International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 170 - 174, 2015, ISSN:- 2319–8656

Adaptive Steganography Based on Logistic Map

Fariba Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University,
Masjedsoleyman Branch, Masjedsoleyman,
Iran

Sajjad Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University,
Masjedsoleyman Branch, Masjedsoleyman,
Iran

Abstract:
umerous novel algorithms have been proposed in the fields of steganography with the goals of increase security,capacity and imperceptibility. In this paper, we introduced a new blind adaptive algorithm in image steganography technique to Improving that goals. The existing methods hide the information using constant bit length in integer wavelet coefficients. This paper uses variable bit length based on float wavelet coefficients to hide the data in a particular positions using secret key. The proposed method try to obtain an optimal mapping function to reduce the difference error between original coefficients values and modified values. we provided with the double security by using a secret key only known to both sender and receiver, therefore improving goals compared to the existing algorithm.

Keywords: Steganography; Security; Logistic Map; capacity; image

1. INTRODUCTION

over the last decade, one of the most significant current discussions in computer science is the field of information security. In general, information security is the techniques, policies and strategies used to protect and secure computer systems, in maintaining the operations of an organization. One of the concerns in information security is the concept of information hiding. It is the process of embedding information into digital content without causing perceptual degradation. Steganography of current information hiding has shown that steganography is one of the recent important subdisciplines. This is because most of the proposed information hiding system is designed based on steganography. Today, steganography is most often associated with the high-tech application where data are hidden with other information in an electronic file[1]. Generally speaking, a good steganographic technique should have good visual imperceptibility and a sufficient capacity of hidden secret data[2]. Steganographic methods can be classified into spatial domain embedding and frequency domain embedding[3,4]. Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [5].

2. RELATED WORKS

In this section we introduce some of the methods described Steganography . For this purpose, two groups of methods in the spatial domain and transform domain techniques will be examined.In the spatial domain techniques, secret messages are placed in a carrier media, without prior information hiding, on a carrier medium, the conversion will be done. Confidential data is actually placed directly on the carrier media. One of the first Steganography techniques, using the least significant bits of the carrier media. The use of this technique for placement of confidential information on a carrier media, not a tangible change in the media.

Steganography the images presented in lots of different techniques, the goal of all of them is the availability of high capacity, security, and resistance. These three criteria are in conflict with each other and simultaneously achieve all three simultaneously is very difficult and perhaps impossible. Three objectives are stated at the three vertices of a triangle. The matter requires attention to each other and not all of these parameters simultaneously met in the best way.Wavelet transform gives the best result for image transformation[6]. the frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: Discrete Wavelet Transformation has its own excellent space frequency localization property. Applying DWT in 2D images corresponds to 2D filter image processing in each dimension. The input image is divided into 4 non-overlapping multi-resolution sub-bands by the filters, namely LL1 (Approximation coefficients), LH1 (vertical details), HL1 (horizontal details) and HH1 (diagonal details). The sub-band (LL1) is processed further to obtain the next coarser scale of wavelet coefficients, until some final scale “N” is reached. When “N” is reached, we’ll have 3N+1 sub-bands consisting of the multi-resolution sub-bands (LLN) and (LHX), (HLX) and (HHX) where “X” ranges from 1 until “N”. Generally most of the Image energy is stored in these sub-bands[7,8,9,10]. The least significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image in spatial domain but it has some limitations such as it is easier to understand using steganalysis[11,12]. Variable Embedding Ratio and LSB is used in [13]. paper[14] proposes a method for image steganography. The chosen Variable Embedding Ratio [VER] is 4:2 that is 4 bits are embedded in edge pixels and 2 bits in other pixels.In[15] uses variable bit length based on integer wavelet coefficients to hide the data in a particular positions using secret key by LSB substitution method. In smooth areas they embed three bits of secret information. In the complicated areas, variable rate bits are embedded[16].

