DOUBLE LAYER SECURITY USING VISUAL CRYPTOGRAPHY AND TRANSFORM BASED STEGANOGRAPHY

PallaviB[1], Vishala I. L[2]

[1]M.Tech 4th SEM, DCN Branch, Visvesvaraya Technological University
[2]Assistant Professor, Dept of ECE, S.J.C Institute of Technology, Chickballapur, India.

Abstract

With the recent advances in internet computing in our day to day life the need for communication has increased. Privacy in communication is desired when confidential information is shared between two parties. Mainly this project uses transform based steganography (DCT) and visual cryptography for hiding data. The proposed system provides double layer security. First level of security is achieved by using visual cryptography for the information to be transmitted and this is embedded onto images by using steganography. This project is implemented using Matlab software. In this project the expected result is we take 2 color images and for those we apply DCT and for the DCT transformed images LSB is applied with the bits of the shares which we would have got from V.C.

Keywords: *DCT, shares, Steganography, Visual Cryptography.*

----------***----------

1. INTRODUCTION

Since the rise of internet one of the most important factors of important technology is security of Information. Cryptography was created as a technique for securing secrecy of communication and many different methods have been developed to encrypt and decrypt the data. An important subdivision of information Hiding is steganography. Sometimes it's not enough to keep contents of message secret but also it's necessary to keep existence of message secret. The technique used to implement this is called steganography. It's made up of 2 Greek words *"stegos"* meaning covered and *"Grafia"* meaning writing. Steganography is the art and science of invisible communication. The technique of steganography requires Cover Object(C), secret message (M), stego key and stego function (Fe).

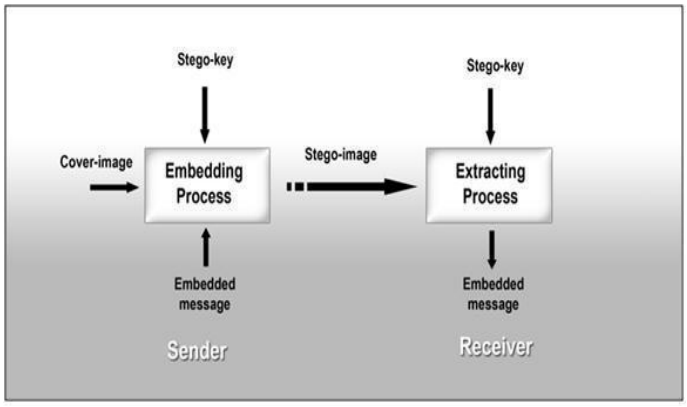


Fig - 1: Basic model of Steganographic system

1.1 Steganography Methods

There are 3 ways namely

- Injection - embeds secret message directly in host medium
- Substitution – normal data is substituted with the secret data.
- Generation of new files

1.2 Steganography Techniques

The different categories of Steganography techniques are

- Substitution system techniques
- Transform domain techniques
- Spread spectrum technique
- Distortion techniques
- Statistical method techniques

Steganographic techniques can be broadly classified as

- Spatial domain techniques
- Transform domain techniques
- Hybrid domain techniques

In case of spatial domain technique all manipulations to the cover object and payload are done in time domain. LSB technique is the most popular spatial domain technique. Transform domain techniques are frequency domain techniques. Image is considered in terms of frequency components. DCT is the most commonly used technique. In case of hybrid domain technique image is divided into cells and then spatial or transform domain technique is applied.

To illustrate the process of steganography we consider figure given below

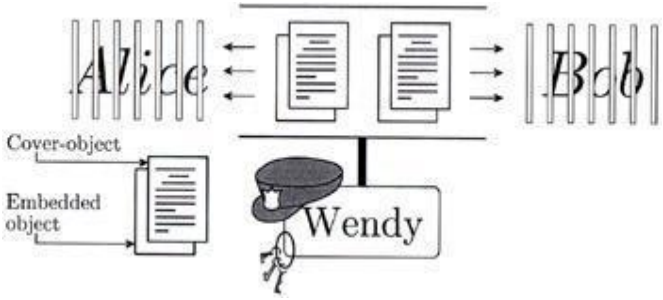


Fig -2: Prisoners problem

The classic model for invisible communication was proposed by Simmons as prisoner's problem. Alice and Bob are arrested are for some crime and they are thrown in different cells. They want to develop an escape plan but all communication is arbitrated by Wendy. She will not let them communicate through encryption and hence both parties should communicate invisibly – have to set up subliminal channel.

