IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013), PP 49-54
www.iosrjournals.org

High Security Cryptographic Technique Using Steganography and Chaotic Image Encryption

Arun A.S.[1], George M. Joseph[2]

[1]*M.Tech Student, Department of Electronics and Communication Engineering, SCT College of Engineering, Kerala, India*

[2]*Assistant Professor, Department of Electronics and Communication Engineering, SCT College of Engineering, Kerala, India*

Abstract : *This paper proposes a novel cryptographic technique that exploits the advantages of two important techniques – steganography and chaotic image encryption. Steganography is the technique of hiding the message within a cover media. Once the message is embedded within the cover image, it is encrypted using triple-key chaotic image encryption. So altogether this method provides a four-layer security to the original message. Various analyses were done and the results of the experiments are very encouraging and in future, this method can be extended to support media other than images.*

***Keywords** - Cryptography, Colour Image, Steganography, Encryption, Chaotic logistic map.*

I. INTRODUCTION

With the advent of internet and other communication methods, the security of the data being transmitted has become important. One of the most important methods for transmitting a data securely is to hide the data within another media and to transmit the cover media. The cover media can be text, image, audio or video. By doing so, a third person is not aware that the transmitted media contains an embedded message. Once the steganography is done, the resulting cover image which contains the embedded message is encrypted using chaotic image encryption technique which uses three keys. For decryption, not only all the keys are required but also they must be entered in the same order as entered for encryption.

II. IMAGE BASED STEGANOGRAPHY

Steganography[1] is the technique of hiding information within any media. The commonly used media are plaintext, images, video, audio and IP datagram. In this paper, we are concerned with image steganography only. Digital image steganography is the most widely used technique of steganography. The existence of large number of digital images in the internet further allows us to use this technique for secure data transmission through the internet. The message that can be embedded in the digital images includes plaintext, ciphertext, other images and any other media which can be encoded as a bit stream. The inability of the human visual system (HVS) to identify minor variations in the luminance of colour vectors is being exploited by the steganography techniques.

All the digital images can be represented as a collection of pixel values. Colour images will have three colour planes – red, green and blue. Each pixel will have optical characteristics like brightness, chroma, hue, saturation etc. Each pixel value can be digitally represented in binary form. For example, a 24bit colour image will have 8 bits each of red, green and blue values at each pixel position. Since 8 bits are used to represent each value, it can have 28 values each of red, green and blue, ranging from 0 to 255. The human visual system is insensitive to the changes in the least significant bits in the image, which enables the user to hide the message in the least significant bits without being identified by an attacker.

The cover image for this technique can be either of uncompressed formats like bitmap or of compressed formats like JPEG. In both formats, the LSBs are modified for hiding the message. If large cover images are used, even audio files can be embedded in them without affecting the quality of the images.

III. IMAGE ENCRYPTION

Encryption is the process of encoding the message in such a way that an attacker will not be able to read it. The media used for encryption can be plaintext, images, audio or video. In this paper, we consider only image encryption. Some of the existing block cipher algorithms are: Data Encryption Standard (DES)[2],Advanced Encryption Standard (AES)[3] and International Data Encryption Algorithm (IDEA)[4].

The problem with these algorithms is that they are not suitable to encrypt bulky data due to their intensive computational costs. Computations can be accelerated by using additional hardware, but it further increases the cost of the system.

In order to overcome these problems, we can make use of chaotic image encryption technique[5]. Chaotic systems are non-linear systems with high sensitivity to initial conditions. Any change in the initial conditions will result in compounding errors in the prediction of the system's future behaviour. To predict the behaviour of such systems, one must have sufficient knowledge about the initial conditions. Some of the important properties of a chaotic system are[6]:

(i) Deterministic, so that they are characterised by mathematical equations.

(ii) Unpredictable and non-linear, and highly sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes.

(iii) Appear to be random and disorderly but beneath the random behavior there is a sense of order and pattern.

The logistic map[7], parameterised by μ, which maps [0,1]→[0,1] is the simplest 1D map which exhibits complicated behaviour.

$$Xi = \mu X_{i-1} (1 - X_{i-1}) \quad (1)$$

(1) can be represented using the bifurcation diagram as shown in Fig.1.

