Journal of Computer Science

Original Research Paper

Information Hiding using Chaotic-Address Steganography

Ola N. Kadhim and Zahir M. Hussain

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

Article history
Received: 07-06-2018
Revised: 09-07-2018
Accepted: 24-09-2018

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

Abstract: In this study, two techniques are introduced for image steganography in the spatial domain. These systems employ chaos theory to track the addresses of shuffled bits in steganography. The first system is based on the well-known LSB technique, while the second system is based on a recent approach that searches for the identical bits between the secret message and the cover image. A modified logistic map is employed in the chaotic map to generate integer chaotic series to extract the shuffled addresses bits. Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), histogram analysis and correlative analysis are used for testing and evaluating the new levels of security for the proposed techniques. The results show that the proposed methods outperform existing systems.

Keywords: Chaos, Steganography, Data Security

Introduction

In modern communication technology, people exchange information by using an open network (the internet). Through the connection, hackers attempt to spy on the secret information (Martin and Barmawi, 2015). In order to prevent them from detecting secret information, it needs to provide high security for data (Bukhari *et al*., 2017). Steganography and cryptography are two techniques which are used to provide a high level of data security (Manjula and Danti, 2015). In cryptography, confidential messages have changed into an encrypted form and transported through the networks. Whereas, in steganography, the secret information is hidden inside a cover medium like text, image, audio, or video (Chang *et al*., 2014).

Steganography is a method for hiding information, which hides secret information such as text, image, audio or video inside a cover medium such as text, image, audio or video in a way that cannot be detected by the Human Visual System (HVS). This makes people unaware of the existing a secret message (except for the sender and receiver). Steganography is a Greek word that means covered writing; the word "stegano" means covered or concealed and the word "graphy" means writing (Muhammad *et al*., 2015). The image is an excellent medium for steganography because of having redundancy in its representation (Khalind, 2015).

There are two domains by using the image as a cover medium for concealing a secret message: Spatial domain and frequency domain (Amirtharajan and Rayappan, 2012). In the spatial domain, intensity values of the cover image are used to hide a secret message (Vigila and Muneeswaran, 2015). In the frequency domain, the image is converted to frequency coefficients then the secret message is hidden inside these coefficients (Wahballa *et al*., 2016). One of the simple and fast-hiding techniques in the spatial domain is the Least Significant Bit (LSB) technique (Sarreshtedari and Akhaee, 2013). It substitutes the least significant bits of the pixels in the cover image with bits of the secret message; the result is a stego image that looks like the cover image.

The recent technique in (Al-Shatnawi, 2012) conceals the secret message inside a cover image depending on the looking for the identical bits between them. This will increase the security level compared to the conventional LSB technique. The random choice of pixels for hiding the secret message gives better security than sequential selection in the conventional LSB technique.

Chaos theory has been founded since the 1970s by many different research fields such as engineering, science, physics, mathematics and biology (Behnia *et al*., 2008). Chaos is a dynamical system that is very sensitive to initial conditions. A small difference in the starting values will lead to a great difference in the output. It is a deterministic nonlinear system that has semi-random behavior (Tayel *et al.*, 2012). Because of the random behavior of chaos, it can be used to ensure a high level of security in steganography (Habib *et al.*, 2015). Chaos has applications in the security of the physical layer as (Lau and Hussain, 2005; Lau *et al*., 2005; Linh-Trung *et al*., 2008).

This work uses chaos theory as additional security dimension in steganography by incorporating it to the LSB technique and technique in (Al-Shatnawi, 2012) (it is called here Identical-Bits Steganography), where the new address can be extracted chaotically.

The paper is structured as follows: A brief about existing systems of steganography has been discussed in section 2. Section 3 handles a description of some chaotic maps with focus on logistic map and its proposed modification to generate integer chaos for the purpose of shuffling addresses. A brief description of the LSB steganography using 1, 2 and 4 LSBs has been illustrated in section 4. A brief description of the improved LSB technique as in (Yadav *et al*., 2011) has been discussed in section 5 for the purpose of fair comparison. Yadav's approach would be named in this study as "improved LSB". The two proposed systems for hiding secret information with algorithms of them have explained in section 6. Experimental results and discussions using some performance measures has discussed in section 7. The conclusion of the paper declared in section 8.

Related Work

The most relevant steganographic techniques are presented below.

Karim *et al.* (2011) have suggested an improved-LSB technique for color images to enhance the security level of the secret message by using a secret key. The methodology is to divide the cover image into three matrices (Red, Green and Blue). The secret key is converted into ASCII value then to binary (1D array of bits). The secret key and Red matrix are used only for decision making regarding where to place hidden information: Either in Green matrix or in Blue matrix. Each bit of secret key is XORed with LSB bits of Red matrix. The resulting XOR value decides where the bits of secret information will be placed: Either in LSB of Green matrix (if XOR bit = 1) or in LSB of Blue matrix (if the XOR bit is 0). The same process will be continued until the secret information is finished.

Viswanatham and Manikonda (2010) have suggested an effective and secure technique of LSB insertion mechanism. The technique involves the generation of random numbers and also selecting a region of interest in which the required message is to be embedded in the random pixels whose addresses are previously generated. The technique also involves a secret key (password to decode the message) which has to be provided by the recipient for decoding the message from the image.

Gutub (2010) has suggested a new steganography method using RGB image pixels as its cover media. The information is hidden into two of the RGB pixel channels based on the indication within the third channel. It uses the size of the message as a selection criterion for the first indicator channel. If type of length of the message is (even number) the first indicator channel is red, If type of length of the message is prime number the first indicator channel is blue, otherwise it is green. The Pixel Indicator Technique (PIT) proposed in this study is for steganography utilizing RGB images as cover media. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of secret data existence in the other two channels. If 2LSB of indicator channel is 00 then no hidden data in the two channels; if 2LSB of indicator channel is 01 then no hidden data in channel 1 and two bits of hidden data in channel 2; if 2LSB of indicator channel is 10 then two bits of hidden data in channel 1 and no hidden data in channel 2; if 2LSB of indicator channel is 11 two bits hidden data in channel 1 and two bits hidden data in channel 2.

Luo *et al.* (2010) have suggested expanding the LSB matching image steganography and proposed an edge-adaptive scheme which can select the embedding regions according to the size of the secret message as well as the difference between two consecutive pixels in the cover image. For lower embedding rates only sharper edge regions are used, while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters.

Al-Shatnawi (2012) has suggested a technique that embeds the secret message based on searching about the identical bits between the secret message and bits of the cover image pixel. This technique was compared with the 2-LSB technique which conceals the secret message immediately.

Al-Taani and Al-Issa (2009) have suggested a new steganographic technique for hiding information in the spatial domain of the grayscale image. This approach works by dividing the cover image into blocks of equal sizes and then hiding the secret message in the edge of each block depending on the number of ones in the left four bits of the pixel. This approach is more efficient as compared with the well-known method Pixel Value Differing (PVD) in (Wu and Tsai, 2003).

The next section presents a brief description of some chaotic maps that generate chaotic series.

Chaotic Maps

Chaos is a random-like behavior of a dynamical system as a function of time. This behavior may happen in continuous-time or discrete-time systems. It can be noted naturally in weather, electrical circuits, liquid elements and mechanical systems. The essential feature of chaos (relevant to information security) is sensitivity to initial conditions, so that small changes in the input can cause large changes in the output. This feature is exploited for implementing information hiding techniques (Valandar *et al*., 2017). Mathematically, any chaotic map can be defined as in Equation (1) (Azou *et al.*, 2002):

DOI: 10.3844/jcssp.2018.1247.1266

$$x_n = f\left(x_{n-1}\right), n = 1,2,... \quad (1)$$

where, x_n is the state of iteration n, the function $f(\cdot)$ is mapping the state x_{n-1} to the next state x_n. This work uses a one-dimensional (1D) logistic map to generate the chaotic series which is used as secret keys to shuffle addresses in a new steganography technique.

The 1D Logistic Map

A logistic map is a simple form of a chaotic system, which it is easy to understand. It is developed by May (May 1976) and is described by Equation (8):

$$x_n = \alpha x_{n-1}\left(1 - x_{n-1}\right) \quad (2)$$

Here x_0 is the initial value α is a control parameter and n refers to the iteration.

The logistic map will generate chaotic series, if the control parameter is in the rang $3.5 \leq \alpha \leq 4$ (Wang *et al*., 2012). The chaotic series is within the range [0, 1]; it is very sensitive to a change in an initial value, where a very small difference of the initial values can cause a large impact in the next values. Figure 1a shows the chaotic behavior of the logistic map with values $\alpha = 4$ and $x_0 = 0.7$; Fig. 1b shows the chaotic behavior of the logistic map with values of $\alpha = 3.95$ and $x_0 = 0.9$.

This chaotic series contains real numbers within the range [0, 1]. It should be modified to produce large integers suitable to extract new addresses. The next section illustrates this modification.

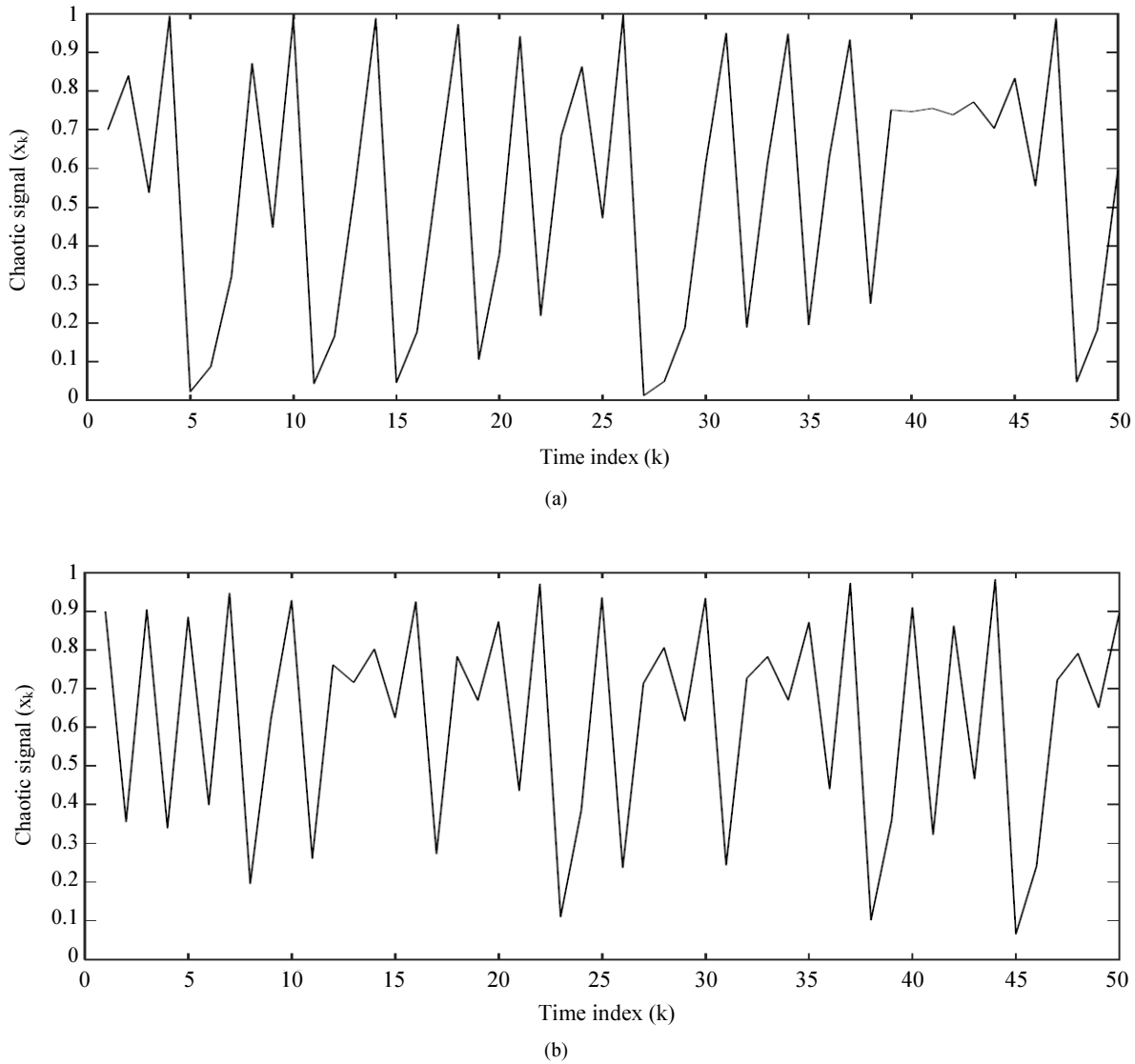


Fig. 1: Random behavior of the logistic map chaotic series (a) $\alpha = 4$ and $x_0 = 0.7$ (b) $\alpha = 3.95$ and $x_0 = 0.9$