3. SECRET KEY

we use chaos theory to produce secret key. The name "chaos theory" comes from the fact that the systems that the theory describes are apparently disordered, but chaos theory is really about finding the underlying order in apparently random data. The nonlinear dynamics researchers have observed an interesting relationship between chaotic behavior and Random number generator systems as many properties of the chaotic systems such as their sensitivity to initial conditions can be considered to the confusion in generation of secret keys. Deterministic pseudorandom numbers are used for the generation of secret key in cryptography system. The logistic map is a very simple mathematical model often used to describe the growth of biological populations. The simple mathematical form of the logistic map is given as [17]:

$$X_{n+1}=r.xn(1-x_n) \quad (1)$$

x_n is the state variable being in the interval [0, 1] and r is system parameter which might have any value between 1 and 4. In this paper we have used the logistic function to generate the secret key. If this function is quite Chaotic behavior, you would have x_0=0.3 amnd 3.57<r<4.

4. PROPOSED METHOD

wavelet transform is applied to the cover image to get the wavelet coefficients. the wavelet coefficients is splitted into RGB planes .The obtained wavelet coefficients from the RGB planes, select one or two or three planes according to the secret key and Each selected plane is decomposed into m*m blocks according to the secret key.Range, the number of bits that can be replaced, between 1 to logarithm biggest coefficient value. According to the value of coefficients, the number of bits replaced The secret message is determined. It makes Optimal Use of the Wavelet Coefficients. While fewer number of coefficients are modified, More bits can be replaced. After replacement, inverse wavelet transform applied to restore the image (Fig 1).

4.1 Embedding procedure:

cover image is splitted into R, G, B planes .
Each RGB is converted into frequency domain by using Haar wavelet transform.
Select RGB plans based on secret key .
selected RGB plane is decomposed into blocks based on secret key .
Value of wavelet coefficient are classified

{D=2^{n-1} –2^n-1,n =log (coefficient)}D is range value of wavelet coefficient, n-1 is number of secret data bits to be embedded and coefficient is value of wavelet coefficient ,dec(n) is the decimal value of secret data bits.

If 2^{n-1} < coefficient <2^n-1 then

(2^n–dec(n bit of secret data))/2

1) Determine the inverse wavelet transform(idwt) on each RGB planes to restore the image.

4.2 Extraction procedure:

1) stego image is splitted into RGB planes .
2) Select RGB plans based on secret key .
3) Each RGB is converted into frequency domain by using Haar wavelet transform.
4) Each RGB plane selected is decomposed into blocks.
5) Select blocks based on secret key.
6) Value of wavelet coefficient are classified :

If 2^{n-1} < coefficient <2^n-1 then

x=(2^n – coefficient)*2

message[]=dec2bin(x)

coefficient is value of wavelet coefficient stego image and message is data extraction from stego image .

If coefficient=18 and secret message is 111011 then
16<23<32 ,n=5, number of bits is 4.select 4 bits of secret message(1110) .dec(1110) is 14.
32-14/2=25
We put 25 instead of 23 in the picture .
For extract,if stego coefficient is 25 then
16<25<32
Secret mesage=dec2bin((32-25)*2)= dec2bin(14)=1110
So we had to replace bits that just were extracted.

