Image Steganography using Index based Chaotic Mapping

Shreenandan Kumar, Suman Kumari, Sucheta Patro,
Tushar Shandilya, Anuja Kumar Acharya
School of Computer Engineering
KIIT University, Bhubaneswar, India

ABSTRACT
There have been many techniques for hiding messages in images in such a manner that the alterations made to the image are perceptually indiscernible. The Least-significant bit (LSB)-based approach is the most popular type of steganographic algorithm. However, we find that in most existing approaches the choice of embedding positions within the cover image are not secure enough. In this paper, we have used 1D chaotic logistic map to generate the pseudo random numbers; the index values of the sorted pseudo random numbers are the positions used to embed the message in the cover image. This technique provides sufficient security as the same set of numbers cannot be generated without knowing the exact key and thus the message is more secure. The proposed technique has been applied and tested successfully on various images producing significant results.

Keywords
Steganography; chaotic map; logistic map; LSB technique.

1. INTRODUCTION
Recently, due to growing internet technologies, there has been a lot of research in the field of data hiding and data security while transmitting the confidential data. The main features of a steganographic system are to get high load capacity and decrease the amount of noise in network/channel. Due to the conflicting behavior of these features, it is not easy to get them at the same time. So, most of the techniques mainly work on improving the space efficiency and stego quality.

The conventional method used for steganography is the LSB technique where each message bit is embedded in the least significant bit of each pixel of the cover image [1], [2].These methods possesses high hiding capacity and imperceptibility but these are not secure to the attacks made to extract the message as the embedding positions are known. The methods proposed by Ali Daneshkhah [3] and Wang [4] along with some other techniques proposed [5], [6] has shown variation in the embedding positions to overcome this attack.

Here in this paper a new technique has been applied to increase the hiding capacity and security of the embedding positions. This algorithm has been put forward for LSB based image steganography in which the last bits of the cover image are replaced by the bits of the message image which is encrypted using Index based 1D logistic chaotic map [7].

Pseudo random numbers are generated using the 1D logistic map which are sorted and their index value is used as the key. The decryption of message image is impossible without the correct key. This increases the security of the whole steganography system. This proposed model has been applied for image messages and texts messages showing better imperceptibility.

The rest of the paper is organized as follows. In Section 2, the proposed steganography system is described. The simulation results are shown in Section 3 and Section 4 includes summary and conclusion for the proposed model.

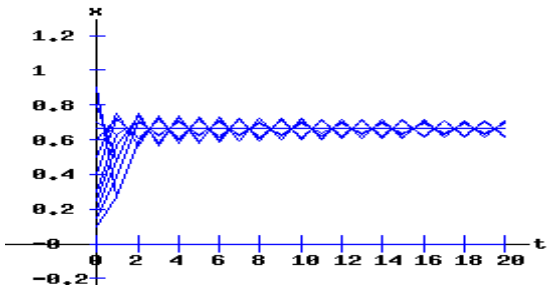
2. PROPOSED MODEL
2.1 Generation of Pseudo Random Numbers
Keeping security of the data as the main focus, chaotic map has been used in the proposed model. These are highly sensitive to the initial conditions.

This paper has focused on 1D logistic mapping which is shown in equation (1).

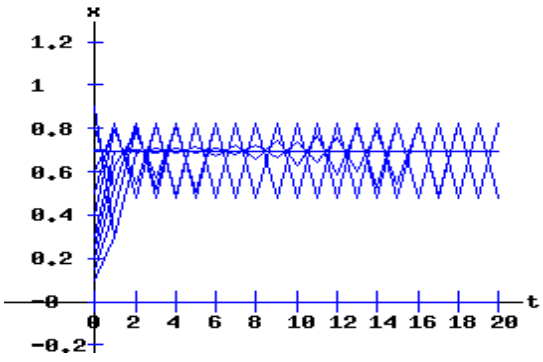
$$X_{n+1} = rX_n(1 - X_n) \quad (1)$$

Here X_n is the initial value and will be between (0, 1). The equation is very sensitive to small change in the value of r (seed value) and the initial parameter X_n.

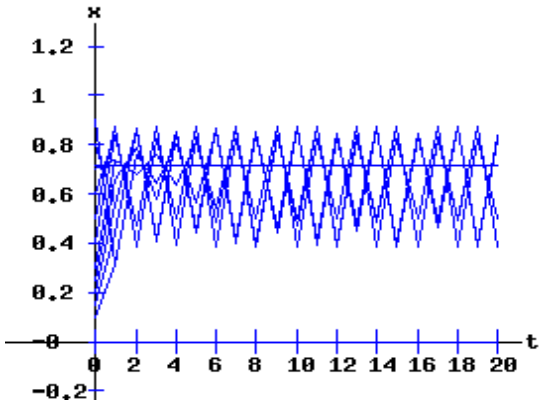
The behavior of signal is completely chaotic (Figure 1.c) for the value of r in the range [3.56, 4] as compared to values outside the range and also there will be fewer tendencies for cyclic randomness.



