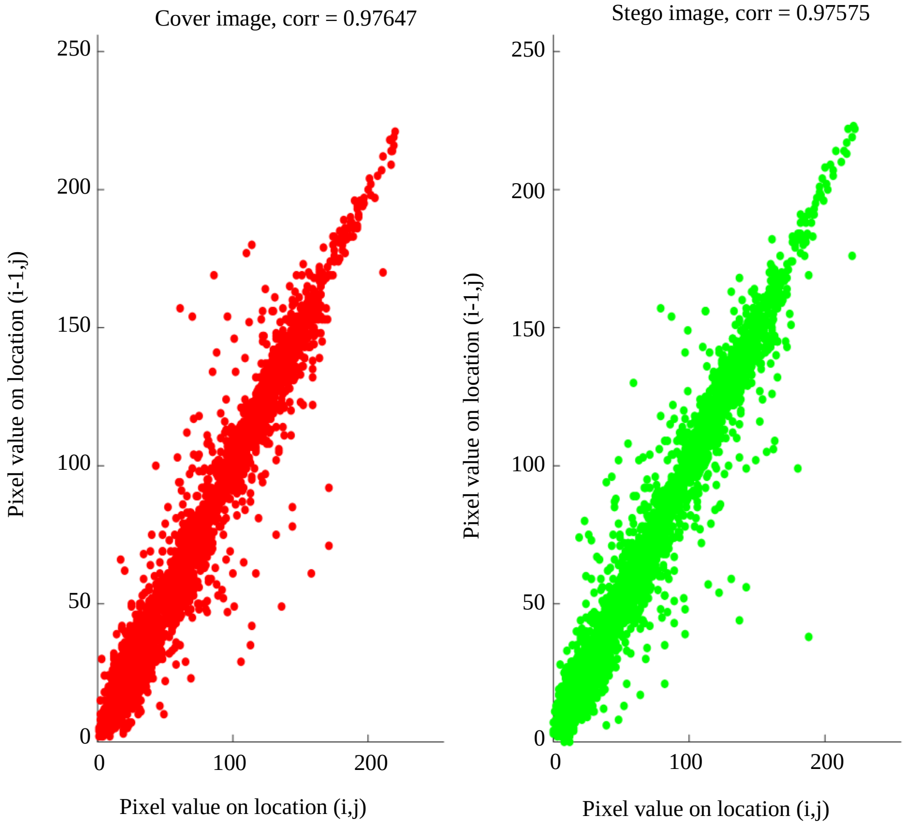
(a)


Cover image, corr = 0.98582
Stego image, corr = 0.98087
Pixel value on location (i,j-1)
Pixel value on location (i,j)
0
50
100
150
200
250

(b)


Cover image, corr = 0.97974
Stego image, corr = 0.97979
Pixel value on location (i+1,j)
Pixel value on location (i,j)
0
50
100
150
200
250

(c)



(d)

Fig. 26: Correlation of adjacent pixels (vertical and horizontal) in the multiple-chaotic- data mapping and LSB substitution technique

Histogram Analysis

It is also an active test of the Stego image. Histogram determine the distribution of pixels by comparing both stego and cover image. Figure 23 show the histogram of cover and stego images when applying the proposed Multiply-Chaos-LSB technique, Multiply-Chaos-identical bits technique and Proposed Multiple Chaotic- Data Mapping and LSB Substitution technique. We note little distortion after the secret message is embedding into the cover image except Multiple chaotic- Data Mapping and LSB Substitution technique.

Correlative Analysis

The correlation between two contiguous pixels (horizontal, vertical and diagonal) is calculated by selecting 3000 pairs of contiguous pixels random from the cover image and the stego images. It can be computed by the following Equations:

$$R_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D_{(x)}} * \sqrt{D_{(y)}}} \tag{10}$$

$$\operatorname{cov}_{(x,y)} = E\left(x-\varepsilon_x\right)\left(y-\varepsilon_y\right) \tag{11}$$

$$\varepsilon_x = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

$$D_{(x)} = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \varepsilon_x\right)^2 \tag{13}$$

$$\operatorname{cov}_{(x,y)} = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \varepsilon_x\right)\left(y_i - \varepsilon_y\right) \tag{14}$$

where, x and y are the intensity values of two adjacent pixels and N is the total number of pixels in the image. Figure 24 to 26 show the correlation between two adjacent pixels of the cover image (Toysnoflash) and stego image after embedding the secret image (cell) by the proposed Multiply-Chaotic-LSB, Multiply-Chaotic-identical bits technique and Multiple chaotic-Data Mapping and LSB Substitution technique. There is no significant difference in correlation coefficient after embedding. This indicates a high security level.

