American Journal of Signal Processing 2014, 4(1): 24-33
DOI: 10.5923/j.ajsp.20140401.04

Stego- Cryptography Using Chaotic Neural Network

N. K. Kamila[1,*], Haripriya Rout[2], Nilamadhab Dash[2]

[1]Department of Computer Science and Engineering, C V Raman College of Engineering, Bhubaneswar, India
[2]Department of Information Technology, C V Raman College of Engineering, Bhubaneswar, India

Abstract Information protection is now a crucial problem and good solution to this problem is cryptography and steganography. The content of message is kept secret in cryptography, where as in Steganography; a message is embedded in a cover image. In our proposed work a system is developed in which LSB Steganography and Cryptography using chaotic neural network is combined together to provide high security to the message during communication in an unsecure channel. In LSB Steganography taking advantage of the way the human eye perceives images, the technique involves of replacing the N least significant bits of each pixel of a container image with the data of a hidden message. Cryptography based on chaotic neural network is used because of its noise like behaviour which is quite significant for cryptanalyst to know about the hidden information as it is hard to predict. Thus the information is being kept secret. In this work we have considered the advantages of both the concepts and developed a model in which initially a message is embedded in a gray scale image using LSB steganography and then the stegoimage is encrypted using chaotic neural network to provide high security to the message. The whole process is implemented using MATLAB. The simulation results show the robustness of the technique.

Keywords Cryptography, LSB Steganography, Chaotic Neural Network

1. Introduction

Cryptography and steganography are two popular techniques for secret communication. The content of message is kept secret in cryptography, where as in steganography message is embedded in to the cover image. In this paper a system is developed in which cryptography and steganography are used as integrated part along with newly developed enhanced security model. In our proposed model initially a message is embedded in a gray scale image using LSB steganography, and then the stegoimage is encrypted using chaotic neural network to provide high security to the message.

Two other technologies closely related to steganography are watermarking and fingerprinting. Watermarking is a protecting technique which protects (claims) the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. Therefore, the goal of steganography is to embed secret messages in the cover image while the goal of watermarking is the cover object itself.

The rest of the paper is organized as follows: related works in section 2, types of steganography and its technique in Section 3, section 4 describes cryptography using chaotic neural network, Cryptographic Algorithm using Chaotic Neural Network has been discussed in section 5, section 6 illustrates Algorithm for LSB Steganography , Proposed problem description with algorithm is presented in section 7 and the simulation result is analysed in section 8. The paper is observed by a conclusion in section 9.

2. Related Works

The most of today's steganographic systems use images as cover object because people often transmit digital images over email and other communication media. Several methods exist to utilize the concept of Steganography as well as many algorithms have been proposed in this regard by many researchers.

Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover object. In LSB steganography, the LSB of a pixel is replaced with M bits[1, 2].

Hiding data in the features of images is also an important technique which uses the LSB Crypto Steganography using linear algebraic equation modification concept. In this method, to hide data in an image the least significant bits of each pixel is modified sequentially in the scan lines across the image in raw image format with the binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An attacker can easily recover the hidden message by repeating the process[2, 3].

An interesting application of steganography and cryptography has been developed by Sutaone, et al.[4] where a steganography system is designed for encoding and

* Corresponding author:
nkamila@yahoo.com (N. K. Kamila)
Published online at http://journal.sapub.org/ajsp

decoding a secret file embedded into an image file using random LSB insertion method. In their method, the secret data are spreaded out among the cover image in a seemingly random manner. The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message is laid out.

The next interesting application of steganography has been developed by Miroslav Dobsicek, where the content is encrypted with one key and can be decrypted with several other keys. In this process, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information[5].

In 2007, Emam proposed an algorithmic approach to obtain data security using LSB insertion steganographic method[6]. In his approach, high security layers have been proposed to make it difficult to break through the encryption of the input data and confuse the steganalysis process too.

There is also a good method proposed by Sahoo et.al.[7] in 2008. Their proposed method works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography. And due to this reason they have used a stego key for the embedding process.

Information hiding is an old but interesting technology [11]. Steganography is a branch of information hiding in which secret information is camouflaged within other information. A simple way of steganography is based on modifying the least significant bit layer of images, known as the LSB technique[12]. The LSB technique directly embeds the secret data within the pixels of the cover image. In some cases (Fridrich et al.[13]) LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value. Habes[14] proposed a new method (4 least Significant) for hiding secret image inside carrier image. In this method each of individual pixels in an image is made up of a string of bits. He has considered the 4-least significant bit of 8-bit true colour image to hold 4-bit of the secret message /image by simply overwriting the data that was already there.

In 2010 Ilker Dalkiran, et al. proposed a model in which different gray scale images are encrypted and decrypted using chaotic dynamics, produced from artificial neural network[15].

