Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network

Kamal[1],
Masters Of Computer Science and Technology,
BMSCE, Sri. Muktsar Sahib

Lovnish Bansal[2],
A.P, Computer Science Department,
BMSCE, Sri.Muktsar Sahib

Abstract: - Steganography and cryptography are two processes used for sending information in a secret way. Goal of both processes is to provide protection for information but in different way. In this paper our motive to represent a new method for protection so that information is not only in coded form but also not visible to intruder that is generated by combination of both processes steganography and cryptography. Neural Networks has been found effective enough to extract data bits without affecting the original pattern of image. There are many algorithms exist for both processes. For cryptography there are algorithms like RSA, IDEA, AES, and DES but here we are using only one algorithm from these that is RSA and DCT with LSB for steganography which is enough to implement combined process. First of all, message to be send is encrypted i.e. in coded form using RSA algorithm, then encoded message is embedded using DCT with LSB in digital media.After that we use custom neural network technique for extracting encrypted data from digital image. All implementation is performed on the basis of PSNR, MSE parameters. It has been evaluated that Proposed method offers better PSNR values than existing methods, so better security and hiding of data..

Keywords: - Steganography, Cryptography, RSA, Neural Network, DCT

I. INTRODUCTION

There are two processes exist that are used for sending information in secret way. These processes are known as cryptography and steganography . Both techniques widely used for protection of information or data. Stenography is art of that technique in which information hides on the way of communication between two nodes. In this paper we hides secret encoded data in digital image. Cryptography covert message in cipher text form so that it is not possible for unauthorized party to understand it. So the information hidden by steganography technique cannot see by any other person that is not authorized for it. In this paper we are going to develop a new system by using both processes steganography and cryptography. New system developed for better protection and confidently. Now days mostly used we have a cryptography technique - RSA very secure technique. This paper will highlight a new method that is developed for more security where data can be encrypted and hidden by using cryptography and steganography. Advantages these processes offers are like:

- It is more secure if we send data in hidden form as compared to send it only in encrypted form.
- Main benefit of hidden data is that attention of intruder cannot notice it.
- By chance if data is extracted then it can't be revealed as it is in encrypted form.

II. PROBLEM STATEMENT

Combining the DCT algorithm along with Back Propagation Neural Network in such a way that the image quality which is measured in terms of PSNR increases and the data remains safe within the image and using RSA is for data encryption. Our Focus is to offer least visibility and interference of secret data.

Our Objective is to divide the image into segments according to 32*32 segmentation plan and to extract the ascii encoded bits from the base image using Back Propagation neural networks. Finally, to compare the results with the previous approaches on the basis of PSNR , MSE .

III. BASIC CONCEPT AND RELATED WORK

There are many techniques available for secure transmission through communication channel, one of these is cryptography. But it should be in mind that when only cryptography is applied for protection that is not sufficient to provide good security. As like cryptography, steganography is other technique that is used for secure communication. In this paper, we hides encoded message inside digital image by combining Steganography with cryptography and using neural networks.

A. Steganography

Steganography is art in which information is hidden on the way of communication between two nodes e.g inside digital image, text message. So the information hidden by Steganography technique cannot seen by any other person that is not authorized for it. Basically two types of Steganography: spatial domain and frequency domain Steganography[1].In this paper ,We have used combination of both techniques so that message resides in more robust areas and it offers less visibility but more security of data. We have used combination of DCT [8] and LSB[3][5] using 32*32 bit DCT segmentation plan.

B. RSA Algorithm For Cryptography

RSA based on a public key system that is generated by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman in 1978. Cryptography covert message in cipher text form so that it is not possible for unauthorized party to understand it.In this proposed work asymmetric cryptography is used as it offers both public and private key .It offers more security, message authentication, non- repudiation of data. We have used RSA algorithm to implement asymmetric cryptography as it offers better integrity and no intermediate loss of data .We generates secret key or private key for transmitting data and receiver having that secret key can only access that data, so results in prevention of unauthorized access[7].Three basic

ISSN: 2278 – 1323

steps are required to complete the process of RSA operations that are; key generation(both public and private key), encryption and decryption. First, messages are converted to numbers (integers), and then the numbers are manipulated according to the prescribed encryption scheme.