Address Shuffling using Integer Logistic Map

After applying Equation (8), the chaotic series contains real numbers within the range [0, 1]. This series should be modified to get integers that will be used to select the new addresses of pixels in the cover image; this modification is achieved by following steps:

1. Determining initial values x_0, α
2. Applying $x_n = \alpha x_{n-1}(1-x_{n-1})$
3. Determining minimum value (e.g., $t_{min} = 5$) of the series
4. Multiplying the number of samples N by any number to get b (e.g., $b = 6 * N$)
5. $t_{max} = t_{min} + b$-1, t_{max} is a maximum value of the series
6. c = ceil ($b * x$); ceil is the MATLAB function for rounding
7. $t = t_{min} + c - 1$, t = new integer chaotic series. $t_{min} <= t <= t_{max}$
8. Sorting the series (t) in ascending order
9. If two elements in the series (t) are equal, add one to the next elements to avoid repetition
10. Saving the new integer chaotic series with no repetition in z

After modifying the chaotic map, the next section shows the autocorrelation of the real chaos signal and the autocorrelation of the integer chaos signal to determine whether the features of the correlation have changed or not.

Autocorrelation Test

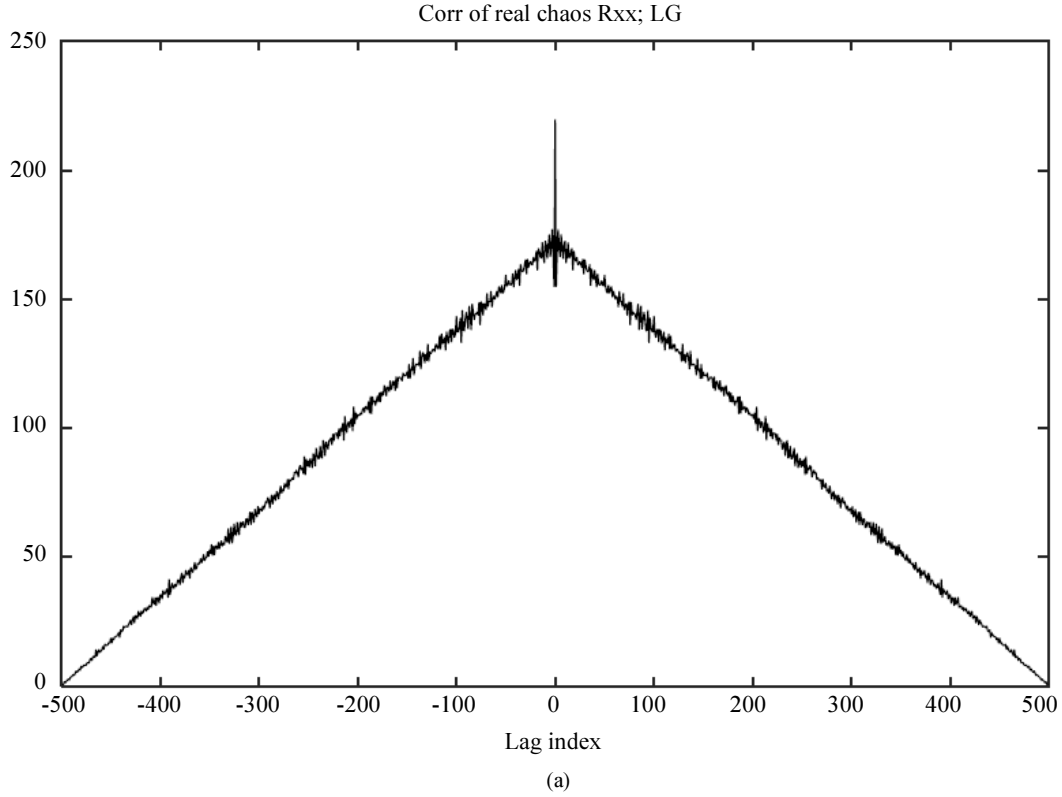
Autocorrelation of chaotic sequences is delta or semi-delta functions in the lag domain, which it is very similar to that of Gaussian noise (Al-Muntafki, 2017) Autocorrelation is calculated according to Equation (3), which can be implemented using the built-in MATLAB function xcorr(·):

$$R_x = \frac{\sum_{i=1}^{N}\left(x_i - m_x\right)\left(x_{i+k} - m_x\right)}{\sum_{i-1}^{N}\left(x_i - m_x\right)^2} \quad (3)$$

Where:
x_i = Chaos sequence
x_{i+k} = Lagged chaos sequence
m_x = Mean of chaos sequence

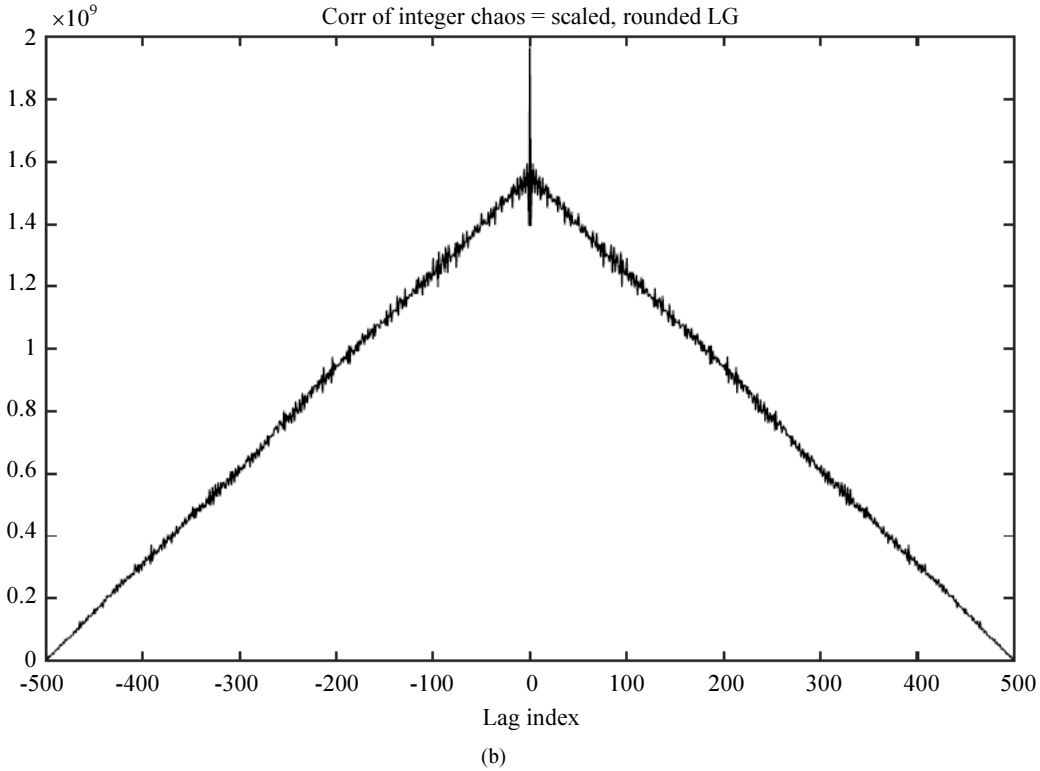
Figure 2a shows the autocorrelation of the real chaos signal; Fig. 2b shows the autocorrelation of the integer chaos signal. They are almost same; hence, autocorrelation features have preserved by the integer transform.

The next section presents a brief description of the LSB technique using 1, 2 and 4 LSBs for hiding a secret message in the cover image.



(a)

DOI: 10.3844/jcssp.2018.1247.1266



(b)

Fig. 2: The autocorrelation (a) correlation of real chaos (b) correlation of integer chaos: scaled and rounded

LSB Steganography Technique

LSB steganography is the most popular technique in the spatial domain steganography; sometimes, it is called a substitution method. It is used for embedding information directly into another information medium in a sequential or random manner without presence significant distortions. In a grayscale image, every pixel is represented in 8-bits; the last bit of each pixel is named Least Significant Bit (LSB). The cover image and secret message have changed into a binary representation, then LSB of each pixel in the cover image is exchanged by secret message bits.

In this study, the 1, 2 and 4 LSB-bits are used for hiding message. This helps to embed extra data (high capacity); but increasing the number of bits for hiding causes significant distortion of the stego image, thus it will reduce the security level.

The next section presents a brief description of an improved LSB technique.

An Improved LSB Technique (Yadav *et al*., 2011)

For a fair comparative study, this section explains an efficient approach that improved the performance of conventional LSB technique (Yadav *et al*., 2011). This improved LSB technique used the last two bits of the cover-image pixels for embedding and retrieval of secret message.

In the embedding process, it embeds the message bit 0 at a pixel value if the last two bits of pixel value are 00 or 10. If the last two bits of pixel value are not 00 or 10, try to make them 00 or 10 by adding or subtracting 1 at that pixel value to embed 0. Also, it embeds the message bit 1 at a pixel value if the last two bits of pixel value are 01 or 11. If the last two bits of pixel value are not 01 or 11 then we try to make them 01 or 11 by adding or subtracting 1 at that pixel value to embed 1.

In the retrieval process, if the last two bits of a pixel are 00 or 10, then 0 is the message bit, otherwise it is 1. In this study we will call this approach as “improved LSB”.

The next section explains two proposed systems for hiding secret information (text or image).

The Proposed Systems

According to the shuffled addresses which are explained above, two extended systems are proposed from the well-known LSB method and the recent Identical-Bits Method.

The Chaos-LSB Steganography

LSB steganography is a method for hiding a secret message inside the cover image directly in a sequential

DOI: 10.3844/jcssp.2018.1247.1266

manner. This makes LSB technique less resistive to cyber-attack. To enhance its security, in this study a modified system is proposed that employs a chaotic map to hide a secret message (text or image) in the cover image via shuffling of addresses bits. The proposed system uses a chaotic map to generate integer chaotic series (secret key), to choose pixel addresses of the cover image for embedding the secret message. The parameters of the chaotic map are secret keys known only to the sender and receiver. The observer cannot detect the existence of a secret message without knowing these secret keys. The proposed system is divided into two processes; the Chaos-LSB encoding and the Chaos-LSB decoding.

Chaos-LSB Encoding

Firstly, the cover image and secret message are entered and then a secret key is generated by a modified logistic map to select addresses pixels of the cover image chaotically. Additionally, the encoding process is done to get the output which represents stego image. The following algorithm shows the steps of this process. Figure 3 shows a block diagram of the proposed system.