2. VISUAL CRYPTOGRAPHY

It was proposed by Naor and Shamir in 1994. It's a scheme which encrypts image into shares but does not require any computations to get back the original image and it's an encryption technique used to hide images in such a way that decryption can be performed by human visual system if key is used. Here V.C operates on binary inputs and initially V.C was applied to black and white images but now it's extended to color and grey scale images. The easiest way to implement visual cryptography is to print two layers on transparencies.

2.1 How Visual Cryptography Works?

Mainly visual cryptography operates on binary inputs. Hence natural images must be converted into halftone images using density of dots in order to simulate grey level. Binary data can be displayed as transparent when printed on transparent screen. Each pixel of the image is divided into smaller blocks. There are always same numbers of black and white blocks. If a pixel is divided into 2 parts there is one black and one white block. If a pixel is divided into 4 parts there are 2 white and 2 black blocks.

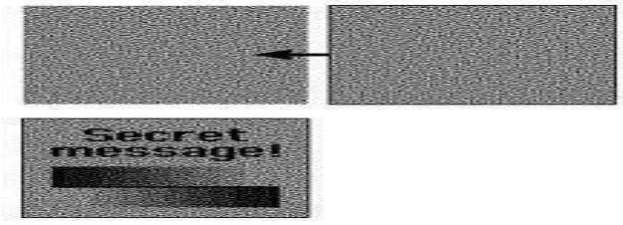


Fig- 3: example of visual cryptography

The basic model of visual cryptography proposed by Naor and Shamir accepts binary image I as secret image which is divided into n number of shares. Each pixel of image is represented by m sub pixels. The resulting structure of shared image is represented by S where S = [Sij], an n x m matrix.

Any black and white visual cryptography scheme can be described using 2 n x m Boolean matrices (S0 and S1). S0 is used if pixel in the original image is white and S1 is used if pixel in original image is black.

The important parameters in visual cryptography schemes are

- Pixel expansion (m)
- Contrast (β)

The formula to compute contrast in different visual cryptography schemes is $B = \alpha m$.

In V.C white pixel is represented by 0 and black pixel is represented by 1.

There are different visual cryptography schemes such 2 out of 2, 2 out of n, n out of n and k out of n V.C Scheme. The most commonly used is 2 out of 2 schemes.

For 2 out of 2 VCS S^0 and S^1 are as follows

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The relative difference α and contrast β is ½ and 1

Fig - 4: construction of (2, 2) VCS

There are 2 collections of matrices C^0 and C^1. To share a white pixel we choose one of the matrix in C^0 and to share black pixel we choose one of the matrix in C^1. The first row of chosen matrix is used for share S1 and the second row is used for share S2.

The disadvantage is that for every pixel encoded from original image into 2 sub pixels and placed on each share – shares have size of s x 2s if secret image is of size s x s. There is a distortion hence we go for 4 sub pixel layout design. Here pixel is expanded into 2 x 2 sub pixels.

$S^0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

The relative difference α and β is ½ and 2 respectively.

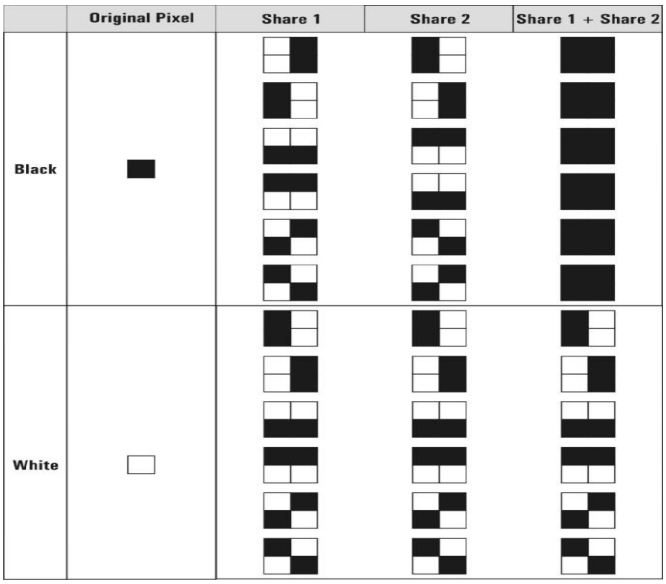


Fig -5: construction of (2, 2) VCS with 4 sub pixel layout design.

There are various visual cryptography schemes such as (2, 2) VCS, (k, n) VCS, halftone VCS, V.C for grey level image and color images.

