International Journal of Computer Applications (0975 - 8887)
Volume 138 - No.12, March 2016

Text Hiding in a Digital Cover Image using Two Dimensional Indexing based on Chaotic Maps

Mervat Mikhail
Teaching Assistant
Department of Engineering Mathematics,
Faculty of Engineering, Alexandria University, Egypt

Yasmine Abouelseoud
Associate Professor
Department of Engineering Mathematics,
Faculty of Engineering, Alexandria University, Egypt

Galal Elkobrosy
Professor
Department of Engineering Mathematics,
Faculty of Engineering, Alexandria University, Egypt

ABSTRACT

This paper presents a new approach for secure hiding of textual data in a colored digital image. Use of images as a cover media in steganography is based on the deficiencies in the human visual system (HVS). The proposed technique employs two independent chaotic sequences for specifying the locations where the message bits are embedded in the cover image using an adapted version of the least significant bit (LSB) method. Message bits are embedded using the 3-3-2 LSB insertion method for the chaotically selected pixels of the cover image. This technique provides sufficient security as the same sequence of numbers cannot be generated without knowing the exact key; that is; the initial conditions of the two chaotic maps used in the index selection process. Moreover, the preliminary results ensure that eavesdroppers will not have any suspicion that there is a message hidden within the sent image since the peak signal to noise ratio (PSNR) is high and the mean-squared-error (MSE) is low. Furthermore, the length of the secret message is another important component of the key, which standard steganography detection methods cannot estimate correctly. Finally, the proposed approach provides better PSNR values and MSE values compared to other existing techniques as apparent from our experimental results.

General Terms

Steganography, Data hiding

Keywords

Chaotic Maps, Cover image, Histogram, LSB method, PSNR, Stego-image, Embedding Capacity

1. INTRODUCTION

Hiding the presence of a secret message in a letter has always been an attractive means for communicating top confidential messages. The use of invisible ink played an important role in World War II. The scientific term for concealing the fact that a secret message is being sent is ”steganography”. Cryptography refers to the practice of concealing the contents of a message during its transmission by making it unreadable except to its intended recipient. Clearly, steganography is advantageous over cryptography since, in addition to hiding the message contents, it conceives eavesdroppers who can no longer detect that critical data is being sent. In steganography, a secret message is embedded in a medium called cover or stego object in such a way that existence of the message is concealed. The cover object could be a digital image, an audio file, or a video file. The hidden message called payload could be a plaintext, an audio file, a video file, or an image.

Early attempts for hiding a text message involved capitalizing the letters of the secret message within the cover message, but later on images have attracted the attention of many researchers as a suitable cover medium. This is because the eye is insensitive to slight variations in an image.

In this paper, a new technique for hiding a text message in a cover image is proposed. The scheme involves the use of a secret key and thus it combines the advantages of both steganography and cryptography. Even if the eavesdropper detects the presence of a hidden message, he cannot predict the key used in the embedding process making the proposed scheme secure.

The rest of the paper is organized as follows. In the following section, related work on steganography techniques employing images as a cover medium is reviewed. The least significant bit method and chaotic maps are defined in Section 3. In Section 4, evaluation techniques used to test the proposed system are described. Our text hiding scheme is introduced in Section 5 and the experimental results used to illustrate and evaluate the performance of our approach are presented in Section 6. In particular, the security of the proposed scheme is analyzed by the use of several well-known metrics. A comparative study between the proposed scheme and other schemes in literature is presented in Section 7. Finally, Section 8 concludes the paper.

2. RELATED WORK

Much attention has been lately devoted to developing efficient and highly secure steganographic schemes. Steganography techniques are classified into four major categories. *Substitution system techniques* are techniques in which redundant bits of a cover image are replaced with the bits from the secret message (spatial domain); for example, Least Significant Bit (LSB) and palette-based techniques. *Transform domain techniques* hide secret data in the "transform space" of a signal (frequency domain), e.g. Discrete Cosine Transform (DCT) and Wavelet Transform (WT). *Statistical techniques* encode information by changing statistical properties of the cover image and hypothesis testing is used in the recovery process; e.g. Pseudo-random Permutations (PP) and Patchwork (PW) techniques. *Spread spectrum techniques* divide the stream of information to be transmitted into small pieces and adopt ideas from spread spectrum communication.
Our proposed technique is classified as a substitution technique and it represents an improved version of the LSB method.

