International Journal of Information Technology and Management

Vol. V, Issue No. I, August-2013, ISSN 2249-4510

# A STUDY UPON COMPRESSION OF DATA USING DCT IN STEGANOGRAPHY CRYPTOGRAPHY

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

*International Journal of Information Technology and Management*
*Vol. V, Issue No. I, August-2013, ISSN 2249-4510*

# A Study upon Compression of Data Using DCT in Steganography Cryptography

**Soniya Wadhwa**

Research Scholar, Lingaya's University, Faridabad, Haryana

***Abstract – Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. In this paper, we propose a LSB & DCT-based Steganographic method for hiding the data. Each bit of data is embedded by altering the least significant bit of low frequency DCT coefficients of cover image blocks.***

----------♦----------

## INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. In this paper we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and security. Presently we have very secure methods for both cryptography and Steganography – AES algorithm is a very secure technique for cryptography and the Steganography methods, which use frequency domain, are highly secured. Even if we combine these techniques straight forwardly, there is a chance that the intruder may detect the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding. This paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography. As we know that-

- Hiding data is better than moving it shown and encrypted.
- To hide data in a popular object that will not attract any attention.
- In case the data is extracted, it will be encrypted.

But still there is a chance that the intruder can break the code. In our new system instead of applying existing techniques directly we will be using the following approach –

- Instead of hiding the complete encrypted text into an image, we will be hiding a part of the encrypted message.
- Unhidden part of the encrypted message will be converted into two secret keys.
- In this system to get the original message one should know, along with keys for Cryptography and Steganography, two extra keys and the reverse process of the key generation.

Cryptography is the widely used well known technique that manipulates information (messages) in order to cipher and Steganography is the art and science of communicating in a way which hides the existence of the communicated message.

Cryptography scrambles a message so it cannot be understood and the Steganography hides the message so it cannot be seen. Inv this paper one new system is proposed, which uses Compression with Cryptography and Steganography.

The Discrete Cosine Transform (DCT): This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of “spreading” the location of the pixel values over part of the image. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT. DCT is used in steganography as- Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT

coefficients and message is embedded in DCT coefficients.

*DCT Based Steganography* Algorithm to embed text message:-

Step 1: Read cover image.

Step 2: Read secret message and convert it in binary.

Step 3: The cover image is broken into 8×8 block of pixels.

Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 5: DCT is applied to each block.

Step 6: Each block is compressed through quantization table.

Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.

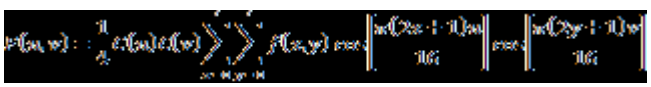
Step 8: Write stego image.

## LITERATURE SURVEY

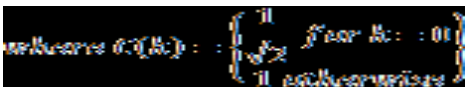
When doing survey and analysis of current methods different methods have so many advantage and disadvantages. . Different Steganography techniques discussed in are spatial domain, frequency domain, and statistical or adaptive. In spatial secret image is embedded in the cover image without any modification to the cover image. That usually it is placed least significant bits of the cover image. But in frequency domain transformation technique such as DCT, DFT or DWT is used. Nowadays DFT is not used. In DCT secret image is placed in the low and mid frequency coefficients and In DWT it is embedded in the frequency sub bands. To provide security and compression different approaches have to be combined with steganography. When dealing with compression algorithms a lossless compression Huffman encoding is combined with LSB, DCT, and DWT.

**Discrete Cosine Transform (DCT) -** DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity.

Let I(x,y) denote an 8-bit grayscale cover-image with x = 1,2,…….,M1 and y = 1,2,…….,N1. This M1×N1 cover-image is divided into 8 × 8 blocks and two-dimensional (2-D) DCT is performed on each of L = M1×N1 / 64 blocks. The mathematical definition of DCT is:



for u=0……..7, for v=0……7



The mathematical definition of IDCT is

DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands which makes it easier to choose the band in which the secret image is to be inserted. Embedding the image in a middle frequency band does not scatter the secret information to most visual important parts of the image i.e. the low frequencies and also it do not over expose them to removal through compression and noise attacks where high frequency components are targeted. Although some of the steganography techniques embed the information in the DC component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of information into a DCT block. DCT block consists of three frequency bands-Low frequency band (FL), High frequency band (FH), mid frequency band (FM). This system uses FM for embedding the watermark. Two locations Mi (u1, v1) and Mi (u2, v2) from the frequency band FM are chosen as the region for comparison.

## CONCLUSIONS

In this paper propose a DCT-steganography based on encryption. To provide high security steganography and cryptography are combined together.

The work accomplished during this project can be summarized with the following points:

- In this paper we have presented a new system for the combination of cryptography and Steganography using four keys which could be proven a highly secured method for data communication in near future.

- Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image.

- The main advantage of this Crypto/Stegno System is that the method used for encryption, AES, is very secure and the DCT transformation Steganography techniques are very hard to detect.

In this paper propose a DCT-steganography based on encryption. To provide high security steganography and cryptography are combined together. This system encrypts secret information before embedding in the image. Steganography uses RSA algorithm for encryption and decryption. According to the simulation results, the stego images of our proposed algorithm are almost identical to the cover images and it is very difficult to differentiate between them. Better PSNR values will get when compared with LSB steganography with Huffman coding. Experimental results shows high PSNR values obtained when the size of secret image is less compared to the size of cover image.

## REFERENCES

Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar," A *Novel Technique for Image Steganography Based on DWT and Huffman Encoding*" , International Journal of Computer Science and Security, (IJCSS)Volume 4

A. Nag, S. Biswas, D. Sarkar, P. P. Sarkar, "*A Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding*". International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010

Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.

K.B.Raja', C.R.Chowdary2, Venugopal K R3, L.M.Patnaik , *A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images*,2005 IEEE

Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY & PRIVACY

RigDas, Themrichon Tuithung," *A Novel Steganography Method for Image Based on Huffman Encoding*",2012 IEEE

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. Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.

Shailender Gupta , Ankur Goyal , Bharat Bhushan ,*Information Hiding Using Least Significant Bit Steganography and Cryptography* , I.J.Modern Education and Computer Science, 2012

Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

William Stallings, *Cryptography and Network Security, Principles and Practice*, Low Price Edition , Second Edition.