International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32477-32492
© Research India Publications
http://www.ripublication.com

A Robust and High Secure LWT based Image Steganography and Optimized Genetic Algorithm based Chaotic Encryption Approach

G.Sudha Devi[1] and Dr.K.Thangadurai[2]

[1]Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Karur, India.
Email: sudhadeviresearch@gmail.com
[2]Associate Professor and Head, PG and Research Department of Computer Science, Government Arts College (Autonomous), Karur, India.
Email: ktramprasad04@yahoo.com

Abstract

Steganography is an ability of concealing information inside the cover in such a way it looks like simple cover though it has concealed information. There are many techniques to carry out steganography on electronic media, most especially audio and image files. In this work, a new digital image security scheme is applied which incorporates Lifting Wavelet Transform (LWT) algorithm and optimized chaotic based image encryption obtained through genetic algorithm with high level of robustness and security. It uses image as cover media for embedding secret image. In this proposed scheme first of all the stego image has been encrypted using the best hybrid model for image encryption composed of genetic algorithm and chaotic function. After that the encrypted image is embedded into original image to form the stego image. In the first stage of proposed encryption algorithm encrypted images is constructed using secret key and chaotic function. In the next stage, these encrypted images are used as initial population for genetic algorithm. In this paper first time genetic algorithm has been applied on the watermark image for encryption with Fourier transform. The similar coefficient Normalized correlation (NC), Peak Noise to Signal Ratio (PNSR) and Correlation Coefficient (CR) are used to evaluate the transparency, robustness and security of algorithm. All the Experiment has been performed on MATLAB and results are provided to illustrate that the proposed approach is provide good results.

Keywords: Image Steganography, Genetic Algorithm, Secret Key, Chaotic Function, Fourier Transform.

1 Introduction

In the recent years, the use of internet services has become more pervasive and affordable than ever before. As a result, today millions of people communicate over the internet and huge volume of data transfer takes place via the plethora of services offered by the web. Despite the role of internet as an excellent worldwide publicized medium for data transmission and sharing, confidentiality of information over the internet demands a lot more. Data over internet may be stolen, intercepted, illegally modified, anonymized [1] or even destroyed by an adversary resulting in intellectual property rights infringement, data loss, data leakage and data damage. Hence, it is vital to maintain the privacy and confidentiality of data during its transit through the internet. To preserve the privacy and confidentiality of important data over the internet it must be provided with a metaphorical envelope such that its contents are revealed only to the intended receiver. Data hiding techniques such as steganography precisely aims at performing this task. There are so many steganographic techniques which are used for hiding data within image. In paper [2] optimized strategy is discussed that uses genetic algorithms to find the best mapping function between cover image and secret data. If iterations are big then this approach cannot be completed in polynomial time. In paper [3] comparison of high capacity filter with low capacity filter is discussed that produces steganography technique to embed the data. Paper [4] presented research work on data hiding in images by hybrid LSB substitution technique. It is the method of Optimal LSB substitution with OPAP. Paper [5] presented pixel-value differencing image steganography method to increase the capacity of the hidden secret information and to provide a stego-image. This method uses the largest difference value between the other three pixels close to the target pixel. Paper [6] proposed (N,1) Secret Sharing Approach Based on Steganography with Gray Digital Images method which contain an embedding and an extraction algorithm. This proposed scheme basically uses an Exclusive-OR (XOR) operation and a binary-to-gray code conversion. In paper [7] least significant bit (LSB) insertion technique is discussed. It is simple approach to embedding information in a cover image. In this method we embed 8th bits of data at (LSB) of each pixel in the cover image in order of 3, 3 and 2 respectively. The altered image is called stego-image. Paper [8] presented number of attacks on information hiding scheme and suggested improved embedding efficiency and public key steganography. Paper [9] proposes novel approach to develop a Secure Image based Steganographic Model using Integer Wavelet Transform. In paper [10] designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used. In Paper [11] discussed image steganography technique based on Integer Wavelet Transform (IWT). IWT converts spatial domain information to the frequency domain information. We use assignment algorithm for embedding secret data and for best matching between blocks. Analysis has been conducted by using number of different steganographic algorithm such as transform domain and spatial do-main etc. One method of common Steganography technique is to hide the secret message in the least significant bits of pixels of the cover image [12, 13]. The image quality of stego image achieved by applying the LSB technique is very closer to the original one. But the drawback is it cannot survive image processing manipulations [14]. One method