Recently, several schemes in steganography are based on embedding the secret data in least significant bits of a pixel value. In [1], a novel data hiding technique is proposed based on the decomposition of a pixel-value as a sum of prime numbers. In [2], an improved adaptive LSB scheme is presented achieving high capacity for hiding a secret message. It shuffle bits-order of the message based on a chaotic map, whose parameters are selected by a genetic algorithm to minimize visual degradation of the stego or cover image. A novel hiding method based on four-pixel differencing and modified least significant bit (LSB) substitution is presented in [3]. The average difference value of a four-pixel block is exploited to classify the block as a smooth area or an edge area. Secret data are hidden into each pixel by the k-bit modified LSB substitution method, where k is decided by the level which the average difference value falls into. This method improved the embedding capacity and provided an imperceptible visual quality.

In [4], a method is proposed for image steganography in which a 1-D chaotic logistic map is used to generate pseudo random numbers, which are sorted and then they are used as positions to embed the message in the cover image. Moreover, authors of [5] proposed a method based on the use of chaotic maps to ensure security in the embedding phase to generate sequence of random numbers by dividing the image into blocks of (3×3).Also authors of [6] proposed an algorithm 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 chaotic maps engaged in proposed algorithm define the exact positions in upper and lower part for embedding of information bits. In [7] a new robust chaotic algorithm for digital image steganography based on a 3- dimensional chaotic cat map and lifted discrete wavelet transforms. The irregular outputs of the cat map are used to embed a secret message in a digital cover image. Discrete wavelet transforms are used to provide robustness.

In [8] a steganographic spatial domain algorithm was proposed based on single chaotic map to determine the pixel position of the host color image, the channel (red, green or blue) and the bit position of the targeted value in which a sensitive information bit can be hidden. While [9] presented an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images by detecting edges in the cover-image using improved edge detection filter. Message bits are then,

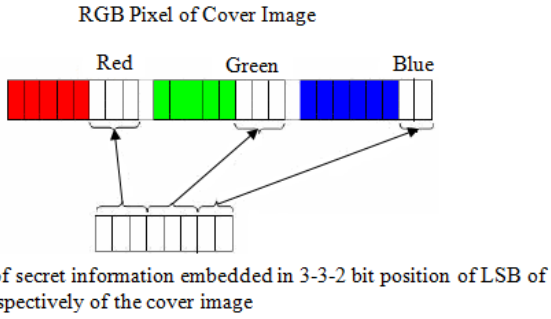

Fig. 1. Base embedding technique showing 1 byte of secret data embedded inside LSB bits in 3, 3, 2 order into corresponding RGB pixels of carrier image [10]

embedded in the least significant byte of randomly selected edge area pixels and 1-3-4 LSBs of red, green, blue component. In [10] a 3-3-2 LSB insertion method has been used for image steganography

3. BASIC TOOLS

In this section, some important definitions are provided which are essential to the development of the proposed scheme. First, least significant bit embedding method is illustrated, and then chaotic maps are described.

3.1 Least Significant Bit Method

LSB method is the most popular technique in steganography. It uses an RGB image as a carrier medium. In this technique, the LSBs of each pixel in the cover medium are replaced with the binary equivalent of the message that is to be hidden.

A recent variant of the basic LSB method, 3-3-2 LSB insertion technique, has been proposed in [10]. In this technique, eight bits of secret data are considered for embedding at a time in the LSBs of the RGB pixel values of the carrier image. The first three bits of the secret message are concealed inside the three LSBs of the red pixel value, and the next three bits in the three LSBs of the green pixel value. The remaining two bits of the secret message byte are concealed in the two LSBs of the blue pixel value.

The detailed technique has been depicted in Figure 1 . This particular distribution among the three color channels is taken considering that the chromatic influence of the blue channel to the human eye is more than that of the red and green channels [11].

3.2 Chaos and its Application in Information Hiding

Chaos is a phenomenon related to non-linear dynamical systems. Chaotic systems are sensitive to changes in initial conditions or parameters, an effect which is commonly referred to the butterfly effect. In fact, small differences in initial conditions provide extreme changes on final results. Recently, chaotic maps are employed in information hiding to increase security. Many approaches have worked to exploit the characteristics of chaotic systems to scramble their domain of insertion.

