A Novel and Innovative Approach for Image Steganography with Chaos

N. Krishnaveni[1], Sudhakar Periyasamy[2]
[1]Research and Development Centre, Bharathiar University, Coimbatore, TamilNadu, India
[2]Department of school of computing EIT, Mekelle University, Ethiopia

Article Info

Article history:

Received Oct 22, 2017
Revised Jan 9, 2018
Accepted Jan 16, 2018

Keywords:

Integer Wavelet Transform (IWT)
Lifting scheme
Logistic map
LSB
Steganograph

ABSTRACT

Steganography is the art/technique of hiding message data inside a carrier file in such a way that unauthorized or unsolicited personnel is not capable of detecting the presence of data inside the carrier file. The Proposed Method provides improved security and improved high embedding capacity image steganography through the usage of Integer Wavelet Transform (IWT) and Chaotic Logistic map. Least Significant Bit technique is used to replace the bits in the coefficient of detail band. The proposed method offers lossless and unnoticeable change in the image steganography. In this paper we focus on both cryptography and steganography for better confidentiality, security and robustness. We find that the proposed algorithm has a better CMPSNR (Chaotic Logistic mapping) value averaging close to 74 after embedding the secret data, while the existing algorithms have values of around 65.

Corresponding Author:

N. Krishnaveni,
Research and Development Centre, Bharathiar University, Coimbatore, TamilNadu, India.
Email: nkrishnaveni2017@gmail.com

1. INTRODUCTION

Steganography is a technique that deals with sharing the confidential or secret data using an appropriate transporter, which normally is referred as carrier, especially a multimedia carrier including image, audio or videos files. The approach followed is novel where the steganography goes hand in hand with cryptography by utilizing the features of wavelets while increasing the security and also to make the data transfer more secure. What cryptography renders is the confidentiality whereas steganography on the other side gets the message hidden and makes sure no intruder gets an idea about the hidden message.

The main aim of steganography is to duck the suspicion to the communication of the secret note. In other words, Steganalysis is a method of sensing likely secret communication using techniques against steganography. There are different methods for image steganography. Using spatial domain in Image steganography is the novelty we are introducing to make the process more robust and free from Steganalysis. Steganography is broadly categorized as follows [1]

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Steganography in TCP/IP Protocols

All these approaches use different techniques to hide the message in the communication. A very less complex and lossless audio steganography pattern based on integer-to-integer Lifting Wavelet Transform (LWT) which was proposed earlier by the researchers [2].

In this research, a simple image steganography constructed with Lifting Wavelet Transform (LWT) is proposed [3]. The use of Logistic chaotic maps in cryptography and applying Least Significant Bit offers more security and robustness. Chaos theory has been widely used in both steganography and Cryptography.

With the use of Integer Wavelet Transform we can find the detailed coefficients for classification [4]. This method focused on improving embedding capacity and bringing down the distortion to the stego image [5]. Bhavanaet.al [6] earlier proposed a chaos based scheme for concealing text within images. Secret text messages can be embedded into an image with Least Significant Bit insertion method along with chaos. Sakthidasan et al [7] earlier proposed a scheme based on chaos for image encryption using three dynamic chaotic systems. The proposed system offers highly appreciable benefits in terms of bigger key space, reduced iteration times and elevated security analysis such as key space analysis and statistical analysis.

2. CHAOTIC SYSTEM–A VIEW

Chaotic system has sensitivity to early settings. As an outcome of this sensitivity, the behaviour of systems looks to be arbitrary in spite of the system being deterministic. Logistic maps are the simplest among chaotic maps. The appreciable features of the logistic map include:

a. Simplicity of its form
b. Complexity of its dynamics

Considering,

$$x=u. *x. *(1-x)$$

When $3.6 \leq u \leq 4$, the map is in the chaotic state.

