ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Performance Upgradation of a Transform Domain based Steganography using Neural Logics

[I]Vikas Nain, [II]Nishu Bansal
[I,II]Dept. of Computer Science, IGEF - Abhipur, Mohali, Punjab Technical University, Jalandhar, India

Abstract
*In this paper, we describe the Image Steganography is a field which refers to hiding some content into another. In our research work we are trying to merge text into image. For any context to be merged into an image it is necessary to change the image in to a form where another content can be added, for the same purpose we are using the DCT vector quantization method. A DCT method changes the entire content into bits and computes the vacant spaces of the image. In our research work we have used 16 * 16 vector matrix. The content to be merged is changed into its relevant ASCII characterization. Both the two context the quantized matrix and the changed ASCII content goes to the artificial neural network for further processing. Artificial neural network takes both as an input and generates the weight of each section accordingly. A bandwidth for both sections composedly gets generated from the neural network accordingly. The neural is then responsible for the merging part so that the bits gets a minimum distortion so that the quality of the image remains unchanged or slightly distorted to maintain the PSNR of the image. The parameters of the judgment of our research work are PSNR, TIME to extract the content.*

Keywords
Capacity, PSNR, NC, CR, TIME, Steganography, DCT (Discrete Cosine Transformation), Cover Image, Stego-Image, Artificial Neural Network, Vector Quantization, Data hiding.

I. Introduction

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 16 x 16 blocks and a two dimensional Discrete Cosine Transform (2-d DCT) is performed on each of the P = MN / 256 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.

The important requirement for a good steganography algorithm is that the stego-media should remain identical to the original carrier media, while keeping embedding rate as high as possible. 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. These methods are based on false assumption that LSB plane of natural images is random enough, thus are suitable for data hiding. Such assumption is not always true, especially for images with more smooth region. A technique based on Least Significant Bits replacement considering DCT coefficient value of pixels. The DCT of carrier image is obtained then based on proper threshold random locations are selected. LSBs of these potential locations in carrier image are replaced with MSBs of the secret image.

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data.

Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectable difference between cover and stego-image, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism.

The standard and concept of "What You See Is What You Get (WYSIWYG)" which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words. For decades people strove to develop innovative methods for secret communication. The remainder of this introduction highlights briefly some historical facts and attacks on methods (also known as steganalysis).

Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart

especially for those coming from different disciplines.

II. Related Work

Data hiding is the most important technique for achieving better data protection by hiding the information into a media carrier. It provides secure method to communicate through public and open channels. Vector Quantization (VQ)-based image focuses on the problem of embedding secret data into a carrier VQ-based image to achieve the secret communication. VQ-based data hiding method [1] which produces stego-image as its output can embed more secret data than a reversible method.

The steganography can be classified into two main types i.e. spatial domain and frequency domain. Some studies also shows that by using Discrete Cosine Transformation (DCT) and JPEG with 32*32 quantization table instead of using 8*8 quantization table, created by a cubic interpolation technique [2] results shows that the computation time can be reduced and it also increases the capacity of the secret messages while maintaining the image quality and the size of the JPEG stego-image.

There is a new method of steganography whose foundation lies on neural network [8]. The amount of data that can be embedded or hidden inside the cover image chosen depends upon the properties of the image like number of noisy pixels. The neural network based image steganography ensures that quality and the size of the image remains the same after embedding the data into the cover image. Neural network based steganography has wide range of applications today like in military, media database systems and secret data storing etc.

III . Proposed Method

In this paper the we are using the .jpg images as the cover image, which are further quantized so that the data can be embedded in the form of text. Then the embedding is done with the help of DCT and Neural network. After the embedding is done the quantized image is again dequantized to make the final output in the form of image, which will look like the original cover image and one cannot distinguish between the cover image and the stego-image with his naked eyes. At the receiver side the user can extract the embedded message in the text form again. The process is shown the fig. 1 below :

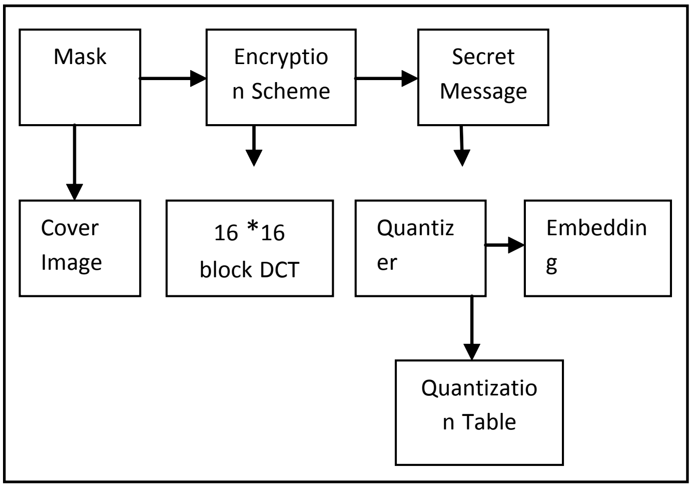

Fig. 1: Flow diagram of the process

A. Cover Image

The cover image is that image in which we want to do the embedding process. Cover image is sometimes called as Carrier image. It will carry the text in hidden form which can't be seen with naked eyes by any unauthorized person.