Chaos-LSB Algorithm

Input// Gray-scale cover image X, secret message M (text or image), secret key.
Output// Stego image Y.
Step 1: Read the cover image and the secret message (text or image).
Step 2:- Convert the cover image to binary.
Step 3:- Convert secret message (image to binary) or (text to ASCII code and then to binary).
Step 4:- Check the size of the cover image and the secret message, the size of the cover image should be larger than the size of the secret message, else go to step11.
Step 5:- Get new addresses of pixels for inserting the secret message into the cover image by generating the secret key (integer chaotic series) as shown in section 3.2
Step 6:- Calculate K-LSBs for each chosen pixels of the cover image, K = 1, 2 and 4.
Step 7:- Replace K-LSBs for each chosen pixels of the cover image with each bit of the secret message K by K.
Step 8:- Repeat Step 6 to Step 7 until all secret message bits are embedded.
Step 9:- Set the image with the new value to produce stego image.
Step 10:- Convert the stego image to the decimal.
Step 11:- Stop.

Figure 4 illustrates the embedding process of Chaos-LSB Algorithm.

Chaos-LSB Decoding

Firstly, the stego image and secret key are entered, then the random pixels of the stego image are determined by the secret key to extract the secret message. The following algorithm shows the steps of this process.

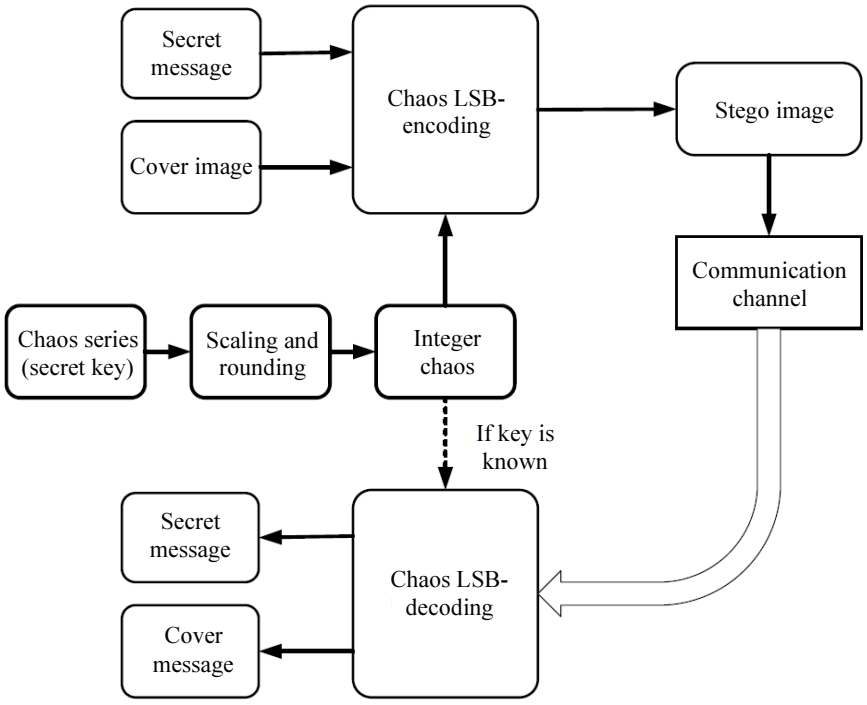


Fig. 3: Block diagram of the proposed system

DOI: 10.3844/jcssp.2018.1247.1266

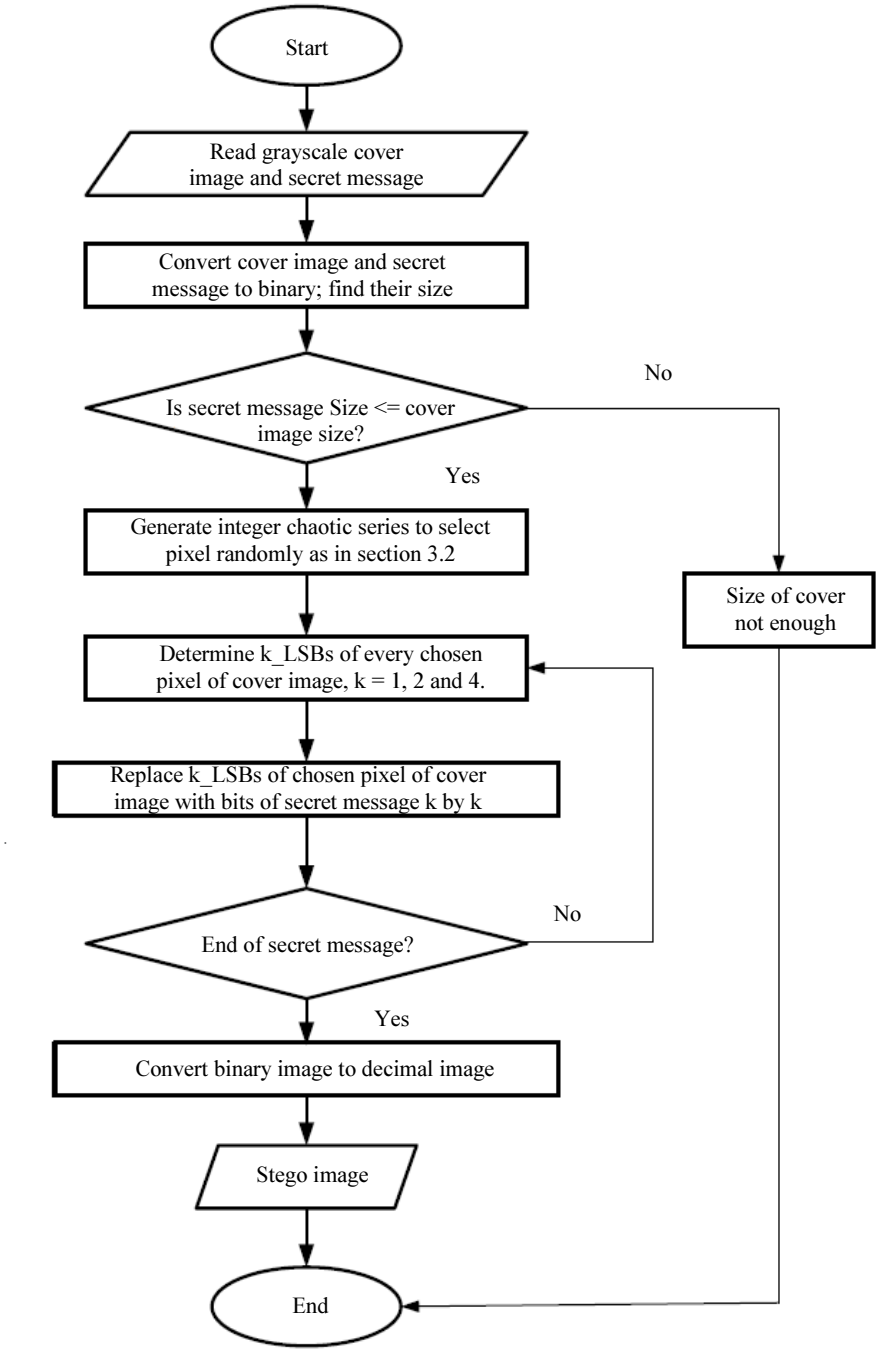


Fig. 4: Embedding Process in Chaos-LSB Algorithm

Retrieval by Chaos-LSB Algorithm:

Input// Stego image Y, secret key.
Output// Secret message M (text or image).
Step 1:- Read stego image.
Step 2:- Choose pixels position in stego image by the secret key.
Step 3:- Convert stego image to binary.
Step 4:- Determine K-LSBs for each pixel of the stego image, K = 1, 2 and 4.
Step 5:- Retrieve bits of the secret message (text or image).
Step 6:- Repeat Step 4 to Step 5 until all secret message bits are retrieved.
Step 7:- Convert secret message (text or image) to decimal, if the secret message is text it will convert to the character.

Step 8:- Stop

The Chaotic Identical-Bits Steganography

The technique in (Al-Shatnawi, 2012) hides 2 bits of the secret message in the color image pixels depending on the searching for the identical bits between the secret message bits and cover image bits. This makes the technique increase the security level comparable to the conventional LSB technique. If the identical bits are not available, it is hidden in 2LSBs of the color image pixels.

In this study, this technique is used for hiding the secret message (text or image) in a grayscale image. Many researchers are based on color image and grayscale image to hide significant information. In the proposed work, the focus is on the grayscale image for information hiding. A grey-scale image is very proper for information hiding than the color image. Because the disorder of the correlation among the color components is detected easily; this will cast doubt on existence hidden information (Chatterjee, 2017).

In this system, chaotic addressing is employed as an additional security dimension in steganography and incorporating it with the technique in (Al-Shatnawi, 2012). The cover image pixels are chosen randomly by a modified logistic map to generate integer chaotic series. This series extracts the address of pixels in the cover image. The proposed system is divided into two processes; the Chaotic Identical-Bits encoding process and the Chaotic Identical-Bits retrieval process Fig. 3 shows a block diagram of the proposed system.

The Chaotic Identical-Bits Embedding Process

Firstly, the cover image and secret message are entered and then a secret key is generated by a modified logistic map to select addresses pixels of the cover image chaotically. Additionally, the embedding process is done to get the output which represents stego image. The following algorithm shows the steps of this process.

Embedding Chaotic Identical-Bits Algorithm

Input// Grayscale cover image X, the secret message M (text or image), secret key.
Output// Stego image Y.
Step 1:- Read the cover image and secret message (text or image).
Step 2:- Convert cover image to binary.
Step 3:- Convert secret message (image to binary) or (text to ASCII code and then to binary).
Step 4:- Check the size of the cover image and the size of the secret message. The size of the cover image should be larger than the size of the secret message, else go to step11.
Step 5:- Get new addresses of pixels for inserting the secret message into the cover image by generating the secret key (integer chaotic series) as shown in section 3.2
Step 6:- Hide 2 bits of the secret message (text or image) in 2bits of a chosen pixel in the cover image by searching for the identical bits. If the matching is achieved go to setp7; otherwise, hide in the 2LSB of the selected pixels.
Step 7:- Sort the positions of the hidden bits in a binary table.
Step 8:-Repeat Step 6 to Step7 until all secret message bits are embedded.
Step 9:- Set the image with the new value to produce stego image.
Step 10:- Convert stego image to decimal.
Step 11:- Stop.

Figure 5 illustrates a flowchart of Embedding Chaotic Identical-Bits Algorithm

The Chaotic Identical-Bits Retrieval Process

Firstly, the stego image, binary table and secret key are entered and then the random pixels of the stego image are determined by the secret key. After that, the stego image is converted into binary, then searching for the location of the hidden bits in a binary table is done to extract the secret message. The decoding algorithm shows the steps of the Retrieval process.

Chaotic Identical-Bits Retrieval

Input// Stego image Y, secret key, binary table.
Output// Secret message M (text or image).
Step 1:- Read stego image.
Step 2:- Choose pixels position in stego image using the secret key.
Step 3:- Convert stego image to binary.
Step 4:- Search for the location of the hidden bits in a binary table.
Step 5:- Retrieve bits of secret message (text or image).
Step 6:- Repeat Step 4 to Step 5 until all secret message bits are retrieved.
Step 7:- Convert secret message (text or image) to decimal, if the secret message is text it will convert to a character.
Step 8:- Stop.

The next section displays experimental results and discussions using some performance measures.

