International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Image Steganography Technique based on the hybridization of RSA, AES and Neural Network

[1]Sandeep kaur
Student
M.Tech Scholar, C.S.E. Department
Adesh Institute of Engineering & Technology
Faridkot, Punjab, India
sandymaan16@gmail.com

[2]Naseeb Singh Dhillon
Assistant Professor
C.S.E. Department
Adesh Institute of Engineering & Technology
Faridkot ,Punjab, India
naseebdhillon@hotmail.com

Abstract: *Steganographic systems are being connected over an expansive arrangement of distinctive advanced advances. The steganographic system will be utilized for web/system security, watermarking etc. Thus, the steganography is the procedure of concealing one medium of correspondence (Text, Sound, and Image) inside another. It can chip away at JPEG 2000 packed pictures & mix Mark pictures. The new technique for steganalysis taking into account hybridization of RES, AES and Neural Network. We first concentrate the elements of picture installed data, then information them into neural system to get the yield. The neural system in still pictures is utilized to beat the obstacles by concealing the information by implication into graphical picture utilizing neural system calculation to get figure bits. The entire recreation has been occurred in MATLAB environment.*

Keywords: *Steganography, Cryptography, Neural Network RSA, AES.*

1. Introduction

The step by step advancement in the correspondence frameworks requests the abnormal state of data security in correspondence systems. As the transmission of data is increments on the web so arrange security is getting exceptionally significance [1]. Consequently the classifiedness and the unwavering quality of the information must be shielded from unapproved access. It implies there must be a touchy improvement in the field of data security alongside the copyrights of the advanced media. For the security of emit data cryptography and steganography are the two usually utilized security apparatuses [2]. Secrecy, availability and uprightness are the three principle ideas of data security. Feelings of the diverse individuals who make the utilization of such data are verification, approval and non-revocation. Cryptography and Steganography are the security apparatuses accessible for the insurance of the mystery data [3].

Many information security algorithms have been developed combining encryption and steganography algorithms to enhance information security. One of the most recent algorithms is the LSB. A LSB image steganography that enhances the existing LSB substitution algorithms was introduced in [4] to improve the security level of secret message. It encrypts the secret message to protect it from being accessed by unauthorized users before being hidden within the LSB of the image. The PSNR of the stego image was estimated to measure the stego images quality. The obtained results demonstrated that using secret key cryptography provides good security and PSNR value higher than general LSB based image steganography methods. Similarly, two algorithms combining cryptography and steganography were introduced in [5], in which the secret message is encrypted before being hidden. Although, such algorithms can provide higher resistance to steganalysis, they usually take long processing time. So in proposed work, neural network with RSA and AES will be introduced with four parameters like MSE, PSNR, Capacity and Node Count.

2. SIMULATION MODEL

Symmetric key algorithms are confronting an issue identified with the security of the keys and lopsided key algorithms are confronting the issue of moderate speed when contrasted with symmetric key algorithms [6]. Symmetric key algorithms can be utilized for both extensive and little message transmission however uneven key algorithms are just well suitable for little message change over the web. Accordingly, to diminish or overcome from the issues of both symmetric and uneven key algorithms a half and half of both these algorithms are utilized which is known as PGP (Pretty Good Privacy). It will give the insurance to the symmetric keys and builds the velocity of the uneven key cryptography [7].

Preferences of crossover cryptography:

- No compelling reason to send DES keys subtly before correspondence.
- Keys are sending by RSA, so it will likewise go about as advanced mark.
- Having same velocity of encryption and unscrambling as AES [8].

3. PROPOSED METHODOLOGY

The proposed scheme is implemented in MATLAB platform using standard cryptography and steganography algorithm [9]. AES-RSA hybrid cryptography is used along with neural Network. Below Figure shows the working of proposed information security scheme.

Embedding Algorithm

a) Read cover Image,
b) Read hidden message
c) For every carrier image selected from image pool, image pool is the buffer of various images.
d) Firstly linearization of image will be done then apply DCT to the selected image.
e) After DCT application, apply Vector quantification for the purpose of the image compression which is well known by DCT matrix.
f) Values will be saved in table of vector quantization.
g) Now calculate LSB bit.
h) There are no. of LSB bits
i) Now choose that bit that has to be replaced.
j) Image. Feasible features are matched then choose bit.
k) Now find out image size.
l) If image size if optimum then select image to be stego image