of LSB Steganography [15] involves manipulating the LSB plane from direct replacement of the cover image with message bits to some type of logical or arithmetic combination between two. Several examples of LSB techniques are found [16]. This technique achieves both high capacity and low perceptibility. But it is not very sophisticated and subject to extraction by unwanted persons. The DCT method [17] applies Discrete Cosine Transform to determine the high frequency areas and the message is embedded on these areas of digital image. Here more security can be achieved but the quality of stego image is poor. In DWT (Discrete Wavelet Transform) scheme [18] the digital image is separated into non overlapping blocks and the message is embedded on those blocks. The wavelet coefficients in low frequency sub bands are more important than the high frequency sub bands. Spatial domain techniques are easy to implement and have high payload as compare to transform domain technique. So we conclude that there are large number techniques for implementing image steganography but when we combine wavelet domain and cryptography together then it provides two levels of security and better quality image. It is quite impossible for hackers to steal the data.

With this motivation, in this paper the combined approach of image watermarking which have been used that satisfies two requirements i.e. imperceptibility and robustness have used combination of Lifting Wavelet Transform (LWT) and optimized chaotic based image encryption obtained through genetic algorithm to achieve the goal. As well as, the secret image is embedded directly on original image's LWT subbands. The encryption method have used for the stego image is combination of a genetic algorithm and a chaotic function and more secured [12]. Every time an encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced. The proposed system is the combination of our different modules, they are as follows:

1. Encryption of stego image using chaotic encryption with GA
2. Embedding the secret image into original image using LWT technique.
3. Extraction of the encrypted stego image from the original image.
4. Decryption of secret image.

The rest of the paper is organized as follows: In section 2 LWT based embedding process is discussed with the encryption and decryption algorithm. In section 3 the experimental results and discussion is discussed with some attacks. Finally, in section 3 discussed the conclusion and future work.

2 Proposed Methodology

In this section, embedding and extraction is done using LWT with the encryption and decryption process. In embedding phase, the cover image and secret images are taken as input, where the secret image is encrypted using GA-chaotic encryption algorithm and the output will be the stego image. After the embedding process, the extraction of the secret image is obtained by using the secret key and inverse Fourier transform.

2.1 Lifting Wavelet Transform

In this work, Lifting Wavelet Transform Technique is proposed and in the first level the wavelet transform decomposes the signal into windows of different resolutions. The wavelet transform is one of the tools for figure up functions, operators, or data into components of various frequencies. In the initial stage the input image is selected, image had better be transformed into a Gray Scale Conversion image. On applying the wavelet transformation technique, binary images are constructed in 5th bit coefficient of CH, CV and CD. The 2 D LWT image split the image into four sub bands LH, HL, HH (LH- Horizontal Edge Data, HL- Vertical Edge Data, HH- Diagonal Edge Data). This LWT watermarking can embed only in HL, LH, HH sub bands then by selecting the sub bands threshold frequency is noted. After 1st-level LWT decomposition, both secret image and cover image are decomposed into LL1, LH1 and HL1. The sub-bands coefficients of secret image are respectively embedded into the corresponding sub-bands of the cover image.

2.2 Genetic Algorithm

The genetic algorithm is optimization and search technique based on the principles of genetics and natural selection. GA composed of five components that are random number generator, fitness evaluation unit and genetic operators for reproduction, crossover and mutation operations. The initial population required at the start of the algorithm is a set of number strings generated by the random number generator. Each string is a representation of a solution to the optimization problem being addressed. Associated with each string is a fitness value (fval) computed by the Fourier transform. The reproduction operator performs a natural selection function known as "seeded selection". Individual strings are copied from one set to the next according to the fitness values, the higher the fitness value, the greater is the probability of a string being selected for the next generation. The crossover operator chooses pairs of strings at random and produces new pairs. The mutation operator randomly mutates or reverses the values of bits in a string. A phase of algorithm consists of applying the evaluation, reproduction, crossover and mutation operations. A new generation of solutions is produced with each phase of the algorithm.