B. Mask

In this regard mask is the 16*16 matrix.

mask = [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0
1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0
1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0
1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0
1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0
1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0
1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]

In this process this mask will be multiplied with the cover image. Mask is used for encryption process or we can say that the embedding process.

C. Discrete Cosine Transformation (DCT)

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio e.g. MP3 and images e.g. JPEG (where some high-frequency components can be discarded), to spectral methods for numerical solution of partial differential equations. The use of cosine rather than the sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient, fewer functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry, since the Fourier transform of a real and even function is real and even, where in some variants the input and/or output data are shifted by half a sample.

The DCT is often used in signal and image processing, especially for lossy data compression, because it has a strong energy compaction property most of the signal information tends to be concentrated in a few low-frequency components of the DCT.

The fig.2 shows the process of implementing Discrete Cosine Transformation (DCT) and Inverse-Discrete Cosine Transformation (IDCT) in the embedding process.

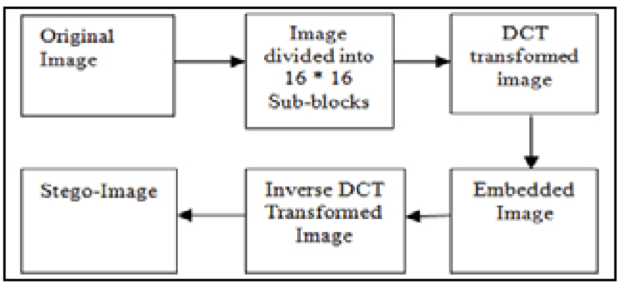

Fig. 2: The process of embedding in DCT domain

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

D. Vector Quantization

Vector quantization is the natural generalization of scalar quantization. It involves the quantization of vectors rather than scalars. A vector quantizer Q of dimension n and size N is a mapping from a vector in n-dimensional Euclidean space Rn into a finite set C containing N reproduction points, called code vectors or codeword. Thus Q: Rn_C, where C = {y1, y2, …, yN} and yi _Rn for each i_J = {1, 2, …, N}. The set C is called the codebook and has N distinct vector in Rn as its elements. The rate of a vector quantizer is r = (log2N)/n and measures the average number of bits spent per input vector component.

A vector quantizer can be decomposed into two operations: the vector encoder and the vector decoder. In more concise notation; Q(x) = D(E(x))

The encoder E is a mapping from Rk onto the set of indices J, while the decoder D maps the index set J onto the reproduction set C.

E. Neural Network

Unlike Von Neumann computation model, artificial neural networks do not separate memory and processing from one another. They operate via the flow of signals. It happens through the net connections. It is somewhat similar to biological neural network. These artificial neural networks may be used for prediction. Other applications include they can be trained via a dataset. A biological neural network is composed of neurons with same functionality. Here the artificial neural network will help in optimization of the process in maintaining the quality of the stego-image after embedding.

IV. Computational Parameters

A. PSNR

Peak Signal-to-Noise Ratio is often abbreviated as PSNR. It is an engineering term for the ratio between the maximum possible power of the signal and the power of corrupting noise that effects the fidelity of representation of the required data.

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) = 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image and MSE is the Mean Squared Error.

B. Capacity

Capacity is the amount of data that can be embedded into the cover image. It is a very important characteristic of the embedding process, because it defines the actual information carrying capability of the cover image. More the capacity better the embedding technique.

C. Computational Time

Time is also an important aspect when we are talking about the embedding process. It is the time required in the embedding process. Generally its output is in mili-seconds (ms). Lesser the time better is the technique.

D. Compression Ratio (CR)

Compression Ratio is an very important aspect. It is the amount of bits in the original image by the amount of bits in the compressed image. Since all values (DCT coefficients) are represented by the same fixed amount of bits, it can be deduced from the counting of the number of coefficients instead of bits.

Compression ratio = num j / num k, where j is the number of coefficients in original image, whereas k is the number of coefficients in compressed image or we can say stego-image.