(a)



(b)



(c)

Figure 1.chaotic behavior at X_n=0.6 and (a)At r=3 (b) At r=3.3 (c) At r=3.6

Now, to determine the locations for embedding the secret message, the following steps were used:

Step 1. Using the X_n(Key) as the initial value for the equation (1) and r=3.6, we get a 1-D chaotic sequence of pseudo random numbers

R=0.2000, 0.5760, 0.3823, 0.5547,…, $M_1 \times N_1$

With the length of $M_1 \times N_1$(total number of pixels in cover image)

Step 2. The chaotic sequence is now sorted in ascending order and the corresponding index value in stored

R=0.2000, 0.3823, 0.5547, 0.5760,…, $M_1 \times N_1$

Index=1, 3, 4, 2,…, $M_1 \times N_1$

Step 3. Now the index values are used as the positions to embed the secret message.

2.2 Encoding

The color cover image (.jpg) $M_1 \times N_1$ should be greater than the size of image $M_2 \times N_2$ to be hidden.

Hide image,

$$\begin{matrix} 210 & 160 \dots \dots & 255 \\ 100 & 240 \dots \dots & 150 \\ \vdots & \vdots & \vdots \\ 230 & 180 \dots \dots & 200 \end{matrix}$$

Cover image,

$$\begin{matrix} 215 & 60 \dots \dots & 215 \\ 130 & 200 \dots \dots & 165 \\ \vdots & \vdots & \vdots \\ 220 & 230 \dots \dots & 170 \end{matrix}$$

(a)

For each pixel of hidden image 8 bit binary value is found,

$$(210)_{10} = (11010010)_2$$

Using the LSB substitution technique each bit is embedded into the pixels of R, G, and B planes of cover image corresponding to the index values generated. After all the bits are embedded, a stego image is formed.

Stego image,

$$\begin{matrix} 216 & 61 \dots \dots & 215 \\ 130 & 201 \dots \dots & 166 \\ \vdots & \vdots & \vdots \\ 219 & 231 \dots \dots & 169 \end{matrix}$$

Algorithm

Step 1. For the hidden image of dimension $M_2 \times N_2$, cover image (.jpg) greater than hidden image is taken.

Step 2. Each pixel of hidden image is converted into corresponding 8 bit binary values and a large sequence of binary stream of length $M_2 \times N_2 \times 8$ is obtained.

Step 3. Using the LSB substitution technique, for each byte of binary stream obtained from the hidden image, 4 bits are encoded in R plane, 2 bits are encoded in G plane and the last 2 bits are encoded in B plane of the cover image corresponding to the index value.

Step 4. After all the bits are embedded, the stego image is formed.

2.3 Decoding

Using the correct key, the hidden image can be decoded using the following algorithm.

Algorithm

Step 1: The reverse of **step 3** in encoding is done on the stego image and the large sequence of the binary stream is obtained.

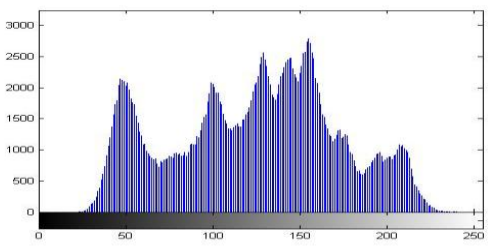
Step 2: Each byte is now converted to the corresponding unit8 pixel values and an image matrix of dimension $M_2 \times N_2$ is formed which is nothing but the hidden image.

3. EXPERIMENTAL RESULTS AND ANALYSIS

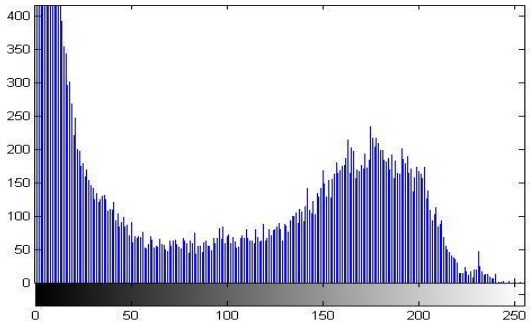
The proposed method has been applied on a number of cover images with different hidden images and excellent results are obtained.

3.1 Histogram Analysis

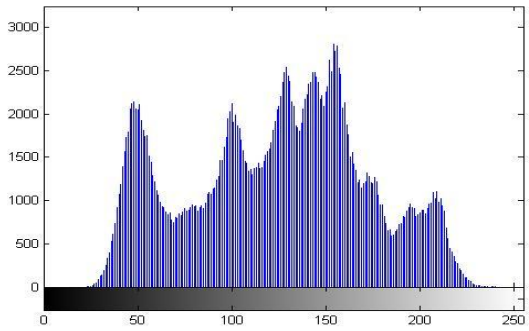
Figure 2.a shows the standard Lena image which is used as the cover image and figure 2.b is its histogram, figure 2.c is the hidden image and figure 2.d is its histogram, figure 2.e is the stego image and figure 2.f is its histogram. The histogram of hidden image is uniform as compared to the cover image. So any statistical attack is unlikely in the proposed technique.