2.3 Chaotic Map

The technology of image encryption that based on chaos is a code encryption technology that having developed in recent years. It looks upon the original image as the binary data stream that according to some encoded mode, then encrypts the image by using chaotic signal. The reason that Chaos is fit to image encryption is closely related to some of its dynamics characteristics. The chaotic signal has natural concealment, high sensibility to initial condition and to tiny perturbation motion, all those make the chaotic signal has an ability of long time unforeseeable. The security of this encryption system depends on the degree of approximation between signal and random numbers that produced by secret key stream generator (be chaotic). The secret key stream is getting higher security as it approaching random numbers, whereas it is easily to be broken through. Logistic map is an example among nonlinear equation which can be applied on the experiment mathematic studies triumphantly. Although it

is simple, it can embody all the nature of nonlinearity phenomenon. Its function is shown as Eq.

(1)

Where μ (3.57, 4), (0, 1). If μ =4 then the system is in chaotic state, and the sequence that the system produces now has the characteristics of randomness, erotic, and the sensibility to original value. And the range of it is (0, 1). All these characteristics can provide a very good maintenance for the image encrypt operation.

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

Figure.1. (a) The Lenna image pixels with 256 gray levels. (b) The Lenna image after applying the Cat map once. (c) The Lenna image after applying the Cat map two times. (d) The Lenna image after applying the Cat map nine times.

2.4 Hybrid GA-Chaotic Encryption Algorithm

1. Divide the input image into our equal quadrants as shown in figure 2.

(a) plain image (b) plain image divide to 4 equal parts

Figure 2(a) plain image (b) plain image divide to 4 equal parts

2. Apply chaotic unction logistic map to individually encrypt pixels o each quadrant of image. Steps for Encryption using chaotic function Fourier map.

a. First of all five pixels are selected from first row of each quadrant of image which is to be used to form the initial value. Now obtain encryption key from each quadrant to the image, in this way First member of population is formed.

b. Now to obtain Initial value of logistic map function, I have used following equation: (Decimal)

c. Given equation is then used to convert K into binary number as follows: (Binary)

d. Next Equation is used to determine initial value of chaotic map function as follows:

$$X_{0+k} = \frac{P_{1,1}\times 2^{39},\ldots,P_{2,1}\times 2^{31}\ldots.,P_{5,7}\times 2^{1},P_{5,8}\times 2^{0}}{2^{40}} \quad (2)$$

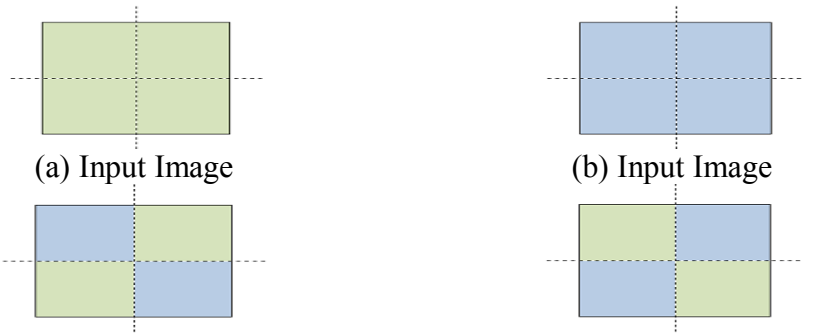
Where k=1,2,3,4

e. For each part of plain image step 2.b & 2.c is repeated

f. For encrypting pixels in each part f plain image following equation is used:

$$NewValue = round\ (X_{ik}\ \times 255) \otimes\ oldValue.$$

3. Genetic Optimization: In this algorithm Genetic algorithm uses crossover operation as shown in fig.3.



(a) Input Image (b) Input Image

(c)image after crossover (d)image after crossover

Figure 3. a, b) input images c, d)image after crossover

4. Correlation coefficient between pairs of adjacent pixels is used to obtain fitness function.

5. Selection of Best cipher image is on the basis of calculation of entropy and correlation coefficient. Image having highest entropy and lowest correlation coefficient is selected as best cipher image and then this image is send to the destination.