Future Work

Future work will include tests over long-range channel models (Mahmoud *et al*., 2002), (Mahmoud *et al*., 2006) and (Gurung *et al*., 2008); also, short-range communications (Lau *et al*., 2005).

Conclusion

Three systems for steganography in the spatial domain are proposed. These systems are based on the well-known LSB, the identical bits and data mapping and LSB substitution. The new systems have improved on the recent approach of using chaos theory for address shuffling, where they added a new security dimension by merging Multiple Chaotic maps for generating chaotic sequences with better chaotic properties. These sequences increase the available chaotic range of parameter and are more secure against attacks even if the existence of a secret message is suspected. Several performance measures have been considered to test security levels, like histogram analysis, PSNR and correlative analysis. Results showed that the proposed systems have much higher security level than their conventional counterparts. It is worth noting that the proposed approach is versatile as it could be added to other steganographic systems to enhance their security.

Acknowledgement

The Authors would like to thank the anonymous reviewers for their constructive comments. Thanks also to the Ministry of Higher Education and Scientific Research in Iraq for supporting this Research.

Author’s Contributions

This is the outcome of original research in MSc project of Ms. Haneen H. Alwan. She has contributed to the analysis and simulation of the proposed steganographic approaches. Also, she contributed to the paper write-up. Prof Zahir M. Hussain is the supervisor of this project. He has contributed to the analysis and simulation of the proposed system. Also, he contributed to the write-up revision and language corrections.

Ethics

The Authors declare that there are no ethical issues related to this research.

References

Al-Shatnawi, A.M., 2012. A new method in image steganography with improved image quality. Applied Math. Sci., 6: 3907-3915.

Anees, A., A.M. Siddiqui, J. Ahmed and I. Hussain, 2014. A technique for digital steganography using chaotic maps. Nonlinear Dynam., 75: 807-816. DOI: 10.1007/s11071-013-1105-3

Bag, A. and B. Ganguli, 2015. Methods to detect chaos and bifurcation analysis. Doctoral dissertation.

Bai, J., C.C. Chang, T.S. Nguyen, C. Zhu and Y. Liu, 2017. A high payload steganographic algorithm based on edge detection. Elsevier B.V., 46: 42-51. DOI: 10.1016/j.displa.2016.12.004

Dogan, S., 2018. A new approach for data hiding based on pixel pairs and chaotic map. Int. J. Comput. Netw. Inform. Security, 1: 1-9. DOI: 10.5815/ijcnis.2018.01.01

Elkamchouchi, H., W.M. Salama and Y. Abouelseoud, 2017. Data hiding in a digital cover image using chaotic maps and LSB technique. Proceedings of the 12th International Conference on Computer Engineering and Systems, Dec. 19-20, IEEE Xplore Press, Cairo, Egypt. DOI: 10.1109/ICCES.2017.8275302

Gottwald, G.A. and I. Melbourne, 2016. The 0-1 Test for Chaos: A Review. In: Chaos Detection and Predictability, Skokos, C., G. Gottwald and J. Laskar (Eds.), Springer, Berlin, Heidelberg, ISBN-13: 978-3-662-48408-1, pp: 221-247.

Gurung, A.K., F.S. Al-Qahtani, A.Z. Sadik and Z.M. Hussain, 2008. Power savings analysis of clipping and filtering method in OFDM systems. Proceedings of the Australasian Telecommunication Networks and Applications Conference, Dec. 7-10, IEEE Xplore Press, Adelaide, SA, Australia, pp: 204-208. DOI: 10.1109/ATNAC.2008.4783323

Hiary, H., K.E. Sabri, M.S. Mohammed and A. Al-Dhamari, 2016. A hybrid steganography system based on LSB matching and replacement. Int. J. Adv. Compt. Sci. Applic., 7: 374-380. DOI: 10.14569/IJACSA.2016.070951

Kadhim, O.N. and Z.M. Hussain, 2018. Information hiding using chaotic-address steganography. J. Compt. Sci., 14: 147-1266. DOI: 10.3844/jcssp.2018.1247.1266

