Chaotic Map Based Random Image Steganography Using LSB Technique

Sujarani Rajendran[1], Manivannan Doraipandian[2]
(Corresponding author: Sujarani Rajendran)
Department of Computer Science & Engineering, SASTRA University[1]
Kumbakonam - 612001, Tamilnadu, India
(Email: rsujarani@src.sastra.edu)
School of Computing, SASTRA University[2]
Tirumalaisamudram Thanjavur-613401, Tamilnadu, India
(Received June 28, 2016; revised and accepted Sept. 3 & Sept. 25, 2016)

Abstract

Steganography play an important role to transfer secret data over insecure network. Moreover digital images are taken as a cover to communicate the sensitive data. One of the simplest approach of embedding the secret data into cover image is Least Significant Bit (LSB) method. This paper aims to propose a new symmetric key based image hiding technique. Pseudo random keys are generated by using 1D logistic map and those keys are used for choosing the pixel position of cover image randomly for hiding the secret image. The main security part of the projected method is the selection of pixel position in the cover image. Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measures are used for comparison and the result analysis shows that the proposed scheme provide efficient level of security.

Keywords: Chaos, image hiding, logistic map, steganography

1 Introduction

In today's communication technology images are playing a vital role in all fields such as military, social network, biometric system and so on. Sensitive images are transferred over insecure network, hiding those images from the intruders is an intellectual task. Steganography and cryptography are the two techniques which provide secure data communication. In cryptography secret images are converted into encrypted form and transferred over the networks. In steganography secret image are hidden in other multimedia carriers such as digital audio, video and images [7]. The encrypted form of images explicitly indicate that some sensitive images are transferred but in steganography secret images are hidden inside an another normal image so even attacker visualize the image he may not identify about the secret image. The traditional mechanism used for hiding the data is watermarking which embed the secret data into cover image [8], then the cover image is considered as stego-image. It act as medium to transfer the secret image over unsecure networks. Two different styles of using the cover image for hiding the secret images are spatial domain and frequency domain [1].

In spatial domain intensity values of cover image are used to hide the secret information [19, 20]. In frequency domain, the secret image pixels are hidden in transforming coefficients values of the pixels in cover image [18, 21]. Different methods of spatial domain steganography techniques has been proposed using Watermarking [9], Least Significant Bit (LSB) substitution [2], Modulus function [6], Pixel Value Differencing method [16, 23], LSB matching [11, 14] and optimal pixel adjustment process [3]. Among these LSB substitution based hiding is one of the simple, fast hiding technology and also it provide efficient security. The proposed scheme utilized the LSB substitution technique for hiding the secret image [5]. In LSB based embedding technique the set of LSB of pixels in cover image are substituted by the bits of secret image. This process can be done either in sequential or in random manner. Randomly chosen pixels for hiding in cover image provide better security than sequential manner [17]. In our proposed scheme cover image pixels are select randomly by using the chaotic sequence generated by the chaotic map.

Chaos means a state of disorder. In mathematics, map is an evolution function that shows some sort of chaotic behavior [10]. A discrete time dynamical system is also called map. chaotic map has some inherent features [13] such as: 1) sensitive to initial conditions (also called butterfly effect) which means a small modification in initial conditions should produce high deviations of the corresponding output. 2) Ergodicity implies the output has the same distribution for any input. 3) Deterministic means a deterministic process can cause a pseudo-random behav-

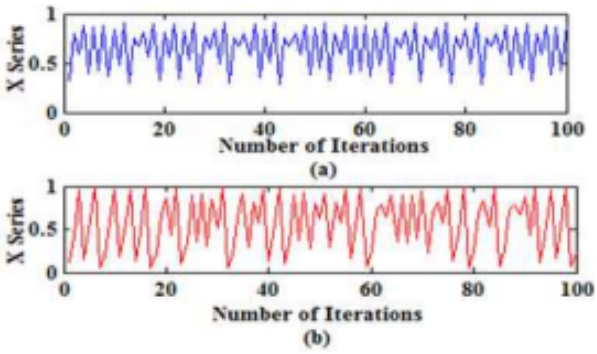

Figure 1: Randomness of 1D logistic map chaotic series (a) $\alpha = 3.95$ and $x_0 = 0.12$ $(b)\alpha = 3.85$ and $x_0 = 0.25$

ior. 4) Structure complexity signifies a simple mathematical function has very high complexity. Different types of information hiding scheme has been proposed used chaotic sequence [13]. In our proposed scheme we have used One Dimentional (1D) logistic map for generating the chaotic sequence, which is used for selecting the pixel values randomly for hiding in cover image.