DOI: 10.3844/jcssp.2018.1247.1266

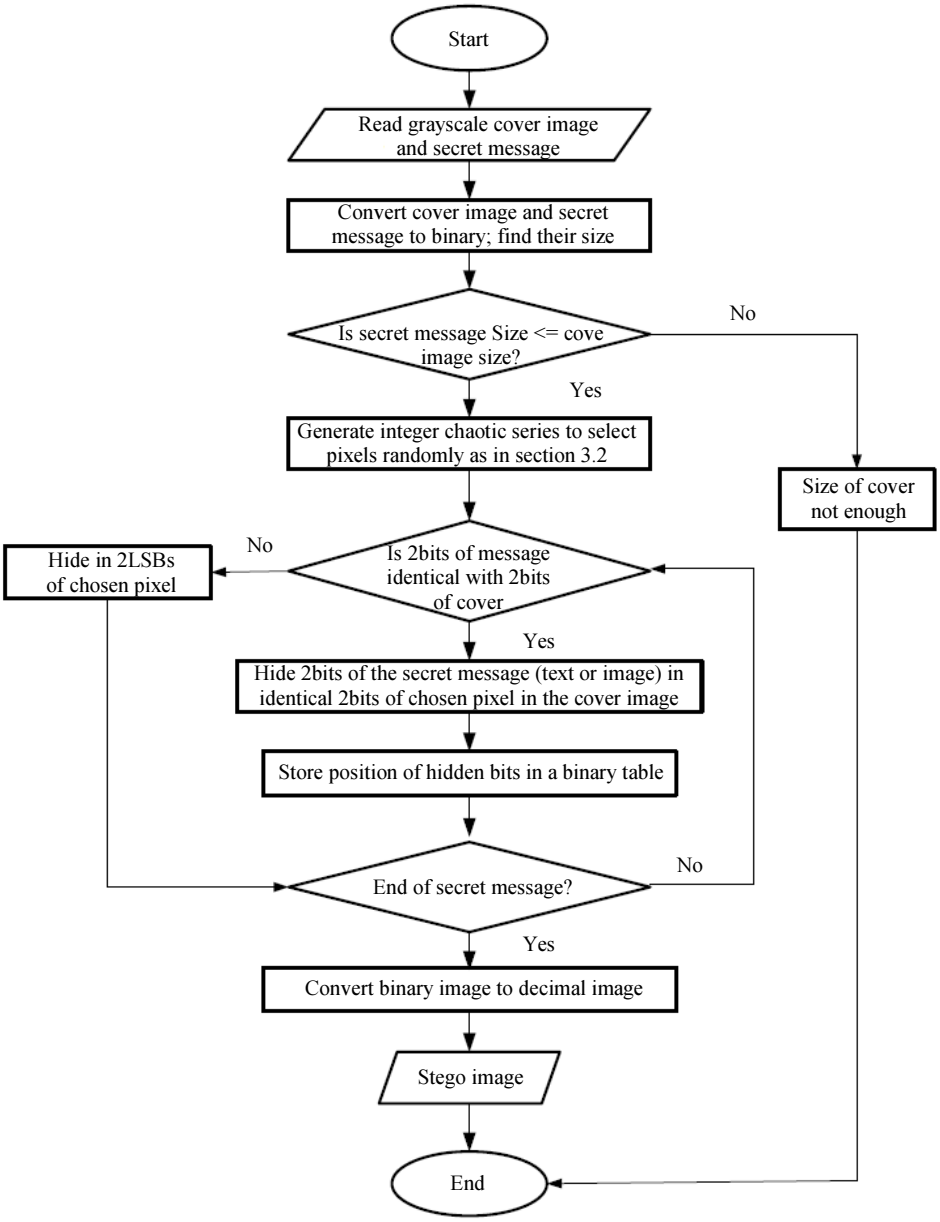


Fig. 5: Embedding process in chaotic identical-bits algorithm

Experimental Results and Discussion

In this study, the 1, 2 and 4LSBs technique, the technique in (Al-Shatnawi, 2012) and the two proposed systems have been implemented on the grey-scale image using MATLAB (R2016a) on windows 10. All techniques are applied to hide the secret messages *(text: A word is enough to the wise)* and *(image: MATLAB cameraman image 100*100)* as shown in Fig. 6. The performance of these techniques has been evaluated using different experiments. Four MATLAB grayscale images with different sizes (lighthouse.png 750*800, toysnoflash.png 912*684, football.jpg 680*930, yellowlily.jpg 950*990) are used as cover images shown in Fig. 7.

Standard performance measures are used to test the performance of the proposed techniques versus existing ones: Mean-Squared Error (MSE) Peak Signal-to-Noise Ratio (PSNR), histogram and correlative analysis.

Quality Measures

The standard measures of image quality are the MSE and PSNR. MSE is the square of the error between the cover image and the stego image. PSNR is the ratio of

the extreme signal to noise power between the stego image and the cover image. It is normally measured in dB (Kutter and Petitcolas, 1999). MSE and PSNR are computed according to Equations (4) and (5) respectively as follows:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(X(i,j)-Y(i,j)\right)^2 \quad (4)$$

$$PSNR = 10\log_{10}\frac{(255)^2}{MSE} \quad (5)$$

where, m and n are row and column indices, $X(i,j)$ denotes the cover image and $Y(i,j)$ denotes the stego image.

Based on analysis of the results given in Table 1 and Table 2 the two proposed systems for hiding the secret message have better quality and higher security than the 1, 2 and 4LSBs technique and the technique in (Al-Shatnawi, 2012) because it provides a balance between PSNR values and security.

From the above results, it can be concluded that the proposed Chaotic Identical-Bits system has better performance than the proposed Chaos-LSB system.

Different sizes of the secret image (cameraman image: 5*5, 10*10, 20*20, 30*30, 50*50 and 100*100) have been applied and the ratio R_m between message size and cover size has been calculated. The size ratio is defined as:

$$R_m = \frac{Message\ Size}{Cover\ Image\ Size} \quad (6)$$

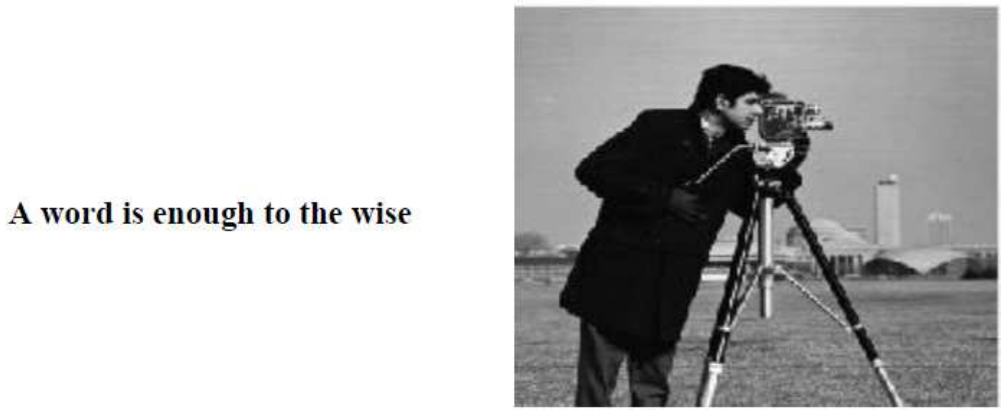
As the size ratio R_m increases, PSNR decreases. Figure 8a shows the relation when applying the proposed Chaos-LSB system. Figure 8b shows the relation when applying the proposed Chaotic Identical-Bits system.

Table 2: Comparison the value of PSNR and MSE between all techniques implemented in this work when hiding an image of size (100*100)

		Technique in (Al-Shatnawi 2012)		Proposed chaotic identical-bits technique		Improved LSB		Proposed Chaos-LSB technique	
Cover image	Size cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lighthouse.png	750x800	0.0579	60.5029	0.0611	60.2684	0.1965	55.1982	0.2506	54.1415
Toysnoflash.png	912x684	0.0527	60.9088	0.0542	60.7933	0.1873	55.4044	0.2419	54.2940
Football.jpg	680x930	0.0368	62.4705	0.0429	61.8025	0.1853	55.4526	0.2376	54.3719
Yellowlily.jpg	950x990	0.0340	62.8201	0.0345	62.7493	0.1251	57.1578	0.1593	56.1089

Table 2: Comparison the value of PSNR and MSE between all techniques implemented in this work when hiding an image of size (100*100)

		Technique in (Al-Shatnawi 2012)		Proposed chaotic identical-bits technique		Improved LSB		Proposed Chaos-LSB technique	
Cover image	Size cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lighthouse.png	750x800	0.0579	60.5029	0.0611	60.2684	0.1965	55.1982	0.2506	54.1415
Toysnoflash.png	912x684	0.0527	60.9088	0.0542	60.7933	0.1873	55.4044	0.2419	54.2940
Football.jpg	680x930	0.0368	62.4705	0.0429	61.8025	0.1853	55.4526	0.2376	54.3719
Yellowlily.jpg	950x990	0.0340	62.8201	0.0345	62.7493	0.1251	57.1578	0.1593	56.1089



(a) (b)