C. Neural Networks

In this paper we are going to implement our method by using both processes steganography and cryptography i.e developed for better protection and confidently. After that we use custom neural network technique i.e using back-propagation feed forward neural networks for extraction of encoded bits. Using neural networks gives best results[6].

There are three layer exist one is input and second is hidden layer and other is output layer. In Feed forward works only in forward direction but in back-propagation feed forward neural networks also works in reverse direction i.e back propagates and find errors and update weights accordingly. In input layer vectors that are pre-processed are presented and at output layer calculation of error performed. If error is finding at output layer then it comes on input layer by backward process. This process is continuing till the last pattern. This form an iteration process. At end of every-iteration test patterns are presented to neural network, and the prediction performance of network is evaluated. This neural Steganography is used for better protection and hiding of data[2].T represents Threshold

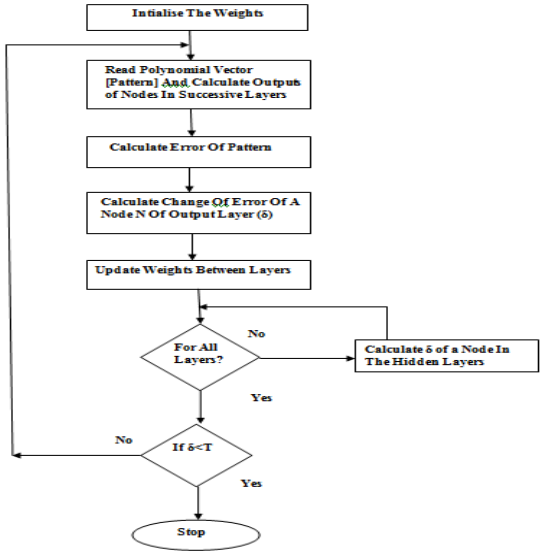

Fig 1: Back Propagation Feed Forward Neural Network Working

IV. PROPOSED ALGORITHM

We have proposed a new algorithm that provides more protection as compared to existing algorithms.The proposed algorithm has following steps:

- First take Cover Image i.e image in which we hide message
- Using DCT 32*32 block
- Perform Quantization
- Input Secret message to embed
- Encryption of message using RSA algorithm
- Embedding of message
- Extraction of message using BPA
- Finally get secret message.

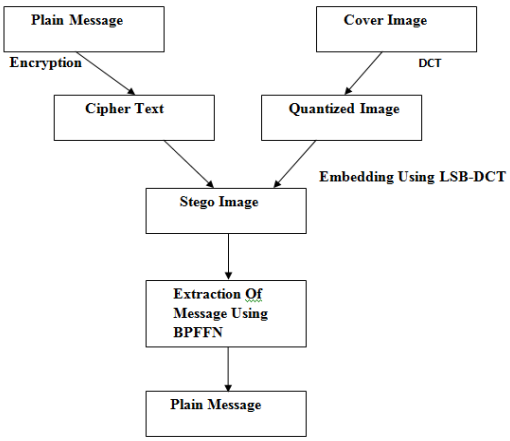

Fig 2: Flow Diagram Of Proposed Method

ISSN: 2278 – 1323

Fig 2 is showing a flowchart that is basic idea for development of new algorithm. The steps shown in flowchart which we need to follow to get results as we expected from new developed algorithm.

V. EXPERIMENTAL RESULTS

The quality of results obtained are depicted by

*a) **PSNR (Peak Signal To Noise Ratio***): Term for ratio between Maximum Possible power of signal and power of corrupting noise .R is maximum fluctuation in input image data type. More PSNR means more image quality and less distortion of secret message.

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \quad \text{.... (1)}$$

b*) MSE (Mean Square Error)*

It is means to quantify difference between values implied by an estimator and true values to quantify. I1 means original image,I2 resultant image and N are number of rows and columns in input image

$$MSE = \frac{\sum_{M,N}\left[I_1(m,n) - I_2(m,n)\right]^2}{M * N} \quad \text{....(2)}$$

Table I: Results of Proposed Algorithm

Image	PSNR	MSE
Lena.jpg	125.34	1.89e-008
Penguins.jpg	131.06	5.08e-009
Jellyfish.jpg	137.12	1.26e-009
Peppers.jpg	122.81	3.40e-008
Trees.jpg	111.31	4.80e-007
Koala.jpg	133.3	2.99e-009

The Proposed Method Offers better PSNR values as Compared to existing techniques. So, It results in Better protection and least visibility of data.

