Performance Enhancement of a Transform Domain Based SteganographicTechnique Using Segmentation

Harjeet Kaur[1], Er Divya Goyal[2]

[1]M-Tech Research Scholar, Swami Vivekanand Institute of Engineering, Banur, India

[2]Assistant Professor, Swami Vivekanand Institute of Engineering, Banur, India

Abstract: ***Steganography is the art of inconspicuously hiding data within data. Steganography's goal in general is to hide data well enough that unintended recipients do not suspect the steganographic medium of containing hidden data. The software and links mentioned in this article are just a sample of the steganography tools currently available. As privacy concerns continue to develop along with the digital communication domain, steganography will undoubtedly play a growing role in society. For this reason, it is important that we are aware of Steganography enhances rather than replaces encryption. Messages are not secure simply by virtue of being hidden.***

Keyword: Stego-object, Cover-object, Steganalysis, Cover Image, Embedding key, Extraction key, Steganography

1. Introduction

The word steganography is derived from the Greek words stegos meaning cover and graphy meaning writing [1] defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data[2].

Image steganography is the art of hiding information into a cover image. This paper presents a novel technique for Image steganography based on Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. Firstly a gray level image of size M x N is divided into no joint 8 x 8 blocks and a two dimensional Discrete Cosine Transform (2-d DCT) is performed on each of the P = MN / 64 blocks. Then Huffman encoding is also performed on the secret messages/images before embedding and each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks. The experimental results show that the algorithm has a high capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows the better results in comparison with other existing steganography approaches. Furthermore, satisfactory security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Huffman table.

Steganography is a technique of information security that hides secret information within a normal carrier media, such as digital image, audio, video, etc. An unauthorized attempt to detect and extract the hidden secret information from stego is known as steganalysis. If any steganalytic algorithm Can detect whether given media is a carrier then the steganography algorithm is considered to be broken.

In this paper we consider digital image as carrier and develop a steganography algorithm in spatial domain with LSB replacement based on DCT coefficients of the pixels. The basic LSB based technique simply replaces the LSB plane of the carrier image with the bit stream of secret information.

Computational Parameters:

a) **PSNR:** Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the powcorrupting noise that affects the fidelity of its representation.
b) **MSE**: In statistics, the mean squared error of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.
c) **CAPACITY**: It is size of the data in a cover image that can modified without deteriorating the integrity of image.
d) **NODE COUNT:** It is the number of nodes count when we hide the information or data behind a image.

2. Related Work

[1]Deeply has research described as the method of Steganography based on embedding encrypted message bits using RSA Algorithm in the 1st least significant (LSB Technique) and last 4 significant bits (Modulus 4 bit technique) of the pixel of image. [2].Attalla M. Al-Shatnawi has discuss the proposed method is compared with the LSB benchmarking method. It is implemented to hide the secret message "I will come to see you on the first of June" on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x

165) respectively. The results of the pr oposed and LSB. [3]. T. Morel et al. research overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm. [4]. PROF. AKHIL KHARE, define main advantage of this project is a simple, powerful and user-friendly Guff that plays a very large role in the success of the application. **[6].** Gabriel Hospodar has provide the information is embedded into Discrete Cosine Transform (DCT)coefficients of 8 fi 8-pixel blocks in a natural digital image. [7]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 talks about LSB Technique. [8] "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, but it does not specify default or standard values for quantization tables. Specifying the quantization values is left up to the application. . A biological neural network [6] is composed of neurons with same functionality.According to them The neural approach to embed information satisfies a secure steganography. Neural approach adds the complexity for the hackers accessing and also presents high potentiality in defense operations.

3. Neural Network

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.

4. Proposed Work

Spatial Domain Technique Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible.

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.

RSA Algorithm.

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. By using the RSA algorithm we are increasing the security to a level above.

RSA Encryption and Hash-LSB Encoding

In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image

Embedding Algorithm:

Step 1: Choose the cover image & secret message.
Step 2: Encrypt the message using RSA algorithm.
Step 3: Find 4 least significant bits of each RGB pixels from cover image.
Step 4: Apply a hash function on LSB of cover image to get the position.
Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.
Step 6: Send steno image to receiver.

Hash-LSB Decoding and RSA Decryption

In the decoding process we have again used the hash function to detect the positions of the LSB's where the data bits had been embedded. After retrieving the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable for Retrieval Algorithm.

Retrieval Algorithm Step1:Receive a steno image.
Step2:Find 4 LSB bits of each RGB pixels from steno image.
Step3:Apply Hash Function to get the position of LSB's with hidden data
Step4:Retrieve the bits using these positions in order of 3,3,and 2 respectively.
Step4:Retrive the bits using these positions in order of 3,3,and 2 respectively.
Step5:apply RSA algorithm to decrypt the retrieved data.
Step6:Finally read the secret message.