The preliminary conditions are altered with every iteration, with fixed quantity of pixels, the preliminary conditions are made chaotic in order to secure the message by hiding it from the attackers or intruders. So, the competence of the technique to retain the secrecy of the message which has to be maintained secret is very high. Also, there was no compromise made and the system still remains robust.

The transform domain image encryption technology deploys the following, which includes, DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform) and FT (Fourier Transform) to accomplish the task of conversion from the spatial to transform domain while making sure that the encryption of the obtained coefficients also happens.

In this paper, a lossless and secure image steganography method is used. In embedding phase, the embedded image is divided into 16 blocks each of size 32 * 32, and then each block sample is XORed with a logistic map of different bifurcation parameter (r). The logistic map is a simple non-linear dynamical map. The encrypted blocks are gathered to obtain final encrypted image of size 128 *128, then image samples are reshaped in one column and converted into binary form. There are various types of wavelet transforms like HaarMorlet, Daubechies, Coiflets, Biorthogonal, Mexican Hat, Symlets and etc. They differ both in formation and construction.

All printed material, including text, illustrations, and charts, must be kept within a print area of 17.2 cm wide by 24.62 cm high. For A4 paper, all the pages should begin 2.54 cm from both the top and the bottom edge, and 1.9 cm both from the left and the right edge. The page header is expected to be 1.5 cm high, and the page footer should be height of 1.75 cm. Do not write or print anything outside the print area. All text must be in a two-column format. Columns are to be 22.2 times of the character size, with a space size of 2.02 times of the character size. Text must be fully justified.

A format sheet with the margins and placement guides is available as both Word and PDF files as <format.docx> and <format.pdf>. It contains lines and boxes showing the margins and print areas. If you hold it and your printed page up to the light, you can easily check your margins to see if your print area fits within the space allowed.

3. LIFTING SCHEME

Lifting scheme gives wavelet filter design to perform discrete wavelet transform. The scheme is shown on Figure 1. Lifting includes 3 steps. Starting with the splitting process, then with prediction and finally with Updation process. Here, in this process, the dataset is split into odd and even elements. The predict step plays the major role in getting the odd elements. The even elements are not touched and they remain the same and serve as the input feed for the next step in the transform.

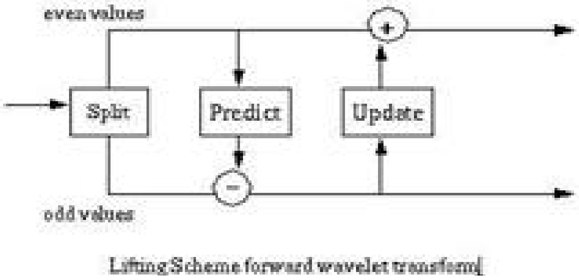

Figure 1. Lifting Scheme Forward Wavelet Transform

The even elements are left unchanged and become the input for the next step in the transform. The update step replaces the even elements with an average. This gives in smoother elements for the next step of the wavelet transform. The odd elements also represent an approximation of the original data set, which allows filters to be constructed. After filter construction, Haar filter is used for lifting transform performed on image to get the approximation & detailed coefficients of an image.

In order to hide a secret image or a data in a source image, we can modify the pixel values either in the spatial domain or in the transformed domain. The transformed domain here refers to the wavelet domain. We use Haar wavelet for this purpose of data hiding in the transformed domain. The Haar transform, which is one of the simplest transforms in wavelet mathematics, is used by us for image steganography purposes. We proposed external encryption keys to select the important part using one-dimensional chaotic map.

3.1. Haar Transform

The two-dimensional Haar transform is globalized into a random number of decompositions. While the two dimensional transform works on a 4×4 block of pixels in wavelet domain, the Lth level decomposition works on a 2n×2n image. Any odd pixels that are found on the borders are not focused as they do not have neighbours on few sides. The wavelet transform further splits the original image into as many as four sub-bands. They are represented by LL (low–low), LH (low-high), HL (high–low), and HH (high-high) frequency sub-bands. The HH sub-image signifies diagonal facts, HL gives horizontal high frequencies, and LH gives vertical high frequencies and the image LL corresponds to the lowest frequencies.

