

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

Securing Images by Combination of Chaotic Map and Steganography

Reshma ¹, Vijaya Murari T ²

P G Scholar, Department of CSE, NMAMIT, Nitte, Udupi District, Karnataka, India¹

Assistant Professor, Department of CSE, NMAMIT, Nitte, Udupi District, Karnataka, India²

ABSTRACT: With increased utilization of exchange of the data through the electronic system, the need to secure the information during the transmission has been a primary concern. Because of growth of the multimedia application, security becomes an important issue of communication and storage of images. The proposed paper is about the security of image by combining chaotic maps and watermarking techniques. In this to provide more security logistic map is used to generate chaotic map. Only complement share will be sent to the recipient the recipient can recover the original hidden message by using the watermarking technique and the complement share. The scheme is evaluated in terms of imperceptibility. The results which among the watermarking technique is efficient.

KEYWORDS: Chaotic Map, Logistic Map, Complement Share.

I. INTRODUCTION

Because of the increasing demand for information security, both the chaotic maps and steganography is widely being used in the security applications. There are several cryptographic algorithms to secure data during transmission, in the cryptographic algorithms data is encrypted using a key at the senders end during transmission on receiving the receiver decrypts the received data using the same key so as to recover the original data. To improve security of the data being transmitted chaotic maps and steganography is combined.

Visual Cryptography is a method in which a original secret binary image will be divided into multiple images of black and white pixels and distributed to several users and when these multiple shares are overlapped they reveal the original secret binary image. To generate shares from secret image several techniques are being used.

Steganography is a technique in which a image to be sent to the receiver is embedded in a host image during transmission such that host image does not reveal the existence of hidden image. The image intended to be viewed only by the receiver is hidden in such a way that when retrieved the quality and the size of the hidden image should remain the same. There are two kinds of steganography methods one is concerned with altering the pixel values and the other is concerned with frequency. Steganography consist of two steps one is embedding the image to be secretly sent to the receiver in a host image and the second step is extraction that is recovering secret image from the cover image, embedding and extraction requires any steganography methods. Steganography contains a host image which is clearly visible, a image to be secretly sent to the receiver which is embedded within a host image which is not visible to naked eye and stego image which contains a visible host image and a embedded secret image. The Image to be secretly sent to the receiver can be extracted from the stego image which is visible to naked eye.

In this paper, we use two different steganography techniques one from spatial domain and one from transform domain. Along with steganography we use chaotic maps to provide additional security to the image being transmitted. The steganography techniques that we use here are Least Significant Bit substitution technique and Discrete Wavelet Transform technique.

This paper is being organized in the following way: Section II is about the literature survey carried out. Section III is about the proposed scheme. Section IV shows the results. Conclusion is provided in section V.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

II. LITERATURE SURVEY

Spatial domain technique is concerned with pixel values of the images, the information of the image to be sent is put into the host image pixel values. C.K. Chan and L.M. Cheng et.al [1] proposed a Least Bit Substitution technique. It is one of the spatial domain technique. In this technique the pixels that carry less information of the host image is replaced with pixels that carry most of the information of the secret image. Apart from Least Significant Bit Technique there are other techniques like patch work, texture block coding. In the Least Significant Bit Technique embedding is easy but it can be attacked easily when compared to transform domain technique like Discrete Wavelet Transform.

Barnali Gupta and Prof. Samir k et.al [2] proposed a DWT method for image steganography. DWT is a transform domain technique which is concerned with embedding a secret image in the selected frequency band of the host image. In DWT low frequency domain will contain most of the information regarding the secret image.

Moni Naor and Adi Shamir et.al [3] proposed a Visual Cryptography technique for binary images. In this scheme the original cover image is encoded into many secret share image and these multiple secret share images individually do not reveal any data relevant to the original cover image. Only when all the secret shares are stacked together it reveals the hidden cover images. A (2,2) scheme was initially proposed. P. Tuyls, H.D.L. Hollmann, J.H. Van Lint, L. Tolhuizen et.al [4] proposed XOR-Based Visual Cryptography Scheme in which using XOR operation the size of the shares produced by the secret image will be reduced as well as shares will have high resolution and high contrast.