In 2009 Vikas Gujral, et al.[16] proposed a model where cryptography was achieved by a chaotic neural network having its weights given by a chaotic sequence.

A good method proposed by Kamila, et al.[17] in 2011 a system was developed in which cryptography and steganography are used as integrated part to enhance information security significantly.

Many authors have used cryptography, steganography and chaotic neural network in different ways for their research works[18, 19, 20, 21, 22] so far.

3. Types of Steganography and Its Techniques

Based on cover medium there are three types of steganography such as i) Image Steganography ii) Audio / video Steganography iii) Text Steganography.

Image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image[6]. Image steganography has come quite far in recent years with the development of fast, powerful graphical computers. Images are used for steganography in following ways. The message in encrypted form or in the original form is embedded as the secret message to be sent into a graphic file. This results in the production of what is called a stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey. The stego-image is then transmitted to the recipient. The recipient extracts the message from the carrier image. The message can only be extracted if there is a shared secret key between the sender and the recipient.

Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, is retrieved using a key similar to (or, in most cases, the same as) the one that was employed during the hiding phase. Audio and multimedia data embedding is a useful means for transmitting covert battlefield information via an innocuous cover audio signal.

Text steganography is considered to be the most difficult kind of steganography due to lack of redundancy in text as compared to image or audio but still has smaller memory occupation and simpler communication. The method that could be used for text steganography is data compression. Data compression encodes information in one representation into another representation. The new representation of data is smaller in size. One of the possible schemes to achieve data compression is Huffman coding. Huffman coding assigns smaller length code words to more frequently occurring source symbols and longer length code words to less frequently occurring source symbols.

Different steganography techniques are LSB, Masking, and Filtering and transform technique. In LSB least significant bit insertion is a common, simple approach to embedding information in a cover image[8]. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data[9]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, of which binary representation is

11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. The human eye cannot perceive these changes, thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [10].

A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover object, but the cover-object is degraded more, and therefore it is more detectable. Other variations on this technique include ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid colour. Changes in these pixels are then avoided because slight changes would cause noticeable variations in the area.

Other techniques of steganography include spread spectrum steganography, statistical steganography, distortion, and cover generation steganography etc.

4. Cryptography Using Chaotic Neural Network

Chaos is statistically indistinguishable from randomness, and yet it is deterministic and not random at all. Chaotic system will produce the same results if given the same inputs, it is unpredictable in the sense that you cannot predict in what way the system's behaviour will change for any change in the input to that system. A random system will produce different results when given the same inputs.

Chaotic system

Chaotic systems are sensitive to initial conditions, system parameters and topological transitivity and these properties are also remarkable for cryptanalysts. Noise like behaviour of chaotic systems is the main reason of using these systems in cryptology. However some properties of chaotic systems such as synchronization, fewness of parameters etc. cause serious problems for cryptology.

Chaotic neural network

Chaotic neural networks offer greatly increase memory capacity. Each memory is encoded by an Unstable Periodic Orbit (UPO) on the chaotic attractor. A chaotic attractor is a set of states in a system's state space with very special property that the set is an attracting set. So the system starting with its initial condition in the appropriate basics, eventually ends up in the set. The most important, once the system is on the attractor nearby states diverge from each other exponentially fast, however small amounts of noise are amplified.

In a chaotic neural network for digital signal encryption and decryption, initially a binary sequence is generated from a chaotic system, the biases and weights of neurons are set. The network's features are high security and no distortion.

The basic ideas behind it can be classified into three major types such as:

- Position permutation - The position permutation algorithms scramble the positions of original data.
- Value transformation - The value transformation algorithms transform the data value of the original signal.
- The combining form - Finally, the combining form performs both operations.

The encryption scheme belongs to the category of value transformation. Based on a binary sequence generated from the 1-D logistic map, the biases and weights of neurons are set in each iteration.[18]

5. Cryptographic Algorithm Using Chaotic Neural Network

Suppose any message of length M needs to be encrypted using chaotic neural network then the algorithm is as follows.

Step 1:

Set the value of the parameter M.

Step 2:

Determine the parameter, μ and the initial point x(0) of the 1-D logistic map.

Step 3:

Evolve the chaotic sequence x(l), x(2), ... , x(M) by x(n+l) = μ x(n)(l-x(n)), and create

b(0), b(l), ..., b(8M-1) from x(l), x(2), ..., x(M) by the generating scheme that 0.b(8m-8)b(8m-7) ….. b(8m-2)b(8m-l) … is the binary representation of x(m) for m = 1, 2,. . ., M.