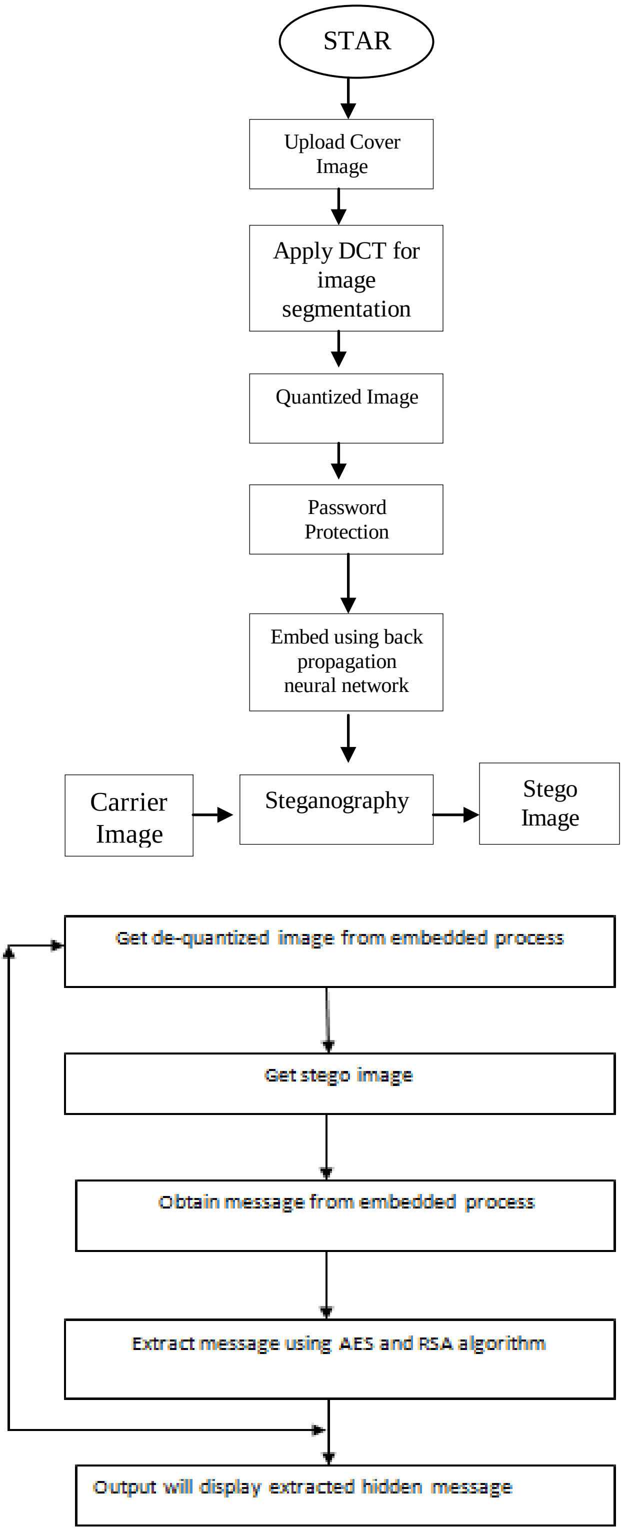

STAR
Upload Cover Image
Apply DCT for image segmentation
Quantized Image
Password Protection
Embed using back propagation neural network
Carrier Image
Steganography
Stego Image
Get de-quantized image from embedded process
Get stego image
Obtain message from embedded process
Extract message using AES and RSA algorithm
Output will display extracted hidden message

Figure no:3.1 Proposed Simulation Model

Extraction Algorithm

The following steps present the different stages that need to be accomplished:

a) Select the cover image.
b) Add mask of 8*8 to the cover image.
c) Choose encryption algorithm like AES and RSA for hiding the message [10].

d) Quantize the image using dct pixel vector quantization matrix

e) Note down the table values of the quantization table.

f) Apply Password.

g) Find suitable LSBs to the image using NEURAL

h) Embed Message into the cover image.

i) Apply the whole process in reverse at receiver end.

j) Calculate the performance parameters like PSNR, MSE.

4. RESULTS AND IMPLEMENTATION

A. Computation Parameters

1. PSNR: The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$PSNR = 10.\log_{10}(MAX^2 \ / \ MSE) \qquad \text{eq.1}$$

2. MSE: The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is

$$MSE = \frac{1}{mn} \sum \sum \ [(I,j) – K\ (I,j)]^2 \text{eq.2}$$

Where M and N are the number of rows and columns in the input images, respectively.