Table II: Comparison of Proposed Algorithm with Existing Techniques

Image Name	Technique	PSNR
 Trees.jpg	LSB-1st	63.9
	LSB-4th	52.41
	Chang	57.44
	LSB-DCT	30.4
	LSB-RSA	51.3
	HLSB-RSA	73.8
	Proposed Method	111.3
 Lena.jpg	LSB-1st	77.8
	LSB-4th	51.4
	Chang	52.7
	LSB-DCT	31.4
	LSB-RSA	51.07
	HLSB-RSA	74.01
	Proposed Method	125.3
 Peppers.jpg	LSB-1st	63.78
	LsB-4th	51.03
	Chang	51.7
	LSB-DCT	30.42
	LSB-RSA	51.3
	HLSB-RSA	73.1
	Proposed Method	122.8
 Baboon.jpg	LSB-1st	62.5
	LsB-4th	50.4
	Chang	51.7
	LSB-DCT	31.24
	LSB-RSA	51.4
	HLSB-RSA	73.85
	Proposed Method	121.5

ISSN: 2278 – 1323

VI CONCLUSIONS

This research paper presented the work that has been implemented to enhance the Steganography technique so that the quality of the image remains the same .Using DCT for 32*32 blocks and RGB image pixel embedding offers better results. It is concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. The Neural Network has been found effective enough to find pixels to extract the data bits with least affecting the original pattern of the image.

Our proposed method offers better psnr, mse values, so results better image quality and better way of hiding messages. 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 while image embedding**.**

ACKNOWLEDGEMENTS

Authors are gratefully thankful to Dr. Manoj Mittal, Principal, Bhai Maha Singh College Of Engineering, Sri. Muktsar Sahib for their support and constant guidance.

REFERENCES

[1] Singla D., "*Data Security using LSB and DCT Steganography in images*", IEEE International Conference ISSN-2332-1545 Vol 8, 2013
[2] Usha B.A ,Srinath N.K *"Data Embedding Technique in Image Steganography using neural network* ,IJARCCE - Vol. 2,Issue 5, 2013
[3] Goel and Rana .A "*Comparison Of Steganography Techniques*" International Journal of Computers and Distributed Systems ISSN: 2278-5183, pp 20-31, 2013
[4] Kumar A, Sharma R, "*A Secure Steganography Based On RSA Algorithm and Hash-LSB Technique*" IJARCSSE, ISSN: 2277, 2013
[5] Deepali, "*Steganography with data integrity*" International Journal Of computational engineering research (IJCER) ,pp. 190-193,2012
[6] Jbara. H, Kiah.L "*Increased Capacity of image based Steganography using artificial neural network*" American Institute Of Physics (AIP) Proc. 1482, International Conference on Fundamental and Applied Science , pp. 20-25.,2012
[7] Karim S., Rahman M , "*New Approach for LSB Based Image Steganography using Secret Key*" IEEE Proceedings of 14th international Conference On Computer and Information Technology(ICCIT) ,pp 286-291,2011
[8] Chang, Chen .T " *A Steganography Method Based Upon JPEG And Quantization Table Modification*" Information Science – An International Journal, pp 12-14,2002

Author(s) Profile

Er. Kamal, Obtained her B.Tech (CSE) Degree from P.T.U, Jalandhar with teaching experience of one year and pursuing MTech (CSE) from BMSCE, Sri. Muktsar Sahib, Affiliated to P.T.U Jalandhar.

Er.Lovnish Bansal (A.P and Head of Department, BMSCE ,Sri. Muktsar Sahib), Mtech (CSE), BTech (CSE) with teaching Experience of 6 years, has got three publications in international Journals and Two in National Conference.

ISSN: 2278 – 1323