Chaotic maps can be applied to choose pixels or blocks that should be modified according to the method of insertion. There are many maps that can exhibit chaotic behaviors such as the Tent map, the Gauss map, the Logistic map, etc [12].

The logistic map is one of the simplest forms of a chaotic process. This map, like any one dimensional map, is a rule for extracting numbers from a recursive relation. It is defined by:

$$X_{i+1} = r[(X_i)(1 - X_i)] \quad (1)$$

where $0 \leq r \leq 4, X_i \in (0, 1)$

Researches on chaotic dynamical systems show that the logistic map is in chaotic state when $3.5699456 < r < 4$; that is, the sequence $X_1, X_2, X_3, ...$ generated by the logistic map is non-periodic and non-convergent. All the sequences generated by the logistic map are very sensitive to initial conditions, in the sense that two logistic sequences generated from different initial conditions are uncorrelated statistically. In our algorithm to be described below, the logistic map is used to generate the sequence of locations of pixels where the secret message bytes should be embedded.

4. PERFORMANCE EVALUATION OF A HIDING TECHNIQUE

Measures for compare the stego image with the original cover image are essential to evaluate the quality of the stego image and thus the quality of the hiding technique. Commonly used measures are the Mean-Squared Error (MSE), the Peak Signal-to-Noise Ratio (PSNR), and histogram analysis. Moreover, the capacity of the hiding technique is an important performance metric [13].

4.1 Mean-Squared Error

The mean-squared error (MSE) between two images $I_1(i, j)$ and $I_2(i, j)$ - cover image and stego image - respectively, is:

$$MSE = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I_1(i, j) - I_2(i, j)]^2}{M \times N} \quad (2)$$

where M and N are the number of rows and columns of the cover image.

4.2 Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) measures the distortion in the stego-image. In fact, the PSNR measures the deviation between the stego-image and the cover image and it is expressed in terms of the logarithmic decibel (dB) as:

$$PSNR = 10 \quad log_{10} \frac{MAX^2}{MSE} \quad (3)$$

Where MAX is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Typical values for the PSNR in lossy image and video compression are between 30 and 60 dB, where higher is better. If the PSNR ratio is high then images are best of quality

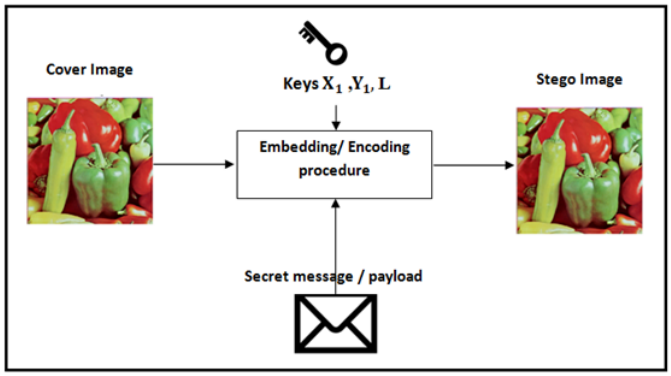

Fig. 2. The block diagram of the encoding process

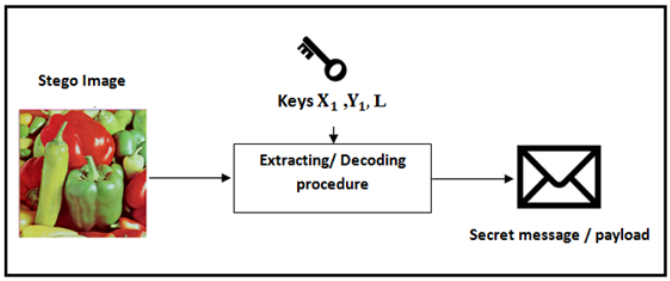

Fig. 3. The block diagram of the decoding process

4.3 Histogram analysis

Histogram is the graphical representation of the distribution of pixel values. It gives the variation in the number of pixels with respect to the color intensities of the image. Both the stego-image and the cover image should possess quite similar histograms for the hiding technique to be considered as successful.