Fig. 6: The secret message (a) text (b) cameraman image

DOI: 10.3844/jcssp.2018.1247.1266

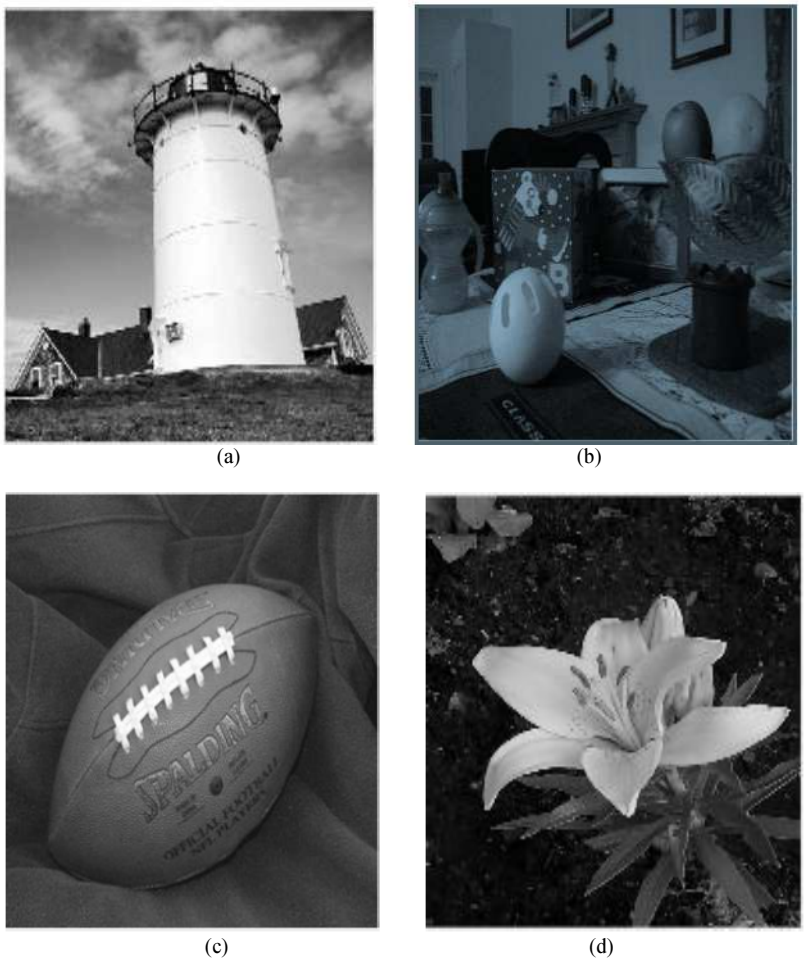
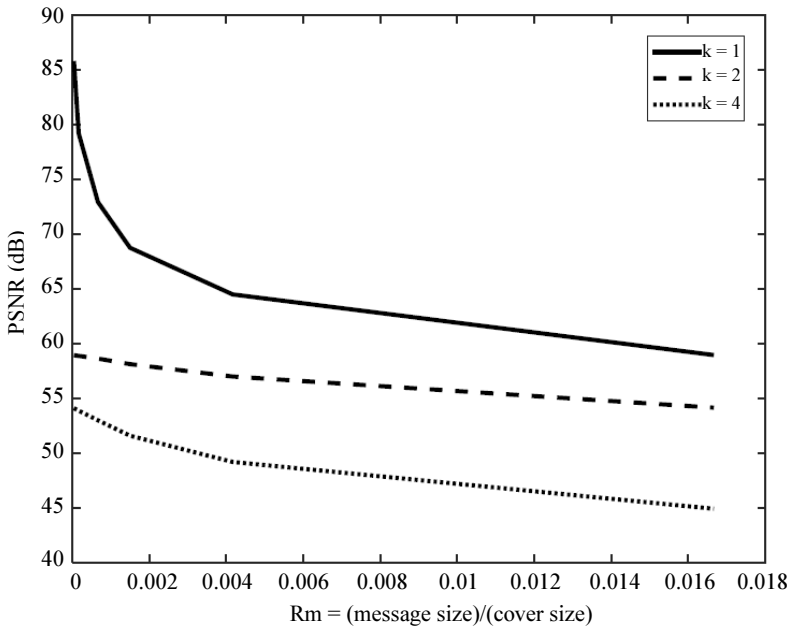
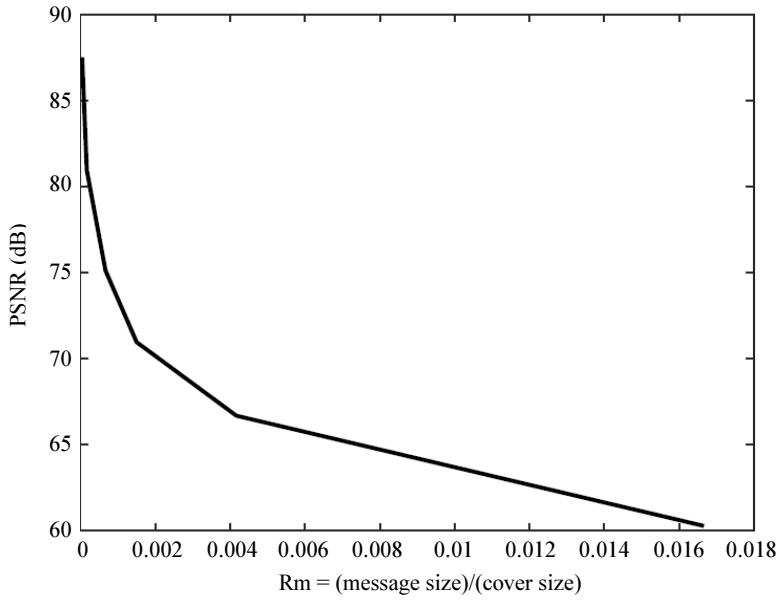


Fig. 7: The cover MATLAB images: (a) lighthouse.png (b) toysnoflash.png (c) football.jpg (d) yellowlily.jpg



(a)

DOI: 10.3844/jcssp.2018.1247.1266



(b)

Fig. 8: The size ratio (message size/cover size) Vs. PSNR by applying (a) the proposed Chaos- LSB system (b) the proposed Chaotic Identical-Bits system

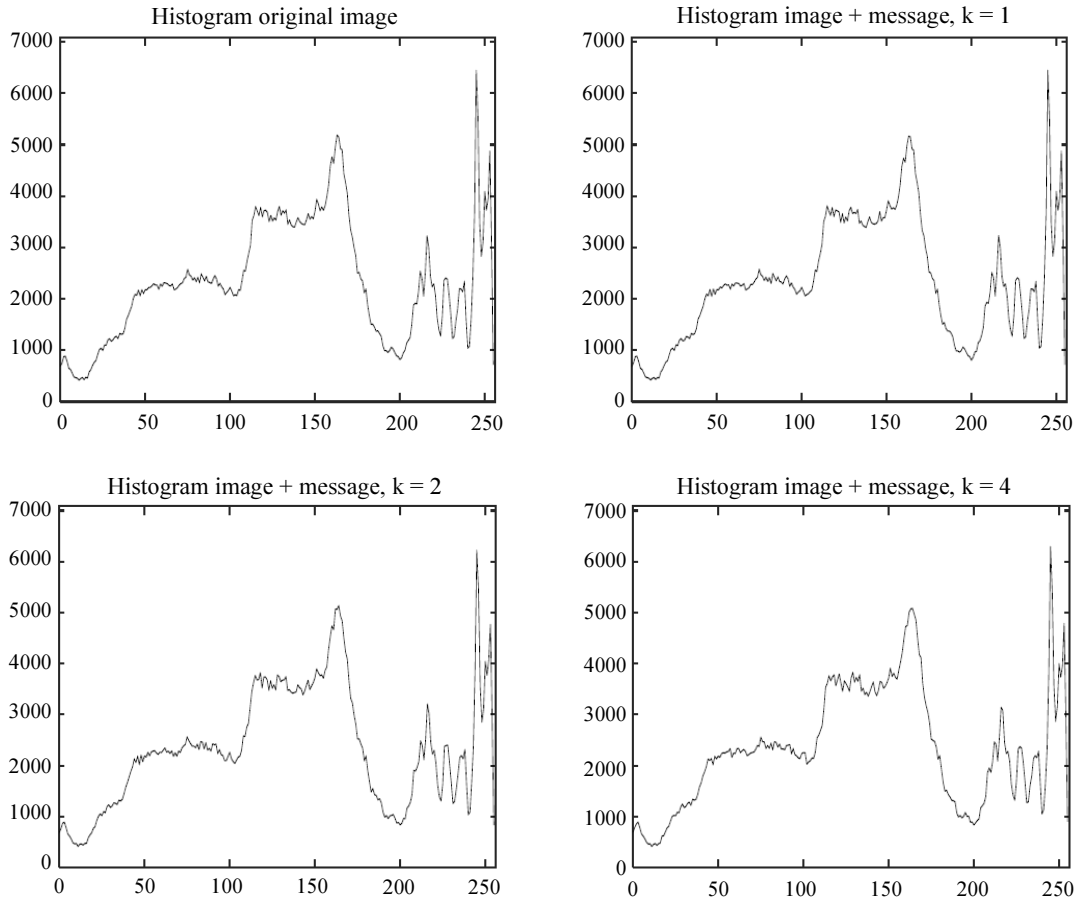


Fig. 9: Histogram analysis for the original image (lighthouse) and stego images when

DOI: 10.3844/jcssp.2018.1247.1266

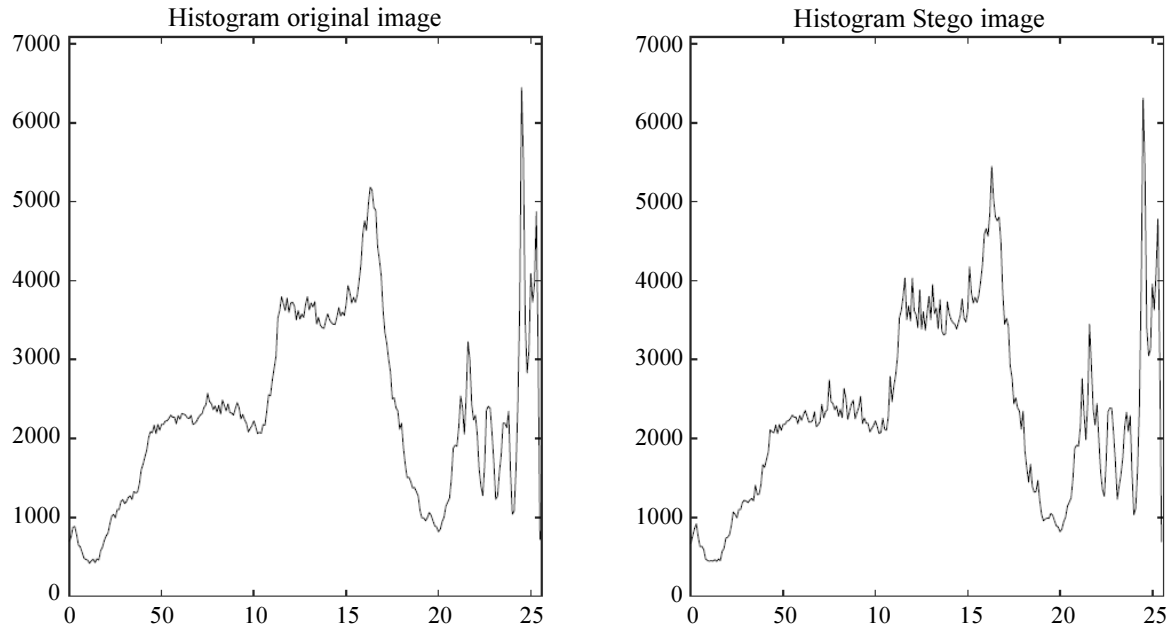


Fig. 10: Histogram analysis for (a) original image (lighthouse) and (b) stego image when applying the Chaotic Identical-Bits system

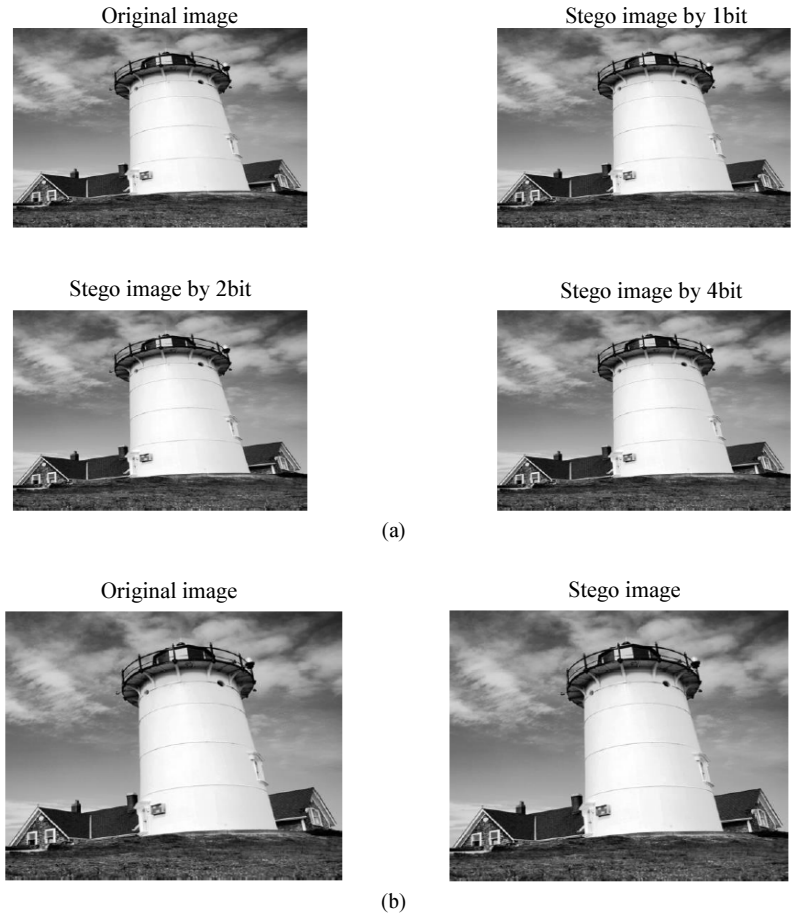


Fig. 11: Original and stego image after applying (a) Chaos-LSB method (b) Chaotic Identical- Bits method