The remaining section of the paper is structured as follows: brief description of one dimensional logistic map has discussed on Section 2. Embedding algorithm proposed for hiding the secret image has illuminated in Section 3. Experimental result and result analysis are discoursed in Section 4. Conclusion of the paper declared in Section 5.

2 One Dimentional Logistic Map

It is the simplest form of chaotic system, which is developed by May [15]. Logistic map is described in Equation (1).

$$X_n = \alpha_{X_n-1}(1-_{X_n-1}). \quad (1)$$

Here x_0 is initial value and n value denotes the number of rounds. 1D logistic map generate chaotic sequences only if the α value must be in the range of $3.5 \leq \alpha \leq 4$ [22]. It produce chaotic sequences within the range [0, 1]. Chaotic sequences generated by a map is greatly sensitive to initial values, a small variation in these parameters will affect the extraction of secret image from cover image, because by using these chaotic sequence only, the position of pixels in cover image are chosen for embedding the bits of secret image. For illustration, the plot diagram for the chaotic sequence generated by 1D logistic map by using the values $\alpha = 3.95$ and $x_0 = 0.12$ is given in Figure 1(a). Tiny changes in the initial parameters of 1D logistic map provide different chaotic sequence, we changed the value of α and x_0 as 3.97 and 0.15 and the plot diagram of the chaotic sequence of the changed values are given in Figure 1(b). From the figure it is clear that the tiny changes in the initial values will greatly affect the values of chaotic series.

3 Proposed Image Hiding Technique

The overall view of the proposed steganography technique is shown in Figure 2.

3.1 Embedding Process

Step by step procedure of the proposed steganography technique is illustrated below.

Step 1: Select the secret image S and cover image C, size of C must be double the size of S.

Step 2: Choose the initial value and system parameter value such as α and x_0 of 1D logistic map for generating the chaotic sequence.

$$X = \{x_1, x_2, x_3, \cdots, x_n\}$$

where n is the row or column size of cover image.

Step 3: Sort the generated chaotic sequence X as follows.

$$[sx_i, ax_i] = sort(X_i), i = 1, 2, 3, \cdots, N,$$

where sx is a new sorted sequence of X; ax is a new index value of the series X.

Step 4: Convert the secret image and cover image in binary format. Binary images are represented as S‘and C‘.

Step 5: The binary value of secret image S‘are divided into four separate two bits and each two bits are stored in separate two dimensional array S“which is equal to the size of the cover image.

Step 6: Algorithm for embedding process is described as follows:

S“ $(M \times N)$ - Two bits representation of secret image;
C‘$(M \times N)$- Eight bits representation of cover image, where M and N denotes rows and columns of the images.

For i = 1: M
  For j= 1: N
    C“$(M \times N)$ = Replaced 2-LSB of cover image C‘(M,ax_j) into S“(M,N)
  End
End

Step 7: Convert the binary format of cover image C“ into 8-bit grayscale pixel value then C“ is considered as stego-image.

Hence, secret image has embedded in to cover image and finally the stego-image is transferred to the receiver. Sender securely communicates the secret key and α value to the receiver.

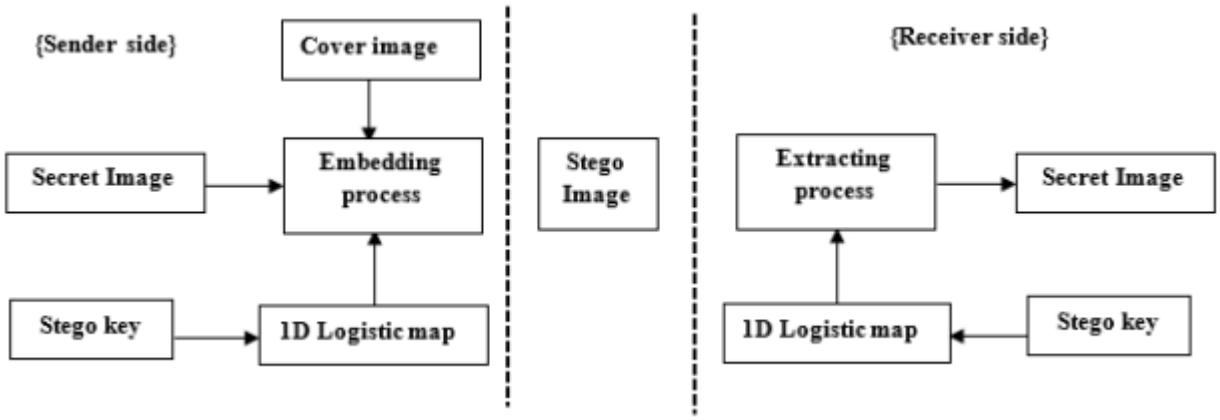

Figure 2: Overall block view of the proposed steganography algorithm

3.2 Extraction Process

Step 1: Generate the chaotic sequence using 1D logistic map and sort it by using the same procedure in embedding process. After sorting new index value (ax) is obtained, which is used for extracting the bits in random manner.