3. Steganographic capacity: It is considered as the size of data embedded within a cover image (KB). Steganographic capacity is the maximum number of bits that can be embedded in a given cover image with a negligible probability of detection by an adversary. However, the embedding capacity is the maximum number of bits that can be embedded in a given cover image. Therefore, the embedding capacity is likely to be larger than the steganographic capacity. Moreover, the size of the hidden information relative to the size of the cover image is known as embedding rate or capacity. However, it defines the capacity as the size of the hidden message relative to the size of the stego image [11].

4. Node Count

Node count is considered as the hiding capacity of per node. As the node count increases then the capacity of the data hiding also increases.

B. Results

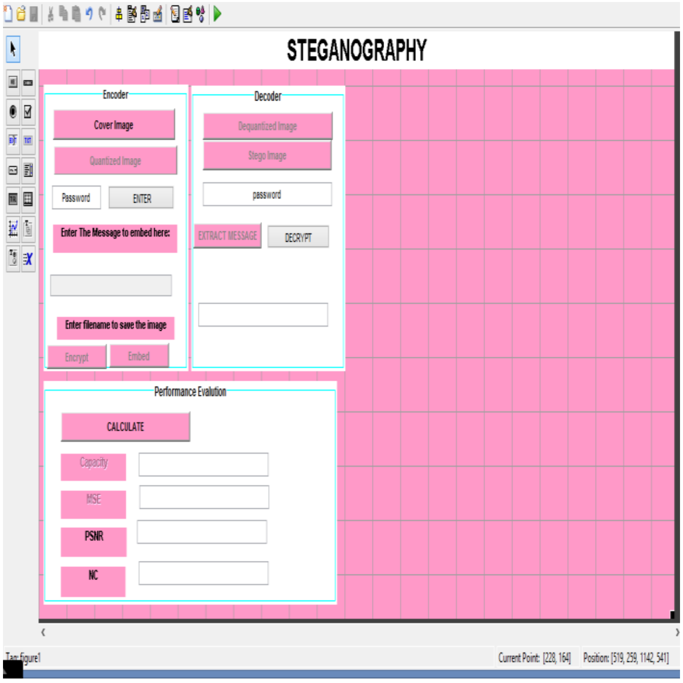


Figure no:4.1 Main GUI

Above window is the master window of the proposed work. Its working is described as follows: read cover Image, read hidden message, for every carrier image selected from image pool, image pool is the buffer of various images. Firstly linearization of image will be done then apply DCT to the selected image. After DCT application, apply Vector quantification for the purpose of the image compression. Values will be saved in table of vector quantization, Now find out image size. If image size if optimum then select image to be stego image, If merging of image is done accurately, Call Neural Network, Neural network has basically 3 layers, input, hidden and output layer. Now output layer gets the value on the account of input value. If error occurred at output then check input values and change accordingly.

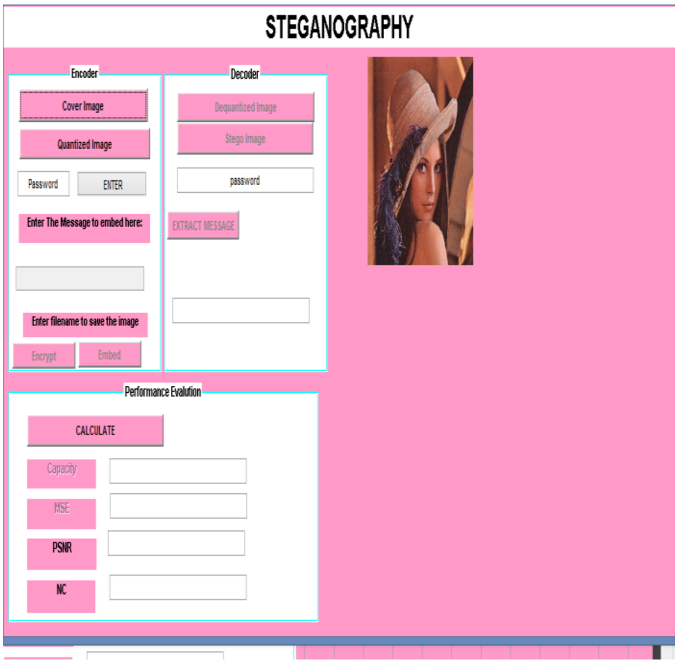


Figure no:4.2 Upload Main image

Above figure shows the main window of the steganography work. In this figure, it has been shown that cover image of leena is being taken on which steganography has to be applied. The main window also includes number of buttons like Embed, extract buttons, calculation of PSNR value, MSE value. Embed id applied to hide the data on which encryption will be done.