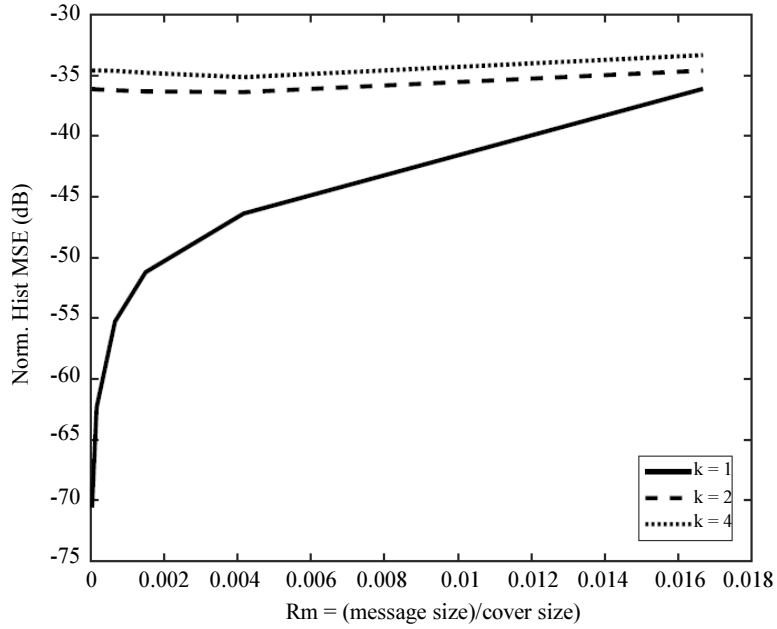
DOI: 10.3844/jcssp.2018.1247.1266

Histogram Analysis

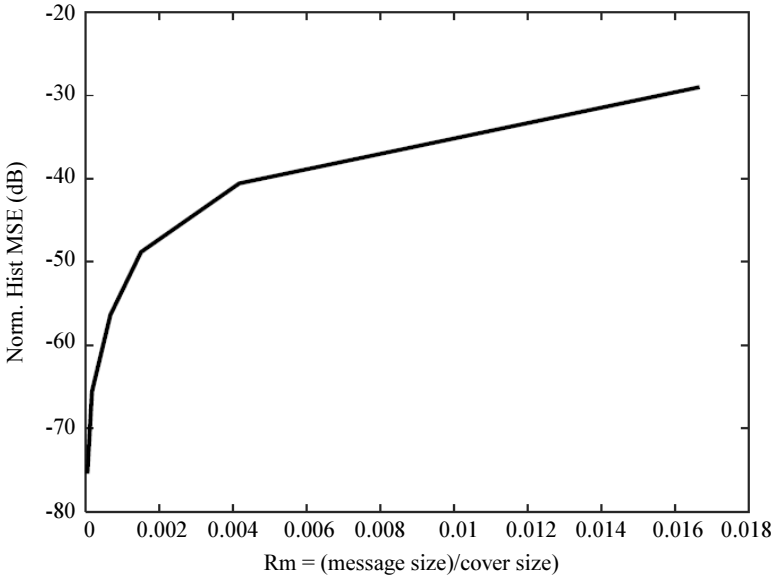
Histogram illustrates the distribution of pixels in an image. This approach is used to test the pixel differences before and after the embedding process. Figure 9 shows the histogram of the original and stego images when applying the proposed Chaos-LSB system. It is noted a significant similarity between the histogram of the cover image and the histogram of the stego image; this means little distortion has happened after embedding the secret message into the cover image.

Figure 10a shows the histogram of the original image when applying the proposed Chaotic Identical-Bits system, while Fig. 10b shows the histogram of stego image when applying the proposed Chaotic Identical-Bits system.

The stego image looks like the original image, so the Human Vision System (HVS) cannot recognize the difference between them. Figure 11a show the stego images after applying Chaos-LSB system. Figure 11b shows the stego image after applying a Chaotic Identical-Bits system.



(a)



(b)

Fig. 12: MSE versus size ratio (message size/cover size): (a) The proposed Chaos-LSB system (b) The proposed Chaotic Identical-Bits system

The histogram MSE values increase when the ratio between message size and cover image size increases as shown in Fig. 12. The MSE (and MSE in dB) are computed according to Equations (7) and (8) below:

$$E = \sum_{i=1}^{256}\left[S(i) - H(i)\right]^2 / \sum_{i=1}^{256}\left[H(i)\right]^2 \quad (7)$$

$$Edb = 10\log_{10}(E) \quad (8)$$

Here E is the error in the histogram, S is the histogram of the stego image and H is the histogram of the cover image. Note that E has been normalized in (7).

Correlative Analysis

To compute the correlation between two contiguous pixels (horizontal, vertical and diagonal), 5000 pairs of contiguous pixels are randomly chosen from the cover image and the stego images. The Correlative analysis is computed according to Equation (9) (Wang *et al*., 2012). The range of correlation coefficient is [−1,1]; it can be implemented using the built-in MATLAB function corrcoef(·):

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

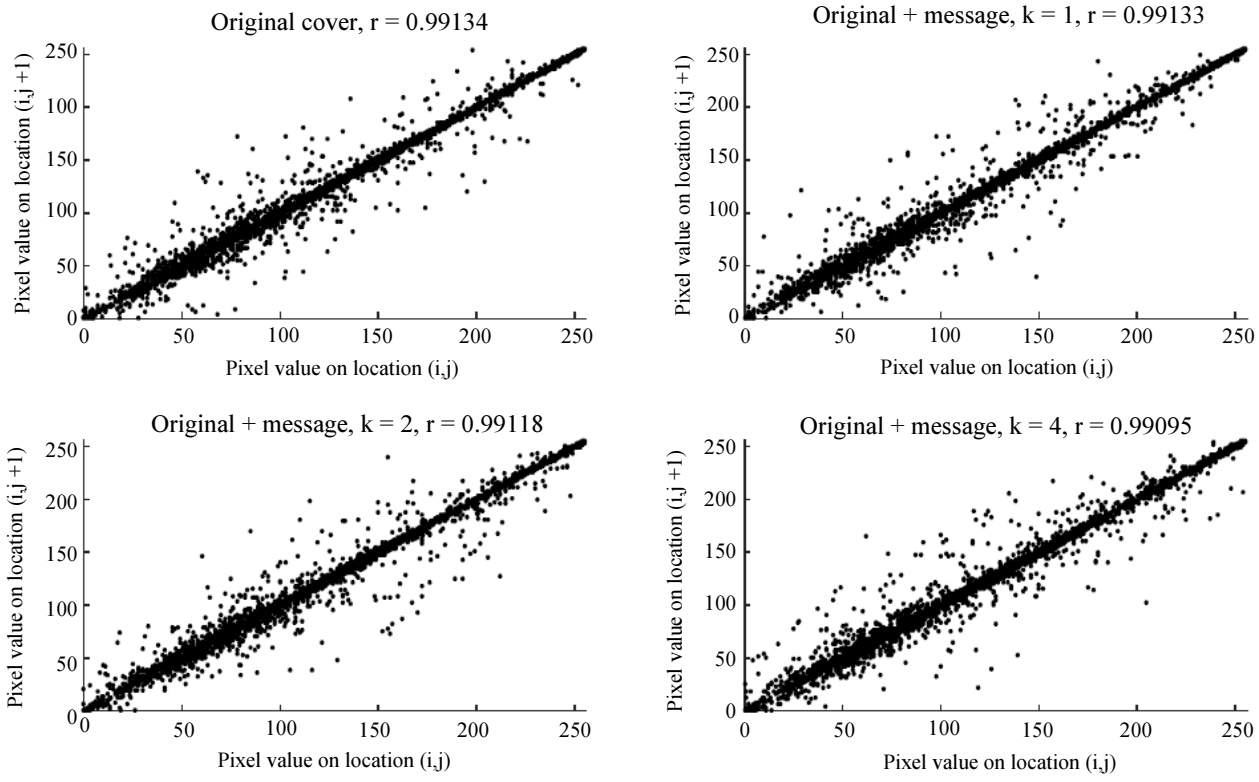
$$\operatorname{cov}(x,y) = \varepsilon\left(x - \varepsilon(x)\right)\left(y - \varepsilon(y)\right) \quad (10)$$

$$\varepsilon(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i\right) \quad (11)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \varepsilon(x)\right)^2 \quad (12)$$

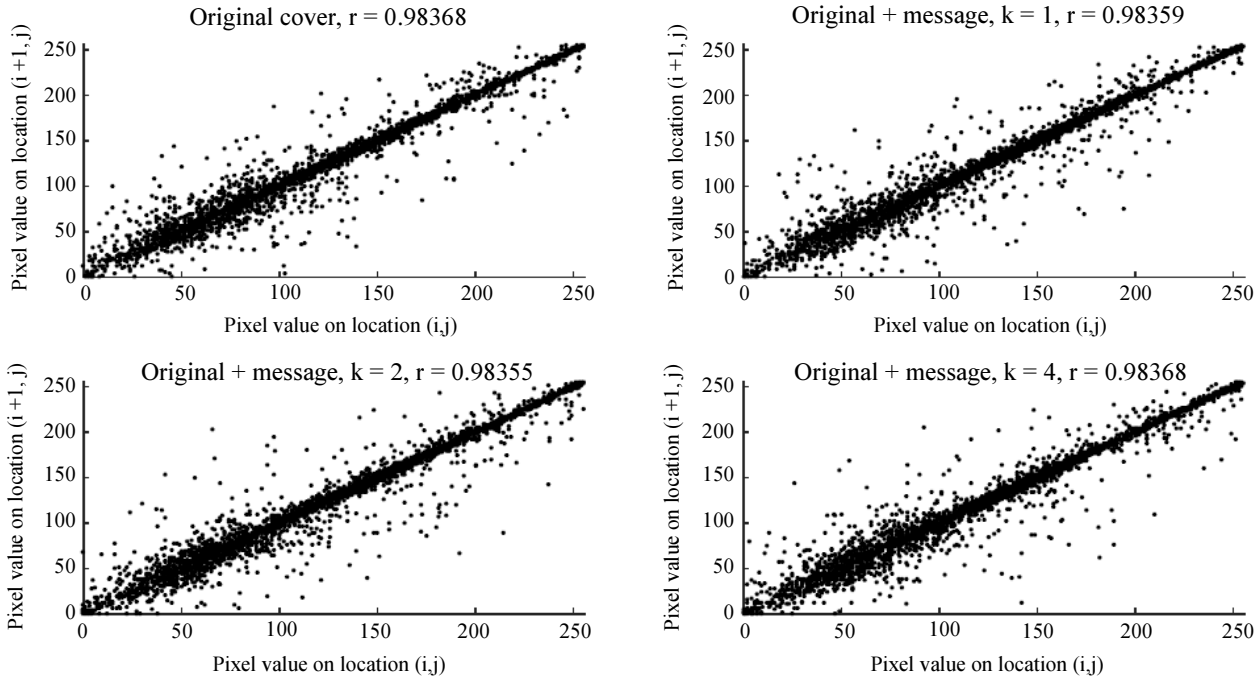
$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \varepsilon(x)\right)\left(y_i - \varepsilon(y)\right) \quad (13)$$

where, x and y are the intensity values of two adjacent pixels in the image and N is the total number of pixels in the image. Figure 13 shows the correlation between two adjacent pixels (vertical, horizontal and diagonal) of the cover image (toysnoflash) and stego image after embedding the secret image (cameraman) by the proposed Chaos-LSB system. Figure 14 shows the correlation between two adjacent pixels (vertical, horizontal and diagonal) of the cover image (lighthouse) and stego image after embedding the secret image (cameraman) by the proposed Chaotic Identical-Bits system. No much difference in the correlation coefficient is noticed after encoding. This is an indication of high security.

