ISSN: 2348 9510
International Journal Of Core Engineering & Management(IJCEM)
Volume 1, Issue 2, May 2014

SECURE AND SECRET TRANSMISSION OF MESSAGES USING THE DCT TECHNIQUE OF STEGANOGRAPHY

Dr. Raman Chadha
Head, Department of Computer Science Engineering
Chandigarh Group of Colleges Technical Campus,
Jhanjeri, Mohali, India
Dr.ramanchadha@gmail.com

Er. Bhavneet Kaur (Assistant Professor),
Asst. Professor, Department of CSE,
Chandigarh Group of Colleges Technical Campus,
Jhanjeri, Mohali, India
bk.cgctc@gmail.com

Abstract: Steganography is the art and technique for hiding the secret message in some cover. The cover may be an image or audio or video. Similarly, the message to be sent may be anything like some form of text, any form of the image etc. There are many techniques available for doing the same. In this paper, we are trying to present the new technique which is Discrete Cosine Transformations and the Vector Quantization for improving the capacity of the cover medium.

Keywords: Cover medium, Stego image, Quantization, DCT, secret message, embedding algorithm, extraction algorithm.

INTRODUCTION

Image steganography is the art of hiding information into a cover image. In this paper, we present a novel technique for Image steganography based on Block-DCT, where DCT is used to transform the original image (cover image) blocks from spatial domain to frequency domain. The important requirement for a good steganography algorithm is that the stego media should remain identical to the original carrier medium and also keeping the embedding rate as high as possible. In this paper we consider digital image as carrier and develop a steganography algorithm in spatial domain based on DCT coefficients of the pixels. The following figure i.e. Figure 1. shows the basic steganographic system in which we have the cover image c(the image in which we can hide our secret information) and the hidden message M(that we need to hide). After combing both these, i.e. the cover medium as well as the secret information, we receive the Stego- Image(i.e. the image that contains both the message as well as the cover). This is known as Steganography and detecting the presence of the steganography is known as Steganalysis.

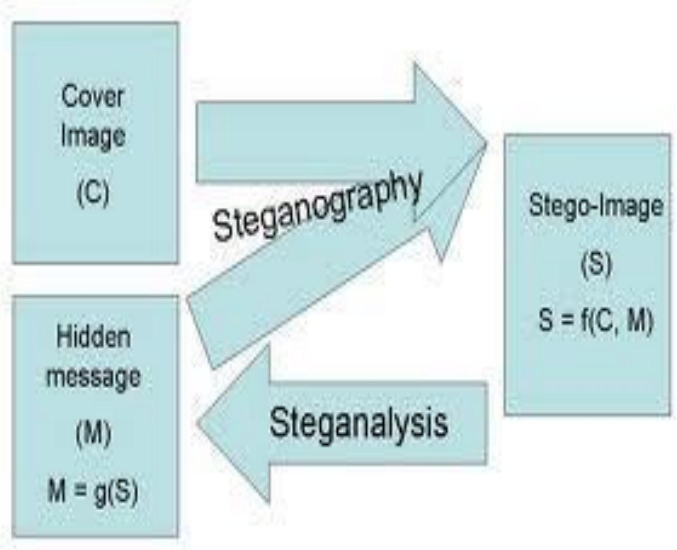

Figure1. The Steganography System

STEGANOGRAPHY APPLICATIONS

Steganography is employed in various useful applications, e.g., copyright control of materials, usage by the intelligent services, usage in modern printers etc.

Steganography is applicable to many areas such as:

1. **Confidentiality of communication and secret storage**

of data.

The "secrecy" of the embedded data is essential in this area. Steganography provides us with the following:

- Potential capability to conceal the existence of confidential data.
- Hardness of detecting the hidden (i.e., embedded) data.
- Strength the secrecy of the encrypted data.

2. **Protection from data alteration.**
   The novel point among others is that no authentication agency is needed. In case it is implemented, people can send their digital certificate data to any place in the world through Internet. No one can forge, alter and nor tamper such certificate data. If forged, altered or tampered, it can be easily detected by the extraction program.

3. **Access control system for the digital content distribution.**

▪ Nowadays, digital contents are getting more commonly distributed on Internet than ever before. For example, music companies release their new albums on their webpage for free or may be charged. However, all the contents are equally distributed to all the people who access the page in. So, an ordinary web distribution scheme is not suitable.

▪ If you have some content which you think it is okay to provide others if needed and if it is possible to upload such a content on the web in some covert manner and if you can issue some special access key to extract the content selectively then you will be very happy about it. A steganographic scheme can help you realize this type of system.

4. **Media Database systems.**
   In this application area of steganography, secrecy is important and also unifying two types of data into one is the most important thing. Media data which can be a photo picture, movie, music, etc. can have some associations with other information.

