ISSN 2395-1621

Secure Data Transmission and Reception using Double Compression Steganography

[#1]Jyoti Ashok Thange, [#2]Prof.Kailas Aade

[1]Jyotithange91@gmail.com
[2]aade.Kailas@raisoni.net

[#12]G.H.Raisoni College of engineering Ahmednagar,Pune University,India

ABSTRACT

This paper gives the steganography, means art of hiding information. In Steganography secret data is hiding behind cover image. Different methods are used for hiding information such as Least Significant Bit (LSB), Discrete cosine transform (DCT), Discrete Fourier transform (DFT) and Discrete wavelet transform (DWT). This paper focuses on image steganography basically. Using these all techniques it is possible to communicate between two authorized parties.

Keywords— a Least Significant Bit(LSB), Discrete cosine transform(DCT), Discrete Fourier transform(DFT), Discrete wavelet transform(DWT), PSNR, MSE.

ARTICLE INFO

Article History

Received : 8th July 2015

Received in revised form :

11th July2015

Accepted : 14th July 2015

Published online :

21th July 2015

I. INTRODUCTION

Steganography is communication between to authorized parties but in invisible manner. This is take place by hiding secret information in other cover information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1]hence it is defined as "covered writing". In image steganography the secret data as well as covered data is image.

Today's world means computer world dueto steganography is mostly used on computers.Important difference between Steganography and cryptography is cryptography focuses only on keeping the contents of a message secret from unauthorized parties and steganography focuses on keeping the existence of a message secret[4].Steganography and cryptography are both types used to protect information from unauthorized parties but neither technology is perfect.So that

for secure purpose steganography with double compression is necessary. The double compression means LSB with DCT, LSB with DFT, LSB with DWT. Due to dual compression secret communication is more secure than the single compression so that hackers and crakers does not detect the message. Because it is very difficult to break the dual compression. Double compression in the communication reduces the risk of information being leaked when transmitted [8] This paper overviews the different algorithms used for image steganography. The security in the communication is the most important in today;s life. Security for business, industrial documents, military applications and personal use also is needed.

Organization of this Paper is as follows. Section I include Introduction. Section II gives brief literature review of Section

III gives the system development and result Section IV gives conclusion with future work.

II. LITERATURE REVIEW

The secure data hiding technique has a long history. In World War II, invisible inks such as milk, vinegar, fruit juices 0r urine were used for secure communication. The message is written using these invisible inks, when these are heated then the message get display which is easilyreadable.

Today Steganography technique is mostly used on computers mostly in internet. Here cover acts as the carriers and message acts as a secret and using networks as the channels the message sends securely. Another technique is also used for secure communication that is cryptography. The difference between Steganography and cryptography is that cryptography keep the message secret but it is in visible form and steganography keep the message secret is in

invisible form. Steganography as well as cryptography both are used for sending the secret but neither technology alone is perfect. The message used for secret communication is in the form of text, audio, video, image and combination of text plus image, audio plus image etc.

In this paper the information keep secure using different techniques such as LSB, DCT, DFT and DWT but for more secure purpose dual compression is used it means combination of LSB with DCT, DFT, and DWT is done.

III. SYSTEM DEVELOPMENT

In cryptography the message is visible one can easily guess that it contain secret data to reduce this problem Steganography is used with different techniques.

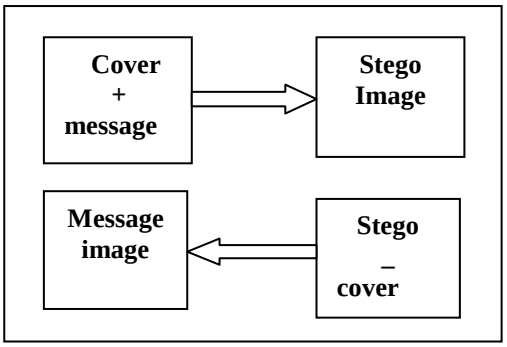


Figure 1: Graphical Version of the Steganographic System.

1) Cover image+ message image=stego image
2) stego image- Cover image= message image

The basic mathematical model of steganography is as shown in the above figure. The cover image act as a carrier for carry the secret data. The secret data is hided behind the cover image by the steganographic techniques. The obtained result is the stego-image is transferred from the sender's end to the receiver's end over the communication channel. At the receivere's end, the same steganographic algorithm works to extract the orginal secret data from the cover image. The sender and receiver must agree upon a common key to embed and extract the secret data from the cover image.

The cover image and the message image create a stego-image. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image and if we subtract cover image from stego image we get message image i.e. secret message.

3.1 Least Significant Bit (LSB)Based Steganography:

Basically 8-bit or 24-bit files are used to store digital images. It gives the colored representation of the pixels and these colors are derived from three primary colorssuch as red, green and blue. Each primary color is represented by 1 byte means 8-bit so each pixels required 24 bit.In this technique the least significant bits are used for hide data, due to that changes occurred are undetectable to human eye. This simple method is known as Least Significant Bit.

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right 1.

The LSB based Steganography is one of the steganographic methods, used to hide the secret data into the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
240 : 011110000
RESULT: (00100110 11101001 11001001)
(00100111 11001001 11101000)
(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed.

3.2 Discrete Cosine Transform (DCT) Based Steganography:

DCT is one of the technique to hide the data. DCT coefficients are used for JPEG compression. It divide the image into DCT coeffficent. It transforms a signal or image from the spatial domain into the frequency domain. It can separate the image into high, middle and low frequency components.