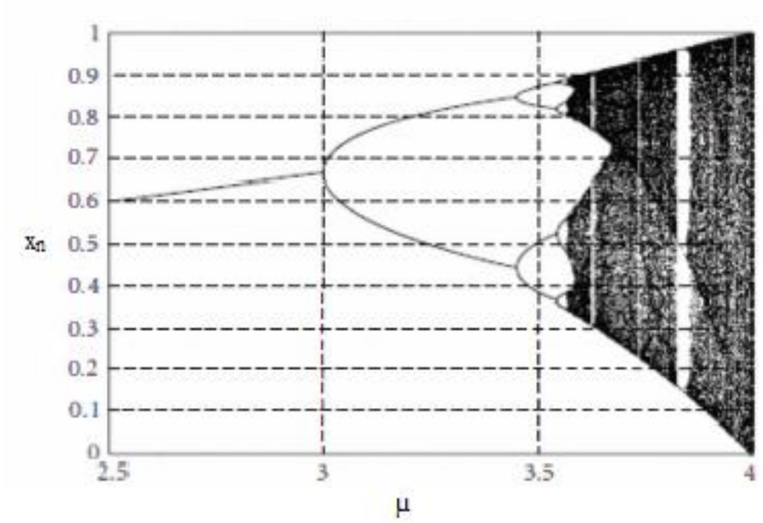

Fig. 1: Bifurcation diagram of 1D logistic map

The horizontal axis of the plot represents the bifurcation parameter μ whereas the vertical axis represents the possible long-term population values of the logistic function. As the value of μ increases bifurcation of the map occurs. From the plot we can see that as the value of μ is close to 4, many bifurcations has occurred and the amount of chaos in the system is very high. We use the same principle in achieving chaotic image encryption.

IV. PROPOSED SYSTEM

The proposed system for cryptography achieves the high security by making use of two powerful techniques- steganography and image encryption. The steganography technique used in this system makes sure that no collisions occur while selecting pixels for embedding the message, thereby improving the speed and efficiency of the system. Once the message is embedded onto the cover image, it is encrypted using chaotic image encryption technique. The proposed system model is shown in Fig.2.

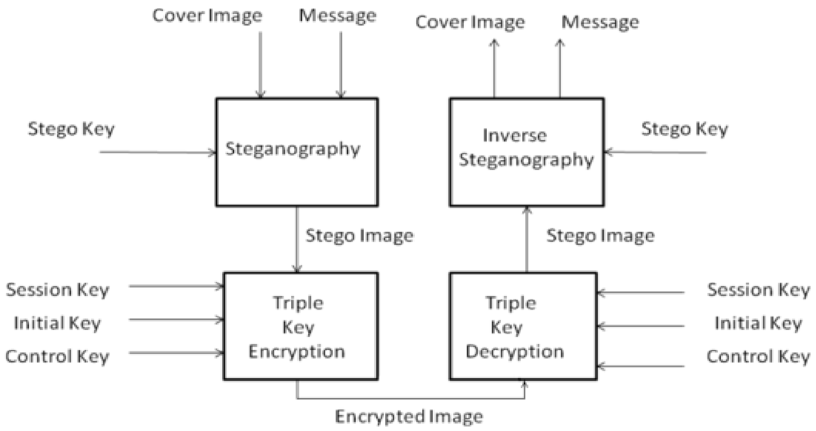

Fig.2: Proposed System

4.1 Method of Encryption

For achieving encryption, steganography is carried out first and then the resulting image is encrypted using chaotic image encryption technique. The cover image used for encryption can be of any format and size.