4. PROPOSED SYSTEM DESIGN

The proposed system is divided into three stages. They are

- Chaos Encryption
- Embedding
- Extracting
- Decryption

The cover image of size 256 * 256 pixels is decomposed using lifting wavelet transform (LWT). The process of decomposition, usually LL, HL, LH, HH, is repeated n times, and it is repeated just on the HH-sub band. The image is decomposed into four sub-images approximation component (LL), and three detail components (horizontal, vertical, and diagonal). Then LWT and embedding are implemented. The output coefficients represent high frequency sub-band (detail) and low frequency sub-band (approximation). The detail coefficient is chosen for LSB embedding. Embedding Key is used to select the pixel value of each 8*8 block of cover image. Encryption key selection using BitXOR.LSB embedding is done based on the mapping key matrix. Finally Stego image is generated.

Algorithm

4.1. Chaos Encryption

a. Cover image is converted into gray scale image.
b. Gray scale image is pre-processed into IWT four subbands are created.
c. Logitech mapping techniques is used Assignbitshift
mapu=3.9999;
{\displaystyle \mu =2} tent mapx=0.40000565;
d. Calculate x= u*x*(1-x)
e. Select image pixel value as key value by Logitech mapping (EThreshold process starts)

f. Select the i value as encryption key value by the following condition, if X>(i/255)&&X<((i+1)/255)), then encryption key=i; otherwise repeat step until assign key value
g. Encryption Key value obtained and do Xor operation is done on secret image pixel values and encryption key.
h. This gives the encrypted secret image

4.2. LSB Embedding

a. Create embedding Key and take HH Subband of the Cover image
b. Initialize len=length(encrypted data);count=1; totalbits=128*len; a=128; k=1;
c. Read every pixel from cover image and make a block of 8x8 matrix
d. Now first 8x8 block of HH subband is selected for hiding the secret data
e. Read every pixel 8x8 block & select the hiding pixel by embedding key Mkey
f. Bit AND operation on Selected pixel by using 254 value.
g. Hiding bits If bitand(secret data,a)==a, then bitoroncoeff,h(=1);
h. Repeat this process until total number of bits
i. Embedded pixels are received as 8x8 matrix block and its replaced in stegosub bands
j. Inverse lifting transform on stegosubbands, LL, LH, HL is performed.
k. From the subbandsstego image is reconstructed.

4.3. Secret Data Extracting

a. Applying lifting wavelet transform on stego image& LL,LH,HL,HH are obtained
b. HHsubbands are selected for data extracting
c. Initializelen=length(encrypted data);count=1; total bits=128*len; a=128; k=1;
d. HH is converted into 8x8 blocks& Read Every pixel of all the blocks
e. Select data hided pixel from the 8x8 block,For extracting bits If bitand(coeff,h)==a, then bitor on a, k(=1);
f. Extract data until th condition if a<1 fails
g. All hided data are extracted as above until if count>totalbits
h. Secret data is extracted from HH band

4.4. Chaos Decryption

a. Logitech mapping technique is used
b. Assign bit-shift
map u=3.9999;
{\displaystyle \mu =2} tent map x=0.40000565;
c. Construct Logitech map from bit-shift & tent map values; Logitech map formula is X=u*x*(1-x)
d. Select image pixel value as key value by Logitech mapping(Ethreshold Process Starts)
e. Select the i value as decrypted key value by the following condition, if X>(i/255)&&X<((i+1)/255)), then encryption key=i; otherwise repeat step until assign key value
f. Decryption key value is obtained
g. XOR operation on secret image pixel values and decryption key is done.
h. This is the Decrypted secret image
i. Steganography is completed