5. Results

The results are taken in matlab programming. The PSNRand MSE values are calculated using equation (1) and (2)The Peak Signal-to-Noise Ratio (PSNR) is defined as:

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

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

$$\text{MSE}=1/mn \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \qquad \text{eq(2)}$$

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

Images

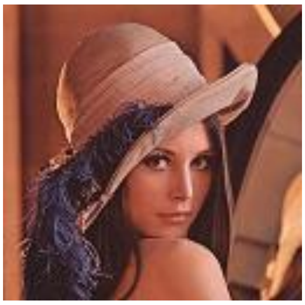

Figure 1.1: Image1(leena)

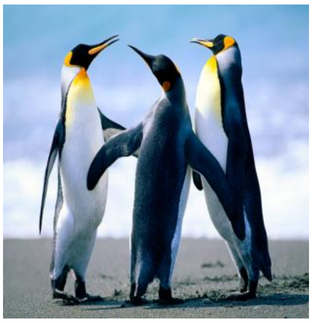

Figure 1.2: *I*mage2(penguins)

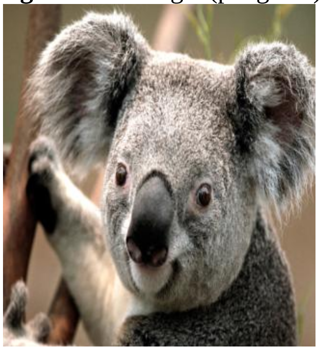

Figure 1.3: Image3(koala)

Table and Graph

Table 1.1: Result of Proposed TechniqueTable

Image	Capacity	PSNR	MSE	NC
Image1	278528	85.11	.0008	.991
Image2	835584	91.81	.00036	.993
Image3	835584	91.43	.00018	.997

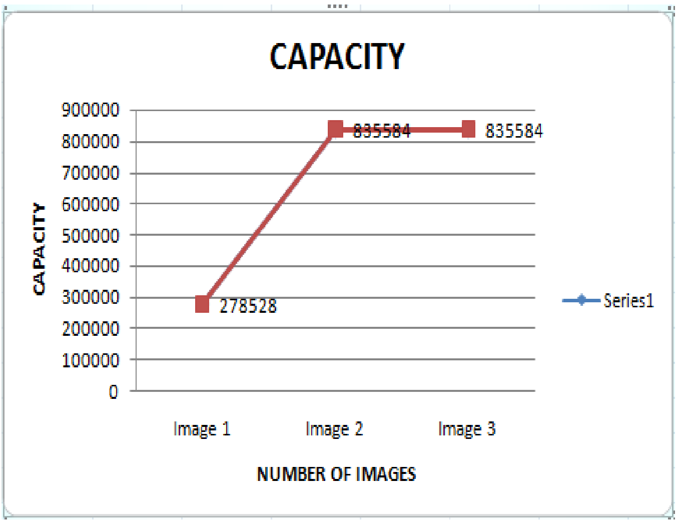

Figure 1.4: Capacity Chart

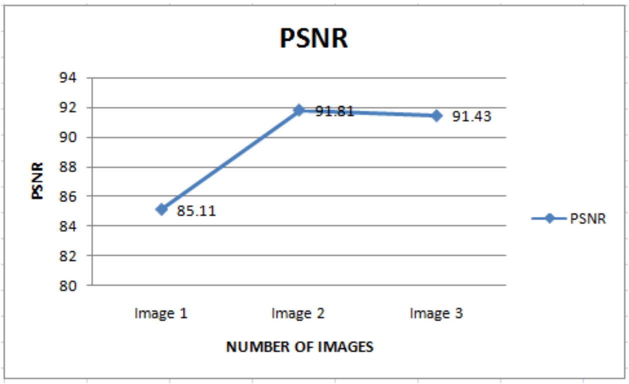

Figure 1.5: PSNR Chart

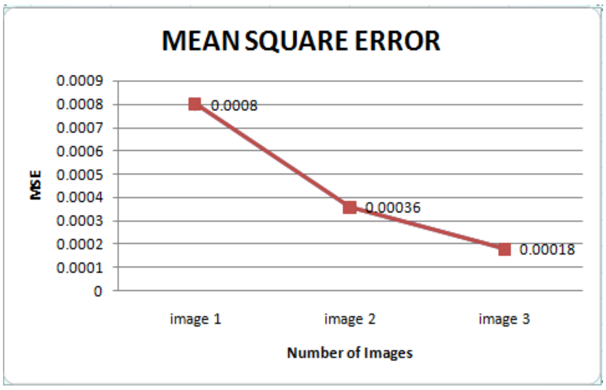

Figure 1.6: Mse chart

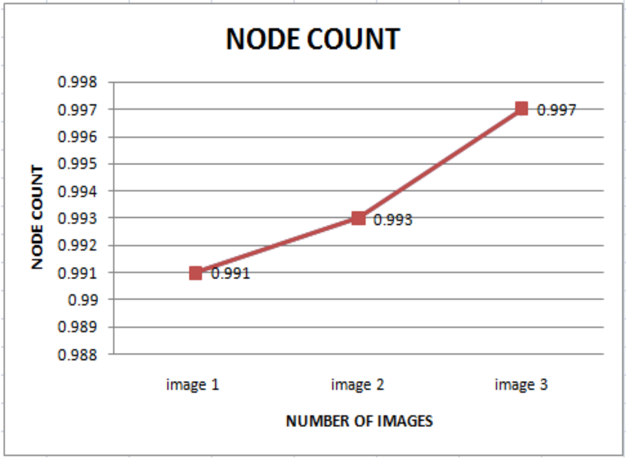

Figure 1.7: NC chart

6. Conclusion

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 ENCRYPTION MECHANISM along with 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.