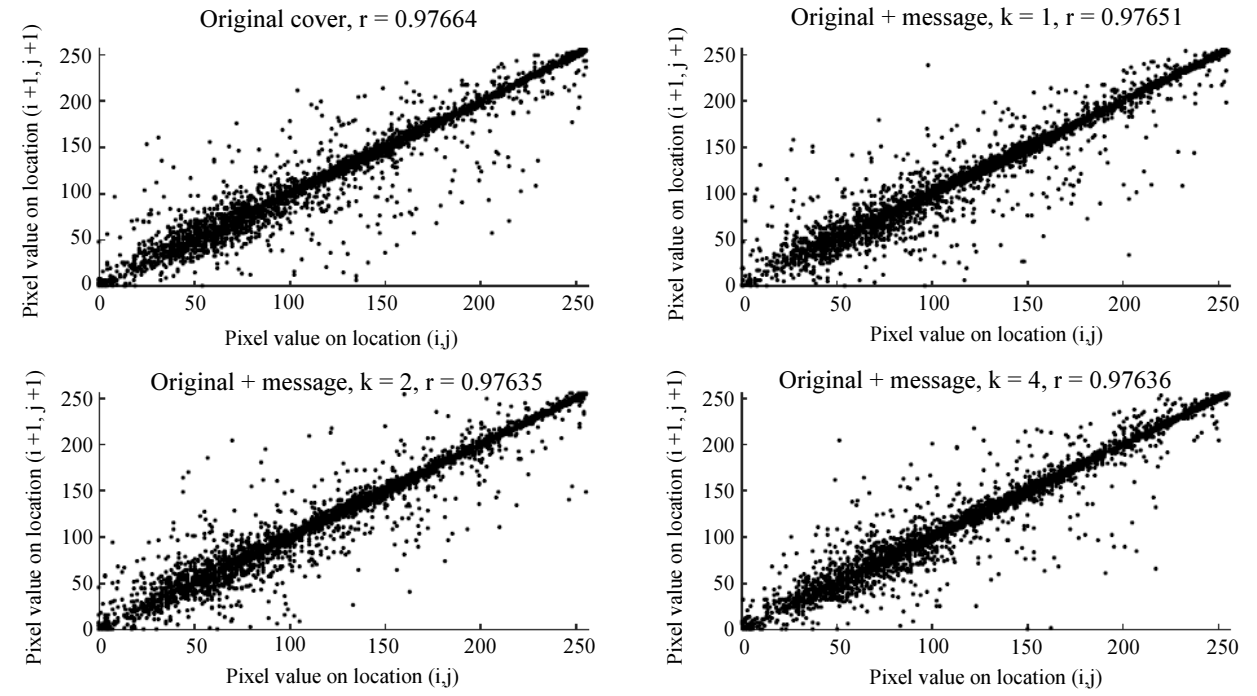


(a)

DOI: 10.3844/jcssp.2018.1247.1266



(b)



(c)

Fig. 13: Correlation of adjacent pixels (a: vertical, b: horizontal and c: diagonal) in the proposed chaos-LSB system

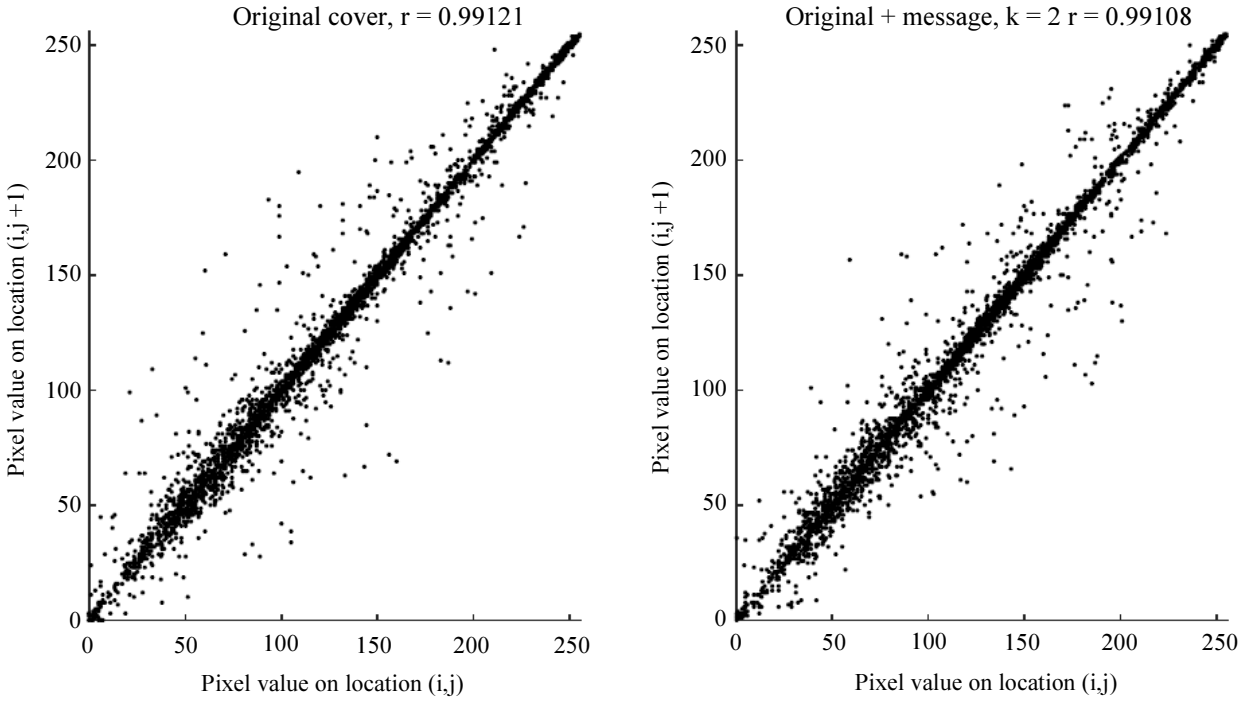
A Comparison with the Improved LSB Steganography (Yadav et al., 2011):

A comparison between the recently-proposed improved LSB (Yadav *et al*., 2011) and the two proposed systems (Chaotic-LSB and Chaotic Identical-Bits) is performed. The cover image is (lighthouse.png 750*800) and the secret message is (cameraman.tif) with six sizes (5*5, 10*10, 20*20, 30*30, 50*50, 100*100). Figure 15 shows the ratio

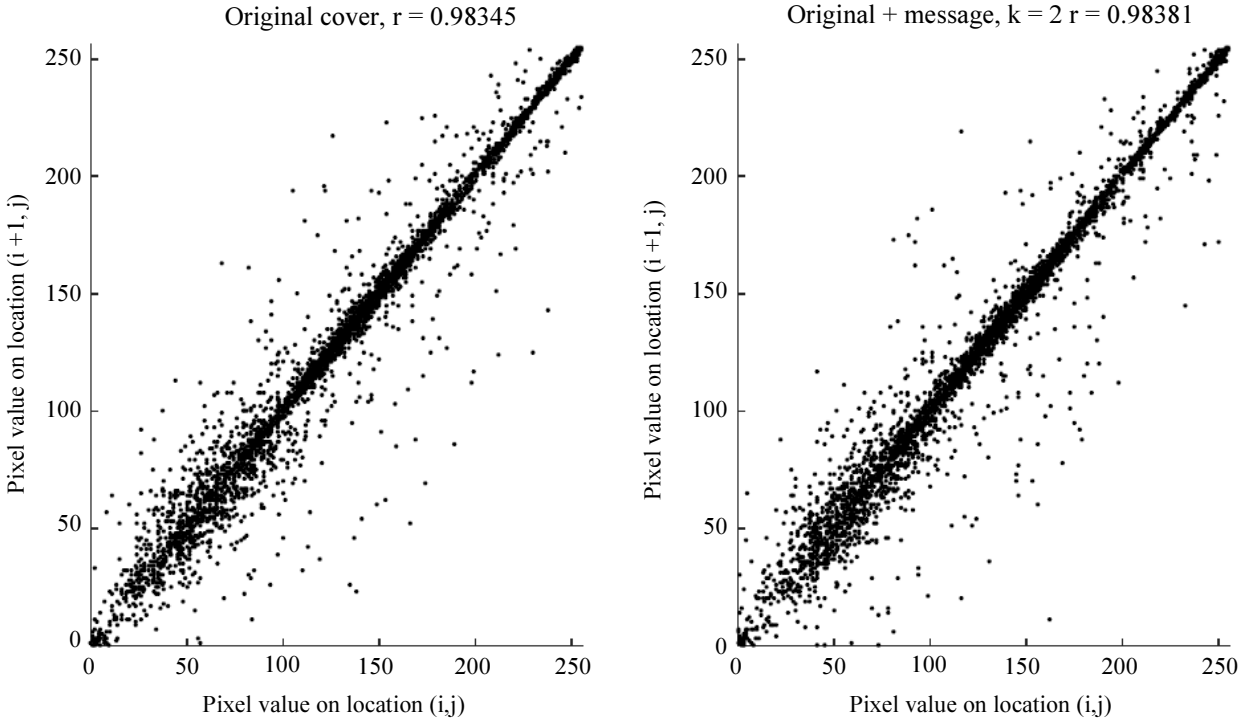
DOI: 10.3844/jcssp.2018.1247.1266

(message size/ cover size) versus PSNR for the three techniques. It is clear that the proposed Chaotic Identical-Bits technique has the best PSNR performance among the techniques.

In future works, the Authors will extend their testing for the performance of these techniques over real-life engineering systems, especially long-range wireless channels as in (Mahmoud *et al.* 2006; 2002).