5. RESULTS AND OBSERVATIONS

For this data hiding project, we used the USC-SIPI image database which is a collection of digitized images. The database is divided across different categories based on the character of the images. The size of the images present in the database varies from 256 * 256 to 512 * 512 or 1024 * 1024. There are both color images as well black and white images present in the database. The color images are of 24 bit depth while the black and white images contain 8 bit for representation. The following volumes are currently available:

From the four different database, Miscellaneous volume database is uses as cover image. This project is simulated in MATLAB R2012a version. To compare the quality of after cover image, two measures are commonly used namely, Mean square error (MSE) & Peak Signal to Noise Ration (PSNR). MSE is defined by

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

PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K. PSNR is defined by,

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

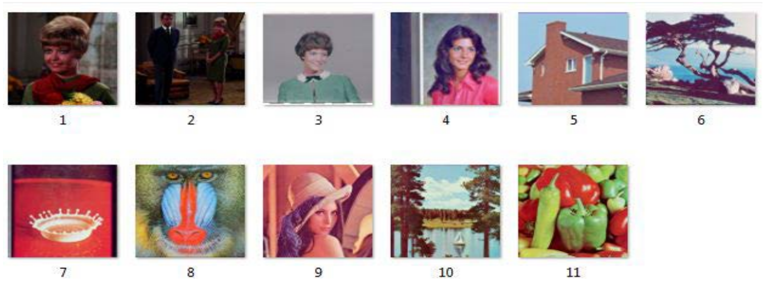

Figure 2. Miscellaneous Volume Database Images Used as Cover Image

Figure 2 represents the volume database images which are used as cover image. Table 1 presents the details of MSE and PSNR values.

Table 1. MSE and PSNR for Images

Image	MSE	PSNR(dB)
1	0.0069	69.7701
2.	0.0073	69.4956
3.	0.0010	78.0106
4.	0.0046	71.5380
5.	0.0022	74.6317
6.	0.0043	71.7970
7.	0.0074	69.4114
8.	0.0038	72.3205
9.	0.0033	73.0054
10.	0.0034	72.7581
11.	0.0040	72.1647

6. CONCLUSIVE REMARKS

In this paper, lifting based LSB embedding and chaos secret data encryption both give excellent quality and security to secret data. Chaos encryption is very simple compared to other encryption techniques like DES, AES and blowfish. And the lifting wavelet transform is more efficient transform than DWT. And HH Subband embedding enhances the image reconstruction. From the experimental results, this proposed system has better PSNR to cover images.

REFERENCES

[1] Anoop Kumar,Ajay Rajpoot,K.K.Shukla S.Karthikeyan ,"A Robust Method for Image Steganography based on Chaos Theory", *International Journal of Computer Applications* Vol.113,March 2015

[2] Said E.EI.Khamy, Noha O.Korany. Marwa H.El-Sherif "Robust Image Hiding in Audio Based on Integer Wavelet Transform and Chaotic Maps Hopping", *Arab Academy for Science,* (NRSC 2017),March 2017

[3] Ahlam majead Kadum,Dr.Saad Najim AI-Saad, "Image Hiding Using Lifting Wavelet Transform" *International Journal of Scientific & Engineering Research,*Vol 7 April 2016

[4] Aref Miri ,Karim Faez ,"An Image Steganography method based on Integer Wavelet Transform" *Springer Multimedia Tools Appl,* June 2017

[5] M.Vijay,V.Vigneshkumar, "Image Stegnography Method using Integer Wavelet Transform", *International Journal of Innovative Research in Science, Engineering and Technology,*vol 3,March 2014

[6] Bhavana S, k.L.Sudha, "Text Steganography using LSB Insertion Method Along with Chaos Theory", *International Journal of Computer Science, Engineering and Applications(IJCSEA*), vol.2, No. 2,April 2012.

[7] Sakthidasan K, B.V.Santhosh Krishna "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images",*International Journal of Information and Education Technology*, Vol 1,No.2, June 2011

[8] Shawn D.Dickman "An overview of Steganography", *James Madison University infosecTechreport,* JMU-INFOSEC-TR-2007-002, July 2007