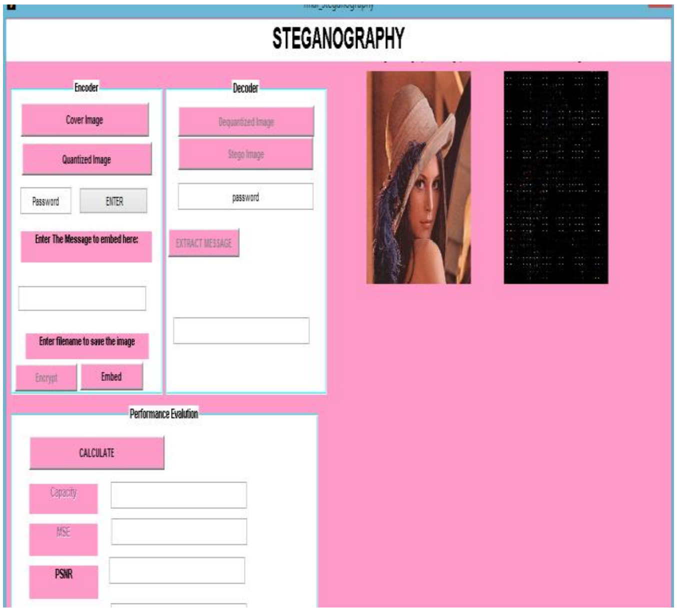
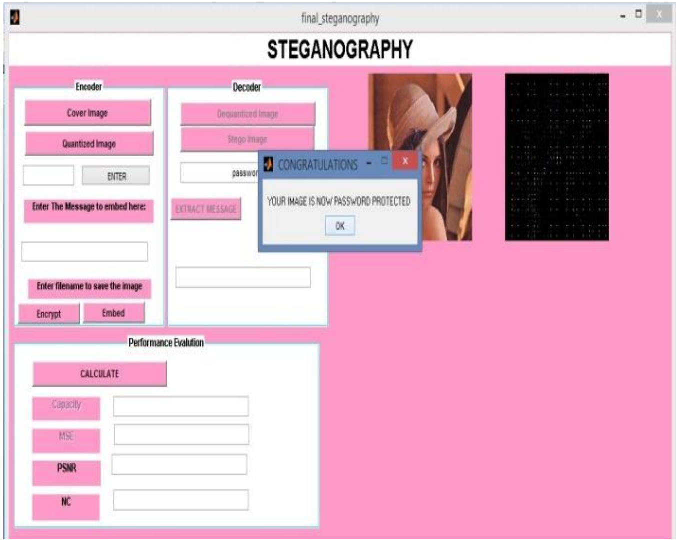


Figure no:4.3 Quantized Process

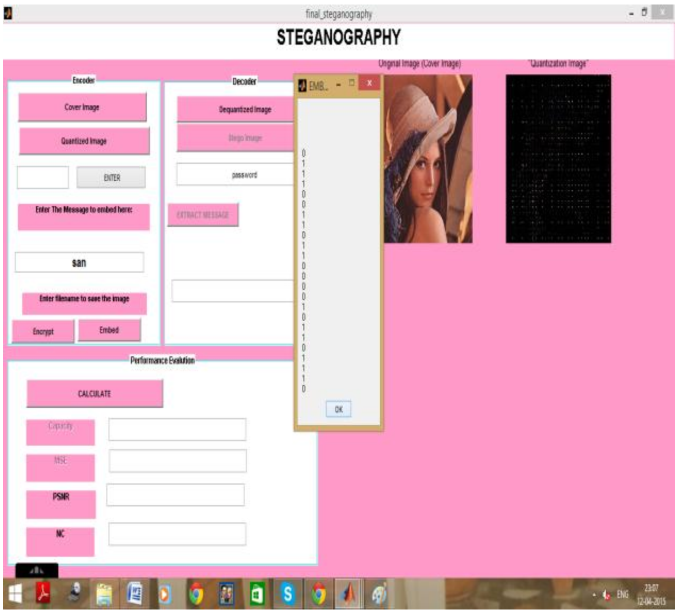
The above figure shows the quantized image after clicking on the quantized button after that we will enter the password for the protection. We obtained quantized encrypted image. Quantization process is needed to divide the image into number of segmentation. Quantization is obtained using vector table. Quantization matrix is needed because to obtain compressed image so that better steganography can be done.