2.5 Embedding Procedure

In this section, we present our algorithm for gray scale images of dimension 256×256. The human eye has different visual sensitivity for different frequency. Low frequency component are basically used for embedding data. For higher security, Fourier transform is used through which image can be scrambled. To embed stego image into original image Alpha blending is used in which we decide alpha factor (range b/w 0 to 1.0). Let I be the original gray scale image of size $N \times N$ and secret data in form of image of size $M \times M$. Steps of embedding process are as follows:

Input: Cover Image(I_C), Secret Image (I_S)

Output: stego image (I_{stgno})

Step 1: Apply Fourier transform on I_C and I_S with secret Key (K_s) //*Scrambled Image I_{SS} will be obtained*//

Step 2: Apply 2DLWT on both I_C and Encrypted I_S //* This LWT watermarking can embed only in HL, LH, HH sub bands*//

Step 3: Extract the approximation coefficient of matrix A1 and A2 with HL, LH, and HH of level1 of the I_C and I_{SS}

Step 4: Apply Alpha Blending on I_C and I_{SS} which add approximation coefficients of I_C and I_{SS}.

Step 5: Apply 2D ILWT (inverse LWT) to get stego image I_{stgno}.

The fig.4 shows embedding process.

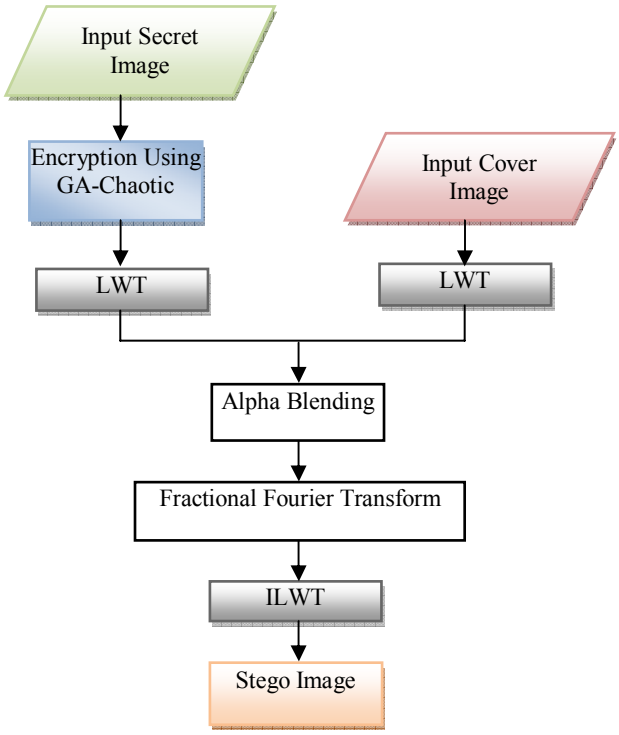


Figure 4. Embedding Procedure

2.6 Extraction Procedure

Steps of Extracting Process are as follows:

Input: Cover Image(I_C), stego image (I_{stgno})

Output: Secret Image (I_S)

Step1: Apply 2-D LWT of level 1 on both on I_{stgno} and I_C.

Step2: Apply Alpha Blending on both I_{stgno} and I_C.

Step3: Perform ILWT on separated wavelet coefficients and get scrambled secret image.

Step5: Take inverse Arnold of scrambled secret image.
Step6: Recovered secret image (which is almost in similar to secret image).

The fig.5 shows extraction process.

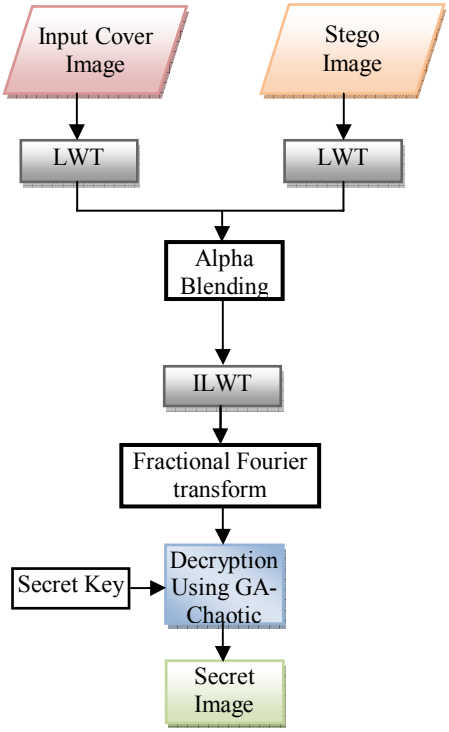


Figure 5. Extraction Procedure

3 Experimental Results And Discussion

The performance of purposed steganography method is implemented by using Matlab 7.10 version. The comparison parameters for performance evaluation are SC (Structural Content) and NC (Normalized correlation), PSNR, MSE and Cross Correlation. In this experiment, considered different gray scale images of size 256 x 256images like cameraman, circles, Goldhill, peppers, Lena and Light house. The six test images used for evaluation are given in Figure 6 (a) – (f).