Step 2: Convert the 8-bit pixel value of stego-image C“ in to binary form C‘.

Step 3: Extraction of secret image from stego-image C‘($M \times N$) M and N are rows and columns of stego-image.

Step 4: Extracting bits from stego-image.

For i = 1: M
  For j= 1: N
    ES‘($M \times N$) = Extract 2 LSB from C‘(M,ax_i)
    //ES = Extracted Stego-Image
  End
End

Step 5: Combining the four separate 2 bits in S‘into 8-bit so ES‘($M \times N$) transferred in to ES“($I \times J$), where I = M/2 and J= N/2.

Step 6: Convert the 8-bit binary form Extracted secret image ES“into 8-bit pixel value and finally the secret image ES is extracted from the stego-image.

3.3 Experimental Result and Discussion

The proposed technique performance has evaluated by using different experiments. Four images with (256x256) size are used as cover images shown in Figure 3. The secret images has used for hiding of size (128x128) are shown in Figure 4. For implementation MATLAB (R2013a) has used on Windows 8. Secret image embedded on the LSB of pixels in cover image, selection of pixels for hiding in cover image has done by using the chaotic sequence generated by the 1D logistic map. Peak Signal to noise ratio (PSNR) and MSE are the standard measures for finding the difference between the original cover image and the stego-image. High PSNR value represents that the cover image has small distortion after embedding. Low PSNR value indicates poor visual quality of the cover image. PSNR is defined in the following Equation (2).

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

where $MSE = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{M} (C_{i,j} - S_{i,j})^2$; MSE stands for Mean Square Error; C represents the original cover image; S represents the Stego image.

Table 1 list the PSNR comparison of proposed technique with other proposed methods. For comparison Boat image has used as secret image and Table 2 shows the comparison of MSE with different proposed scheme, house image has taken as secret image for MSE comparison. Based on the result analysis given in Tables 1 and 2 the proposed technique has better visual quality and less distortion then other techniques.

Table 1: PSNR value of different cover images after hiding the Boat image

Cover image	Basic LSB Hiding	Method given in Ref [12]	PSO Method Ref [4]	Hide 4 MSB in Ref [4]	Proposed Method
Lena	35.40	35.84	36.29	38.98	44.53
Baboon	35.61	36.14	36.64	39.29	44.54
Airplane	35.70	36.08	36.41	39.19	44.42
Elaine	35.55	36.02	36.20	39.36	44.53

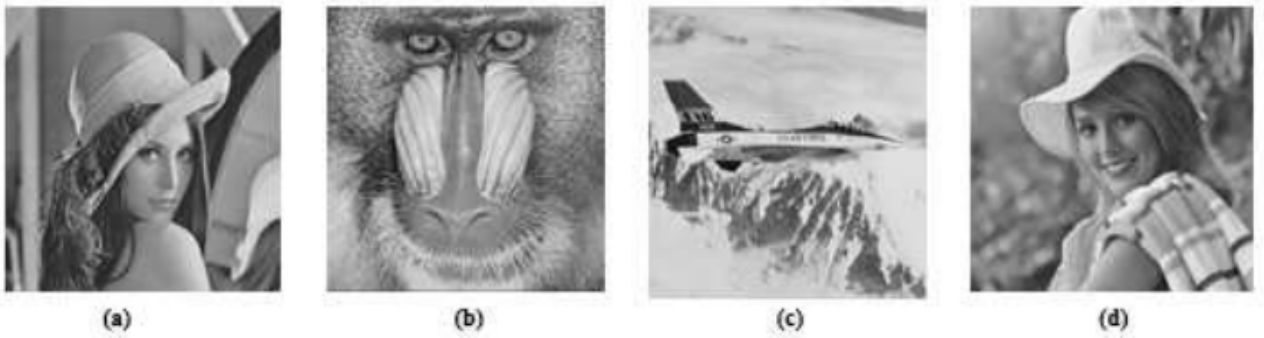

Figure 3: Standard 256 x 256 cover images (a) Lena (b) Baboon (c) airplane (d) Elaine

Figure 4: Standard 128 x 128 Secret images (a) Boat (b) House

Table 2: MSE value of different cover images after hiding the Boat image

Cover image	Basic LSB Hiding	Method given in Ref [12]	PSO Method Ref [4]	Hide 4 MSB in Ref [4]	Pro-posed Method
Lena	18.36	17.01	15.75	10.85	2.28
Baboon	17.51	15.89	14.59	9.68	2.28
Airplane	17.32	15.47	14.42	10.13	2.34
Elaine	17.55	16.09	15.73	9.78	2.28

Figure 5 Illustrates the graph format result of the PSNR and MSE comparison of different cover images and with different existing proposed techniques, it depicts that the proposed steganography technique has better visual quality than other proposed scheme.