(b)



(c) **(d)**



(e) **(f)**

Figure 2. Experimental Results (a) Cover Image (b) Histogram of Cover Image (c) Hidden Image (d) Histogram of Hidden Image (e) Stego Image (f) Histogram of stego Image

3.2 PSNR

The PSNR [8] is used as the scale for image quality (which computes the peak signal-to-noise ratio) between the original image and stego image. The mathematical representation is as follows (equation 2).

$$PSNR = 10log_{10}\left(\frac{P^2}{MSE}\right) \quad (2)$$

Where p is the maximum pixel value.

Also, the MSE is,

$$MSE = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M\times N} \quad (3)$$

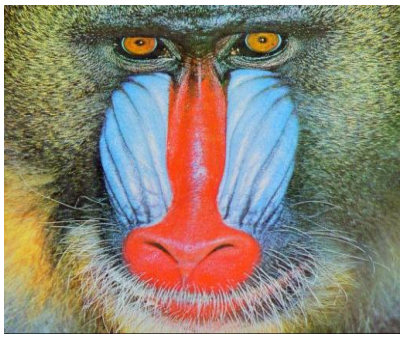
The PSNR is defined using the MSE [8] which is the mean squared error between the Stego Image I1 and the cover image I2, shown in equation (3).

Table 1 is the experimental analysis of the different cover images (.jpg) which were used, shown in figure 3.

Larger PSNR values imply better quality of the stego image.

PSNR values in earlier proposed model [9] is much less as compared to the PSNR values obtained in this proposed model which implies this model has better stego image quality. Thus, the imperceptibility is higher.

The experimental result of the figure 2.a gives an efficient result with the PSNR value of 56.2965, 60.2245, and 60.4429 of R, G, and B planes respectively.



(a) **(b)** **(c)**

Figure 3. Cover Images (a) Lena (b) Baboon (c) Peppers

Table 1. PSNR value Analysis

Image Name	Size	MSE			PSNR		
		R	G	B	R	G	B
Lena.jpg	512×512	0.15	0.06	0.06	56.2965	60.2245	60.4429
Baboon.jpg	512×512	0.15	0.06	0.06	56.3087	60.1871	60.4534
Peppers.jpg	512×512	0.15	0.06	0.06	56.3392	60.3137	60.5805

3.3 Space Efficiency

For the hidden image of order M×N, cover image (.jpg) of at least 3M×N is required.

4. CONCLUSION

This paper has demonstrated a new approach for LSB based Image steganography. As the index based 1D logistic mapping method has been used, it is found to be more effective. The method was applied to various standard test images in MATLAB and the results thus obtained shows efficient experimental values (Histogram and PSNR) which ensure better security. Further, this method can be used for video as well as audio steganography as the hiding capacity and the imperceptibility is better.

5. REFERENCES

[1] A. Tirkel , R. Schyndel and C. Os born, "A digital watermark", in Proc. IEEE Int. Conf. Image Processing. 1994, vol. 2, pp. 86-90.

[2] R. Wolfgang and E. Delp, "A watermark for digital image", in Proc. IEEE Int. Conf. Image Processing, 1996, vol. 3, pp. 219-222.

[3] A. Daneshkhah, H. Aghaeinia, and S. H. Seyedi, "A more secure steganography method in spatial Domain," in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, pp. 189–194, IEEE, 2011.

[4] R.-Z.Wang, C.-F.Lin, and J.-C.Lin, "Image hiding by optimal lsb substitution and genetical algorithm," Pattern recognition, vol. 34, no. 3, pp. 671–683, 2001.

[5] R. Mersereau and F. Alturki, "Secure Blind Image Steganographic Technique Using Discrete Fourier Transformation", in Proc.IEEE Int. Conf. on Image Processing, vol. 2,2001, pp. 542-545.

[6] W.Sweldens y B. Yeo ,A. R. Calderbank, I. Daubechies, "Lossless ImageCompression Using Integer to Integer Wavelet Transforms", Proc. of Int. Conf. on Image Proc, 1997, pp. 596-599.

[7] Anuja Kumar Acharya, 2011. Image encryption using new chaos based encryption algorithm. In International Conference on Communication, Computing & Security (ICCCS).

[8] D. N. Naitik P Kamdar, Dipesh G. Kamdar, "Performance evaluation of lsb based steganography for Optimization of psnr and mse," Journal of information, knowledge and research in electronics and Communication engineering, vol. 2, no. 2, pp. 505–509.

[9] N. S. Raghava1, Ashish Kumar, Aishwarya Deep and Abhilasha Chahal, "Improved LSB method for Image Steganography using H´enon Chaotic Map", open journal of information security and applications volume 1, number 1, june 2014.