(a) Elephant


(b) Cameraman


(c) Goldhill

(d) peppers

(e) Staple Remover

(f) Lena

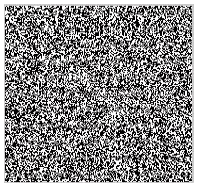
Figure 6. Original test images: (a) Elephant (b) Cameraman (c) Goldhill (d) Peppers (e) Staple Remover (f) Lena

For example, Figure 7(a) shows the cover image as Lena, 7(b) shows the secret image, 7(c) shows the Alpha Blending Image, 7(d) shows the Fractional Fourier Transform, 7(e) shows the Encrypted Image-chaos with optimized GA, 7(f) shows the Stego image, and 7(g) shows the recovered secret image. The experimental results shows that secret image and recovered secret image are exactly similar to each other as PSNR value is very high i.e. 78.35. A good encryption algorithm is one in which the correlation coefficients between pairs of encrypted adjacent pixels are at the least possible level. In Figure 8 correlation coefficient is -0.2419. So this algorithm also provides higher security. The comparison is done also on the basis of Embedding Time.

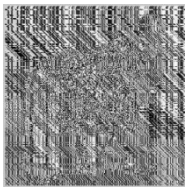
(a) Cover image

(b) Secret image

(c) Alpha Blending Image



(d) Applying Fractional Fourier Transform



(e)Encrypted Image-chaos with optimized GA encryption

(f) Stego image

(g) Recovered Secret image

Figure 7. Results after Applying the Proposed Model

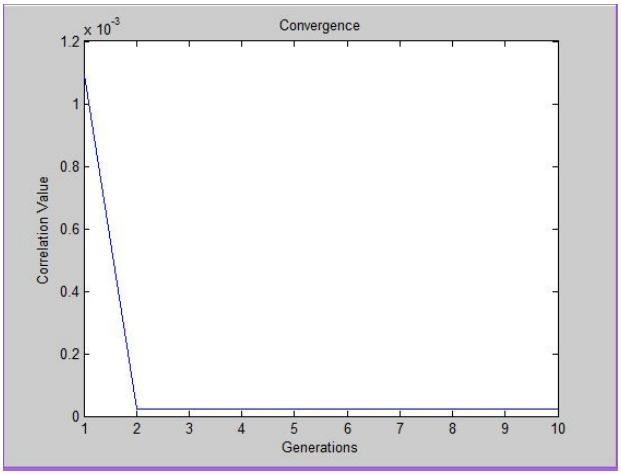


Figure 8. Correlation Coefficient

For various cover image and secret images, we have plotted the graphs for the PSNR, MSE, NC and embedding Time by values obtained in LWT based digital image steganography versus values obtained in DWT based digital image steganography, using the data from Table-1-2.

Table 1. MSE, PSNR, SC, NC and Time for Proposed GA-Chaotic Map with LWT

Cover image	Stego image	MSE	PSNR	SC	NC	Time (s)
Cameraman	Lena	0.0015	92.95	1.000	0.999	17
Lena	Goldhill	0.0014	93.96	1.000	0.997	18
Elephant	Peppers	0.0015	92.90	1.000	0.998	19
Goldhill	Staple Remover	0.0016	93.25	1.000	0.997	16
Peppers	Goldhill	0.0015	94.25	1.000	0.996	15
Staple Remover	Elephant	0.0013	92.50	1.000	0.995	18
Peppers	Lena	0.0014	93.95	1.000	0.997	16