3.4 Histogram Analysis

Histogram shows the exact occurrence of each pixels in the image. High similarity between the cover image histogram and stego image histogram shows that a tiny distortion occurred after embedding the secret image into cover image [22]. Figure 6(a) shows the histogram of cover image Lena and Figure 6(b) shows histogram after embedding the boat image into Lena image. As a result the proposed scheme fight against visual attack and statistical attack.

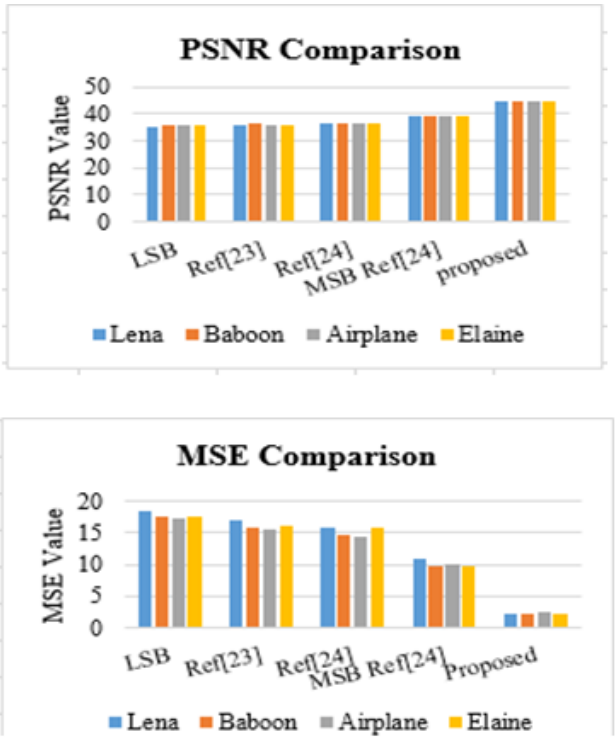

Figure 5: comparison chart (a) PSNR Values of Stego images(b) MSE values of Stego images

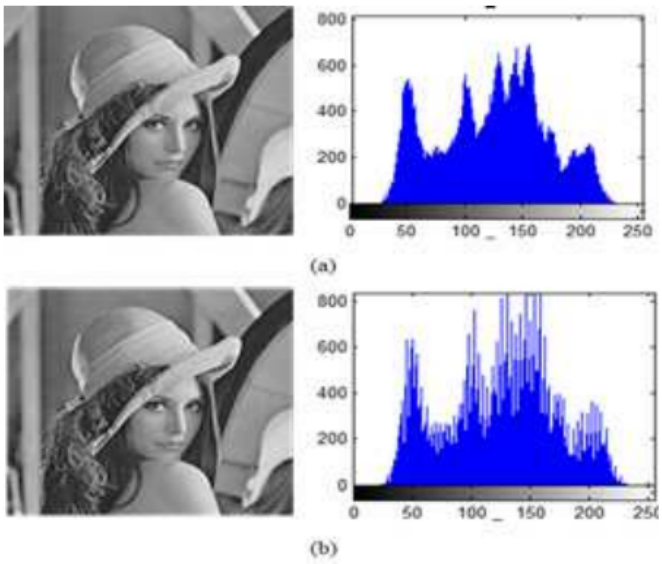

Figure 6: Histogram analysis (a) cover image (b) Stego image

4 Conclusion and Future Work

A new chaotic series based image hiding scheme has proposed by using 1D logistic map. Cover image pixel position has chosen randomly for embedding the secret image bits, so it minimize the security risk and increase the efficiency of the proposed algorithm. Four different grayscale images are used for testing to prove the performance, image quality and capacity of the proposed scheme. Comparison result proved that the proposed scheme provide better result than other steganography schemes.In future the proposed algorithm can also be used for securely transferring and storing the medical images.

References

[1] R. Amirtharajan and J. B. B. Rayappan, "An intelligent chaotic embedding approach to enhance stego-image quality," *Information Sciences*, vol. 193, pp. 115–124, 2012.