4.2 Steganography

The steganography system takes in three inputs- cover image, message which is to be embedded and the key for steganography. The message as well the key can contain alphabets, digits and special characters. The message which is read from the user is converted to the binary value of its ASCII code. The key is used to find the pixel positions for embedding the message. While selecting the pixel positions, the system makes sure that no collisions occur. Had there been any collisions, there will be loss of data which will reduce the efficiency of the system. Once the pixel positions are selected, the message in the binary form is embedded on to the image. While embedding the message, the binary stream of the ciphertext is used to replace lowest 2 bits of red plane, lowest 1 bit of green plane and lowest 3 bits of blue plane. Selecting different number of bits from each plane is in accordance with the sensitivity of the human visual system(HVS)[8] to different colours. By doing so, we can embed total of 6 bits at each pixel position without being detected by the human eye.

4.3 Chaotic Image Encryption

Once the message has been embedded in the image, the stego-image is given to the chaotic image encryption system[6]. This system requires 3 keys for encryption - an 80 bit session key, an initial parameter key and a control parameter key. The various steps for encryption are as given below:

Step 1: The Stego-image is converted to its equivalent binary image matrix form. Let the image contains R rows and C columns. Then total number of pixels in the image is R × C = N pixels. The image is first converted into a 1-dimensional array of size N × 1 and then each pixel is converted into 8-bit binary form. The resulting binary image matrix can be represented as follows:

$$P_{nk} = \begin{bmatrix} p_{11}\ p_{12} & & p_{18} \\ p_{21}\ p_{22} & \cdots & p_{28} \\ \vdots & \ddots & \vdots \\ p_{N1}\ p_{N2} & \cdots & p_{N8} \end{bmatrix} \qquad (2)$$

Step 2: The next step of triple-key encryption is to compute the initial parameter key which will act as the initial value of the chaotic logistic map. To compute the initial parameter key, the user is asked to enter two keys – an 80 bit session key and a second key whose value is in between 0 and 1. The 80 bit session key can be entered in the form of 20 hexadecimal characters.

$$K = k_1k_2k_3\ldots k_{20} \qquad (3)$$

These hexadecimal characters are converted into the equivalent binary form. A block k of 24 bits, say, $k_5k_6k_7k_8k_9k_{10}$, is extracted from the session key K. Any number of bits can be extracted depending upon the requirement of the chaos that needed to be introduced into the system.

Compute X_{01} as given in (4):

$$X_{01} = (k_{51} \times 2^0 + \ldots + k_{54} \times 2^3 + k_{61} \times 2^4 + \ldots + k_{64} \times 2^7 + \ldots + k_{10} \times 2^{20} + \ldots + k_{104} \times 2^{23}) / 2^{24} \qquad (4)$$

Now, the initial parameter key, X(1) is computed when the user enters key X_{02} using (5).

$$X(1) = (X_{01} + X_{02}) \bmod 1 \qquad (5)$$

Since, X(1) is the remainder of the division by 1, it will be a value between 0 and 1.

Step 3: Once the keys are generated, the next step is to generate the chaotic sequence that follows the 1D logistic map. The Chaotic sequence $X_1\ X_2\ X_3 \ldots X_N$ is generated as in (6).

$$X_i = \mu\, X_{i-1}\,(1 - X_{i-1}) \qquad (6)$$

The initial parameter key X(1) is used as the initial value for the generation of the chaotic sequence. The control parameter key µ is entered by the user. Since all the values in the chaotic sequence X_i are between 0 and 1, it must be normalized to the image scale, between 0 and 255.
For normalization (7) can be used:

$$Xi = \frac{xi - \min(Xi)}{\max(Xi)} \times 255 \qquad (7)$$

Now, X_i is an array of size $1 \times N$. After normalizing the chaotic sequence, all the values in X_i are converted to their equivalent binary representations. Each pixel value is represented as 8-bit binary number so that an $N \times 8$ matrix B is obtained.

$$B = \begin{bmatrix} b_{11} b_{12} & & b_{18} \\ b_{21}\ b_{22} & \cdots & b_{28} \\ \vdots & \ddots & \vdots \\ b_{N1}\ b_{N2} & \cdots & b_{N8} \end{bmatrix} \qquad (8)$$