5. **Usage in modern printers**
   Steganography is used by some modern printers. The tiny yellow dots are added to each page. These dots are barely visible and contain the encoded printer serial numbers and the date and time stamps.

6. **Use by intelligence services.**
   The intelligent services also make use of steganography techniques for communicating the secret information from place to another.

DCT IN IMAGE STEGNOGRAPHY

DCT stands for Discrete Cosine Transformations. In this scheme, we embed the secret data within the cover image that has been transformed such as DCT (discrete cosine transformation). It transforms the cover image from the image representation into the frequency representation by grouping the pixels into non-overlapping blocks of pixels and transforming the pixel blocks into DCT coefficients. The DCT for each block of pixels was applied in order to improve the capacity and control the compression ratio.

Steganography is an important area of research in recent years involving a number of applications. Steganography is the science of embedding the information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The new secure image steganography presents a challenging task of transferring the embedded information to the destination without getting detected. In this work, we have an image based steganography that combines Discrete Cosine Transform (DCT), Least Significant Bit (LSB) and the compression techniques on some raw images to enhance the security of the payload. Firstly, the LSB algorithm is used to embed the payload bits into the cover image to derive the stego-image. Then this stego-image is transformed from the spatial domain to the frequency domain using DCT. Finally quantization and run length coding algorithms are used for compressing the stego-image to enhance its security. The largest amount of information that can be embedded into a cover data without producing either statistical or visual distortion to some extent is called steganography capacity. The objective of this work is to hide the maximum amount of information within natural digital images in order to compute the steganography capacity. We hide information within the discrete cosine transform (DCT) coefficients of digital images. Part of these coefficients are used to actually hide the message, whilst another set of coefficients are used to statistically restore, or compensate, the stego image.

Like other transforms, the Discrete Cosine Transform (DCT) attempts to de correlate the image data. Then after de correlation each transform coefficient can be encoded independently without losing compression efficiency. This part describes the DCT and some of its important properties. The very common definition of DCT –I is:

$$C(u) = \alpha \; u \; \sum_{x=0}^{N-1} f \;\; x \; \cos\left[\frac{\pi \;\; 2x+1 \;\; u}{2N}\right],$$

(1)

for $u = 0,1,2,\ldots,N-1$. Now, the inverse transformation is defined as

$$f(x) = \sum_{u=0}^{N-1} \alpha(u) C(u) \cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

(2)

The objective of this document is to study the efficacy of DCT on images. This makes it necessary for the extension of ideas presented in the last section to a 2-D space. This 2-D Discrete Cosine Transformation is a direct extension of the 1-D case and is given by:

$$C(u,v) = \alpha \;\; u \;\; \alpha \;\; v \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f \;\; x,y \;\; \cos\left[\frac{\pi \;\; 2x-1 \;\; u}{2N}\right]\cos\left[\frac{\pi \;\; 2y+1 \;\; v}{2N}\right],$$

(3)

For $u, v = 0, 1, 2,\ldots, N-1$ and $\alpha(u)$ and $\alpha(v)$ are defined in (3). The inverse transform is defined as

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha \;\; u \;\; \alpha \;\; v \;\; C \;\; u,v \;\; \cos\left[\frac{\pi \;\; 2x+1 \;\; u}{2N}\right]\cos\left[\frac{\pi \;\; 2y+1 \;\; v}{2N}\right],$$

(4)

For $x,y = 0,1,2,\ldots,N-1$.The 2-D basis functions can be generated by multiplying the horizontally oriented 1-D basis functions with vertically oriented set of the same functions. The basic functions for $N = 8$ are shown. Also, it can be noted that the basic functions exhibit a progressive increase in frequency both in the vertical and horizontal direction. Top left basic function of results from multiplication of the DC component with its transpose. Therefore, this function assumes a constant value and is referred to as the DCT coefficient.

Discussions in the preceding sections have developed a mathematical foundation for DCT. However, the insight into its image processing application has not been presented. This section outlines (with examples) some properties of the DCT which are of particular value to image processing applications.

As discussed previously, the principle advantage of image transformation is the removal of redundancy between neighboring pixels. It leads to uncorrelated transform coefficients which can be encoded independently.

Efficacy of a transformation scheme can be directly gauged by its ability to pack input data into as few coefficients as possible. It allows the quantizer to discard the coefficients with relatively small amplitudes without introducing visual distortion in the reconstructed image. DCT has an excellent energy compaction for highly correlated images.

VECTOR QUANTIZATION

Quantization is the process of mapping an infinite set of scalar or vector quantities by a finite set of scalar or vector quantities. It has applications in the areas of speech processing, Image processing and signal processing. In case of speech coding, quantization is required to reduce the number of bits used to represent the sample of speech signal. In case, less number of bits are used to represent a sample, then the bit-rate, complexity and memory requirement gets reduced. Usage of Quantization results in the loss in the quality of a speech signal, which is undesirable. Therefore, some compromise must be made between the reduction in bit-rate and the quality of speech signal.