[2] R. Arnirtharajan, R. Subrahmanyam, J. N. Teja, K. M. Reddy, and J. B. B. Rayappan, "Pixel indicated triple layer: A way for random image steganography," *Research Journal of Information Technology*, vol. 5, no. 2, pp. 87–99, 2013.

[3] O. Banimelhem, M. Mowafi, M. Al-Batati, et al., "A more secure image hiding scheme using pixel adjustment and genetic algorithm," *International Journal of Information Security and Privacy*, vol. 7, no. 3, pp. 1–15, 2013.

[4] P. Bedi, R. Bansal, and P. Sehgal, "Using pso in image hiding scheme based on lsb substitution," in *International Conference on Advances in Computing and Communications*, pp. 259–268, 2011.

[5] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[6] C. S. Chan, C. C. Chang, and Yu-C. Hu, "Image hiding scheme using modulus function and optimal substitution table," *Pattern Recognition and Image Analysis*, vol. 16, no. 2, pp. 208–217, 2006.

[7] C. C. Chang, T. S. Nguyen, and C. C. Lin, "Reversible image hiding for high image quality based on histogram shifting and local complexity," *International Journal of Network Security*, vol. 16, no. 3, pp. 201–213, 2014.

[8] H. Chen, X. Du, Z. Liu, and C. Yang, "Optical color image hiding scheme by using gerchberg–saxton algorithm in fractional fourier domain," *Optics and Lasers in Engineering*, vol. 66, pp. 144–151, 2015.

[9] D. Essaidani, H. Seddik, and E. B. Braiek, "Asynchronous invariant digital image watermarking in radon field for resistant encrypted watermark," *International Journal of Network Security*, vol. 18, no. 1, pp. 19–32, 2016.

[10] M. François, T. Grosges, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 887–895, 2014.

[11] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.

[12] M. Khodaei and K. Faez, "Image hiding by using genetic algorithm and lsb substitution," in *International Conference on Image and Signal Processing*, pp. 404–411, Springer, 2010.

[13] Z. Liu and L. Xi, "Image information hiding encryption using chaotic sequence," in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*, pp. 202–208, Springer, 2007.

[14] T. C. Lu, C. Ya Tseng, and J. H. Wu, "Dual imaging-based reversible hiding technique using lsb matching," *Signal Processing*, vol. 108, pp. 77–89, 2015.

[15] R. M. May, et al., "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[16] S. Manoharan, D. RajKumar, "Pixel value differencing method based on CMYK colour model," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 37–46, 2016.

[17] A. N. Pisarchik and M. Zanin, "Chaotic map cryptography and security," *International Journal of Computer Research*, vol. 19, no. 1, p. 49, 2012.

[18] S. A. Seyyedi, V. Sadau, and N. Ivanov, "A secure steganography method based on integer lifting wavelet transform," *International Journal of Network Security*, vol. 18, no. 1, pp. 124–132, 2016.

[19] Y. Yu Tsai, J. T. Chen, and C. S. Chan, "Exploring lsb substitution and pixel-value differencing

for block-based adaptive data hiding.," *International Journal of Network Security*, vol. 16, no. 5, pp. 363–368, 2014.

[20] S. M. C. Vigila and K. Muneeswaran, "Hiding of confidential data in spatial domain images using image interpolation," *International Journal of Network Security*, vol. 17, no. 6, pp. 722–727, 2015.

[21] O. Wahballa, A. Wahaballa, F. Li, and C. Xu, "A secure and robust certificateless public key steganography based on svd-ddwt," *International Journal of Network Security*, vol. 18, no. 5, pp. 888–899, 2016.

[22] X. Wang, J. Zhao, and H. Liu, "A new image encryption algorithm based on chaos," *Optics Communications*, vol. 285, no. 5, pp. 562–566, 2012.

[23] Da-C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613–1626, 2003.

Biography

Sujarani Rajendran received her M.Tech (Computer science and engineering) in 2010, from SASTRA University, Thanjavur. She is currently working as an Assistant Professor in the Department of CSE in SASTRA University, kumbakonam. She is currently working towards her Ph.D. Degree in SASTRA University. Her research area includes Chaotic Cryptography, DNA Cryptography and Steganography.

Manivannan Doraipandian obtained M.Tech and Ph.D. degree in Computer Science from SASTRA University, Thanjavur, India in 2002 and 2013, respectively. He is currently working as Senior Assistant Professor in the department of School of Computing, SASTRA University. His current research interests includes cryptography, Security in Embedded Systems, Wireless Sensor Networks using reconfigurable processors and Embedded Communication Systems.