4.4 Embedding Capacity

The steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. The capacity of an embedding technique is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. Therefore, capacity depends on the total number of bits per pixel and the number of bits embedded in each pixel.

The capacity ratio percentage equals =

$$\frac{\text{Number of embedded characters (bytes)}}{\text{Total number of bytes per color channel}} \times 100\% \quad (4)$$

5. THE PROPOSED TEXT HIDING SCHEME

The proposed scheme for both encoding and decoding a secret textual message are given in this section. In Figure 2 and Figure 3, the block diagrams for the encoding process and the decoding process are illustrated, respectively.

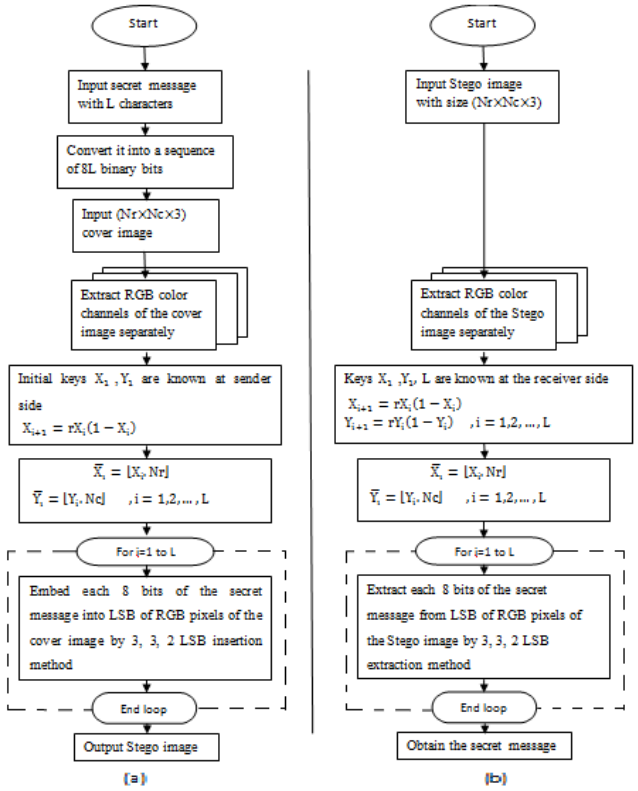

Fig. 4. Scheme flowchart (a) Encoding process and (b) Decoding process

5.1 Embedding/Encoding Scheme

As illustrated in Figure 4 -(a), the encoding steps are summarized below.

(1) Input secret message with L characters and convert it into a sequence of 8L binary bits.
(2) Input color RGB cover image $(Nr \times Nc \times 3)$
(3) Extract RGB color channels of the cover image separately.
(4) Generate replacement indices where the secret message bits are embedded in the cover image by using two chaotic maps; one for specifying the row number and the other for the column number. These two functions are called horizontal and vertical chaotic maps, respectively.

$$X_{i+1} = r[X_i(1 - X_i)] \quad (5)$$

$$Y_{i+1} = r[Y_i(1 - Y_i)] \quad (6)$$

where $i = 1, 2, ..., L$ and $X_1, Y_1, X_2, Y_2, ..., X_L, Y_L$ are sequences that will range between [0,1].

(5) Update the horizontal and vertical chaotic sequences range to match the number of rows N_r and the number of columns N_c of the cover image by using the following two formulas:

$$\bar{X}_i = \lfloor X_i \times N_r \rfloor \quad (7)$$

$$\bar{Y}_i = \lfloor Y_i \times N_c \rfloor \quad (8)$$

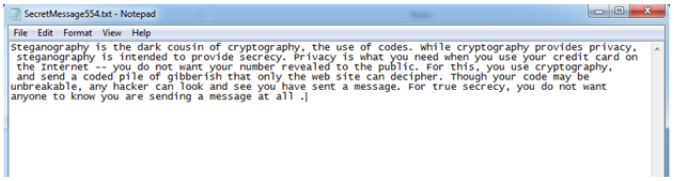

Fig. 5. The embedded secret message file

Table 1. MSE and PSNR values of some 512×512 cover image with 1 KB message file.