7. Future Scope

The current work does not comprises 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] Deeply *"Steganography With Data Integrity"* International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 7 Sins 2250-3005(online) November| 2012.

[2] Attalla M. Al-Shatnawi "*A New Method in Image Steganography with Improved Image Quality"*Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 - 3915

[3] T. Morel , J.H.P. Elf , M.S. Olivier "*An Overview Of Image Steganography* " Information and Computer Security Architecture (ICSA) Research Group Department of Computer ScienceUniversity of Pretoria, 0002, Pretoria, South Africa.

[4] Prof. Akhil Khare, 2Meenu Kumar, J Palla VI Khare "*Efficent Algorithm For Digital Image Steganography"*Journal Of Information, Knowledge And Research In Computer Science And Application ISSN: 0975 - 67281 NOV 09 TO OCT 10 1Volume 1, Issue 1

[5] Sneak Arora1, Sanlam An and "*A Proposed Method for Image Steganography Using Edge Detection* "International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2, February 2013).

[6] Gabriel Hospodar "*Algorithms for Digital Image Steganography via Statistical Restoration"*_ ESAT/SCD-COSIC and IBBT, Katholieke Universities Leuven Kasteelpark Ehrenberg 10, bus 2446, 3001 Heerlen, Belgium.

[7] Vardeep Kaur Mann and Harmanjot Singh Dhaliwal "*32*32 Colour Image Steganography*" International Journal of Engineering Trends and Technology (IJETT) Vol.4,Issue 8 August 2013

[8] Deepak Singla,"*Data Security using Lsb &Dct Steganography In Images"*(IEEE) vol 8 2013.

[9] 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

[10] 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,

[11] 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.

[12] 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

[13] 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

[14] Hafiz Malik, K. P. Subbalakshmi,*"Nonparametric Steganalysis of QIM Steganography Using Approximate Entropy"* IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[15] Dr. Ekta Walia, Payal Jain, Navdeep, *"An Analysis of LSB & DCT based Steganography"*, Global Journal of Computer Science and Technology, Vol. 1, pp. 4-8, April, 2010.

[16] F. Alturki ,R. Mersereau, *"Secure blind image steganographic technique using Discrete Fourier Transformation"*, IEEE Proc. Int.Conf. on Image Processing, 2001, vol. 2, pp. 542-545.

[17] Wenqiong Yu, *"Blind Detection for JPEG Steganography"*, International Conference on Networking and Information Technology , pp. 128-132, July 2010.

[18] Yasser M. Behbahani, Parham Ghayour,*"Eigenvalue Steganography Based on Eigen Characteristics of Quantized DCT Matrices"* Proceedings of the 5th International Conference on IT & Multimedia at UNITEN (ICIMU 2011) Malaysia .

[19] Natee Vongurai and Suphakant Phimoltares, *"Frequency-Based Steganography Using 32x32 Interpolated Quantization Table and Discrete Cosine Transform"* 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation.

[20] P.Nithyanandam, T.Ravichandran, N.M.Santron and E.Priyadarshini, *"A spatial domain image steganography technique based on matrix embedding and huffman encoding"*, Int. J. ofComputer Science and Security, vol. 5 , issue 5, 2011, pp. 456-468.

[21] Daemen J., and Rijmen, V. *"Rijndael: The Advanced Encryption Standard"*, Dr. Dobb's Journal, March 2001.

[22] Zhang Chun-e, QIU Zhengding, Cheng L.L, *"Analysis Based on Generalized Vector Quantization for Information Hiding"* International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2008.

[23] M.H. Lin, Y.C. Hu, C.C. Chang, *"Both color and gray scale secret images hiding in a color Image"*, International Journal of Pattern Recognition and Artificial Intelligence 16 (2002)

Author Profile

Harjeet Kaur is Student of M.Tech in the Department of Computer & Sci Engineering at Swami Vivekanand Institute of Engineering, Banur under Punjab Technical University, Jalandhar. She has done B.Tech From Yadawindra College of Engg & Tech Talwandi Sabo(Punjabi Uni Patiala).

Er Divya Goyal is the Astt. Proff in the Department of Computer & Sci Engineering at Swami Vivekanand institute of Engineering, Banur under Punjab Technical University, Jalandhar. She has done her B.tech From PIET college of Engg & Technology under PTU & her M.Tech is from Lovely university Jalandhar.