Scientific Online

OPEN JOURNAL OF INFORMATION SECURITY AND APPLICATIONS
VOLUME 1, NUMBER 1, JUNE 2014

OPEN JOURNAL OF INFORMATION SECURITY AND APPLICATIONS

Improved LSB method for Image Steganography using Hénon Chaotic Map

N. S. Raghava[1]*, Ashish Kumar[1], Aishwarya Deep[2] and AbhilashaChahal[1]

[1] *Department of Information Technology, Delhi Technological University, Delhi.*

[2] *Department of Computer Engineering, Delhi Technological University, Delhi.*

***Corresponding author**: nsraghava@gmail.com

Abstract:

Image steganography conceals secret information in a cover image .It is used for secure data transfer. Various LSB (least significant bits) approaches have been used over the years in steganography. This paper proposes a novel technique to improve the conventional LSB technique for image steganography by using pseudo random number generation using Hénon chaotic map. The random numbers are used to encrypt the hide image which is embedded in the cover picture. This encryption using pseudo random generator provides sufficient security to the payload as the same set of random numbers cannot be regenerated without knowing the exact random generator function and thus the secret data cannot be retrieved easily. The proposed technique has been tested successfully on various .jpg files and corresponding PSNR values have been calculated.

Keywords:

Hénon chaotic map; Information hiding LSB modification; PSNR (peak signal to noise ratio); Steganography

1. INTRODUCTION

Communication is an important aspect in today's world. Information is transmitted through different data channels for communication and it suffers from serious security problem. Protection of important information during transmission becomes an important issue and is therefore concealed by encryption. Encryption [1] is the art of writing in cipher which is not intelligible to the person who does not have the key to decipher it. The two kinds of encryption are cryptography and steganography. Steganography is a Greek word which means covered writing. It is a technique of hiding secret information in the cover image and the extraction of it at its destination. Steganography [2] takes cryptography a step further by hiding an encrypted message so that no one suspects it exists. In cryptography, the text is random streams of data which makes it vulnerable to the intruder whereas in steganography, the secret information is hidden thus the intruder is unaware of the fact that some information is concealed in it, thus making it more secure.

Steganography has three parts-the hidden information, the cover image and the key. The hidden information is embedded in the cover image in such a way that no outsider can decode it and only the party having the valid key for deciphering it can retrieve the hidden information from it. Various forms of

(a) (b) (c)

Figure 1. (a) Hide Image (b) Original cover image (c) stego image

data like audio, video file, image, and text can be encoded using steganography

An example shown in **Figure 1** illustrates the concept of steganography. The secret image shown in **Figure 1(a)** is hidden in the cover image shown in **Figure 1(b)** to produce a stegnographic image as shown in **Figure 1(c)**.

In this paper, a new efficient algorithm has been proposed for LSB based image steganography in which the last four bits of the cover image are replaced by the hide image which is encrypted using Hénon chaotic map [3] encryption technique. This algorithm uses pseudo random numbers [4] generated using Hénon map for one time padding [5] of the hide image. Two dimensional nonlinear dynamical Hénon map generates a pseudo-random binary sequence. It is used as a symmetric key stream cipher cryptographic system. The encryption was done using Hénon map, results in one time padding. One time padding (OTP) is used, as it makes the decryption of the image impossible without knowing the key as image is encrypted by the modular addition with a secret random key.

The LSB technique [6] proposed in this paper has a better space efficiency as compared to the steganographic algorithms proposed earlier as the minimum size of the cover image required for transmission of the hide image of size (n×m) is only (n×2m).

2. RELATED WORK

Many different techniques for data hiding have been proposed till date. One of the widespread techniques is based on manipulating the least-significant-bit (LSB) by replacing the LSBs of the cover-image with the secret message bits. In paper [7] , Ali Daneshkhah proposed that the two bits of the message is inserted in a pixel of an image in a way that second bit plane and fourth bit plane are allowed to be manipulated. The results shows this method is an effective and secure steganography technique.

Wang et al. [8] proposed a method for data hiding scheme through optimal LSB substitution and genetic algorithm. The worst mean-square-error (WMSE) between the cover image and stego image is shown to be half of that obtained by simple LSB substitution method in proposed algorithm.

In paper [9], an optimal pixel adjustment is proposed for data hiding by simple LSB substitution. Its result for four bit manipulation technique gives a PSNR value of 24.56, while the method proposed in this paper gives a PSNR value of 34.87 for four bit replacement.

In paper [10], a survey has been done on various image encryption methodology. In this paper a new method is proposed to increase the space efficiency and security of steganography.

255	255	255	250	….
252	254	254	255	…
		…	…	…
…	…	…	…	….

Figure 2. Hide Image

58	84	21	83	….
42	233	58	213	…
…	…	…	…	….

Figure 3. Pseudo Random numbers

3. PROPOSED IMAGE STEGANOGRAPHY ALGORITHM

Our proposed algorithm is based on encrypting the hide image using pseudo random numbers by LSB technique.

