International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

SECURE DATA HIDING USING NEURAL NETWORK AND GENETIC ALGORITHM IN IMAGE STEGANOGRAPHY

Sakshi[1] and Amandeep Kaur[2]

[1] *Department of Information Security, Chandigarh Engineering College, Mohali, India,*
[2] *Assistant Professor, Department of Information Technology, Chandigarh Engineering College, Mohali, India*

Abstract - Due to the high growth of Internet and its applications over the network, there is a need of high level of security while doing the data to transfer between the networks. Steganography is a technique of hiding the data over the medium so that no one knows that there is any communication going on except the sender and receiver. This paper gives an approach for Image Steganography to improve the level of security for information exchange over the web. The 24-bit RGB image is picked as a cover picture which hides the encrypted secret message inside red, green and blue pixel values. The combination approach of DWT, Masking, Artificial Neural Network (ANN) and Genetic Algorithm (GA) has been implemented on cover image and text data that is to be hidden in cover image is encrypted with Elgamal and AES algorithm (hybrid approach). This technique gives a level of security to the mystery message which makes it troublesome for the gatecrashers to remove the concealed data. A Peak Signal-to-Noise Ratio, Mean Square Error and Decryption Time is calculated which measures the quality of images used. Larger PSNR and lower MSE value indicates lower distortion and hence a better quality of image.

***Key Words**: Cover image, Stego image, PSNR, MSE, LSB insertion, DWT, Masking, ANN, GA, AES, Elgamal*

1.INTRODUCTION

The Information Security is picking up significance due to the utilization of information being exchanged on the internet. Subsequently, the information respectability and secrecy are vital angles in the field of Network Security. Presently days, the assailants have additionally registering energy to have the capacity to break encryption calculations and these abilities will just increment later on. Here, "the significance of steganography lies as it shrouds the presence of the mystery message which makes the occupation of aggressor more troublesome".

1.1 STEGANOGRAPHY

Steganography shrouds a mystery message inside a cover medium which by and large could be a picture, sound record, video document and so on. "It is the craftsmanship and investigation of tricky correspondence". In the event of a picture, Image steganography is utilized as a part of which "the picture which is utilized to convey the shrouded information is called as cover picture and the picture which conveys the concealed information are called as stego picture".

The word Steganography is gotten from the Greek words [1] "stegos" which means cover and "grafy" which means composing all things considered called as secured composition. To conceal the mystery message inside any picture requires the accompanying components [1].

- The Cover picture into which the mystery message stows away
- The Secret message which might be a plaintext, figure content or some other sort of information ‘
- The Hiding Function or the key
- The Stego picture which is created after the installing of mystery message into the cover picture
- The Extract Function which will isolate the mystery message and the cover picture

There are three fundamental elements which rely on upon the installing of the information [2]:

- Visual nature of stego pictures (the picture with lower contortion is more best for a high visual nature of picture) ‘
- Security (how secure is the picture from outside components like clamor, altering, fashion and so on).
- Embedding limit (identified with the difference and luminance attributes which have a most extreme limit of implanting information in the picture)’

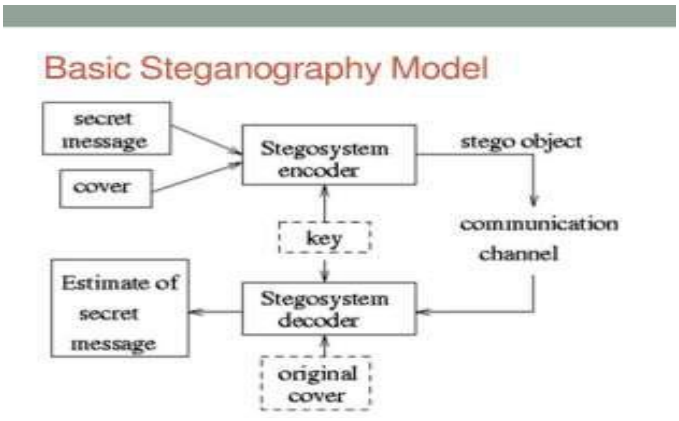

Fig -1: Basic Image of Steganography

Image Steganography is separated in two sections:

Spatial space and Transform area. Spatial area otherwise called Image space bargains straightforwardly with the pixels. The message is inserted in the pixel forces and subsequently controls and adjusts the picture.[3] LSB Substitution procedure is a case of spatial space strategy. Change area otherwise called Frequency space changes the picture first and after that the cover picture gets incorporated with the message. The change is done starting with one space then onto the next area. By changing the space, the information could be taken care of all the more effectively as far as lossy pressure of pictures, honing and so forth. There are different change methods [4] like "discrete cosine change procedure (DCT), Quick Fourier change procedure (FFT) and Discrete Wavelet change system (DWT)".

Limit, security and power are the three fundamental parts of Steganography [5]. Limit is the measure of the mystery message that the cover picture could convey. Security alludes to the location of the concealed message inside the cover picture is not caught and vigor alludes to the ability of the stego picture to withstand the progressions in regards to picture controls, trimming, pressure and so on.

1.2 ARTIFICIAL NEURAL NETWORKS

The neural system is roused by natural neural framework. It is made out of a few interconnected components to take care of a gathering of fluctuated issues[6]. The mind is made out of billions of neurons and trillions of associations between them. The nerve motivation goes through the dendrites and axons, and after that treated in the neurons through neurotransmitters. This outcomes in the field of simulated neural systems in a few interconnected components or having a place with one of the three imprints neurons, information, yield or covered up. Neurons having a place with layer n are viewed as a programmed limit. Furthermore, to be actuated, it must get a flag over this edge, the yield of the neuron subsequent to considering the weight parameters, providing every one of the components having a place with the layer n +1. As organic neural framework, neural systems can realize, which makes them helpful. The fake neural systems are units of investigating, fit for taking care of fluffy data in parallel and turn out with one or more results representing the postulated solution. The fundamental unit of a neural system is a non-direct combinational capacity called manufactured neurons. A manufactured neuron speaks to a PC recreation of an organic neuron human mind. Each simulated neuron is portrayed by a data vector which is available at the contribution of the neuron and a non-direct numerical administrator fit for computing a yield on this vector. The following figure shows an artificial neuron:

The synapses are Wij (weights) of the J neurons; they are real numbers between 0 and 1. The function is a summation of combinations between active synapses associated with the same neuron. The activation function is a non-linear operator to return a true value or rounded in the range [0 1].

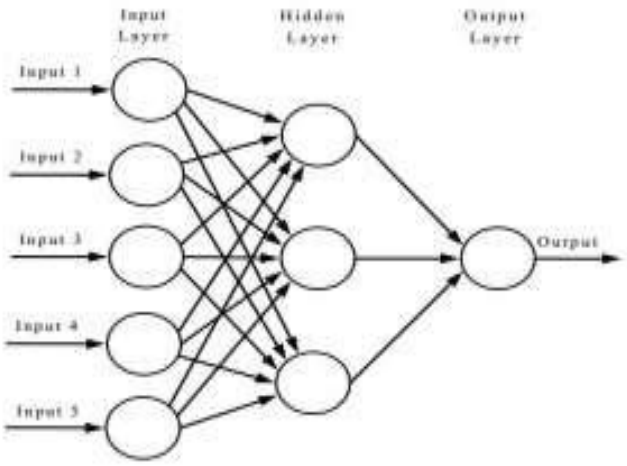

Fig -2: Artificial Neural Network

1.3. GENETIC ALGORITHM

In the field of computerized reasoning, a hereditary calculation (GA) is an interest heuristic that duplicates the strategy of regular assurance.[7] This heuristic is routinely used to create accommodating responses for upgrade and chase issues. Innate computations have a place with the greater class of formative estimations (which deliver answers for upgrade issues using techniques moved by natural evolution, for instance, legacy, change, decision, and mixture)[8].