Two types of quantization techniques exist. These are vector quantization and scalar quantization. The scalar quantization deals with the quantization of samples on sample by sample basis whereas the vector quantization deals with quantizing the samples in groups called vectors. The latter helps increase the optimality of the quantizer at the cost of increased memory requirements and computational complexity.

Shannon theory states that “quantizing a vector is more Vector quantization technique has become a great tool with the development of non variational design algorithms like the Linde, Buzo, Gray (LBG) algorithm. On the other hand besides spectral distortion the vector quantizer is having its own limitations like the computational complexity and memory requirements required for the searching and storing of the codebooks. In case of applications that require higher bit-rates the computational complexity and memory requirements increases exponentially.

In the vector quantizer design, we use quad tree segmentation to partition the training set so that all the high detail regions are isolated into the 4x4 blocks, which is used to design the codebook using the greedy tree growing algorithm. For the encoding process, quadtree segmentation is used to partition the test image into high detail 4x4 blocks and low detail large blocks. The high detail 4x4 blocks are encoded by the VQ codebook generated by greedy tree growing algorithm. The low detail large blocks are encoded by their block means to achieve further compression.

Since variable block sizes are used in quad tree segmentation, decoding of transmitted images requires the information about the size and location of each block. In designing the tree-structured codebook, we use an efficient and faster splitting algorithm which requires a much more complex one step look ahead splitting. Due to quadtree segmentation, training vectors for designing codebook are more compactly located and therefore the computationally intensive look-ahead splitting is not needed.

Let D be the total distortion contributed by a particular node and N be the number of vectors within that node. The goodness of a split among all the terminal nodes is determined by A = DIN. That is, we split the node that contributes the largest average distortion. The unbalanced tree is grown until its average rate equals the target rate. The transmitted index of a particular vector is the binary sequence indicating the path from the root of the tree to that leaf.

Vector Quantization greatly affects the performance of quantization. The vectors of large dimensions produces the better quality as compared to the vectors of small dimensions and in vectors of small dimensions, the transparency in the quantization is not good at a particular bit-rate chosen. This is because in vectors of smaller dimension the correlation that exists between the samples is lost and the scalar quantization itself destroys the correlation that exists between successive samples. Therefore the quality of the quantized speech signal gets lost. Hence, quantizing the correlated data requires such techniques that preserve the correlation in the samples that can be achieved by the vector quantization technique (VQ). Vector quantization is the simplification of scalar quantization. In case of vector quantization, the quantization of data is in the form of contiguous blocks called vectors rather than individual samples. But afterwards, with the development of better coding techniques, it is now possible that transparency in quantization can be achieved even for vectors of the small dimensions.

THE PROPOSED ALGORITHM:

The algorithm is divided into two parts:

1. Embedding Algorithm and
2. Extraction Algorithm.

1. THE EMBEDDING ALGORITHM:

Step1: Choose a Cover Image C.

Step2: Choose the Message that has to be communicated secretly (M).

Step3: Now find the DCT coefficients of the Image that you have chosen as the cover i.e.C.

Step4: The DCT coefficients are calculated using the formula:

$$C(u)=\alpha\ u \sum_{x=0}^{N-1} f\ \ x \cos\left[\frac{\pi\ \ 2x+1\ \ u}{2N}\right],$$

for $u = 0,1,2,\ldots,N-1$.

The objective of this document is to study the efficacy of DCT on images. This makes it necessary for the extension of ideas presented in the last section to a 2-D space. This 2-D Discrete Cosine Transformation is a direct extension of the 1-D case and is given by:

$$C(u,v)=\alpha\ u\ \alpha\ v \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f\ \ x,y \cos\left[\frac{\pi\ \ 2x-1\ \ u}{2N}\right]\cos\left[\frac{\pi\ \ 2y+1\ \ v}{2N}\right],$$

Step5: Now, apply the technique of vector quantization.

Step6: Obtain the Quantization Table.

Step7: Finally, we can embed our secret information M into our cover medium.

Step8: For the purpose of embedding, we find the low intensity bits of the quantized image.

Step9: First it tries to merge the data into low intensity bits and then to high intensity bits.