YOUR IMAGE IS NOW PASSWORD PROTECTED

Figure no:5.4 Security

Above figure shows when cover image is tried to get encrypted, then a security pop up window comes, that needs password security so that encryption is done effectively.



san

0
1
1
1
0
0
1
1
0
1
1
0
0
0
0
1
0
1
1
0
1
1
1
0

Figure no:4.5 Embedding Process & apply DCT

Above figure shows that embedding process after applying 2-D DCT and quantization matrix. Encryption is done to encrypt the message mainly to obtain the good quality image. The inverse masking is done to retrieve the image

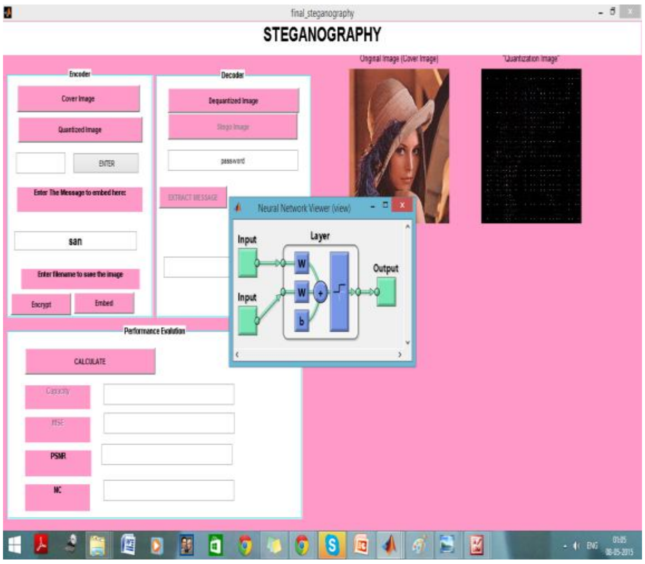
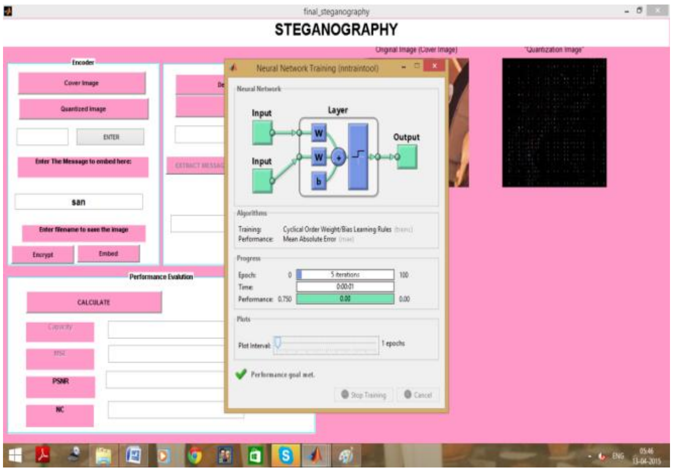


Figure no:4.6 Neural Network apply to extract message

After this neural network can be applied to extract the message embedded into the image. . Neural Network has been found effective enough to find pixels to merge the data bits without much affecting the original pattern of the image. It has been also concluded that if we can encrypt the data up to some level before merging it to the image, it may enhance the chances of security into the image embedding.It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems as shown above. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons. This is true of ANNs as well.



Algorithms
Training: Cyclical Order Weight/Bias Learning Rules (trainc)
Performance: Mean Absolute Error (mae)
Progress
Epoch: 0 5 iterations 100
Time: 0:00:01
Performance: 0.750 0.00 0.00
Plots
Plot Interval: 1 epochs
Performance goal met.

Figure no:4.7 Structure of Neural Network

Above figure shows the structure of the neural network, Nodes represent the neurons, and arrows represent the links between them. Each node has its number, and a link connecting two nodes will have a pair of numbers (connecting nodes 1 and 4). Networks without cycles (feedback loops) are called a feed-forward networks (or perceptron). Features used in neural network are epoch, time, performance etc.