A typical genetic algorithm requires:

1. a genetic representation of the solution domain,
2. a fitness function to evaluate the solution domain.

Basic Genetic Algorithm

1. [Start] Generate irregular populace of n chromosomes (reasonable answers for the issue)
2. [Fitness] Evaluate the wellness f(x) of every chromosome x in the populace
3. [New population] Create another populace by rehashing taking after strides until the new populace is finished
   a) [Selection] Select two parent chromosomes from a populace as indicated by their wellness (the better wellness, the greater opportunity to be chosen)

b) [Crossover] With a hybrid likelihood traverse the guardians to shape another posterity (kids). On the off chance that no hybrid was performed, posterity is precise of guardians.

c) [Mutation] With a transformation likelihood change new posterity at every locus (position in chromosome).

d) [Accepting] Place new posterity in another populace

4. [Replace] Use new created populace for a further keep running of calculation
5. [Test] If the end condition is fulfilled, stop, and give back the best arrangement in current population[9].

6. [Loop] Go to step 2

1.4. CRYPTOGRAPHY

Cryptography is the limit of finishing security by encoding the data into an indiscernible edge[10]. Cryptography is the branch of cryptology which oversees computation gets ready for encryption and interpreting, prompts to the legitimacy of the message. A system to cover the substance of encoding plain substance is returned to encryption and to get the figure substance to its one of a kind plain substance is known as unscrambling. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. Cryptosystem shows as a stand-out security game plan in various creating applications stressed to equipment, correspondence, frameworks where confirmation of security is basic. It is furthermore used to focus electronic stamp progressions. A server-based electronic stamp system is huge amounts of transmitting messages and on different riddle keys. Despite this it is moreover used to arrange a detached stamp check in perspective of the evacuation extraction procedure. There are two sorts of encryption figuring's: symmetric encryption count and hilter kilter encryption estimation [11]. In symmetric key encryption sender and gatherer will have a comparative key for the methodology of encryption and unscrambling of data [12]. In a symmetric key encryption count assorted keys are used as a piece of sending and getting site for encryption and disentangling. The Digital Signature Scheme Algorithm (DSA) used as a piece of this paper is of upside down sort count [13].

Below are different symmetric and asymmetric algorithms:

List of Symmetric Algorithms:

i. Data Encryption Standard (DES)
ii. Advanced Encryption Standard (AES)
iii. Blowfish Encryption Algorithm
iv. International Data Encryption Algorithm
v. Triple Data Encryption Standard

List of Asymmetric Algorithms:

i. Diffie-Hellman
ii. RSA
iii. DSA
iv. Elgamal Encryption
v. ECC

2. PROPOSED METHOD

The proposed method is combination of Steganography and Cryptography. The implementation has been done in MATLAB simulator. Here is step by step approach of proposed method:

2.1. ENCODING ALGORITHM:

1. Upload any RGB image in which you want to embed your secret data.
2. Find the frequency domain representation of blocks by 1D Haar Discrete Wavelet Transform and get four sub bands LL1, HL1, LH1, and HH1.
3. Masking of image by applying different filters and find the zero level contour using 1726 iteration in which initial data is being saved.
4. Train the neural network by inputting the features extracted from LL1 band and find the blank locations
5. Genetic algorithm is used by optimizing the neural network.
6. Input the message and password and Encrypt the message using hybrid algorithm (AES and elgamal algorithm).
   a. Calculate the length of the text to determine the number of LSB's used for embedding.
7. Embed the encrypted message bits , password and key in k-LSBs DWT coefficients each pixel according to mapping function.

B. DECODING ALGORITHM:

1. Decrypt the message by entering the password used and by reverse AES and elgamel algorithm.

2. Extract the message length from the stego image and after extracting the length apply reverse 2DWT algorithm on image to extract the message from stego image
3. Calculate the PSNR, MSE, and Decrytion time between the input image and stego image.

