PERFORMANCE ENHANCEMENT OF A STEGANOGRAPHIC TECHNIQUE IN INFORMATION HIDING

Snehlata

***Abstract*- Steganography is the art of inconspicuously hiding data within data.Steganograhy goal in general is to hide data well enough so that unintended recipients do not suspect the Steganographic medium of containing hidden data. As privacy concern to develop along with the digital communication domain, steganography will undoubtedly play a growing role in the society. For this reason, it is important that we are aware of steganography technique and its implications. This paper shows a combining technique of using DCT and Neural Network together so that a large amount of data can be store inside the image showing invisibility to the users and also enhances the level of security.**

***Keywords*- Stego object, Cover object, DCT (Discrete Cousin Transform), Steganography, NN (Neural Networks), RSA.sss**

I. INTRODUCTION

The word steganography is originally derived from Greek words which mean "Covered Writing". Steganography [4] is employed in various useful applications, e.g., copyright control of materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Secret information can be hiding in any sorts of covers like image, in form of videos, audios and more.

Information hiding [1] is a popular technique now a days and spread over the World Wide Web by which the level of security for data is less and safety of information is gone. So, to maintaining the security measure in this paper we proposed two methods for hiding the information used for image processing.

METHODS:

A. Discrete Cosine Transform (DCT)

Information hiding is an old but interesting technology. Steganography is a branch of information hiding in which secret information is camouflaged within other information. The schemes of embedding the secret data within the cover image that has been transformed such as DCT (discrete cosine transformation). The DCT transforms a cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8 × 8pixels and transforming the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data. Tseng and Chang in proposed a novel steganography method based on JPEG. The DCT for each block of 8×8pixels was applied in order to improve the capacity and control the compression ratio.

B. Neural Networks (NN)

An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. 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.

ISSN: 2278 – 1323

Neural networks [7], with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends [8] that are too complex to be noticed by either humans or other computer techniques. A trained neural network can be thought of as an "expert" in the category of information it has been given to analyze.

II. RSA ALGORITHM

The RSA algorithm [6] is introduced in 1978, when Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm; RSA consists of two types of the keys that are Public-Key and Private-Key. In the Cloud environment, the Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps that are: key generation, encryption and decryption.

A. Key Generation

1. Choose two distinct prime numbers that are as p and *q*.
   - For security purposes, the integers *p* and *q* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a optimality test.
2. Compute $n = pq$.
   - *n* is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Choose an integer *e* such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. *e* and $\varphi(n)$ are co prime.
   - *e* is released as the public key exponent.
5. Determine *d* as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., *d* is the multiplicative inverse of *e* (modulo $\varphi(n)$). This is often computed using the extended Euclidean algorithm. *d* is kept as the private key exponent.

B. Encryption

Computes the cipher text *c* corresponding to

$$c \equiv m^e \pmod{n}.$$

C. Decryption

Recover *m* from *c* by using her private key exponent *d* via computing

$$m \equiv c^d \pmod{n}.$$

III. PROBLEM STATEMENT

Steganography [3, 4] is a technique which leads to hiding content of one format to another or within the same format. In case of an image there has been a lot of work has been done in the same contrast .The techniques have been proved to a revolutionary step in the field of data hiding. As the passes on , the complexity to hide the data increases .We also need to prevent the base image (refers to the image in which we are hiding the data), so that if the image gets hacked the hacker won't be able to assume that some data has been into the base image by looking at the image. To achieve the same, a lot of previous algorithms have been proposed like DWT, DCT and so many other algorithms. This gives rise to our problem statement. Our problem statement involves combining the DCT algorithm along with

ISSN: 2278 – 1323

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.

IV. METHODOLOGY

This section describes the methodology and its related parameters used in our work:-

(a) System Parameter-The process is conducted using Intel i5 32bit processor with 4GB RAM and experimented algorithm that we perform is coded in Mat lab.

(b) *Experimental Factors*-Following are the evaluation parameters that have been considered for performance analysis:

- *PSNR (Peak Signal to Noise Ratio)*-It is the ratio of maximum possible power of corrupting noise that affects the fidelity of its representation.

$$\text{PSNR} = \frac{20 \log_{10} 256}{\sqrt{MSE}}$$

- *MSE (Mean Square Error)*-Defined as the square of the error between the cover image and Stego image, i.e. the distortion in the image can be measured using MSE.

$$\text{MSE} = \sum_{i=1}^{all\ pixels} \sum_{j=1}^{all\ pixels} \frac{(cov\,(i,j) - steg\,(i,j))^2}{N*N}$$

V. RESULT ANALYSIS

This section describe the result that we have obtained after implementation of our technique as from the previous .The following table has shown an improved PSNR values as compared from the previous value.

Table 1

Different Images showing Different Values

	Image Name	Image size	PSNR	MSE
Previous work	Lena	256*256	40.6	5.5
	Pepper	256*256	42.5	0.5
Our work	Lena	512*512	62.2	0.0
	Pepper	676*470	64.2	0.0

VI. CONCLUSION

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 our objectives, we have used Neural Network in a combination with DCT vector quantization method of 8*8 pixel management. 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. 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.

REFERENCES

[1] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta",HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY(HLSB)International Journal of Security, Privacy and Trust Management IJSPTM), Vol. 1, No 2, April 2012.

[2]Shamim Ahmed Laskar1 and Kattamanchi Hemachandran2 High Capacity data hiding using LSB Steganography and Encryption International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.

[3] "Adel Almohammad Robert M. Hierons" High Capacity Steganography Method Based Upon JPEG The Third International Conference on Availability, Reliability and Security The JPEG standard uses 8x8 quantization tables.

[4] "Ross J. Anderson, Fabien A.P. Petitcolas" On The Limits of Steganography IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

ISSN: 2278 – 1323

[5]"Usha B A1, Dr. N K Srinath2, Dr. N K Cauvery" DATA EMBEDDING TECHNIQUE IN IMAGE STEGANOGRAPHY USING NEURAL NETWORK International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013.

[6]" Ms. P. T. Anitha1, Dr. M. Rajaram2 ,Dr. S. N. Sivanandham" AN EFFICIENT NEURAL NETWORK BASED ALGORITHM FOR DETECTING STEGANOGRAPHY CONTENT IN CORPORATE MAILS: A WEB BASED STEGANALYSIS IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

[7] "Nameer N. EL-Emam" Efficient Steganography using NEURAL.

[8] "Imran Khan" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 2.

Snehlata is a student of M.Tech in Information Security at Chandigarh Engineering College, Landran, Mohali, Punjab, India. She is Bachelors in Information Technology. Her area of interests are Database and Security.

ISSN: 2278 – 1323