In this project we mainly focused on (2, 2) V.C.S- here both the shares are required to reveal the secret information.If one share gets lost due to some problem the secret information can't be revealed.

If V.C has to be used for grey level images dithering technique is used and if V.C has to be used for color images additional processing has to be done – R, G, B has to be used for additive model and cyan, magenta, yellow is used for subtractive model and then the normal V.C scheme is used.

3 METHODOLOGY USED

A few techniques are there to implement both steganography and visual cryptography. Among them optimal one can be found out by analyzing tools.

As mentioned both steganography and visual cryptography have problems. Whenever they are used independently we have only single layer of security which can be easily broken by intruders. If we combine features of both steganography and visual cryptography then we have 2 layers of security. The steganography technique used in this project is DCT. The advantage in visual cryptography is we don't need any computation to decrypt the data.

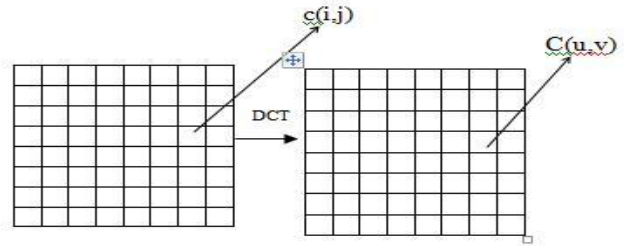
Previously the methodology used for encrypting information is steganography or cryptography but in this project we used both – First the information which is to be transmitted is encrypted using visual cryptography and this is embedded onto images using steganography.

4 ANALYSIS OF THE PROJECT

This project is analyzed in terms of DCT transform and V.C. DCT coefficients are used for JPEG compression. We have 1 D DCT and 2 D DCT. 2 D DCT is used.

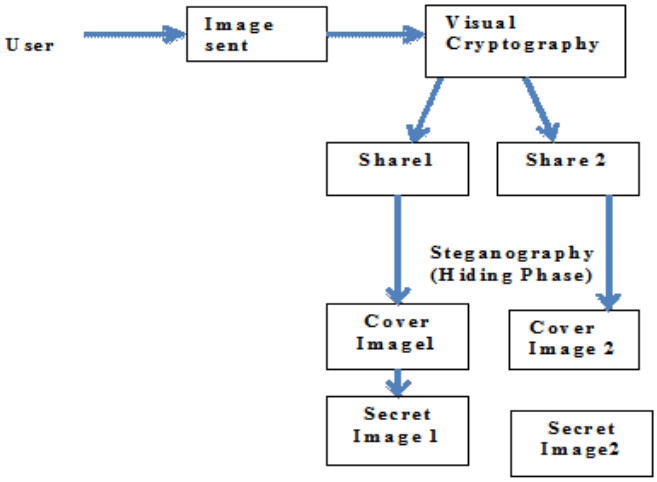
Image compression using DCT is done in the following way

- Image is broken to smaller blocks of pixels
- DCT is applied to each block.
- Each block is compressed through quantization and quantization matrix is entropy encoded.
- The array of blocks that constitute the image is stored in reduced amount of space.



c (i, j) is the intensity of pixel in row i and column j and C (u, v) is DCT coefficients.

5 IMPLEMENTATION OF THE PROJECT



User will send an image and that image with the help of visual cryptography is broken down into 2 shares. We have used (2, 2) V.C.S – in that image is broken down into 2 shares such that no information can be reconstructed without any single

share. The shares are printed in transparencies and the decryption process is performed by stacking the 2 shares.
Steganography hiding phase is nothing but here we consider cover image which is split into 3 components – R, G, B. we consider individual shares (bit streams) and they are hidden using bit and, bit or operation. After we complete hiding process for all the pixels present in R, G, B we merge them to get stego image.

Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel .In 8 bit images one bit of information can be hidden.