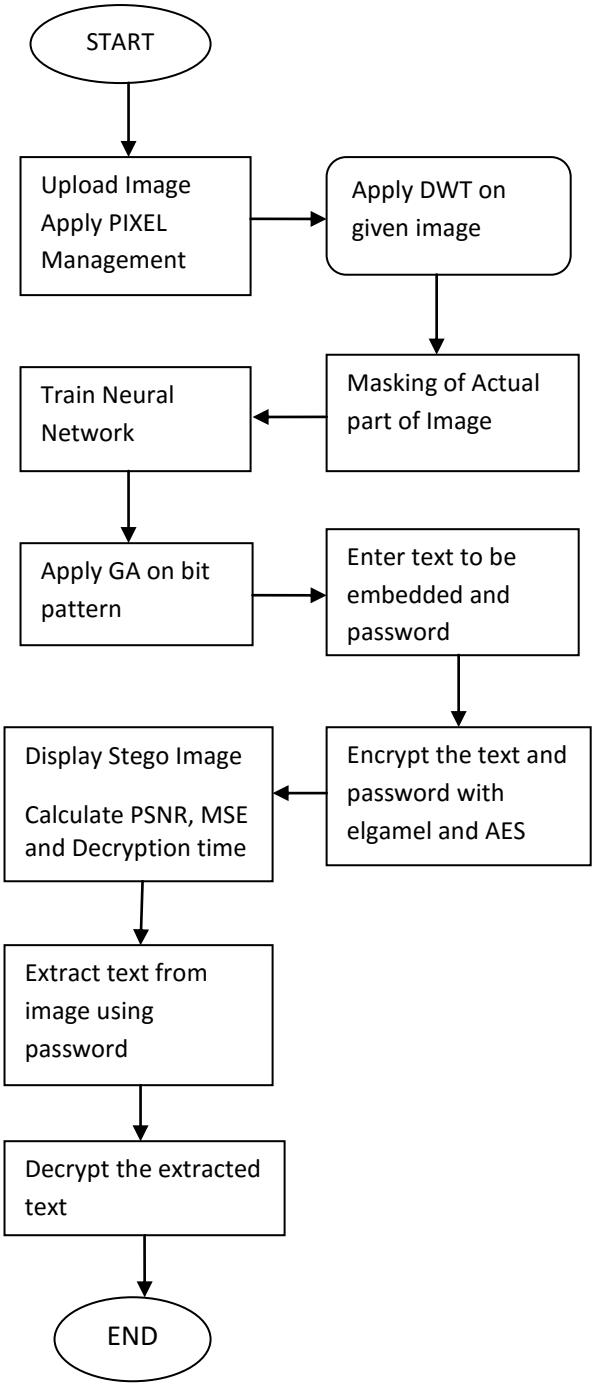

Fig -3: Flow Chart of Proposed Method

3. RESULT AND DISCUSSION

This section presents the obtained results of the proposed method. Here, two 24- bit RGB images are taken as used in[11] such that results can be compared with other existing methods.

Fig -4: Leena Image (Cover Image)