Step 4:

FOR n: 0 TO (M - 1) DO

$$\text{Let } g(n) = \sum_{i=0}^{7} d_i \times 2^i ; \tag{5.1}$$

For i= 0 TO 7 DO

$$w_{ji} = \begin{cases} 1 & \text{if } j = i \text{ and } b(8 \times n + i) = 0, \\ -1 & \text{if } j = i \text{ and } b(8 \times n + i) = 1, \\ 0 & \text{if } j \neq i, \end{cases} \tag{5.2}$$

$$J \in (0,1,2,3,4,5,6,7)$$

$$\theta_i = \begin{cases} -\frac{1}{2} & \text{if } b(8 \times n + i) = 0, \\ \frac{1}{2} & \text{if } b(8 \times n + i) = 1, \end{cases} \tag{5.3}$$

END
For i= 0 TO 7 DO

$$d_i' = f(\sum_{i=0}^{7} w_{ji} \times d_i + \theta_i), \quad (5.4)$$

where f(x) is 1 if x >=0 and 0 otherwise.
END

$$g'(n) = \sum_{i=0}^{7} d_i' \times 2^i. \quad (5.5)$$

END

Step 5:

The encrypted signal g' is obtained and the algorithm is terminated.

The decryption procedure is the same as the above one except that the input signal to the decryption CNN should be g'(n) and its output signal should be g''(n).

6. Algorithm for LSB Steganography

Least Significant Bit (LSB) technique is used for message hiding which replaces the least significant bits of pixel selected to hide the information.

Step 1:

Input the message to be embedded in binary form along with the cover image.

Step 2:

Convert each pixel of the cover image into 8 bit binary form.

Step 3:

Store each bit of the message in the least significant bit of the pixel of the binary cover image until all the bits of the message are stored.

Step 4:

The binary stego image is converted to stego image with decimal intensity values for each pixel.

Step 5:

Histogram of original and stego image are generated and compared.

7. Proposed Problem Description with Algorithm

In the proposed work at the sender end the plain text is embedded in a gray scale cover image by LSB Steganography technique[1]. Subsequently the produced stego image is encrypted using chaotic neural network. Then the encrypted image is transmitted to the recipient. The recipient decrypts the encrypted image using same chaotic neural network to extract the stego image. From the stego image the original plain text message is extracted.

8. Simulation Result and Analysis

In this section, some experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 7 program on Windows 7 platform. The proposed high secured system for cryptography is tested by taking different messages with different gray scale cover images.

In our proposed work at the sender end a plain text message / string is converted to its corresponding integer value, for a to z we are taking values as 1 to 26. Then each integer value is converted to its corresponding binary equivalent. Similarly the cover image is converted to binary equivalent. Here we can take both colour or gray scale image as cover image but if we are taking colour image it has to be converted to gray scale image.

According to LSB steganography 8^{th} bit of 1^{st} pixel of gray image contains 1^{st} bit of text message, 8^{th} bit of 2^{nd} pixel of gray image contains 2^{nd} bit of text message and so on till all the bits of text message is embedded in the gray scale image.

So here we can keep maximum of 256 characters in a 256 x 256 gray scale image which will not affect the cover image. Though we can keep more text message but it will degrade the gray scale image quality which is not preferable.

Now the stego-image is converted to its integer equivalent after that the image is given as input to Chaotic Neural Network to get corresponding encrypted image.

At the receiver end just the reverse process takes place to get the original plaintext from the encrypted image.