V. Experimental results

These experiments are conducted on MATLAB 2010 on Windows7 Professional 32-bit, 2304MB RAM, 1.9GHz Intel Celeron(R) M CPU. The experimental results shows the following results. Fig.3, Fig.5 and Fig.7 shows the cover / original image showing image of Lena.jpg, Baboon.jpg and Pepper.jpg which are before doing the information embedding process, whereas fig.4, Fig.6 and Fig.8 shows stego-image of Lena, Baboon and Pepper after information embedding process. As we can see there not so of much visible difference between these under-lying images. These images are not distinguishable by naked eyes. There is not so called degradation in the second image i.e. Lena.jpg, Baboon.jpg and Pepper.jpg stego-images.


Fig. 3: Cover Image (Lena)


Fig. 4: Stego-Image (Lena)


Fig. 5: Cover Image (Baboon)


Fig. 4: Stego-Image (Baboon)


Fig. 7: Cover Image (Pepper)


Fig. 8: Stego-Image (Pepper)

Table 1 shows the experimental outputs as on conducted on above shown image of 512*512 Lena.jpg, 512*512 Baboon.jpg and 512*512 Pepper.jpg images.

Table1 :Table showing Performance Evaluation

		Capacity	PSNR	CR	Time
Lena	Our Method	336794	79.27	4.4	0.477
	Previous Research	256000	39.6	3.02	0.34
Baboon	Our Method	336794	77.20	4.56	0.598
	Previous Research	256000	42.3	2.47	0.35
Pepper	Our Method	336794	78.04	4.56	0.658
	Previous Research	256000	36.4	2.92	0.33

VI. Conclusions

As we have already discussed above 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 16*16 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.

VII. AcknowledgEment

I would like to place on record my deep sense of gratitude to my guide Asst. Professor Nishu Bansal, Dept. of Computer Science, IGEF, Abhipur, Mohali, India, for her generous guidance, help and useful suggestions.

I also wish to extend my thanks to Mr. Bhupinder Singh, H.O.D of Computer Science Department of IGEF, Abhipur and all faculty member of CSE department for attending my seminars and for their insightful comments and constructive suggestions to improve the quality of this research work.

I am extremely thankful to Dr. Promila Kaushal Principal, IGEF Abhipur, for providing me infrastructure facilities to work in, without which this work would not have been possible.

References

[1] *Wei-Jen Wang, Cheng-Ta Huang and Shiuh-Jeng Wang. 2011 VQ applications in steganographic data hiding upon multimedia images. IEEE Systems Journal, VOL. 5, NO. 4.*

[2] *Natee Vongurai and Suphakant Phimoltares. 2012 Frequency-based steganography using 32x32 interpolated quantization table and discrete cosine transform. Fourth international conference on computational intelligence, modelling and simulation.*

[3] *Zhang Chun-e, Qiu Zhengding, Cheng L.L. and Cheng L.M.. Analysis based on generalized vector quantization for information hiding. International conference on intelligent information hiding and multimedia signal processing.*

[4] *Yasser M. Behbahani. 2011 Eigenvalue steganography based on eigen characteristics of quantized DCT matrices. 5th international conference on IT & multimedia at UNITEN (ICIMU 2011) Malaysia.*

[5] *Hafiz Malik, Member IEEE, K. P. Subbalakshmi, Senior Member IEEE, and R. Chandramouli, Senior Member IEEE. 2012 Nonparametric steganalysis of QIM steganography using approximate entropy. IEEE transactions on information forensics and security, Vol. 7, No. 2.*

[6] *Chin-Chen Chang, Fellow, IEEE and Chih-Yang Lin. 2006 Reversible steganography for VQ-Compressed images using side matching and relocation. IEEE transactions on information forensics and security, Vol. 1, No. 4.*

[7] *Yi-zhen Chen, Zhi Han, Shu-ping Li, Chun-hui Lu, Xiao-Hui Yao. 2010 An adaptive steganography algorithm based on block sensitivity vectors using HVS features. 3rd International congress on image and signal processing (CISP 2010).*

[8] *Usha B A, Dr. N K Srinath, Dr. N K Cauvery. 2013 Data embedding technique in image steganography using neural network. International journal of advanced research in computer and communication engineering, Vol. 2, Issue 5.*

[9] *Ms. P. T. Anitha, Dr. M. Rajaram, Dr. S. N. Sivanandham. 2012 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.*

[10] *Nameer N. EL-Emam. Embedding a large amount of information using high secure neural based steganography algorithm. International journal of signal processing, Vol. 4, No. 2.*

[11] *Imran khan. 2011 An efficient neural network based algorithm of steganography of image. International journal of computer technology and electronics engineering (IJCTEE), Vol. 1, Issue 2.*

Author's Profile

Department of Computer Science, IGEF - Abhipur, Mohali,, Punjab Technical University, Jalandhar, India. Email id – vikas1nain@gmail.com