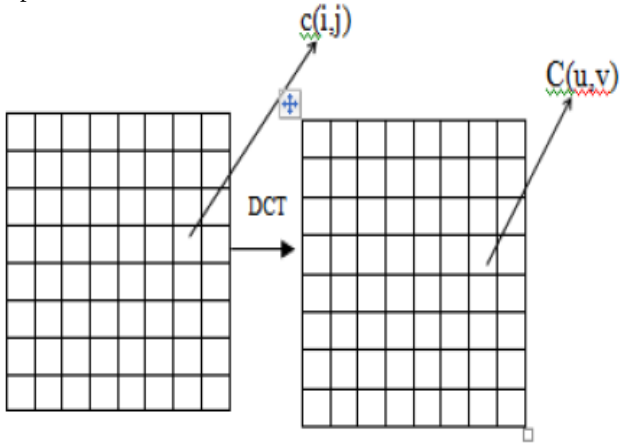


Figure 2 Discrete Cosine Transform of An Image

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. For DCT with block size (M _N), the connection between the spatial domain image pixels X(i; j) and the transform domain coefficients Y (u; v) is

Y (u; v) is

$$Y(u,v) = \frac{2c(u)c(v)}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} X(i,j) \cos\left[\frac{(2i+1)u\pi}{2M}\right] \cos\left[\frac{(2j+1)u\pi}{2N}\right]$$

$$where\ u = 0,1, \ldots . M-1, v = 0,1, \ldots \ldots N - 1, and$$

$$c(k) = \begin{cases} \frac{1}{\sqrt{2}}, & if\ k \\ 1, & otherwise \end{cases}$$

$$= 0,$$

3.3 Discrete Fourier Transform (DFT) Based Steganography:

The relationship between the spatial/temporal domain signals, f[n], and their corresponding transform in the frequency domain, F[k], is

$$F[k] = \sum_{n=0}^{M-1} f(n) . W_M^{kn}$$

Where $W^r_{M=e^{-j2\pi r/M}}$

For digital image,the 2D DFT can be defined as

$$Y(u,v) = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} X(i,j) . W_M^{iu} . W_N^{jv}$$

The DFT of an image is always complex valued. This leads to the magnitude and
phase representation for the image

$$M(u,v) = |Y(u,v)|$$
$$\emptyset(u,v) = \prec Y(u,v)$$

3.4Discrete Wavelet Transform (DWT) :

The field of Discrete Wavelet Transforms is an recent one. The Discrete Wavelet Transform (or DWT), is an orthogonal function applied to a finite group of data. Functionally, it is very similar to the Discrete Fourier Transform, in that the transforming function is orthogonal.

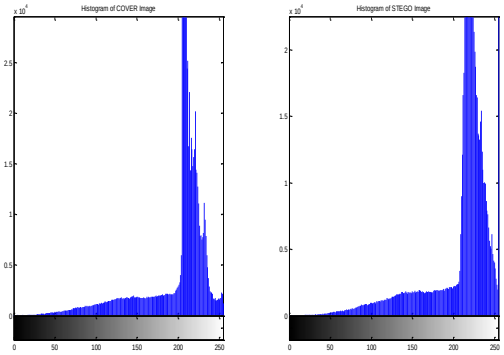
Wavelet transform is used to convert a spatial domain into frequency domain. The link between the spatial/temporal domain signals, f(t), and the DWT of f(t), d(k; l), is

Figure 3 DWT Band

$$f(t) = \sum_{k=-\infty}^{\infty}\sum_{l=-\infty}^{\infty} d(k,l)2^{-\frac{k}{2}}\Psi(2^{-k}t - 1)$$

Where Ψ (·)denotes the mother wavelet.

IV. RESULT



V. CONCLUSION

As steganography becomes more widely used in computing there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of double compression that is combination of LSB with DCT, DFT and DWT gives us more security than the other techniques.

VI. FUTURE WORK

1. We can also implement the Steganography techniques on Audio+image.

2.We can also implement the Steganography techniques on Video+image.

3.We can also implement the Steganography techniques on Text+image.

4.We can also improve this project for defence purpose.

5.We can also implement different parameters such as capacity, normalized mean square error (NMSE), root mean square error (RMSE), quality etc.

6.We can embed voice recognisation system in our project.

7.We can implement total software work with the help of hardware also.

REFRENCES

[1] G. Sahoo and R. K. Tiwari "Designing Some Imperceptible Data HidingMethodologies Using SteganographicTechniques" International Journal Of Information Technology and Knowledge ManagementJuly-December 2008, Volume 1, No. 2, Pp. 209-217.

[2] T. Morkel, J.H.P. Eloff, M.S. Olivier "An Overview Of Image Steganography" Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa. Tel: +27 12 420-2361.

[3] Ken Cabeen and Peter Gent "Image Compression and the Discrete Cosine Transform" Math45 College of the Redwoods.

[4] Po-Yueh Chen* and Hung-JuLin "A DWT Based Approach for Image Steganography" International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[5] Mr.PushparajP.Nerkar, Vishwajit K. Barbudhe, Prof. Aumdevi K. Barbudhe "Steganography for Colored Images" International Journal of Electronics, Communication & Soft Computing Science and Engineering ISSN: 2277-9477, Volume 2, Issue2.

[6] Syed Ali Khayam "The Discrete Cosine Transform (DCT): Theory and Application1" Department of Electrical & Computer Engineering Michigan State University March 10th 2003.

[7] Hardik Patel, PreetiDave "Steganography Technique Based on DCT Coefficients" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717.

[8] Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt "Digital image steganography: Survey and analysis of current methods" Signal Processing 90 (2010) 727–752 Accepted 18 August 2009