3.1 Image Encoding

Consider hide image of order (n×m) represented by the **Figure 2** which is given below:

3.1.1 Generation of Pseudo Random Numbers

Number Pseudo random numbers are used for the encryption of the hide image. Hénon map is used for generating the pseudo-random sequence. Two dimensional discrete-time nonlinear dynamical Hénon chaoticmap generates a pseudo-randombinary sequence which has been described as below

$$X_{n+1} = 1 + Y_n - aX_n; \;\; Y_{n+1} = bX_n; \;\; n = 0,1,2,\ldots \tag{1}$$

Here, the parameters, a and b are prime importance as the dynamic behaviour of system depends on these values [11].

For a hide image of n×m, a pseudo random matrix of size n×m is generated as shown in **Figure 3**.

The hide image matrix is XORed with the pseudo random matrix.

For an example, the cell of hide image having pixel value 255 is XORed with the cell value of the pseudo random matrix having value 58

$$(11111111)\; XOR\; (00111010) = 110000101$$

$$(11000101)_2 = (197)_{10}$$

3.1.2 Bit Representation and Bit-Division

Each value in the encrypted image matrix thus obtained, is represented by an 8-bit number.

Now, we need to divide this 8-bit value into 2 parts containing 4 bits each having value between 0 and 15.

$$(197)_{10} = (11000101)_2$$

The resultant matrix G, of order (n×2m) is obtained.

If the size of cover image is greater than n×2m, then padding is required for the hide image to make its size same as that of the cover image.

3.1.3 Bit Insertion into the Cover Image

After getting the resultant encrypted hide image of order (n*2m), we insert it into the cover image. The last four bits of the cover image matrix are reset and replaced by the values of the resultant encrypted hide image. The cover image is represented by **Figure 4**.

For e.g., 222 is converted to value 220 after replacing last four least significant bits with hide image

The final steganographic image is represented by **Figure 5**.

3.1.4 Encoding Algorithm

1. For a hidden image of dimensions n×m and a cover image of dimensions greater than at least n×2m, a matrix of pseudo random numbers are generated of the order n×m.
2. These random numbers are XORed with the value of the hidden image to form the encrypted image.
3. Each value of the encrypted image matrix is broken into two halves of 4 bits each to give a value between 0-15.
4. The least significant last 4 bits of the cover image is reset and substituted by the corresponding values of the encrypted hide image.
5. Thus the final image after the manipulation of the LSBs are sent with the image hidden in it.

222	225	226		224	….
227	227	227		223	…
		…		…	…
…	…	…		…	….

Figure 4. Cover Image

220	229	234	235	....
231	230	225	215	...
		...	...	...
...	...	...	...	....

Figure 5. The final stego image

220	229	234	235	....
231	230	225	215	...
		...	...	...

Figure 6. Stego image

3.2 Image Decoding

To decode the stego image, we perform the following operations:

3.2.1 Extraction of 4 LSBs from stego image

The last four bits of every pixel value are taken and the values in each row are combined in pairs to form 8-bit numbers, giving a (n×m) matrix.

For eg: taking the first two cell values in the stego image:

$$10 = (11011100)_2$$

$$(229)_{10} = (111000101)_2$$

Taking the last four bits from each value

1	1	0	0
0	1	0	1

3.2.2 Retrieval of the encrypted hide image

Combine these two extracted values to form an 8 bit number values between 0 and 255:

1	1	0	0	0	1	0	1

$$(11000101)_2 = (197)_{10}$$

These values correspond to the values of the encrypted hide image.

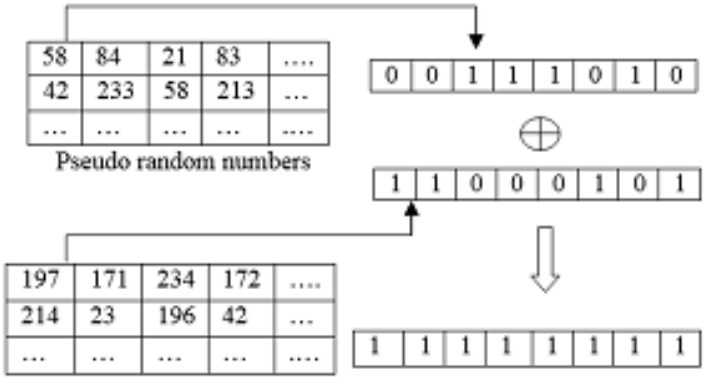

Figure 7. Retrieval of the encrypted hide image

222	225	226	224	....
227	227	227	223	...
...	...	...	...	....

Figure 8. Original hide image

3.2.3 Retrieval of hide image

The encrypted hide image is XORed with the pseudo random matrix to obtain the original hide image as shown in **Figure 7**.

Similarly other values are obtained to form the original hide image as shown in **Figure 8**.

3.2.4 Decoding Algorithm

The received image is read and the same set of random numbers are generated as on the sender's side using the same random function generator

1. The last 4 LSB's of every 8 bit value of the stego image are retrieved.
2. Values of each row are clubbed together in pairs to give an 8 bit value of the encrypted image.
3. This encrypted image matrix is XORed with the random number matrix to retrieve the original hide image.