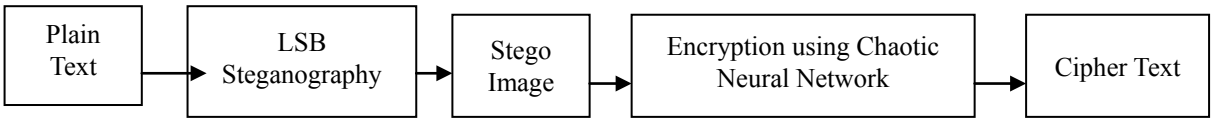

Figure 1. Encryption at sender end

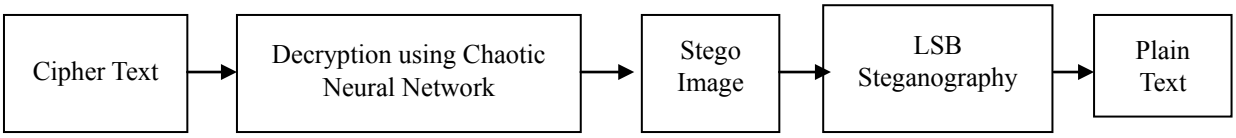

Figure 2. Decryption at receiver end

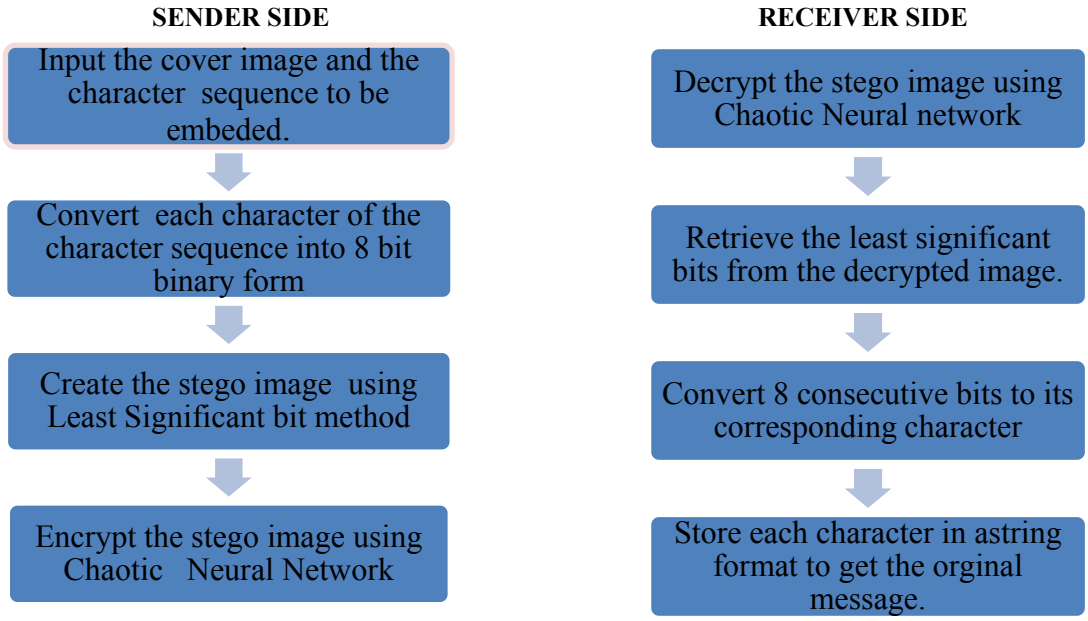

Figure 3. Stego-Cryptosystem using chaotic neural network

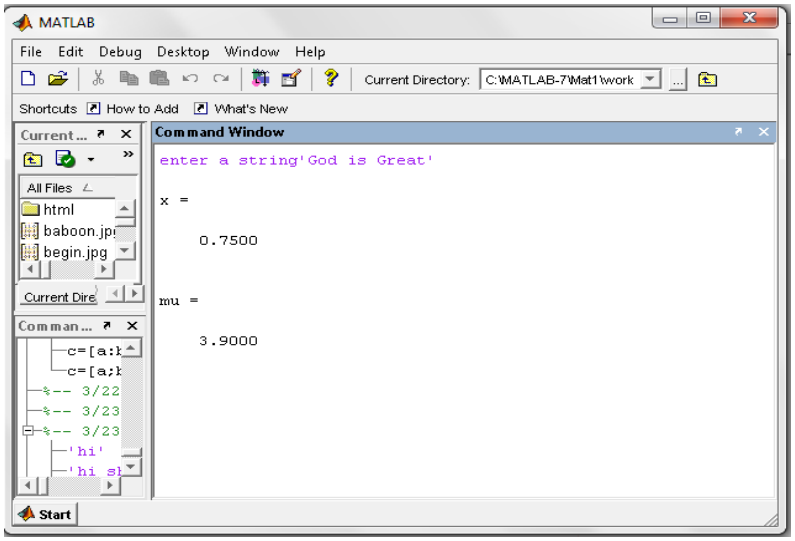

Figure 4. Input to the Stego-Crypto System during Encryption

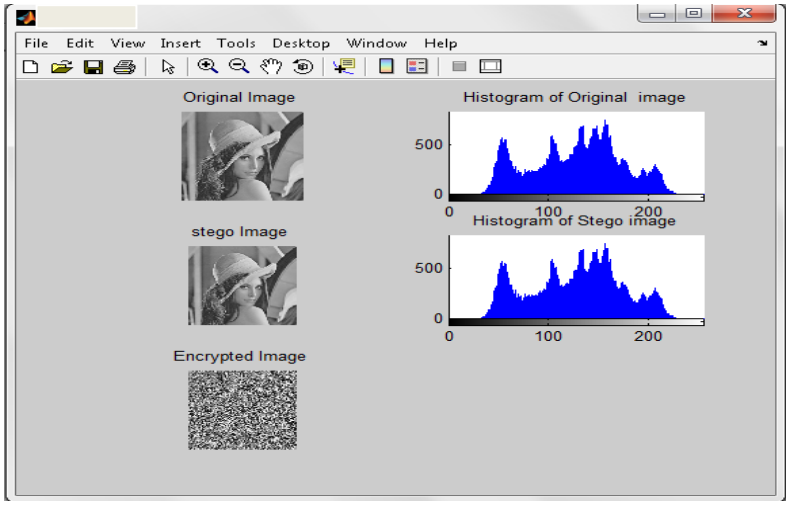

Figure 5. Histogram of original image and stego image

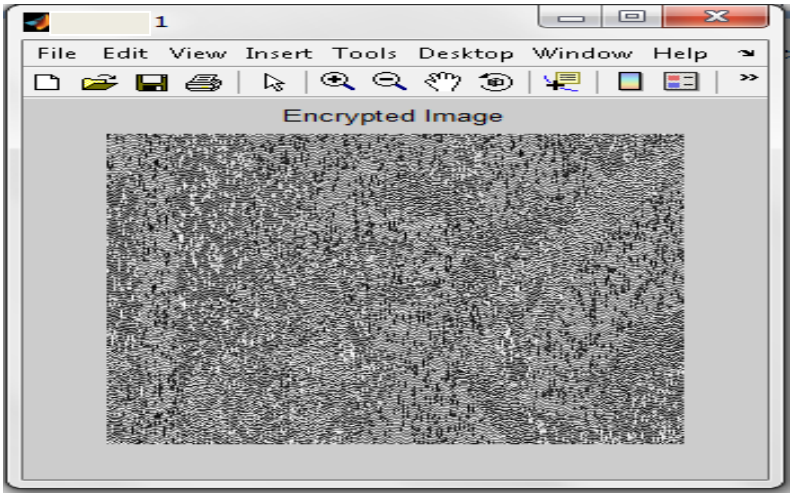

Figure 6. Output from the Stego-Crypto System during Encryption

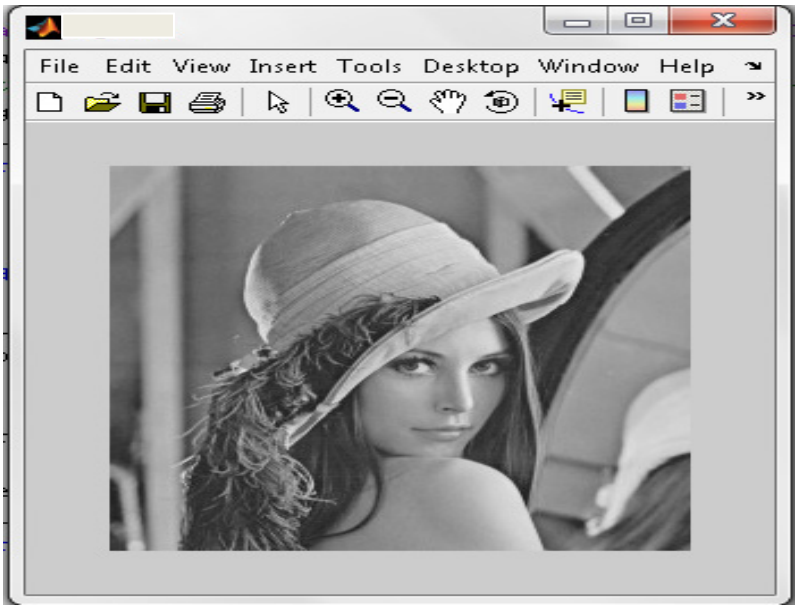

Figure 7. Stego Image generated during Decryption

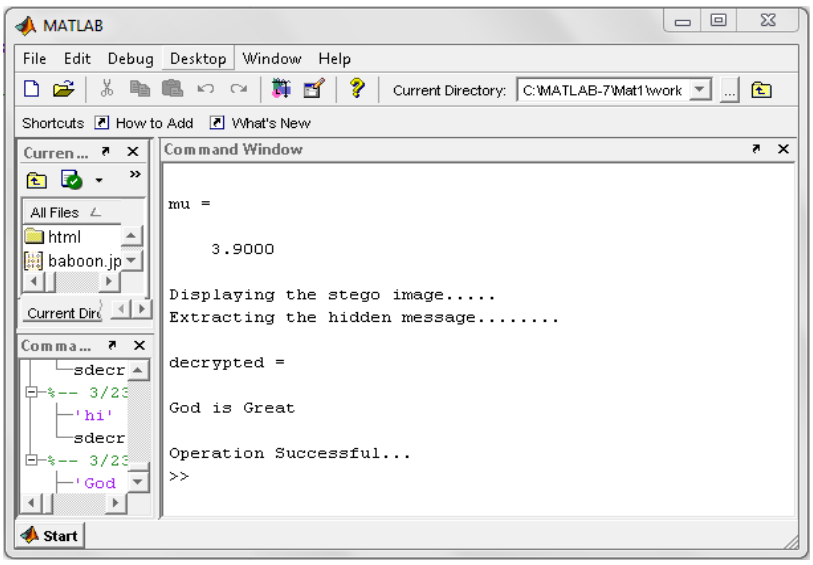

Figure 8. Output from the Stego-Crypto System during Decryption

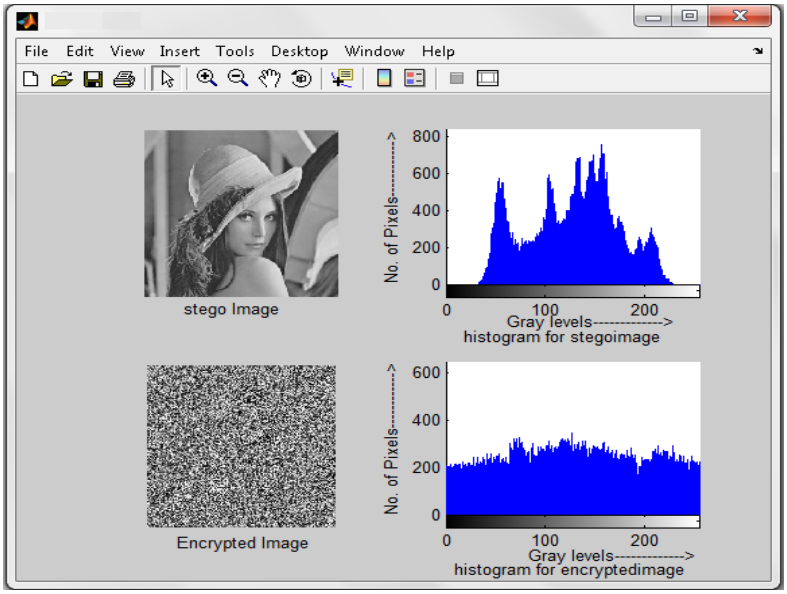

Figure 9. Histogram of both stego image and encrypted image using Chaotic Neural Network

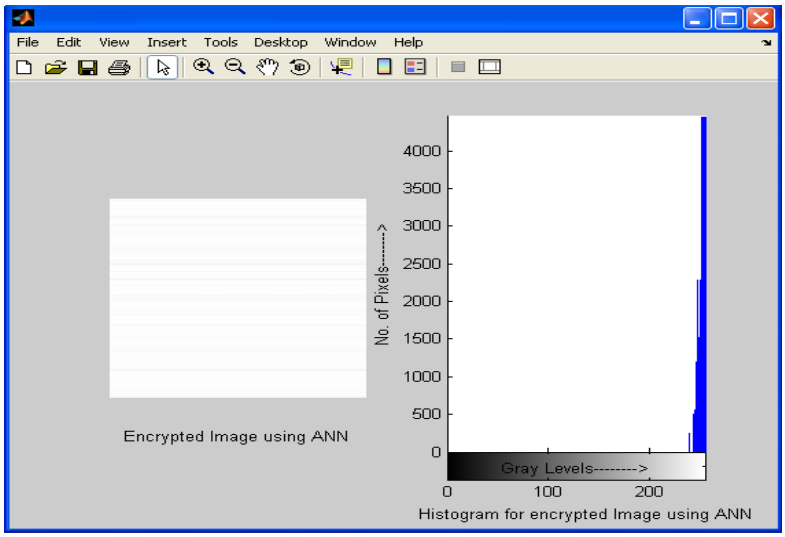

Figure 10. Encrypted stego image of Lena and it's histogram using Artificial Neural Network