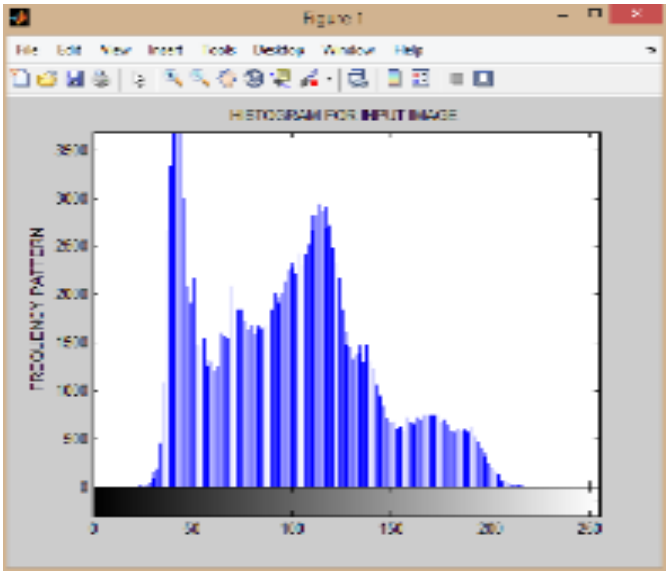

Fig -5: Histogram of Cover Image

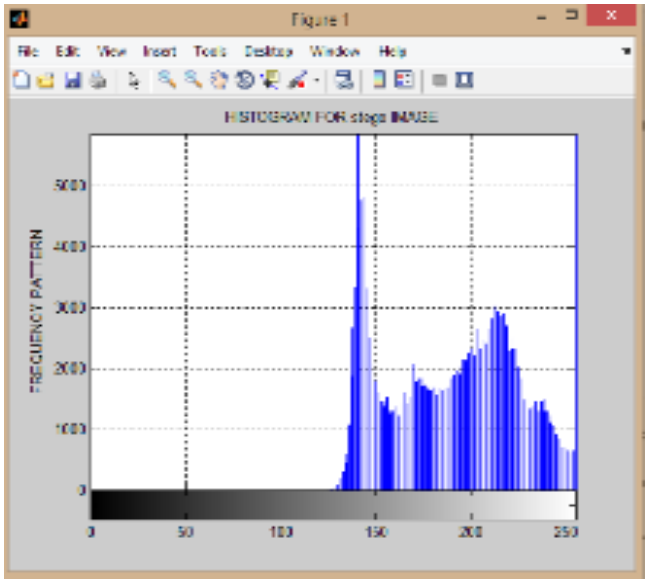

Fig -6: Histogram Of Stego Image

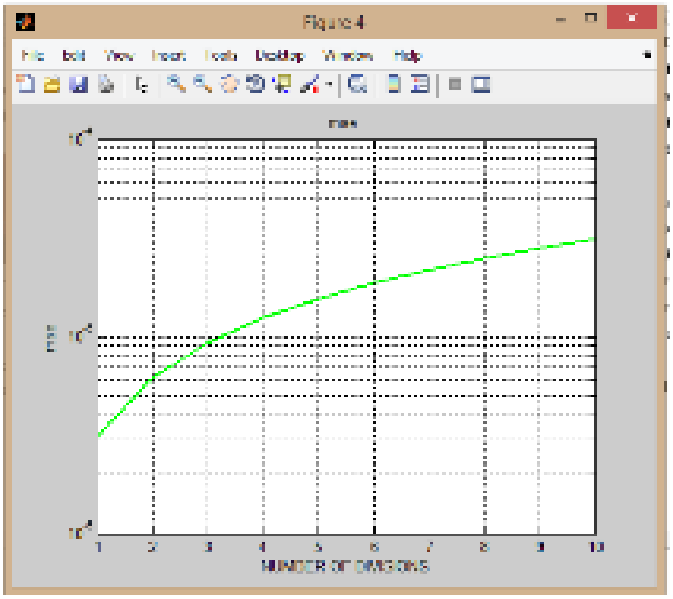

Fig -7: MSE Graph of Stego Image

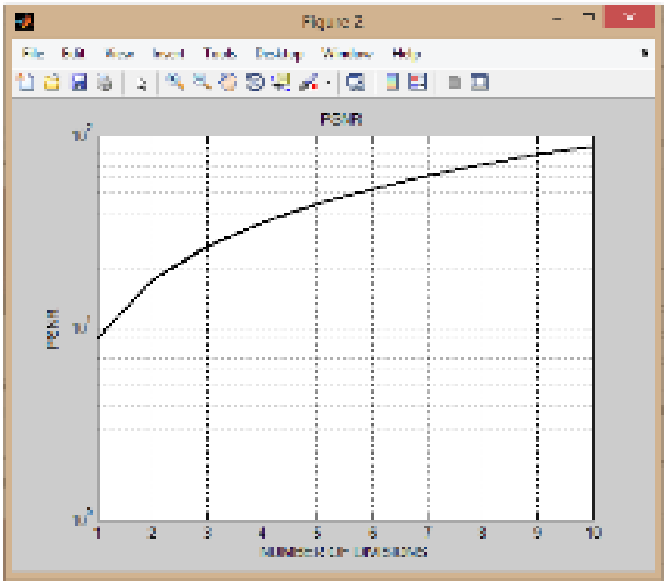

Fig -6: PSNR Graph of Stego Image

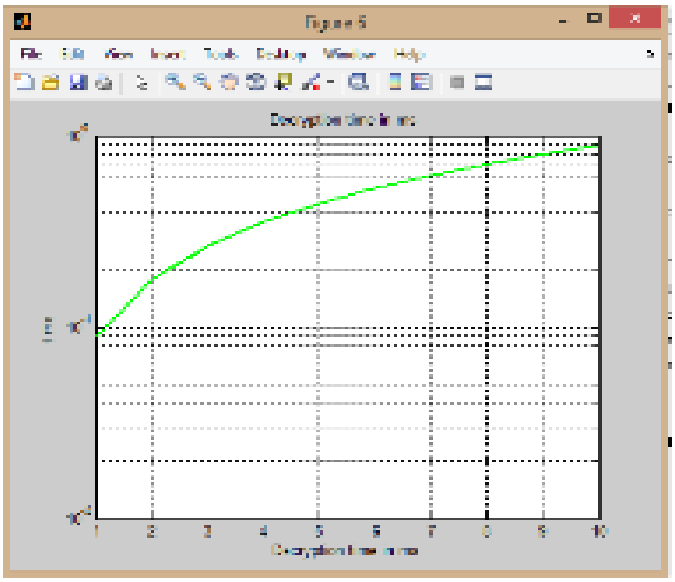

Fig -8: Decryption time Graph of Stego Image

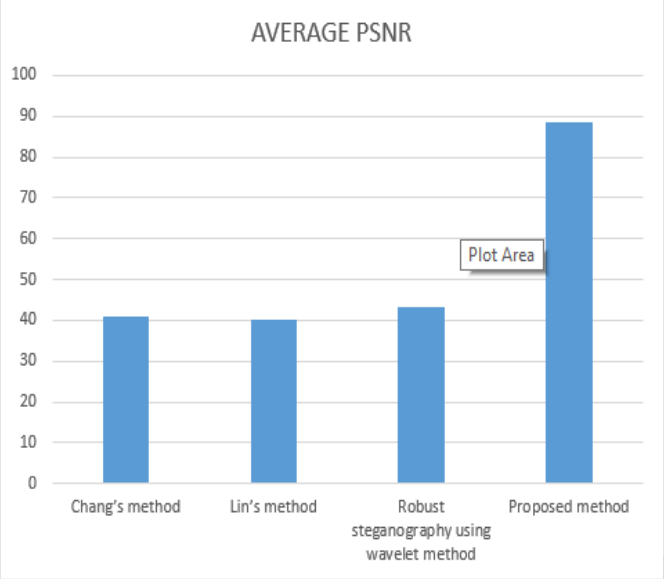

Chart -1: Comparison of different methods in terms of PSNR ratio

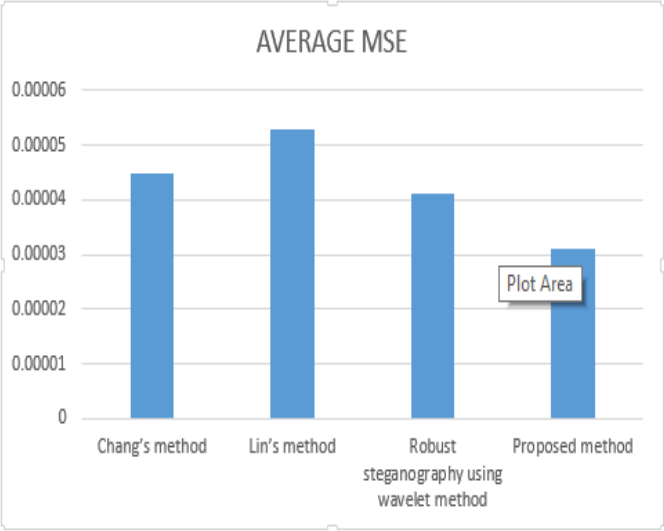

Chart -2: Comparison of different methods in terms of MSE ratio

4.CONCLUSION AND FUTURE SCOPE

In this dissertation, the steganography technique which is implemented with genetically modified neural network is proposed. The power of this technique is illustrated by means of PSNR value which is high. PSNR will represent the image quality. Enhanced PSNR value is needed in order to avoid the suspicious images to be known by hackers that might creep in across the network. The abnormality of the image is avoided for acquiring the confidentiality of data. The aim of the proposed technique is to conjugate cryptography and steganography together. The results and the discussions have clearly shown this idea. The security is added to the technique by doing the hybridization of an asymmetric cryptography algorithm with the symmetric cryptography algorithm. If