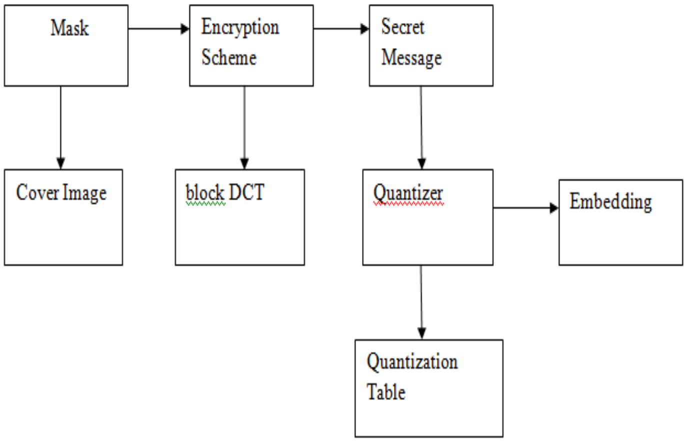

Figure2. The Embedding Procedure

2. THE EXTRACTION ALGORITHM:

Step1: We have the Stego Image S.

Step2: We need to extract two things out of the Stego Image i.e. the Secret message and the Cover Image.

Step3: Apply the Inverse DCT using the formula:

$$f(x)=\sum_{u=0}^{N-1}\alpha(u)C(u)\cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

For $u,v = 0,1,2,\ldots,N-1$ and $\alpha(u)$ and $\alpha(v)$. The inverse transform is defined as

$$f(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha\ u\ \alpha\ v\ C\ u,v\ \cos\left[\frac{\pi\ 2x+1\ u}{2N}\right]\cos\left[\frac{\pi\ 2y+1\ v}{2N}\right],$$ Ste4:

After this, we can extract the secret message and have two things i.e. the secret message as well as the cover.

The Embedding algorithm is used at the transmitter's side when the user wants to embed the secret message that he/she wishes to transfer securely. Data embedding is the process of embedding the information in the data source without any change in its perceptual quality. In our proposed algorithm, firstly in case of the embedding algorithm used at the transmitter's side, we have two things i.e. the cover medium and the secret message that is to be transmitted securely.

First of all, we select the cover edium or the cover image in which the secret message to be transmitted is embedded. After the image is selected, its DCT quantization is performed. Then the message that you want to transmit is entered. Till image= Current DCT, we keep on incrementing the value by 1. For the purpose of embedding, we find the low intensity bits of the quantized image. The binaries weight of bits to be merged are found and then merged. First it tries to merge the data into low intensity bits and then to high intensity bits. That is how the merging of the message takes place at the transmitter's end as shown in Figure 2.

The second part of our algorithm consists of the Extraction Algorithm at the receiver's end. At the receiver's end, firstly, dequantization is performed and then the stego video is obtained. Afterwards, the secret message is extracted and the calculations are performed.

CONCLUSION:

In this paper, we have tried to apply the DCT i.e. Discrete Cosine Transformations and Vector Quantization Technique to the images so as to increase the capacity of the cover medium. As we are applying these techniques, of course the capacity is much more than any other normal techniqu like LSB and in our next work, we can try mixing it with some other technique so as to get even better results.

REFERENCES:

1. Chan C K. and Cheng L. M., 2004, "Hiding data in images by simple LSB substitution." *Pattern Recognition, The Journal of the Pattern Recognition Society*, Vol. 37, no. 3, pp. 469-474.

2. Kaur G. and Kochhar A., 2012. "A Steganography Implementation based on LSB & DCT", *International Journal for Science and Emerging*

Technologies with Latest Trends, vol 4(1), pp. 35-41.

3. Khare P., Singh J. and Tiwari M., 2011, “Digital Image Steganography”, *Journal of Engineering Research and Studies,* Vol. II, Issue III, pp. 101-104.

4. Mohamed A., Hatem M.A., Hani M.I., and Ahmed S.S., 2014 “A Steganographic Method Based on DCT and New Quantization Technique International Journal of Network Security”, Vol.16, No.3, pp. 214-219.

5. Patel H. and Dave P., 2012, “Steganography Technique Based on DCT Coefficients” *International Journal of Engineering Research and Applications*, Vol. 2, Issue 1, pp.713-717.

6. Rabah K. 2004, “Steganography – The Art of Hiding Data”, *Information Technology Journal*, Vol.3, no.3, pp. 245-269.

7. Shamim A.L and Hemachandran K., 2012 “High Capacity data hiding using LSB Steganography and Encryption” *International Journal of Database Management System(IJDMS)*, Vol.4, No.6, pp. 57-68.

8. Sudhanshu S G. and Jagdish B W., 2013, “ Robust digital watermarking technique by using DCT and spread spectrum” *International Journal Of Electrical, Electronics and Data Communication,* volume 1, issue 2, pp.27-32.

Author

Er. Bhavneet Kaur is B. Tech and M. Tech in Computer Science & Engineering from Rayat Institute of Engineering and Technology, Railmajra. Her research interests include Steganography, Watermarking, Steganalysis, Digital Image Processing and Software Engineering. She has 13 publications including National and International (Conferences & Journals). Currently she is working with CGC Technical Campus, Jhanjeri (Mohali), Punjab as an Assistant Professor in CSE department.