8.1. Simulation Result 1

At sender end a plain text message 'God is Great' is embedded in a 256 x 256 gray scale 'Leena Image' using LSB steganography then the stego image is encrypted taking x=0.75 and mu=3.9 as the chaotic dynamics to obtain the encrypted image using Chaotic neural network and output is shown.

This histogram result shows that there is no distinct difference between original image and stego image; hence it proves its efficiency.

At the receiver end the stegoimage is retrieved from the encrypted image using CNN decryption technique and from that original message is retrieved using LSB Steganography technique.

Figure 9 exhibits the stego image and encrypted image of Lena with their histogram using chaotic neural network. However figure 10 shows the encrypted stego image and it's histogram using artificial neural network. In case of chaotic neural network, histogram represents uniform distribution of pixels over the gray levels as chaotic neural network preserves the dynamic range of gray levels in the output image. That shows the difficulty for cryptanalysts to guess the exact information being carried out by the image during transmission. However, decryption is possible in same way with known parameter as shown in figure 8. But decryption is not possible in case ANN because the mapping of pixels over gray level is not uniform which decreases the dynamic range of gray levels in the output image. And also the information are lost due to the reason that pixels are wrongly mapped to higher gray levels as shown in fig10. Even maximum pixels loss their entity in the encrypted image using ANN.

8.2. Simulation Result 2

At sender end a plain text message ‘hi everybody’ is embedded in a 204 x 204, colour image ‘camera Image’ is taken, which is converted to gray scale image then stego image then the stego image is encrypted using CNN taking same x and μ as chotic dynamics from which encrypted image is obtained and output is shown.