Chaotic maps can be generated by logistic maps. A dynamic system can be stated as chaotic if it is sensitive to initial conditions. Elabady N.F, Abdal Kader H.M, Mousa M.I and Sabbeh S.F et.al [5] proposed Image Encryption Based On New One-Dimensional Chaotic Map in which the image is encrypted using chaotic maps generated by one dimensional logistic map. Logistic maps are used to generate the chaotic sequences there are two variants of logistic maps which can be used for the generation of chaotic sequence they are one dimensional logistic map and multidimensional logistic map. The equation for one dimensional logistic map is

$$x_{q+1} = rx_q(1 - x_q) \quad (1)$$

III. PROPOSED SCHEME

In this section we explain proposed scheme in detail. In this we use two steganography techniques and logistic map will be used for the generation of chaotic map.

A. Embedding and Extraction Process

In embedding process initially a cover image will be selected in which the complement share is to be hidden. Using the transformation technique the complement share is hidden in the cover image. The hiding of the complement share in the cover image will be dependent on the watermarking scheme being used. The embedding scheme varies from one watermarking scheme to another watermarking scheme. Inverse of the transformation technique is applied to obtain the watermarked image also called as stego image. To produce the complement share an XOR operation is applied to the secret message and the chaotic share. Chaotic share is produced by using one dimensional logistic map.

In extraction process the transformation technique will be applied on the stego image and the inverse transformation will be applied so as to obtain the complement share. The secret message is obtained by XOR operation between the complement share and the chaotic share. Chaotic share is produced by using one dimensional logistic map.

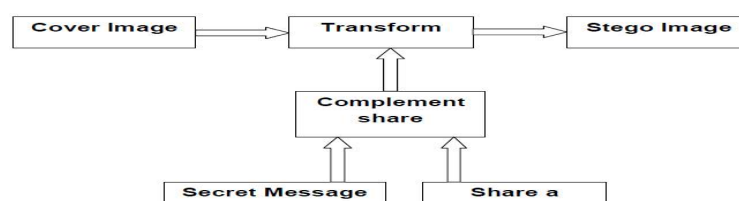


Figure 1: Embedding Process

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

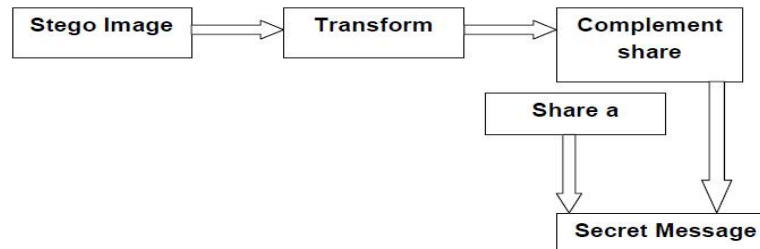


Figure 2: Extraction Process

B. LSB Method

Least Significant Bit substitution method is easy to implement. This method is concerned with the pixel values of the image. In the embedding technique read the host and the secret image and check for the dimension if the dimensions are equal. Select the number n of LSB bits to be substituted. Set n bits of each byte of host image to zero by and operation on the size of the cover image and the size of the complement share. Equation for embedding is

$$y_j = y_j - y_j \bmod (2^l) + m_j \quad (2)$$

In the above equation

y_j is the J_{th} pixel value of the stego image.

m_j is the decimal value of J_{th} block in secret image.

l is the number of LSB substituted

Equation for extraction is

$$m_j = x_j \bmod 2^l \quad (3)$$

C. DWT method

Discrete wavelet transform captures both the frequency and location information. The wavelet transform is useful to divide an image into its four frequency bands. Image has four frequency bands namely LL that contains the approximation, HL which contains the horizontal details, LH which contains the vertical details and HH which contains the diagonal details. Initially dwt is applied to the host image and later dwt is applied to the secret image now the LL band of the host image contains most of the information of the host image and the LL band of the secret image contains most of the information of the secret image. To make the secret image invisible to human eye the approximation part of both the host and secret images will be used this image is now called as newhost image. To obtain the stego image the inverse dwt is applied to altered approximation part of the newhost, all the other parts that is vertical, horizontal and diagonal parts of the host image is used. So the stego image contains less information about the secret image and more information about the cover image.