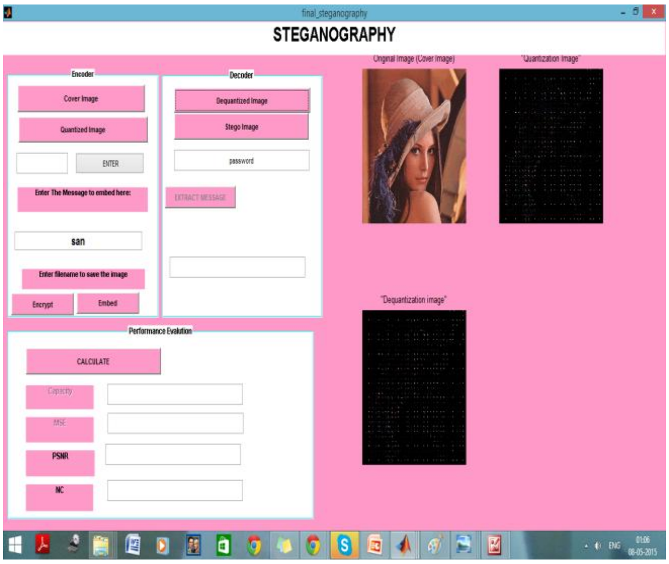


Figure no: 4.8 Pattern after quantized

Above figure shows the patter after applying de quantization for the password protected steno image

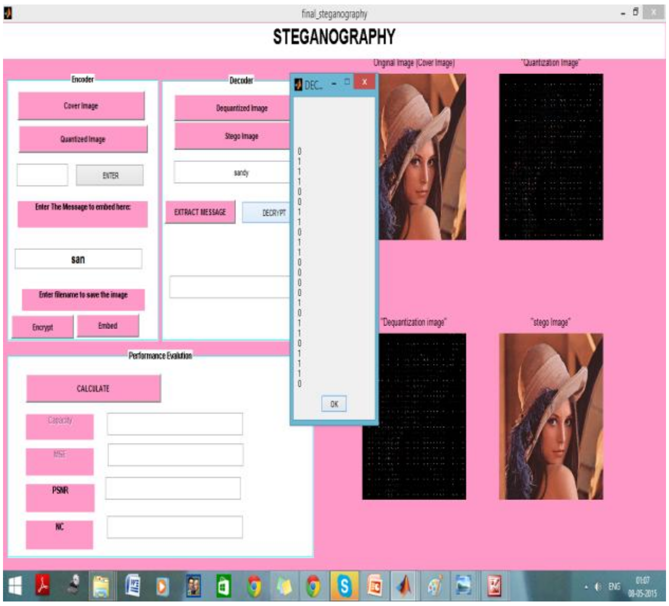
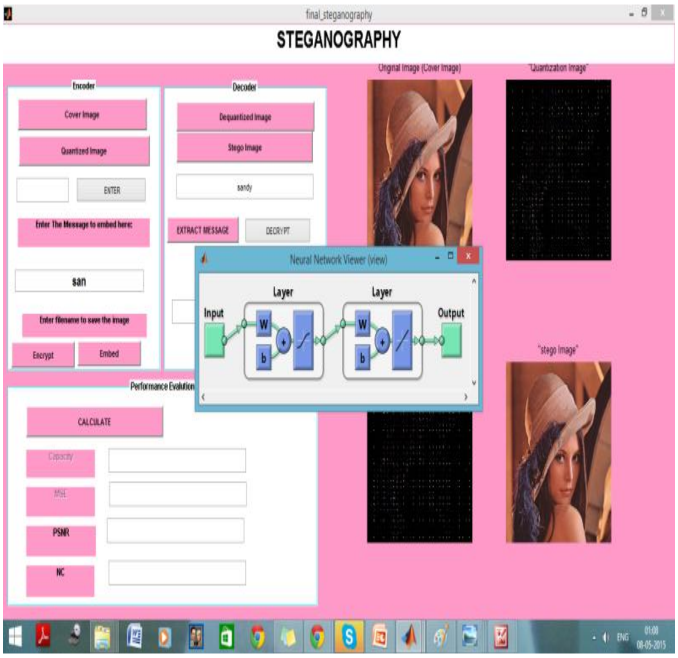


Figure no:4.9 Quantized image with decrypted process

Above figure shows the de quantized image with decryption process for the retrieval of the password protected image after applying password in the graphical user interface .