Table 2. MSE, PSNR, SC, NC and Time for Proposed GA-Chaotic Map with DWT

Cover image	Stag image	MSE	PSNR	SC	NC	Time (s)
Cameraman	Lena	0.0018	88.50	1.000	0.995	15
Lena	Goldhill	0.0019	89.25	1.000	0.996	14
Elephant	Peppers	0.0017	87.75	1.000	0.997	14
Goldhill	Staple Remover	0.0018	88.50	1.000	0.995	15
Peppers	Goldhill	0.0016	89.75	1.000	0.997	16
Staple Remover	Elephant	0.0017	87.90	1.000	0.996	15
Peppers	Lena	0.0019	88.5	1.000	0.997	17

3.1 Objective analysis

Peak-Signal-To Noise Ratio

As a performance measure for image distortion due to embedding, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. The good visual quality of stego images (ie-images embedded with a secret image) is the most important property of steganography system because it is hard to detect by detectors. It is defined as:

$$\text{PSNR(dB)} = 10\log_{10}\left[\frac{255^2}{\text{MSE}}\right] \tag{3}$$

A large PSNR value means that the stego image is most similar to original image and vice versa. It is hard for the Human eyes to distinguish between original cover image and stego image when the PSNR ratio is larger than 30db.

Fig. 8 shows a graph of PSNR comparison between proposed approach and existing approach. It is clear from the graph that, at a particular time PSNR value is increased in proposed work. Both cannot have maximum at same time. In proposed method PSNR is 78.35 dB that is good which is higher than existing approach. This graph shows that the proposed method have good PSNR.

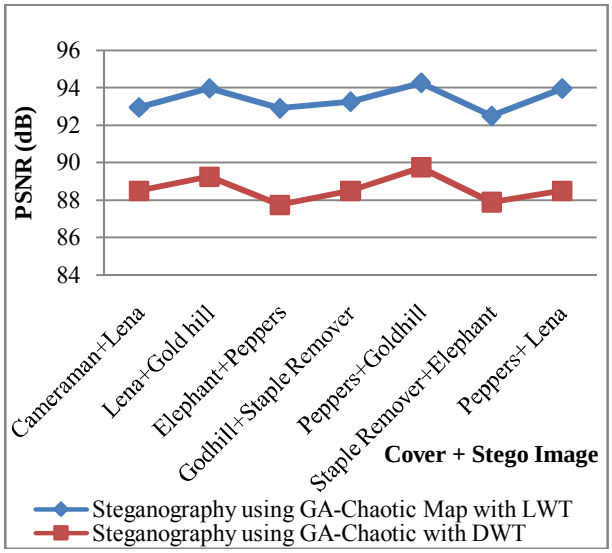


Figure.8. PSNR Comparison Results Mean Square Error

MSE is the mean square error representing the difference between the original cover image I_C sized M × N and the stego image I_S sized M × N.

$$\text{MSE} = \frac{\sum_{\forall(m,n)}[I_C(m,n) - I_S(m,n)]^2}{m \times n} \tag{4}$$

Fig. 9 shows a graph of MSE comparison between proposed approach and existing approach. It is clear from the graph that, at a particular time MSE value is

decreased in proposed method. Both cannot have maximum at same time. In proposed method MSE is 0.0018 that is good which is lesser than existing approach is. This graph shows that the proposed method have good PSNR.

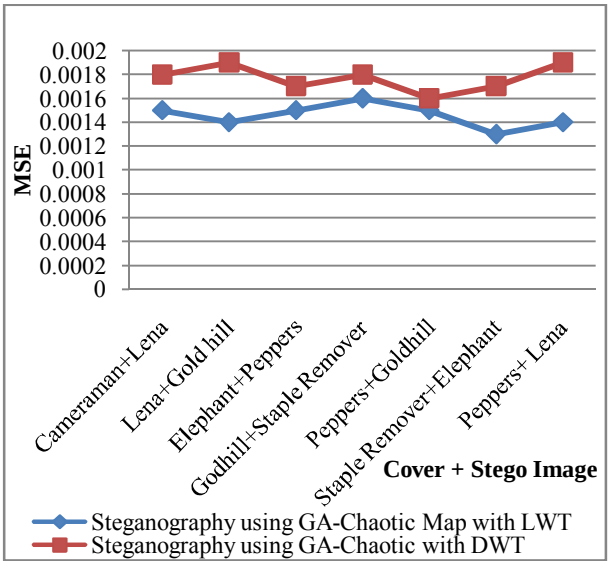


Figure.9. MSE Comparison Results Normalized Correlation (NC)