somehow there are chances that steganography has been revealed by intruders, the second level of security provided to the secret message always keeps the contents secrecy. Thus, the proposed technique works both on keeping the secrecy of the contents as well as existence of the message.

In the present work, genetically modified neural network along with hybrid approach to encryption has been used. Improvement of the technique can still be emerged by making neural network work as steganalysis tool, so that there is no need for decryption across the receiver side.

REFERNCES

[1] Dagar E. and Dagar S. , " LSB Based Image Steganography Using X-Box Mapping", In the Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) , India, pp. 351-355. 2014.

[2] Shamim Ahmed Laskar1 and Kattamanchi Hemacha0ndran2, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS), Vol.4, No.6, December 2012, pp. 57-68.

[3] Ross J. Anderson and Fabien A.P. Petitcolas, " On the Limits of Steganography" , IEEE Journal of Selected Areas in Communications, May 1998., Vol.16, No.4, pp. 474-481.

[4] Pradeep Kumar Singh and R.K.Aggrawal, "Enhancement of LSB based Steganography for Hiding Image in Audio", (IJCSE) International Journal on Computer Science and Engineering Vol.2, No.5, 2010, pp. 1652-1658.

[5] Nameer N. EL-Emam , "Embedding a LargeAmount of Information Using High Secure Neural Based Steganography Algorithm", World Academy of Science, Engineering and Technology, Vol.2, No.11, Nov 2008, pp. 566-577.

[6] Imran Khan, "An Efficient Neural Network based Algorithm of Steganography for image", International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, No.2, pp. 63-67.

[7] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol.6, No.79, 2012, pp. 3907 – 3915 .

[8] Saravanan V. and Neeraja A., " Security Issues In Computer Networks And Steganography", In the Proceedings of the 2013 Intelligent Systems and Control (ISCO), India, pp. 363-366, 2013.

[9] Wu H. , Huang J. , "Secure Jpeg Steganography By Lsb+ Matching And Multi-Band Embedding" In the Proceedings of the 2011 International Conference on Image Processing (ICIP) , India, pp. 2737-2740, 2011.

[10] Manoj gowtham. G.V, Senthur.T, Sivasankaran.M, Vikram.M, Bharatha Sreeja.G, "AES BASED STEGANOGRAPH" , International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol.2, No.1, January 2013.

[11] Arvind Kumar , Km. Pooja, "Steganography-A Data Hiding Technique", International Journal of Computer Applications, Vol.9, No.7, November 2010.

[12] Ajit Singh, Swati Malik, "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering , Vol.3, No.5, May 2013 .

[13] Mohammad Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion" , IJCSNS International Journal of Computer Science and Network Security, Vol.8, No.6, June 2008.