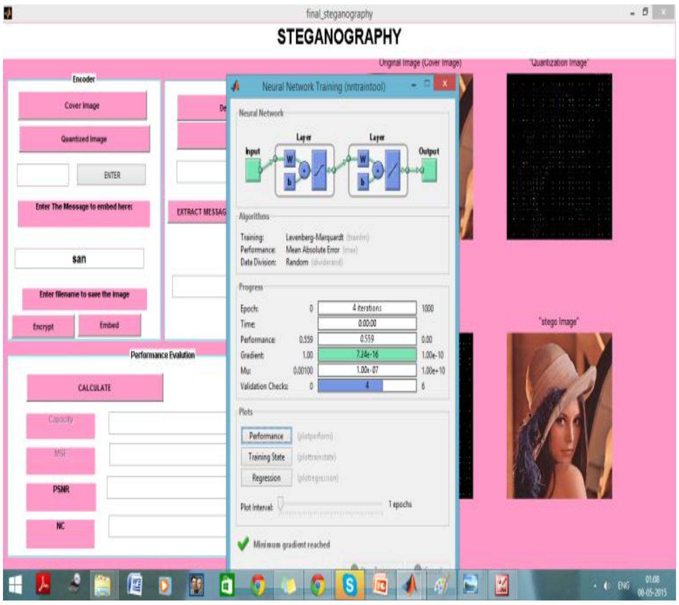


sandy

san

Figure no:4.10 Extract Process

Above figure shows the extraction process using neural after decryption process. The structure of the neural network shows the input layer, hidden layers and the output layer in which synaptic weights are included for the calculations and displays steno image.



san

Training: Levenberg-Marquardt (trainlm)
Performance: Mean Absolute Error (mae)
Data Division: Random (dividerand)

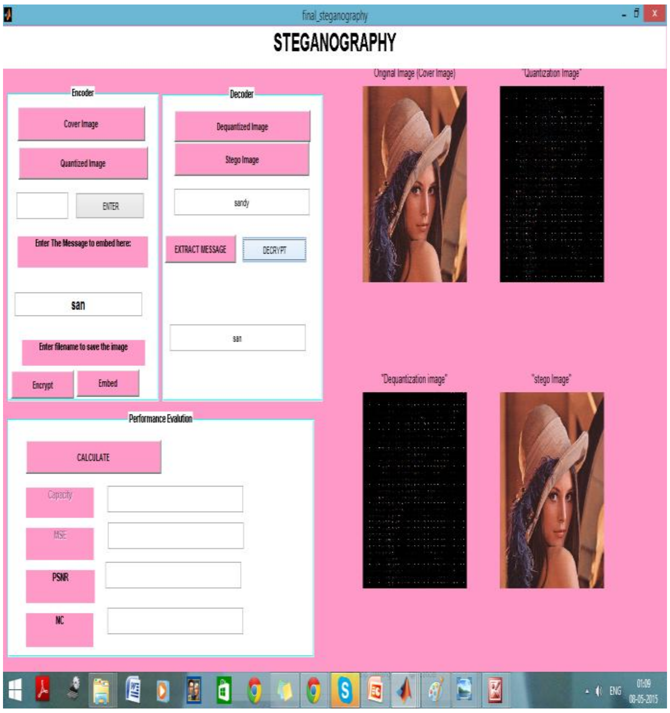
Epoch: 0 | 4 iterations | 1000
Time: 0:00:00
Performance: 0.559 | 0.559 | 0.00
Gradient: 1.00 | 7.24e-16 | 1.00e-10
Mu: 0.00100 | 1.00e-07 | 1.00e+10
Validation Checks: 0 | 4 | 6

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)
Plot Interval: 1 epochs

Minimum gradient reached

Figure no:4.11 Architecture Neural Network

The above figure shows the neural network tool box which is having features for the Number of Epochs, Time to execute the training process with respect to the number of iterations, Performance and validation checks which shows the evaluation process through neural network.



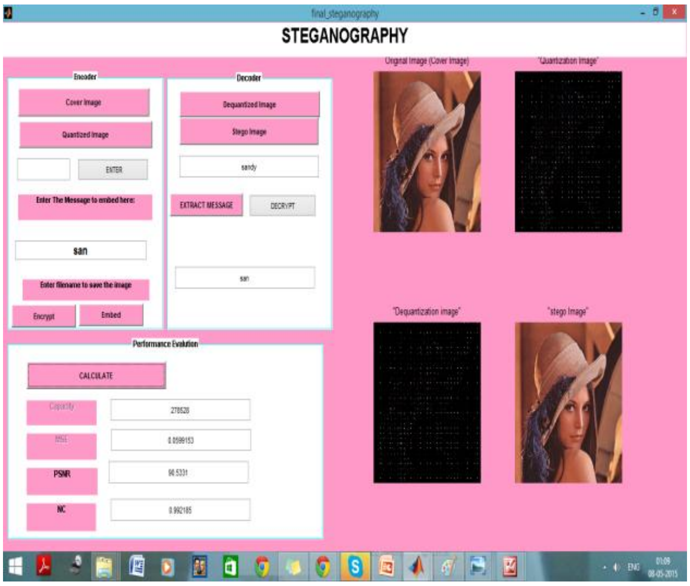
sandy

san

san

Figure no:4.12 Extract message after apply NN

The above figure shows the extracted message after applying neural network and decryption process and the message will be displayed in the edit box of the Graphical user interface.