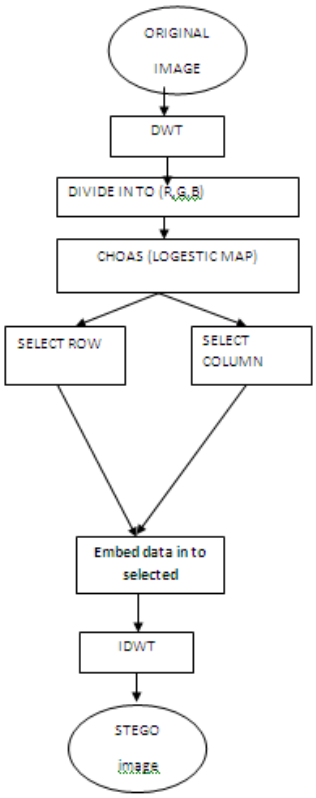

Fig 1. Proposed Block Diagram Data Embedding

5. RESULTS AND DISCUSSION

My proposed algorithm was implemented in MATLAB and are tested with many colored images. In this paper We selected 512x512 "Lena" jpeg image to perform our testing. Fig 2 has been shown cover image, Fig 3 has been shown stego image. The performance of various steganographic methods can be rated by the three parameters: security,capacity and imperceptibility. The steganographic methods proposed in this paper are very secure as variable number of bits are hidden in different coefficient of wavelet. This method embeds secret information in a random order using a secret key only known to both sender and receiver So it is very difficult to find out the hidden data from the stego image. The same stego image can also bear different secret image for different receiver depending on their secret key. Capacity means the amount of message that can be embedded. Table I, show Average PSNR values and Embedding Rate achieved using standard images.

Table I. Average PSNR values achieved using standard images

Embedding Rate	0.01	0.02	0.05	0.20	0.25	0.35
PSNR	64	61	55	49	48	46

Fig 2.Cover Image Stego image

Fig3 indicative of the blue before placing a secret message in an image and then paste the information is confidential, tangible change in the color chart, as we will be created.

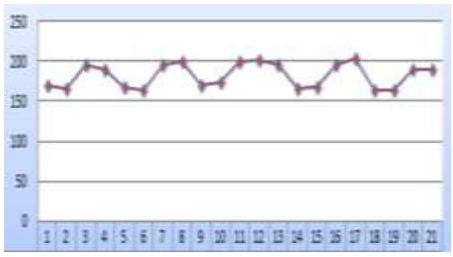

Fig 3. blue before and after placement

In the proposed algorithm [18] The image edges are detected by using the cany operator. In this way, four bits per pixel that are on the edge, and two bits in the others pixels are hidden hidden. Since a variable number of bits of the secret message in different parts of the image data, the method is safe, Because if that person is suspected of carrying forward the media until the algorithm is not available, the least significant bits of the secret message can not be retrieved. The disadvantage of the method is to extract the secret message from the carrier at destination media, the media must also be present. We have the advantage of variable bit rate method [18] in the proposed algorithm, we use the other hand to eliminate the disadvantage of my method.

Compare the signal to noise of the proposed method and algorithm [18] shown in Fig 4. As we observe the same replacement rate, the proposed algorithm provides better results.

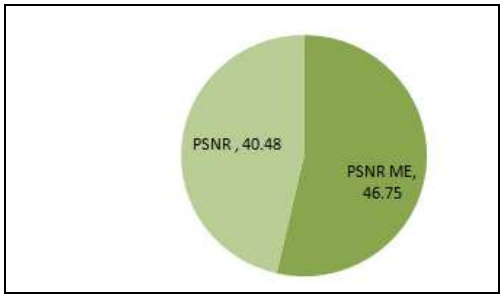

Fig4. compares the psnr in the replacement rate of 262,144

If Steganography image H1 and original image H ,HWIDTH, HLEN number of rows and columns of the image are calculated PSNR and MSE of the Equation (2) , Equation (3) is calculated.

(2)

$$MSE=\frac{\sum_{i=1}^{H\ LEN}\sum_{j=1}^{H\ WIDTH}[H(i,j)-H1(i,j)][H(i,j)-H1(i,j)]}{HLEN*HWIDTH}$$

(3)

PSNR=10* $log_{10}\left(\frac{255*255}{MSE}\right)$

The mean square error (MSE) is reduced, the image quality was high. Low value, the maximum amount of signal to noise ratio (PSNR) of the carrier image is of poor quality

6. CONCLUSION

In this paper we proposed a data hiding scheme that hides data into the float wavelet coefficients of an image. The system combines a float wavelet transform and the variable rate of embedding to maximize performance of steganographic method proposed. Because of the the chaos system is used, the proposed method is secure.