To test the robustness of the proposed work, NC parameter is utilized. To find robustness, after extracting the secret image, similar measurement of the extracted and the cover image are used as validation. It can be defined by NC as follows:

$$NC = \sum_{\forall(m,n)} \left(\frac{I_C(m,n) \times I_S(m,n)}{(I_S(m,n))^2} \right) \quad (5)$$

Structural Content (SC)

SC is also correlation based measure and measures the similarity between two images. Structural Content (SC) is given by the equation:

$$SC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} \left(w'(i,j) \right)}{\sum_{i=1}^{N} \sum_{j=1}^{N} w(i,j)} \quad (6)$$

Correlation Coefficient

The Correlation Coefficient of two identical size images also tells the similarity between the images. If the value of Correlation Coefficient is near to 1, then two images are very similar. If value is 1 i.e. both are same images. Here we use it to compute the similarity measurement of original secret image and recovered secret image, which is defined as

(7)

Where is the size of secret image, and represents the original and recovered secret images respectively.

Embedding Time

Fig.10 shows the processing time for embedding the information compressed using LWT based technique and DWT based technique. From the figure, it is noted that the processing tome for the proposed work is less when compared to existing approach. At the same time, the proposed method results in good visual quality of the stego image with perceptual invisibility of the secret image and high security.

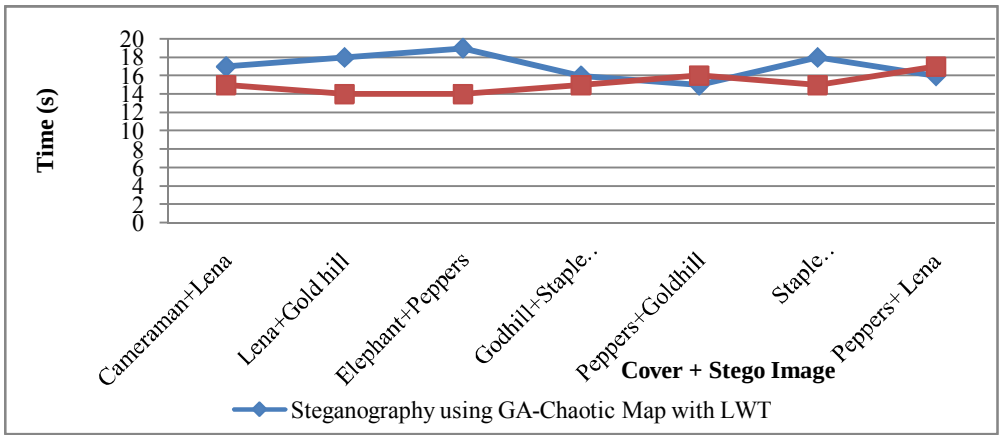
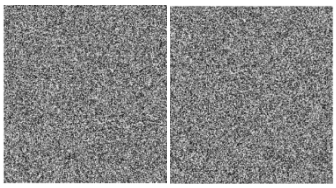


Figure 10. Time Comparison Results

3.2 Key analysis

A suitable encryption algorithm must be sensitive small changes in keys. Moreover, the key must be long enough to resist the attacks. To test the sensitivity of the key in the proposed method, first the cameraman image (Fig. 11a) was encrypted using the proposed method (Fig. 11b).

(a) Plain-image



(b) Encrypted images using user keys with 1-bit difference in each part

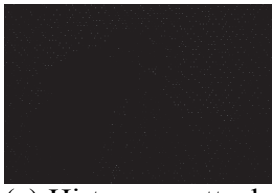
Figure 8. Results for Key analysis

3.3 Attack analysis

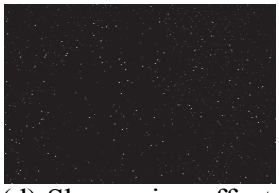
In order to measure the robustness of proposed scheme various attacks have been performed on test image. The scheme can withstand with number of attacks such as Gaussian white' noise of zero mean and 0.001 variance, contrast variations, histogram attack, sharpening attack and median filtering attack. Recovered watermark with accuracy rate and correlation coefficient are shown below in figure 5 for camera man.