Step 4: Next step is to construct the neural network using the values of the matrix B. Both weight matrix and bias matrix are calculated using the matrix B. N weight matrices, each of size 8 x 8, are computed by mapping each row of the matrix as follows:

$$W_{ik} = \begin{cases} 0, & i \neq k \\ 1 - 2b_{nk}, & i = k \end{cases} \qquad (9)$$

where i and k vary from 1 to 8 and n varies from 1 to N. Weight matrix W is a diagonal matrix whose diagonal contains only values ±1. The diagonal element is 1 if the corresponding bit in chaotic sequence is zero and -1 if the corresponding bit is one.
The bias matrix of size 1 x 8 is computed by mapping each row of B as given below:

$$\theta_j = \begin{cases} 1/2, & b_{nk} = 0 \\ -1/2, & b_{nk} = 1 \end{cases} \qquad (10)$$

Therefore θ_j contains values ± 1/2.

Step 5: Once the weight matrix and bias matrix are computed, then the encryption process can be carried out. The cipher bit p'_{nk} corresponding to each bit p_{nk} is computed as in (11) :

$$p'_{nk} = \text{sign}\left(\sum_{i=0}^{7} w_{ik}\, p_{nk} + \theta_k\right) \qquad (11)$$

(11) can be simplified as given below

$$p'_{nk} = p_{nk} \oplus b_{nk} \qquad (12)$$

These steps are repeated for all the rows of B to obtain the encrypted matrix

$$P'_{nk} = \begin{bmatrix} p'_{11}\ p'_{12} & & p'_{18} \\ p'_{21}\ p'_{22} & \cdots & p'_{28} \\ \vdots & \ddots & \vdots \\ p'_{N1}\ p'_{N2} & \cdots & p'_{N8} \end{bmatrix} \qquad (13)$$

This binary matrix is converted to its decimal equivalent with values ranging from 0 to 255 and is converted to a two dimensional array of size R × C. The red, green and blue plane of the colour images are encrypted separately. The output of this process gives the encrypted image which contains the original message.

4.4 Decryption Process

Decryption consists of two processes - triple key decryption and inverse steganography. The encrypted image is first decrypted using triple key decryption for which the system requires three keys - 80 bit session key, initial parameter key and the control parameter key. The same keys which were used for encryption are required for the decryption process also. Once triple key decryption is done, the resulting image is given to the inverse steganography system which uses the stego-key to find the location of the pixels where the message was originally embedded. Once the positions are calculated, the message bits are extracted and converted back to alphanumeric form and displayed.

V. Observations and Results

Simulation was done in MATLAB and efficiency of the proposed method was calculated. The proposed system was tested in images of different sizes and formats by using different combinations of keys. The results of the simulation are presented in the paper. Fig. 3 shows the original image, image after steganography and the final encrypted image.

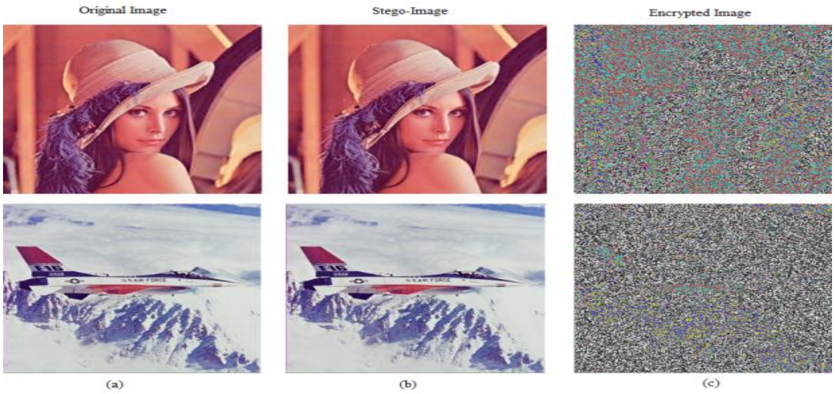

Fig 3: (a): Original Image. (b) Image after steganography (c) Image after encryption

From the simulation diagrams of Fig.3, we can observe that after the first process of steganography, the resulting does not differ from the original image. So visually it is not possible to identify the existence of the embedded message in the image. From the result of the second process of the proposed method, the chaotic image encryption, it can be inferred that the amount of confusion and diffusion introduced by the method is sufficient enough that the original image can never be identified from the encrypted image without the knowledge of the keys.