During the extraction process the secret image that is embedded within the cover image must be extracted and must be visible. During the extraction process modification will be done using the approximation part of stego image and the host image if we subtract the approximation part of stego image from the cover image we get the approximation part of hidden secret image. To recover the hidden secret image inverse dwt will be applied to the modified approximation part and other subband information will be same as that of the secret image. Now we obtain the hidden secret image which is visible to human eye.

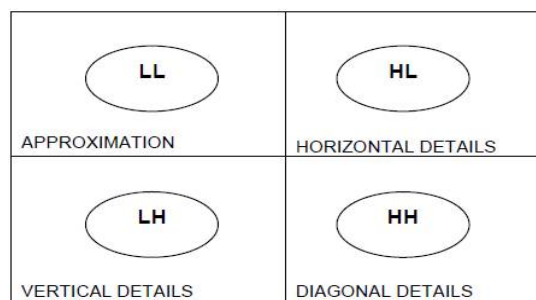


Figure 3: Frequency Bands of a Image by DWT Method

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

D. Complement Share Generation

Visual cryptography is a concept in which a secret image will taken and it will be divided into numerous unique shares and this unique shares do not reveal any information regarding the hidden secret image. On stacking together the numerous unique shares hidden secret image is revealed. In this project a secret image is taken and instead of generating shares from the same image itself a logistic one dimensional equation can be used to generate a one share. The share that is used by generating logistic equation is XORed with the secret image to obtain the second share also called as complement share. The complement share will be used instead of the secret image in embedding phase of the transformation techniques. During the extraction process the complement share will be obtained as output which is then XORed with the share obtained by using logistic equation so as to obtain the hidden secret image.

E. Evaluation Parameters

The comparison of the original image, stego image and secret image extracted secret image are done based on the parameters like MSE and PSNR.

MSE: Mean squared error is used to compare two images by providing the degree of similarity between the images.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (4)$$

PSNR: Peak Signal to noise Ratio gives the quality of the reconstructed image as seen by the human eye. High PSNR value indicates that the reconstruction is of higher quality, in some cases it may not.

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

IV. RESULTS

We have performed simulation using two steganography technique and chaotic map is used for generation of logistic map. Initial condition for generation of logistic map is taken as $y_0=0.5$ and value of p is taken as $[3.9999, 4]$.

Table 1: PSNR, MSE values of DWT and LSB method of Complement Share and Extracted Complement Share

	DWT	LSB
PSNR	50.0699	29.6824
MSE	2.5796	282.0342

Table 2: PSNR, MSE values of DWT and LSB method of Secret image and Extracted Secret Image

	DWT	LSB
PSNR	30.0990	99
MSE	256	0

V. CONCLUSION

By observing the psnr value of comparing complement share with the reconstructed complement share the value obtained by dwt is higher which means that the reconstructed complemented share obtained by dwt method is better when compared to lsb method. By observing the psnr value of comparing secret image with the secret image the value obtained by lsb is higher which means that the reconstructed secret image obtained by lsb method is better when

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

compared to dwt method. Future enhancement is this entire program can be parallelized to improve the speed of operation.

REFERENCES

- [1] C.K. Chan and L.M. Cheng, "Hiding Data In Images By Simple LSB Substitution", Pattern Recognition, pp 469-474, 2004.
- [2] Barnali Gupta and Prof. Samir k, "A DWT Method For Image Steganography", International Journal Of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, 2013.
- [3] Moni Naor and Adi Shamir, "Visual Cryptography", Advances in Crptology- Eurocrypt94, pp 1-11, 1995.
- [4] P. Tuyls, H.D.L. Hollmann, J.H. Van Lint, L. Tolhuizen, " XOR-Based Visual Cryptography Schemes", Designs Codes and Cryptography, pp 169-186, 2005.
- [5] Elabady N.F, Abdal Kader H.M, Mousa M.I and Sabbeh S.F, "Image Encryption Based On New One-Dimensional Chaotic Map", International Conference On Engineering and Technology (ICET), pp 1-6, 2014.