Image Name	MSE			PSNR		
	R	G	B	R	G	B
Baboon (4.2.03)	0.0205	0.0247	0.0053	65.0108	64.1984	70.8673
Airplane (4.2.05)	0.0239	0.0248	0.0052	64.3442	64.1857	70.9553
pepper (4.2.07)	0.0220	0.0241	0.0055	64.7060	64.3104	70.7356

$\bar{X}_1, \bar{X}_2, ..., \bar{X}_L$ and $\bar{Y}_1, \bar{Y}_2, ..., \bar{Y}_L$ are integer sequences ranging between $[0, N_r]$, $[0, N_c]$ respectively

(6) Embed each 8 bits of the secret message into LSBs of RGB pixels of the cover image in the order 3, 3, 2 respectively in the row, column indices determined by $\bar{X}_i, \bar{Y}_i$ until all the bits of the secret message are embedded.
(7) Output stego image with the same size of cover image $(N_r \times N_c \times 3)$

5.2 Extraction / Decoding scheme

As illustrated in Figure 4 -(b), the decoding steps are given as follows.

(1) Input stego image with size $(N_r \times N_c \times 3)$
(2) Extract RGB color channels of the stego image separately.
(3) Generate the two chaotic sequences $X_1, X_2, ..., X_L$ and $Y_1, Y_2, ..., Y_L$ using Eq.(5) and Eq.(6), respectively.
(4) Compute $\bar{X}_1, \bar{X}_2, ..., \bar{X}_L$ and $\bar{Y}_1, \bar{Y}_2, ..., \bar{Y}_L$ replacement indices where the secret message bits are embedded in the cover image by using Eq. (7) and Eq. (8), respectively.
(5) Extract each 8 bits of the secret message from the LSBs of RGB pixels of the stego image in the order 3, 3, 2 respectively in the row, column indices generated by $\bar{X}_i, \bar{Y}_i$ until all the bits of the secret message are recovered.
(6) Restore the equivalent secret message.

6. EXPERIMENTAL RESULTS

All the work is implemented using MATLAB. Our MATLAB program is applied to $512 \times 512 \times 3$ standard images available from the USC-SIPI image database [14]. In order to evaluate the performance of the proposed scheme, our scheme has been tested on some standard images, e.g. Baboon (4.2.03) and Peppers (4.2.07) with the embedded secret message indicated in Figure 5. The secret message is read from a text file whose size is 1 K bytes. In our experiments, we set $r = 3.9999$, and the initial values for the horizontal and vertical maps are $X_1 = 0.5$ and $Y_1 = 0.4$, respectively. The quality of the proposed scheme is assessed based on different analysis techniques such as MSE, PSNR, histogram

Table 2. Space efficiency analysis for 512×512 "Baboon" Cover image.

Number of embedded bytes)	Text File Size	Capacity ratio	Capacity ratio percentage %	PSNR		
				R	G	B
554	1 KB	0.002113	0.2113	65.0108	64.2314	70.8705
1107	2 KB	0.0042	0.4223	61.7232	61.3582	67.7999
17 706	18 KB	0.0675	6.7543	50.1788	49.7516	56.0657
30 986	31 KB	0.1182	11.8202	47.8323	47.5636	53.8338
79 683	80 KB	0.3040	30.3967	44.2742	43.9863	50.3128
131 072	132 KB	0.5	50	42.2109	41.8028	48.1415
159 365	160 KB	0.6079	60.7929	39.2109	38.8028	46.1415