This can further be proved from the Peak-Signal-to-Noise-Ratio (PSNR) between final images and original images as given in Table 1. It can be seen that the PSNR values after steganography are very high which implies that the amount of noise introduced in the image as a result of steganography is very low. However, the PSNR values after encryption is very low. These low values are the results of the chaos introduced in the image. So it can clearly be stated that the original image can never be identified by mere inspection.

Figure	**Format**	**Size**	**PSNR after Steganography (dB)**	**PSNR after Encryption (dB)**
Cablecar	Jpg	256x240	65.3882	4.8790
Sailboat	Jpg	256x256	65.6274	5.1705
Goldhill	Bmp	300x256	66.0808	5.0659
Peppers	Bmp	400x400	69.4901	5.9828
Lena	Jpg	512x512	71.6319	5.1773

Table 1. Comparison of psnr values of various images after encryption using the proposed system

We are providing another analysis based on the histogram of the image. Histogram of an image gives the relative frequency of occurrence of each pixel value in an image. Since we are considering colour images in this paper, the histogram of red, green and blue plane of the images are considered separately. The histograms of the original image show non-uniform distribution whereas the histograms of the encrypted image show a uniform distribution of pixels. Due to this uniform distribution, it will be extremely difficult for an attacker to extract the original information from the image without the keys.

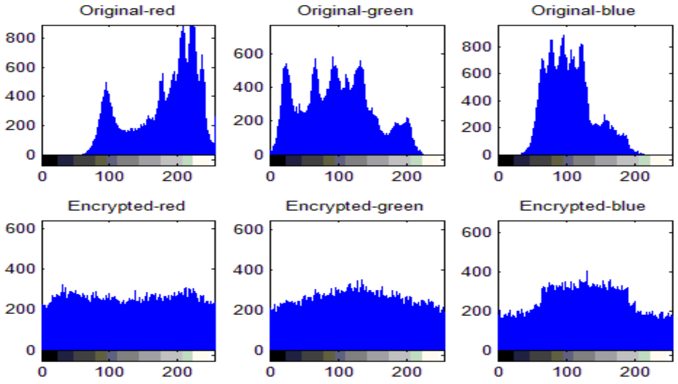

Fig. 4: Histogram Analysis

VI. CONCLUSION

In this paper, we presented a novel system for encryption which makes use of steganography and triple-key chaotic image encryption. The system can work with images of various formats and sizes. Due to the presence of four keys, this system provides very high level of security. We have presented the results of various analyses and the results are very encouraging. However, the used algorithms can be improved in the future to get accurate results.

REFERENCES

[1] F. Shih, *Digital Watermarking And Steganography-Fundamentals And Techniques*(USA: CRC Press, 2008).

[2] D. Coppersmith, “Data encryption standard and its strength against attacks”, *IBM J. Res. Develop*, vol. 38 no. 3 may 1994.

[3] M. Zeghid et al., "A modified AES based algorithm for image encryption", *International Journal of Computer Science and Engineering,* 1(IX2006) 70-75.

[4] Xuejia Lai and James L. Massey, “A Proposal for a New Block Encryption Standard”, *Eurocrypt* 1990, pp389–404

[5] N. K. Pareek, Vinod Patidar, K. K. Sud; "Image encryption using chaotic logistic map", *Image and Vision Computing* 24 (2006) 926-934.

[6] G. Srividya, P. Nandakumar, "A Triple-Key chaotic image encryption method," *Communications and Signal Processing (ICCSP), 2011 International Conference on* , pp.266-270, 10-12 Feb. 2011.

[7] C.W. Wu and N.F. Rulkov, "Studying chaos via 1-Dmaps-a tutorial," *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10,* pp. 707-721, 1993.

[8] T. Fei, L. Shaojun, "Research and implementation of information hiding based on RSA and HVS," *E -Business and E -Government (ICEE), 2011 International Conference on* , pp.1-4, 6-8 May 2011.