Ker, A.D., 2005. Steganalysis of LSB matching in grayscale images. Proceedings of the IEEE Signal Processing Letters. May 16, IEE Xplore Press, pp: 441-444. DOI: 10.1109/LSP.2005.847889

Lau, Y.S., K.H. Lin and Z.M. Hussain, 2005. Space-time encoded secure chaos communications with transmit beamforming. Proceedings of the TENCON IEEE Region 10 Conference, Nov. 21-24, IEEE Xplore Press, Melbourne, Qld., Australia, pp: 1-5. DOI: 10.1109/TENCON.2005.301120

Li, B., J. He, Y.Q. Shi and J. Huang, 2011. A survey on image steganography and steganalysis. J. Inform. Hid. Multimedia Signal Process., 2: 142-172.

Mahmoud, S.S., Z.M. Hussain and P. O'Shea, 2002. Geometrical model for mobile radio channel with hyperbolically distributed scatterers. Proceedings of the 8th International Conference on Communication Systems, Nov. 28-28, IEEE Xplore Press, Singapore, pp: 17-20. DOI: 10.1109/ICCS.2002.1182428

Mahmoud, S.S., Z.M. Hussain and P. O'Shea, 2006. A geometrical-based microcell mobile radio channel model. Wireless Netw., 12: 653-664. DOI: 10.1007/s11276-006-6061-0

Ramadan, N., H.H. Ahmed, S.E. Elkhamy and F.E. Abd El-Samie, 2016. Chaos-based image encryption using an improved quadratic chaotic map. Am. J. Signal Process., 6: 1-3. DOI: 10.5923/j.ajsp.20160601.01

Sathishkumar, G.A., K.B. Bagan and N. Sriraam, 2011. Image encryption based on diffusion and multiple chaotic Maps. arXiv preprint.

Sharif, A., M. Mollaeefar and M. Nazari, 2016. A novel method for digital image steganography based on a new three-dimensional chaotic map. Multimedia Tools Applic., 76: 7849-7867. DOI: 10.1007/s11042-016-3398-y

Sun, K., 2016. Chaotic Secure Communication. 1st Edn., Walter de Gruyter GmbH and Co KG, ISBN-10: 3110433265, pp: 346.

Tayel, M., H. Shawky and A.D. Sayed Hafez, 2012. A new chaos steganography algorithm for hiding multimedia data. Proceedings of the 14th International Conference on Advanced Communication Technology, Feb. 19-22, IEE Xplore Press, Pyeong Chang, South Korea, pp: 208-212. https://ieeexplore.ieee.org/document/6174644

Tutuncu, K. and B. Demirci, 2018. Adaptive LSB steganography based on chaos theory and random distortion. Adv. Electrical Comput. Eng., 18: 15-22. DOI: 10.4316/AECE.2018.03003

Vigila, S.C. and K. Muneeswaran, 2015. Hiding of confidential data in spatial domain images using image interpolation. Int. J. Netw. Security, 6: 722-727.

Wu, Y. and J.P. Noonan, 2012. Image steganography scheme using chaos and fractals with the wavelet transform. Int. J. Innovat. Manage. Technol., 3: 285-289.

Yu, L., Y. Zhao, R. Ni and T. Li, 2010. Improved adaptive LSB steganography based on chaos and genetic algorithm. EURASIP J. Adv. Signal Process. DOI: 10.1155/2010/876946

Zaghbani, S. and R. Rhouma, 2013. Data hiding in spatial domain image using chaotic map. Proceedings of the 5th International Conference on Modeling, Simulation and Applied Optimization, Apr. 28-30, IEEE Xplore Press, Hammamet, Tunisia, pp: 1-5. DOI: 10.1109/ICMSAO.2013.6552626

Zakaria, A.A., M. Hussain, A.W. Abdul Wahab, M.Y. Idna Idris and N.A. Abdullah *et al*., 2018. High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. Applied Sci., 8: 2199-2199. DOI: 10.3390/app8112199

Zhang, H., X.K. Ma, M. Li and J.L. Zou, 2005. Controlling and tracking hyperchaotic rössler system via active backstepping design. Chaos Solitons Fractals, 26: 353-361. DOI: 10.1016/j.chaos.2004.12.032