sandy

san

san

Capacity 278528
MSE 0.0599153
PSNR 98.5331
NC 0.992185

Figure no: 4.13 Evaluation Parameters

The above figure shows the evaluation parameters like capacity which should be high, mean square error rate which should be less for the appropriate output, peak signal to noise ratio which should be high and node count. The Peak Signal-to-Noise Ratio (PSNR) is calculated to measure the quality of stego image. PSNR is defined as the performance of the image in terms of noise. More the PSNR better will be the quality of the image. The PSNR is calculated in db. MSE is defined as the Mean square error which defines the average of all the errors in the system and for better quality of the system the MSE parameter should be minimum.

PSNR: The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

MSE: The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where M and N are the number of rows and columns in the input images, respectively.

5. CONCLUSION AND FUTURE SCOPE

As we have already discussed about the need of the steganography and its uses. This research work has been implemented to enhance the steganography technique so that the quality of the image remains the same .To implement these objectives; Neural Network has been used in a combination with DCT, LSB and quantization matrix and the encryption of the text using security algorithms AES and RSA.

We overall concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. Neural Network has been found effective enough to find pixels to merge the data bits without much affecting the original pattern of the image. Then the parameters evaluate the Means Square Error, Peak Signal to noise ratio, Node count and Capacity.

Although the results are quite satisfactory but there is always a hope of improvement in the current work .Our current approach opens up a lot of premises of development for the future users of Neural Logics. The current work does not comprise with the noisy image. Future research workers can get to see how the current scheme goes with different levels of noise. The effect of different types of noise may also put some different effect on the approach. Also some other methods of Neural Network can be also tried.

REFERENCES

1. A. Tirkel , R. Schyndel and C. Os born, "A digital watermark", in Proc. IEEE Int. Conf. Image Processing. 1994, vol. 2, pp. 86-90.
2. R. Wolfgang and E. Delp, "A watermark for digital image", in Proc. IEEE Int. Conf. Image Processing, 1996, vol. 3, pp. 219-222.
3. A. Daneshkhah, H. Aghaeinia, and S. H. Seyedi, "A more secure steganography method in spatial Domain," in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, pp. 189–194, IEEE, 2011.
4. Sujay Narayana and Gaurav Prasad. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. The International Journal of Signal & Image Processing (SIPIJ), Vol.1, No.2, pp. 60-73, December 2010.
5. S. M. Masud Karim M. S. Rahman, and M. I. Hossain. A New Approach for LSB Based Image Steganography using Secret Key. Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp. 286 – 291, 2011.
6. R. -Z. Wang, C. -F. Lin, and J. -C. Lin, "Image hiding by optimal lsb substitution and genetical algorithm," Pattern recognition, vol. 34, no. 3, pp. 671–683, 2001.
7. R. Mersereau and F. Alturki, "Secure Blind Image Steganographic Technique Using Discrete Fourier Transformation", in Proc. IEEE Int. Conf. on Image Processing, vol. 2,2001, pp. 542-545.
8. W. Sweldens y B. Yeo ,A. R. Calderbank, I. Daubechies, "Lossless ImageCompression Using Integer to Integer Wavelet Transforms", Proc. of Int. Conf. on Image Proc, 1997, pp. 596-599.
9. Anuja Kumar Acharya, 2011. Image encryption using new chaos based encryption algorithm. In International Conference on Communication, Computing & Security (ICCCS).
10. D. N. Naitik P Kamdar, Dipesh G. Kamdar, "Performance evaluation of lsb based steganography for Optimization of psnr and mse," Journal of information, knowledge and research in electronics and Communication engineering, vol. 2, no. 2, pp. 505–509.
11. N. S. Raghava1, Ashish Kumar, Aishwarya Deep and AbhilashaChahal, "Improved LSB method for Image Steganography using H´enon Chaotic Map", open journal of information security and applications volume 1, number 1, june 2014.