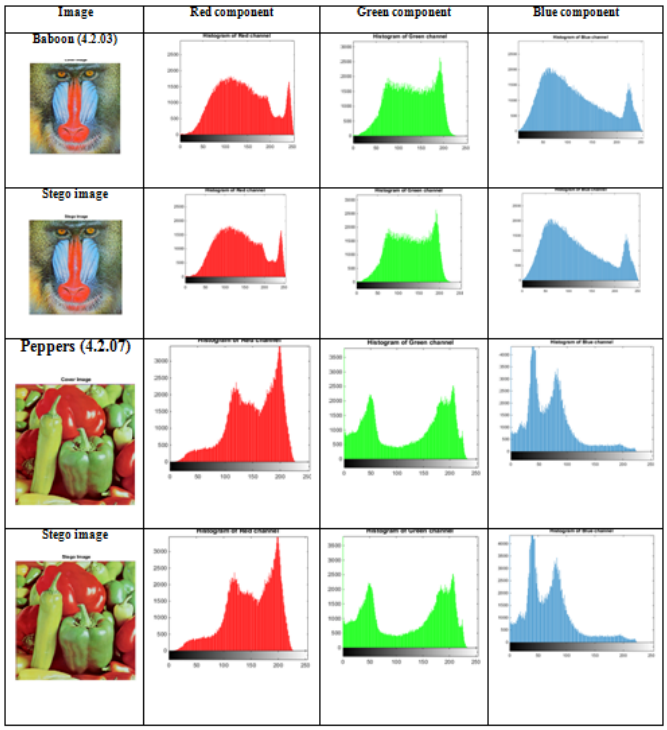

Fig. 6. Histogram analysis of cover image and stego image with 1 KB message file.

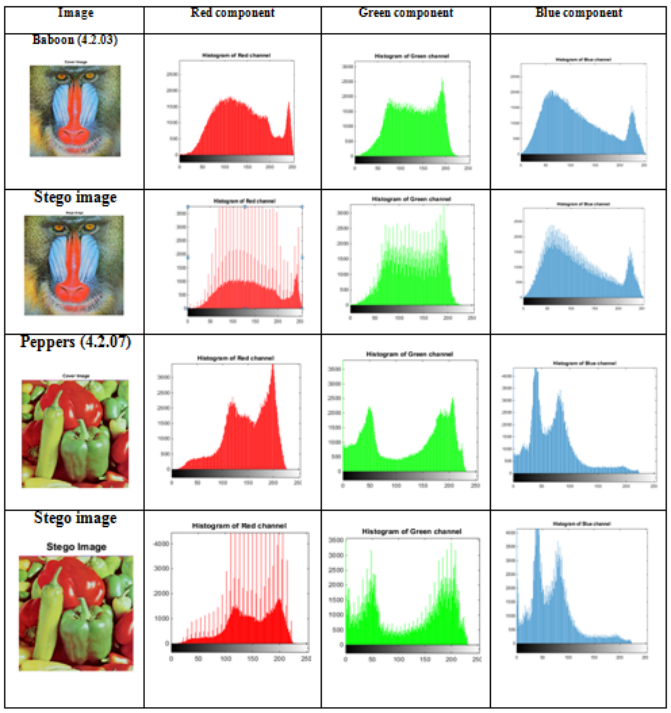

Fig. 7. Histogram analysis of cover image and stego image with 160 KB message file length (more than 50% embedding rate

analysis and capacity analysis.

It is clear from the above result figures that the proposed scheme successfully meets various requirements for hiding a text in a cover image as detailed in the following points.

(1) As apparent in Table 1, the mean square errors between the cover image and the stego image are too small values and less than values in other researches.

(2) In Table 1, PSNR (Peak Signal-to-Noise Ratio) values are reasonably high and may be better than other researches. If PSNR ratio is high, then images are best of quality.

(3) In Figure 6, the cover image and the stego photo are almost the same and therefore, the secret message is hidden in the cover image without any noticeable effect.

(4) In Figure 6, the histograms of the cover image and the stego-image are almost identical for the three color channels.

As shown in Table 2 the embedding capacity of the scheme is investigated. The amount of embedded text is increased until significant deterioration in the PSNR value is observed until reaching an embedding rate of 50% , the PSNR is within the acceptable range. Moreover, as clear from Figure 7, the image quality is still quite satisfactory.

In the proposed technique, the private key only known to the sender and the receiver consists of four components:

(1) The initial condition of the vertical chaotic sequence Y_1, whose value is in the unit interval.

(2) The initial condition of the horizontal chaotic sequence X_1, whose value is in the unit interval.

(3) The value of the parameter r in the definition of the logistic map, which should take values in the range $3.5699456 < r < 4$, so that the logistic map is non-periodic and non-convergent as desired.

(4) The length of the embedded secret message L, which should take on a value less than $(M \times N)/2$

Table 3. Comparison among the proposed scheme and other schemes in literature (average values) after using some 512×512 cover images, 1 KB message length.