entirely By using this method the data hiding capacity is improved and secrecy of the embedded data bits can be provided. It is also seen that the stego image formed is of good quality. Future work may be carried out to increase the capacity and enhance the visual quality of the stego image by improving the PSNR value . The methods proposed in this paper are:

- very secure
- capacity is good.
- PSNR obtained is approximately maximum compared to the existing algorithm which confirm imperceptibility of the host and the stego image.
- The proposed system also reduces the difference between original coefficients values and modified values by using the adaptive float coefficient adjustment.
- Blind steganogeraphy method

7. REFERENCES

[1] Roshidi Din and Azman Samsudin," Digital Steganalysis: Computational Intelligence Approach", INTERNATIONAL JOURNAL OF COMPUTERS Issue 1, Volume 3, 2009

[2] Arun Rana, Nitin Sharma, Amandeep Kaur," IMAGE STEGANOGRAPHY METHOD BASED ON KOHONEN NEURAL NETWORK", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2234-2236

[3] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science ISSN:2229-371X www.jgrcs.info, Volume 2, No. 4, April 2011

[4] Lifang Yu, Yao Zhao, Rongrong Ni (EURASIPMember), and Ting Li,"Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", EURASIP Journal on Advances in Signal Processing,Volume 2010, Article ID 876946, 6 pages

[5] Souvik Bhattacharyya, Gautam Sanyal,"A Robust Image Steganography using DWT Difference Modulation (DWTDM)", I. J. Computer Network and Information Security, 2012, 7, 27-40 Published Online July 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012.07.04

[6] Saddaf Rubab, M. Younus," 29 Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal of Computer Applications (0975 – 8887) Volume 39– No.14, February 2012

[7] Po-Yueh Chen* and Hung-Ju Lin,"A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[8] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri,"A Session based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012

[9] S. Jayasudha," Integer Wavelet Transform based Steganographic Method using OPA Algorithm", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

[10] N S T Sai, R C Patil," Image Retrieval using DWT with Row and Column Pixel Distributions of BMP Image", N S T Sai et al. / (IJCSE) International Journal on Computer Science and Engineering ,Vol. 02, No. 08, 2010, 2559-2566

[11] Dr. Mohammed Abbas Fadhil Al-Husainy,"COMPARISON STUDY BETWEEN CLASSIC-LSB, SLSB AND DSLSB IMAGE STEGANOGRAPHY", ICIT 2013 The 6th International Conference on Information Technology

[12] S.Shanmuga Priya, K.Mahesh, Dr.K.Kuppusamy,"Efficient Steganography Method to Implement Selected Lease Significant Bits in Spatial Domain (SLSB – SD)", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[13] Tanmay Bhattacharya, Bikash Debnath,S. R. Bhadra Chaudhuri," A Session based Spatial Domain Multiple Image Hiding Technique using Variable Bit Replacement and Multiple Passwords", International Journal of Computer Applications (0975 – 8887) Volume 56– No.13, October 2012

[14] Geetha C.R, H. D. Giriprakash," Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator", International Journal of Computer Applications (0975 – 888) Volume 48– No.16, June 2012

[15] Sumanth Sakkara.,Akkamahadevi D.H, K. Somashekar," Integer Wavelet based Secret Data Hiding By Selecting Variable Bit Length", International Journal of Computer Applications (0975 – 888) Volume 48– No.19, June 2012

[16] Moazzam Hossain, Sadia Al Haque, and Farhana Sharmin," Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information", The International Arab Journal of Information Technology, Vol. 7, No. 1, January 2010

[17] Grummt, E., Ackermann, R.: Proof of Possession: Using RFID for large-scale Authorization Management.
In: Mhlhuser, M., Ferscha, A., Aitenbichler, E. (eds.) Constructing Ambient Intelligence, AmI-07 Workshops

Proceedings. Communications in Computer and Information Science, pp. 174, 182 (2008)

[18] Geetha C, Giriprakash H.2012. image steganography by variable embedding and multiple edge detection using canny operator . International Journal of Computer Applications (0975 – 888) 48:15-19