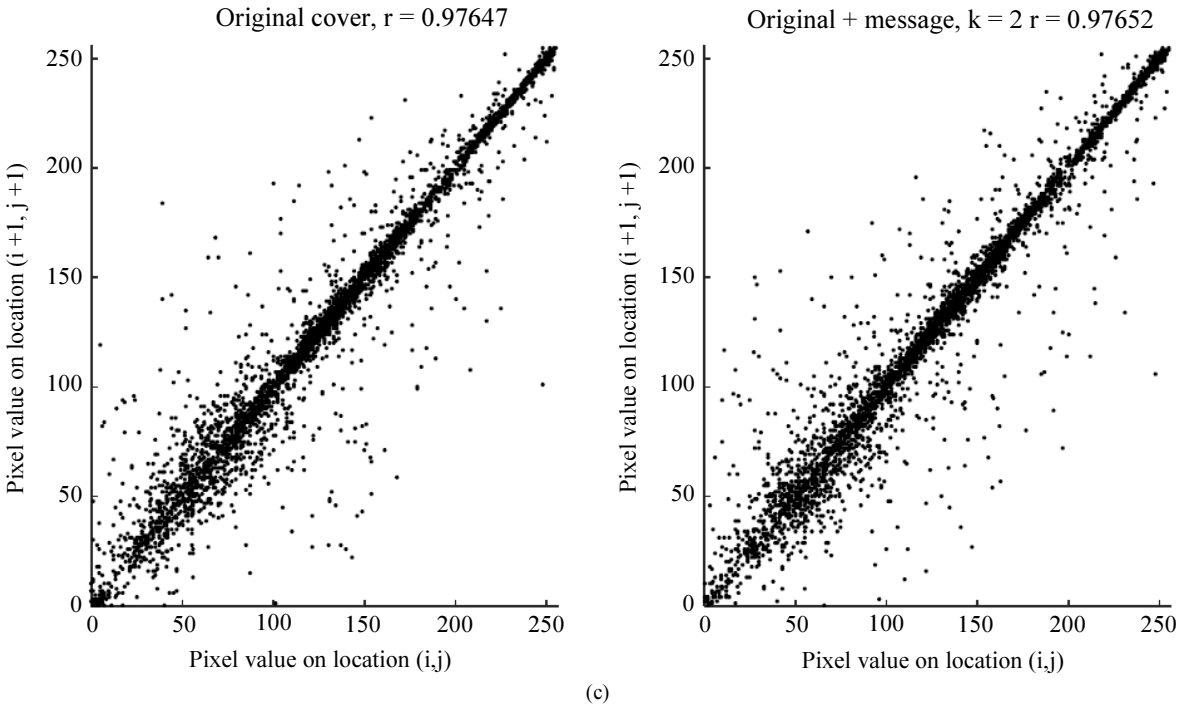


(a)



(b)

DOI: 10.3844/jcssp.2018.1247.1266



(c)

Fig. 14: Correlation of adjacent pixels (a: vertical, b: horizontal and c: diagonal) in the proposed chaotic Identical-Bits system

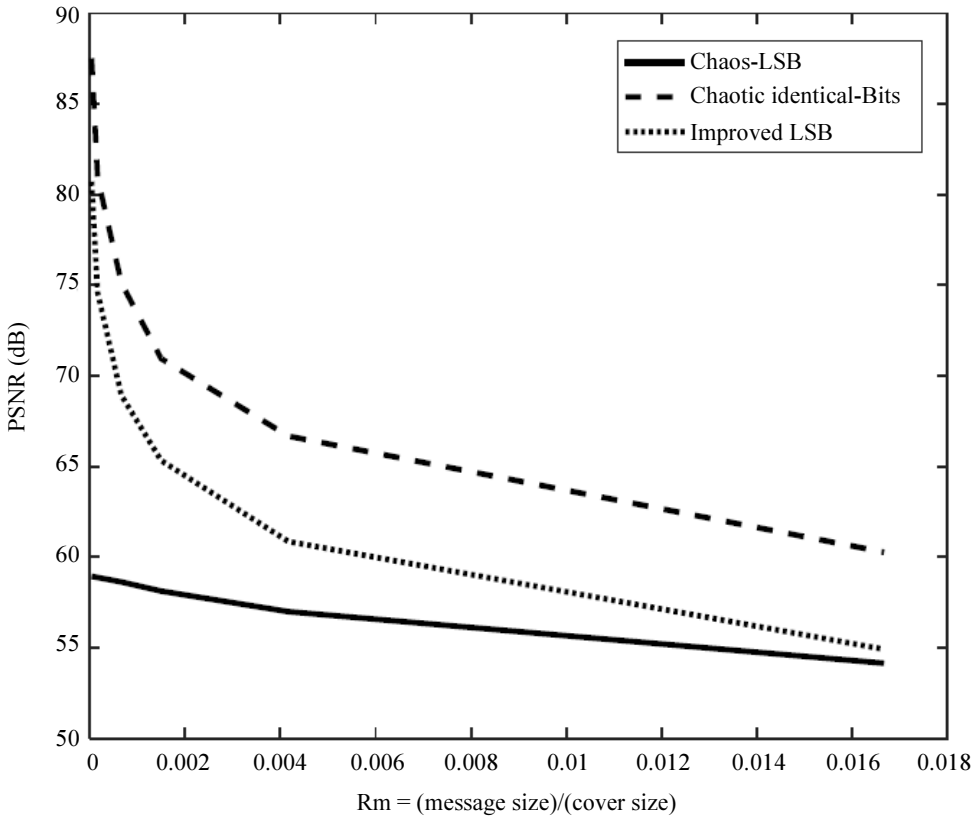


Fig. 15: Size ratio (message size/cover size) versus PSNR for the proposed systems and the improved LSB (Yadav *et al*., 2011)

Conclusion

Two systems for steganography in the spatial domain are proposed. These systems are based on the well-known LSB and the recently-proposed identical-bits steganography. The new systems have utilized chaos theory for address shuffling to add a new security dimension. The first system is based on the LSB technique for hiding the secret message (text or image). The chaotic map used for address shuffling has been modified in order to generate integer chaotic series. The proposed systems have much higher security level than their conventional counterparts. The approach is versatile as it could be added to other steganographic systems to enhance their security. Various performance measures have been considered to test security levels. Results showed that the two proposed systems have higher security and reliability than their existing counterparts.

Acknowledgement

The Authors would like to thank the Ministry of Higher Education and Scientific Research (Iraq) for their financial support of this project. Many thanks to the (anonymous) reviewers for their constructive comments; without these comments the paper would never be in this readable form.

Author's Contributions

Ola N. Kadhim: Contributed to the design and simulation of the proposed system. She did most of the paper write-up.

Zahir M. Hussain: Contributed to the design, analysis and simulation of the proposed system. He has also contributed to the write-up and language revision.

Ethics

The Authors declare that there are no ethical issues regarding this project.

References

Al-Muntafki, Z.A., 2017. Chaos generation in non - linear digital systems. University of Kufa.

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

Al-Taani, A.T and A.M. Al-Issa, 2009. A novel steganographic method for gray-level images. Int. J. Comput. Inform. Syst. Sci. Eng., 3: 5-10.

Amirtharajan, R. and J.B.B. Rayappan, 2012. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124. DOI: 10.1016/j.ins.2012.01.010

Azou, S., G. Burel and C. Pistre, 2002. A chaotic direct-sequence spread-spectrum system for underwater communication. Proceedings of the MTS/IEEE, Oct. 29-31, IEEE Xplore Press, Biloxi, MI, USA, pp: 2409-2415. DOI: 10.1109/OCEANS.2002.1192004

Behnia, S., A. Akhshani, H. Mahmodi and A. Akhavan, 2008. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals, 35: 408-419. DOI: 10.1016/j.chaos.2006.05.011

Bukhari, S., M.R. Anjum, I.S. Bajwa and S. Dilbar, 2017. Chaos image encryption followed by the steganography technique. Sindh Univ. Res. J., 49: 113-118.

Chang, C.C., T.S. Nguyen and C.C. Lin, 2014. Reversible image hiding for high image quality based on histogram shifting and local complexity. Int. J. Netw. Security, 16: 201-213.

Chatterjee, U., 2017. Image steganography and it's application. MSc Thesis, Maulana Abul Kalam Ajad University of Technology.

Gutub, A., 2010. Pixel Indicator technique for RGB image steganography. J. Emerg. Technol. Web Intell., 2: 1-9. DOI: 10.4304/jetwi.2.1.56-64

Habib, M., B. Bakhache, D. Battikh and S.E. Assad, 2015. Enhancement using chaos of a steganography method in DCT domain. Proceedings of the 5th International Conference on Digital Information and Communication Technology and its Applications, Apr. 29-May 1, IEEE Xplore Press, Beirut, Lebanon pp: 204-209. DOI: 10.1109/DICTAP.2015.7113200

Karim, S.M.M., M.S. Rahman and M.I. Hossain, 2011. A new approach for LSB based image steganography using secret key. Proceedings of the 14th International Conference on Computer and Information Technology, Dec. 22-24, IEEE Xplore Press, Dhaka, Bangladesh, pp: 286-291. DOI: 10.1109/ICCITechn.2011.6164800

Khalind, O.S., 2015. New methods to improve the pixel domain steganography, steganalysis and simplify the assessment of steganalysis tools. PhD Thesis, University of Portsmouth.

Kutter, M. and F.A.P. Petitcolas, 1999. Fair benchmark for image watermarking systems. Proceedings of the Security and Watermarking of Multimedia Contents, (WMC' 99), SPIE, USA, pp: 226-240. DOI: 10.1117/12.344672

Lau, Y.S. and Z.M. Hussain, 2005. A new approach in chaos shift keying for secure communication. Proceedings of the 3rd International Conference on Information Technology and Applications, Jul. 4-7, IEEE Xplore Press, Sydney, Australia, pp: 630-633. DOI: 10.1109/ICITA.2005.30

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

Linh-Trung, N., D.V. Phong, Z.M. Hussain, H.T. Huynh and V.L. Morgan *et al*., 2008. Compressed sensing using chaos filters. Proceedings of the Australasian Telecommunication Networks and Applications Conference, Dec. 7-10, IEEE Xplore Press, Adelaide, pp: 219-223. DOI: 10.1109/ATNAC.2008.4783326

Luo, W., F. Huang and J. Huang, 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inform. Forens. Security, 5: 201-214. DOI: 10.1109/TIFS.2010.2041812

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

Manjula, G.R. and A. Danti, 2015. A novel hash based least significant bit (2-3-3) image steganography in spatial domain. Int. J. Security Privacy Trust Manage., 4: 11-20.

Martin, D. and A.M. Barmawi, 2015. List steganography based on syllable patterns. Proceedings of the International Conference on Electrical Engineering and Informatics, Aug. 10-11, IEEE Xplore Press, Denpasar, Indonesia, pp: 275-282. DOI: 10.1109/ICEEI.2015.7352510

Muhammad, K., J. Ahmad, N.U. Rehman, Z. Jan and R.J. Qureshi, 2015. A secure cyclic steganographic technique for color images using randomization. Techn. J. Univ. Eng. Technol. Taxila, 19: 57-64.

Sarreshtedari, S. and M.A. Akhaee, 2013. One-third probability embedding: A new±1 histogram compensating image least significant bit steganography scheme. IET Image Process., 8: 78-89. DOI: 10.1049/iet-ipr.2013.0109

Tayel, M., H. Shawky and A.D.S. Hafez, 2012. A new chaos steganography algorithm for hiding multimedia data. Proceedings of the 14th International Conference on Advanced Communication Technology, Feb. 19-22, IEEE Xplore Press, PyeongChang, South Korea, pp: 208-212.

Valandar, M.Y., P. Ayubi and M.J. Barani, 2017. A new transform domain steganography based on modified logistic chaotic map for color images. J. Inform. Security Applic., 34: 142-151. DOI: 10.1016/j.jisa.2017.04.004

Vigila, S.M.C. and K. Muneeswaran, 2015. Hiding of confidential data in spatial domain images using image interpolation. IJ Netw. Security, 17: 722-727.

Viswanatham, V.M. and J. Manikonda, 2010. A novel technique for embedding data in spatial domain. Int. J. Comput. Science Eng., 2: 233-236.

Wahballa, O., A. Wahaballa, F. Li and C. Xu, 2016. A secure and robust certificateless public key steganography based on SVD-DDWT. IJ Netw. Security, 18: 888-899.

Wang, X., J. Zhao and H. Liu, 2012. A new image encryption algorithm based on chaos. Opt. Commun., 285: 562-566. DOI: 10.1016/j.optcom.2011.10.098

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Patt. Recog. Lett., 24: 1613-1626. DOI: 10.1016/S0167-8655(02)00402-6

Yadav, R., R. Saini and G. Chawla, 2011. A novel approach for image steganography in spatial domain using last two bits of pixel value. Int. J. Security, 5: 51-61.