(a) Contrast variation

(b)Addition of Gaussian white noise with 0 mean and 0.01variance



(c) Histogram attack



(d) Sharpening effect

Figure 9. Results for Attack analysis

4 Conclusion

In this paper, a new method has been suggested for encrypting images with a chaotic function and a genetic algorithm. In this method, the chaotic function is employed for initial encryption, and the genetic algorithm is used to improve the encryption process of the image. The main advantage in this paper is that is the genetic algorithms are used to encrypt images. This algorithm can be used with crossover operator to encrypt and paper, images. In this paper, an algorithm based on LWT based embedding and extraction is done. The security is enhanced by randomized nature of genetic algorithm and it also provides good robustness. The result obtained and proves that this method has high efficiency when compared with other methods for image encryption. Moreover, this method, compared to other methods mentioned in this has a higher resistance against common attacks in this area.

References:

[1] Kelly, Grant, and Bruce McKenzie. 2002, "Security, privacy, and confidentiality issues on the Internet." Journal of Medical Internet Research, 4 (2).

[2] Fard, A.M., Akbarzadeh-R., M., and Varasteh-A., F. 2009, "A new genetic algorithm approach for secure JPEG steganography", in Proc. of IEEE

International Conference on Engineering of Intelligent Systems ICEIS, 60(1), pp. 216-219.

[3] Ahuja, B., and Kaur, M., 2009), "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, 1(1),pp.510-514.

[4] Chang, C., and Tseng, H., 2009, "Data Hiding in Images by Hybrid LSB Substitution", Third International Conference on Multimedia and Ubiquitous Engineering, 3(2), pp- 360 – 363.

[5] Zhang, H., Geng, G., Xiong, C., 2009, "Image Steganography using Pixel-Value Differencing", Second International Symposium on Electronic Commerce and Security, pp- 109 - 112.

[6] Baekl, J., Kim, C., Fisherl, P.S., and Cha, H., 2010, "(N, 1) Secret Sharing Approach Based on Steganography with Gray Digital Images", IEEE International Conference, Wireless Communications, Networking and Information Security (WCNIS), pp-325 – 329

[7] Sutaone, M. S., and Khandare, M.V., 2008, "Image Based Steganography Using LSB Insertion Technique", IET International Conference on Wireless, Mobile and Multimedia Networks, pp-146 – 151.

[8] Ross J. Anderson and Fabien A. P. Petitcolas, 1998, "On the Limits of Steganography", IEEE Journal on selected areas in Communications, 16(4), pp- 474 - 481.

[9] Bhattacharyya, S., Kshitij, A.P., Sanyal, G., 2010, "A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform", International Conference on Recent Trends in Information, Telecommunication and Computing,pp- 173-178.

[10] Ren, W., Miao, Z., 2010, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", IEEE Second International Conference on Modeling, Simulation and Visualization Methods, pp-221-225.

[11] Raftari, N., 2012, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", Sixth Asia Modeling Symposium., pp.523-527

[12] Petitcolas, F.A.P., Anderson, R.J. and Khan, M.G. 1999, "Information hiding – A survey", IEEE Proceedings, 87(7), pp.1062-1078.

[13] Chan.C.K., and Cheng.L.M., 2003, "Hiding data in image by simple LSB substitution". Pattern Recognition, pp. 469 – 474.

[14] Fridrich, P.M, Goljan, M., Du, R. 2011, Detecting LSB Steganography in color and grayscale images, IEEE Multimedia Special Issue on Security, pp.22–28.

[15] Thangadurai, K., Sudha devi, G. 2014, "An analysis of LSB Based Image Steganography Techniques", International conference on Computer Communication and Informatics (ICCCI),IEEE, pp.1-4.

[16] Arafat Ali, H., 2007, "Qualitative Spatial Image Data Hiding for Secure Data Transmission". GVIP Journal, 7(1): pp 35-43.

[17] Anderson, R.J., and Petitcolas, F.A.P., 2004, "On the Limits of Steganography", IEEE Journal on selected Areas in Communication, 16(4), pp.474-481.

[18] Chin-Chen Chang, Yung-Chen Chou, 2006, "Quantization Index Modulation using Vector Quantization with DWT based State-Codebook search", International conference on Intelligent Information hiding and Multimedia, pp. 549- 554.