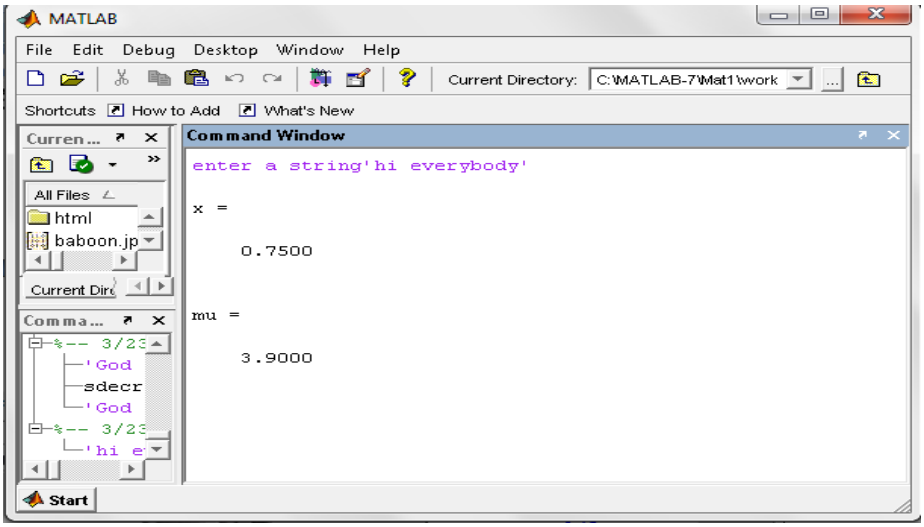

Figure 11. Input to the Stego-Crypto System during Encryption

Figure 12. Output from the Stego-Crypto System during Encryption

At the receiver end the stegoimage is retrieved from the encrypted image using CNN decryption technique and from that original message is retrieved using LSB Steganography, technique. And the output is shown as bellow:

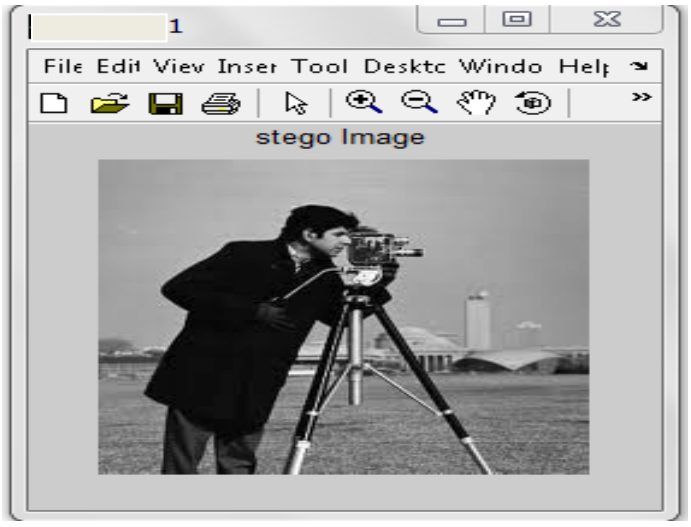

Figure 13. Stego Image generated during Decryption

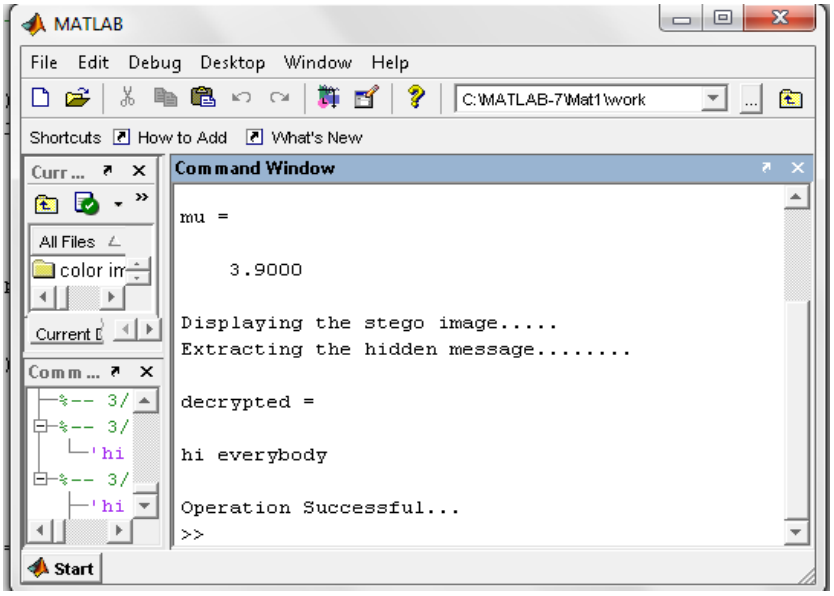

Figure 14. Output from the Stego-Crypto System during Decryption

9. Conclusions

In this paper we have presented a new system by combining the LSB Steganography and ANN based Chaotic Cryptography to make the message highly secure. Here both gray scale and colour image can be taken into consideration as cover image. Different simulation results show that for chaotic dynamics the value of x and μ should be taken 0.75 and 3.9 respectively. Rather than 0.75 and 3.9 if we consider any other values it will reveal the embedded image partially, this may help later on to cryptoanalyst to guess about secret information flow. That violates our objective. In order to provide high security for message encryption, the above values of chaotic dynamics should be kept constant and secret. The similarity of both original and stego image shows that the cryptoanalyst gains no knowledge about secret information to break. In other words the cryptoanalyst does not have any confusion about the flow of secret information. Hence it is not prone to attack. After comparing with the histograms of encrypted stego image using chaotic and artificial neural network, it is observed that decryption is possible in case chaotic network only due the uniform distribution of pixels over the gray levels. Thus the combination of both steganography and cryptography with chaotic neural network is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication.

REFERENCES

[1] Johnson, N. F. and Jajodia, S, "*Exploring steganography: Seeing the unseen*", IEEE Computer Magazine, pp.26-34, February 1998.

[2] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "*A Tutorial Review on Steganography*", IC3 Noida, pp. 106-114, August 2008.

[3] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "*Hiding Encrypted Message in the Features of Images*", IJCSNS, VOL. 7, No.4, April 2007.

[4] Sutaone, M.S., Khandare, M.V, "*Image based steganography using LSB insertion technique*", IEEE WMMN,pp. 146-151, January 2008.

[5] M. Dobsicek, *"Extended steganographic system"*, 8th International Student Conference on Electrical Engineering, Poster 04,FEE CTU 2004.

[6] Nameer N. EL-Emam, "*Hiding a large amount of data with high security using steganography algorithm*", Journal of Computer Science, Page(s): 223 – 232, April 2007.

[7] G. Sahoo & R. K. Tiwari, "*Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization*", IJCSNS, Vol. 8, No. 1, pp. 228-233, January 2008.

[8] Moulin P and Koetter R, *"Data-hiding codes",* Proceedings of the IEEE, 93 (12), pp 2083-2126, 2005,

[9] Krenn, R., *"Steganography and Steganalysis"*, http://www. krenn.nl/ niv/cry/steg/article.pdf.

[10] Johnson N.F. and Jajodia S, "Exploring steganography: Seeing the Unseen", IEEE Computer, 31(2), pp 26-34, 1998.

[11] N. F. Johnson and S. Katzenbeisser, "*A survey of steganographic techniques*", in S. Katzenbeisser and F.Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[12] Li, Zhi., Sui, Ai, Fen., and Yang, Yi, Xian. "*A LSB steganography detection algorithm*", IEEE Proceedings on Personal Indoor and Mobile Radio Communications: 2780-2783, 2003.

[13] J. Fridrich and M. Goljan, "*Digital image steganography using stochastic modulation*", SPIE Symposium on

Electronic Imaging, San Jose, CA, 2003.

[14] Alkhrais Habes, "*4 least Significant Bits Information Hiding Implementation and Analysis*", ICGST Int. Conf. on Graphics, Vision an, 2004.

[15] Ilker DALKIRAN, Kenan DANIS MAN, —"*Artificial neural network based chaotic generator for cryptology*", Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010.

[16] G. S. Rath & Satish Kumar Pradhan —*"Cryptography using Artificial Neural Networks"*, 2009.

[17] Narendra Kumar Kamila ,Pradeep Kumar Mallick ,"*Crypto Steganography using linear algebraic equation*", International Journal of Computer & communication Technology Volume-2 Issue-VIII, 2011.

[18] Ritesh Mukherjee and Nabin Ghoshal, "Steganography based Visual Cryptography", Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) Advances in Intelligent Systems and Computing Volume 199, pp 559-566, 2013.

[19] G.Prema and S. Natarajan, "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application", Proceedings of International Conference on Information communication and Embedded Systems, 727-730, IEEE Xplore digital library, 2013.

[20] Joshi Rana, Amanpreet Kaur and Nitin Malik, "Network based Steganography", *International Journal of Computer Applications*, Vol. 74(4),12-16, 2013.

[21] Mohamed Amin, Hatem M. Abdullkader, Hani M. Ibrahem and Ahmed S. Sakr, "A Steganographic Method Based on DCT and New Quantization Technique", *International Journal of Network Security*, Vol.16, No.3, PP.214-219, May 2014.

[22] Gang Yang and Junyan Yi, "Delayed chaotic neural network with annealing controlling for maximum clique problem", Advances in Intelligent Systems(Special Issue),Vol. 127,114-123, Elsevier, 2014.