	Average results mentioned					
	MSE			**PSNR**		
	R	**G**	**B**	**R**	**G**	**B**
This Work	0.0220	0.0241	0.0055	58.7060	58.3104	60.7356
[2]	-	-	-	38.521	39.72	39.93
[3]	-	-	-	44.58		
[4]	0.15	0.06	0.06	56.3392	60.3137	60.5805
[5]	-	-	-	52.8754		
[6]	0.0441	0.0108	0.0025	55.4126	55.4126	55.4126
[8]	-	-	-	45.04	46.46	47.74
[9]	-	-	-	45.9238		

It is thus a difficult task for the eavesdropper to guess all four components correctly, in addition to the fact that the message is perfectly hidden in the cover image without being noticeable.

7. COMPARISON BETWEEN THE PROPOSED SCHEME AND OTHER SCHEMES IN LITERATURE

In order to further assess the success of the proposed scheme, its performance is compared to several other schemes in literature. Table 3 shows the results obtained when the proposed technique is applied to pepper.jpg $(512 \times 512 \times 3)$ system and compares its performance with best results of other related recent schemes in literature, which are reviewed in Section 2 above. The comparison involves the mean square error (MSE) and the Peak Signal-to-Noise Ratio (PSNR). In this figure, if only one value of the PSNR is provided, this means that the research had been applied to a grey scale cover image. The obtained results show great potential of the proposed technique compared to other techniques.

8. CONCLUSION

In this paper, a new LSB technique based on 2-D chaotic maps for specifying the location to embed the message bits in the cover image is proposed. Message bits are embedded using 3-3-2 LSB insertion method. The use of chaotic maps enhances the security provided by the proposed scheme where even if the eavesdropper detected the presence of a hidden message, it does not have access to the private key required identifying the locations of the embedded secret message bits. The proposed technique has been applied and tested successfully on various images producing promising results. The proposed scheme provides desirable PSNR values and MSE values as shown experimentally and also provides high embedding capacity.

9. REFERENCES

[1] Dey, S., Abraham, A., Sanyal, S. (2007, August). An LSB data hiding technique using prime numbers. In Information Assurance and Security, 2007. IAS 2007. Third International Symposium on (pp. 101-108). IEEE.

[2] Yu, L., Zhao, Y., Ni, R., Li, T. (2010). Improved adaptive LSB steganography based on chaos and genetic algorithm. EURASIP Journal on Advances in Signal Processing, 2010, 32.

[3] Liao, X., Wen, Q. Y., Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. Journal of Visual Communication and Image Representation, 22(1), 1-8.

[4] Kumar, A., Kumari, S., Patro, S., Sh, T., Acharya, A. K. Image Steganography using Index based Chaotic Mapping., IJCA Proceedings on International Conference on Distributed Computing and Internet Technology, ICDCIT 2015(1):1-4, January 2015.

[5] Zaghbani, S., Rhouma, R. (2013, April). Data hiding in spatial domain image using chaotic map. In Modeling, Simulation and Applied Optimization (ICMSAO), 2013 5th International Conference on (pp. 1-5). IEEE.

[6] Anees, A., Siddiqui, A. M., Ahmed, J., Hussain, I. (2014). A technique for digital steganography using chaotic maps. Nonlinear Dynamics, 75(4), 807-816.

[7] Ghebleh, M., Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898-1907.

[8] Kanso, A. (2012). Steganographic algorithm based on a chaotic map. Communications in Nonlinear Science and Numerical Simulation, 17(8), 3287-3302.

[9] Juneja, M., Sandhu, P. S. (2013). An improved LSB based steganography technique for RGB color images. International Journal of Computer and Communication Engineering, 2(4), 513.

[10] Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., Dutta, P. (2014). A novel secure image steganography method based on Chaos theory in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1), 11-22.

[11] Dasgupta, K., Mandal, J. K., Dutta, P. (2012). Hash based least significant bit technique for video steganography (HLSB). International Journal of Security, Privacy and Trust Management (IJSPTM), 1(2), 1-11.

[12] Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), 727-752.

[13] Goel, S., Rana, A., Kaur, M. (2013). A review of comparison techniques of image steganography. Global Journal of Computer Science and Technology, 13(4).

[14] The USC-SIPI Image Database, University of Southern California, Signal and Image Processing Institute. Available at: http://sipi.usc.edu/database/, last accessed in November 2015.