4. EXPERIMENTAL RESULTS AND ANLYSIS

The proposed framework has been applied on a number of images with different hide images and excellent results are obtained.

(a) (b) (c)

Figure 9. Encoding by system: (a) original image (b) secret image (c) steganographic image.

(a) (b) (c) (d)

Figure 10. Cover Images; (a) fish (b) Desert (c) Lena (d) Baboon

4.1 Mean Squared Error

The MSE [12] represents the cumulative squared error between the cover image g and the stego image ĝ of size (n×m).

$$e_{MSE} = \frac{1}{MN} \int_{n=1}^{M} \int_{m=1}^{N} [\hat{g}(n,m) - g(n,m)]^2 \tag{2}$$

The lower the value of MSE, the lower is the error.

4.2 PSNR (Peak Signal to Noise Ratio)

The quality difference between the cover image and the stego-image is measured through PSNR [11].PSNR represents a measure of the peak error. It is defined as:

$$PSNR = -\log_{10}\left(\frac{e_{MSE}}{S^2}\right) \tag{3}$$

Where S is the maximum pixel value. Larger the PSNR, higher is the image quality, i.e. smaller the difference between cover image and stego image.

Experimental Result of **Figure 9** gives a result with efficient PSNR value 33.6773.

The experimental analysis of the images which were used as a cover images as shown in **Figure 10**. are given in **Table 1**.

Table 1. PSNR Value Analysis

Image Name	Size(in pixel)	Capacity (%)	MSE	PSNR
Lena.jpg	200*200	50%	31.916	34.8739
fish.jpg	768*1024	50%	19.573	35.6252
Baboon.jpg	512*513	50%	28.102	33.6773
Desert.jpg	455*500	50%	30.745	33.6728

4.3 Space Efficiency

The space efficiency of the algorithm described above is 50% which is much more than the algorithms proposed earlier. For a hide image of order (n×m), a cover image of size at least (n×2m) is required.

5. CONCLUSION

In this paper, a new LSB technique for steganography is proposed, in which pseudo random numbers are generated by Hénon chaotic maps. Further they are used to encrypt to hide the image and the four LSB's of the cover image are replaced by the hide image.

This method was applied to various test images in MATLAB and results thus obtained proved a higher level of security of images.This method is space efficient and more secure than algorithms proposed earlier.

References

[1] Z. Yun-Peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Wei-di, "Digital image encryption algorithm based on chaos and improved des," in *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, pp. 474–479, IEEE, 2009.

[2] J. Fridrich and M. Long, "Steganalysis of lsb encoding in color images," in *Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on*, vol. 3, pp. 1279–1282, IEEE, 2000.

[3] L. Guo, Z. Shi-ping, X. De-ming, and L. Jian-wen, "An intermittent linear feedback method for controlling henonlike attractor," *Journal of Applied Science*, pp. 288–290, 2001.

[4] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.

[5] C. Jeyamala, S. GopiGanesh, and G. Raman, "An image encryption scheme based on one time padsa chaotic approach," in *Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on*, pp. 1–6, IEEE, 2010.

[6] R. Chandramouli and N. Memon, "Analysis of lsb based image steganography techniques," in *Image Processing, 2001. Proceedings. 2001 International Conference on*, vol. 3, pp. 1019–1022, IEEE, 2001.

[7] 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.

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

[9] 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.

[10] M. Philip and A. Das, "Survey: Image encryption using chaotic cryptography schemes," *IJCA Special Issue on Computational ScienceNew Dimensions & Perspectives*, vol. 1, pp. 1–4, 2011.

[11] N. RAGHAVA and A. KUMAR, "Image encryption using henon chaotic map with byte sequence," *International Journal of Computer Science*, vol. 3, no. 5, pp. 11–18, 2013.

[12] 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.

About This Journal

ISA is an open access journal published by Scientific Online Publishing. This journal focus on the following scopes (but not limited to):

- Access Control
- Authentication and Authorization
- Database Security
- E-Commerce Security
- Encryption and Decryption
- Grid Security
- Information Hiding and Watermarking
- Information Privacy
- Intrusion Detection
- Network Security
- OS Security
- Security Engineering
- Security for Personal Information
- Security Models
- Security Protocols

Welcome to submit your original manuscripts to us. For more information, please visit our website: http://www.scipublish.com/journals/ISA/

You can click the bellows to follow us:

- Facebook: https://www.facebook.com/scipublish
- Twitter: https://twitter.com/scionlinepub
- LinkedIn: https://www.linkedin.com/company/scientific-online-publishing-usa
- Google+: https://google.com/+ScipublishSOP

SOP welcomes authors to contribute their research outcomes under the following rules:

- Although glad to publish all original and new research achievements, SOP can't bear any misbehavior: plagiarism, forgery or manipulation of experimental data.
- As an international publisher, SOP highly values different cultures and adopts cautious attitude towards religion, politics, race, war and ethics.
- SOP helps to propagate scientific results but shares no responsibility of any legal risks or harmful effects caused by article along with the authors.
- SOP maintains the strictest peer review, but holds a neutral attitude for all the published articles.
- SOP is an open platform, waiting for senior experts serving on the editorial boards to advance the progress of research together.