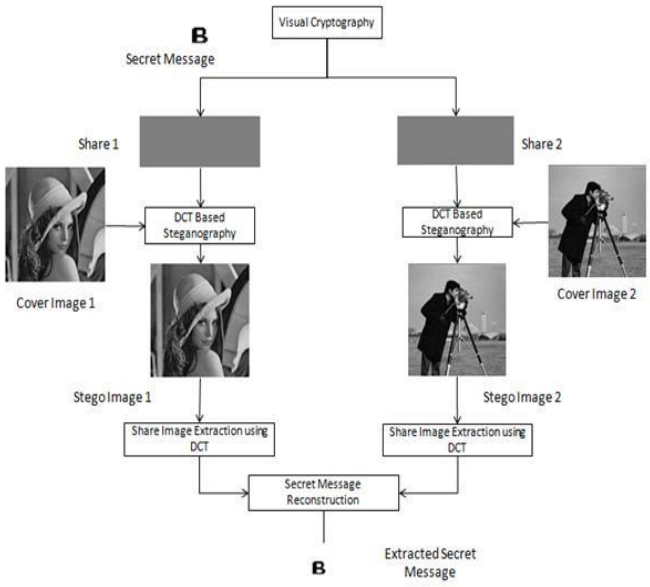
Least significant 3 bits are cleared in the red and green bytes and 2 bits from the blue byte. This can be done by using bit and with 248 which has 3‘0’ in its last 3 least significant bit. This we will do for both red and green bytes. And in the blue byte we bit and with 252 which has 2 ‘0’s in its least significant bits. And then we bit or the bits of the text on to these emptied bits

Suppose the original 3 pixels are:

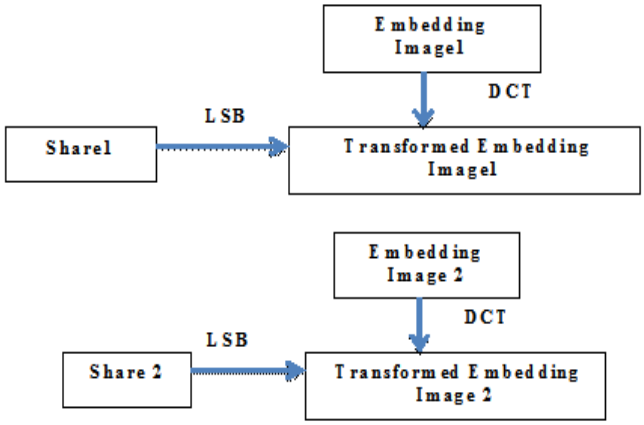
(11101010 11101000 11001011)

Consider binary representation of 74 = 01001010

The first byte 11101010 is converted to 11101000 by using bit and with 248 (11111000). First bit is 1 so the third last bit is left disturbed. Second bit is 1 bit or it to the emptied byte. Third bit is 0 and the emptied bit is kept as such. The same way the last three bits in green byte and last two bits in the blue bit are placed and again filled in the target image called the stego image.



5.1 Conceptual Design of Project



5.2 Block Diagram of DCT based Steganography

The proposed method is used to hide secret object (text, image) into a cover image. DCT transforms image from spatial domain to frequency domain. We convert secret object into binary form and hides the bits chosen in middle and high frequency coefficients.DCT decomposes signal into low, middle and high frequency coefficients. The secret image is hidden in high and middle frequency regions but not in lower region because human visual system is more sensible to modifications that may occur in lower frequency band.

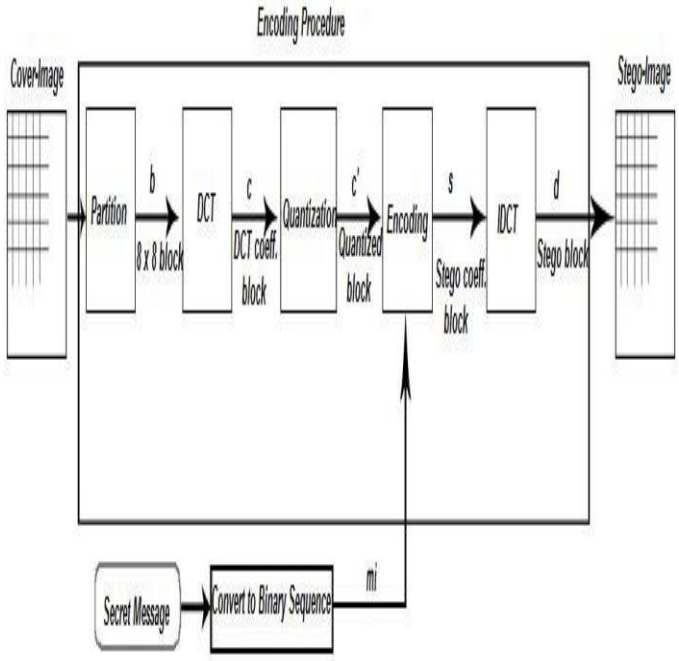


Fig - 6: Block diagram of DCT Steg Encoding process

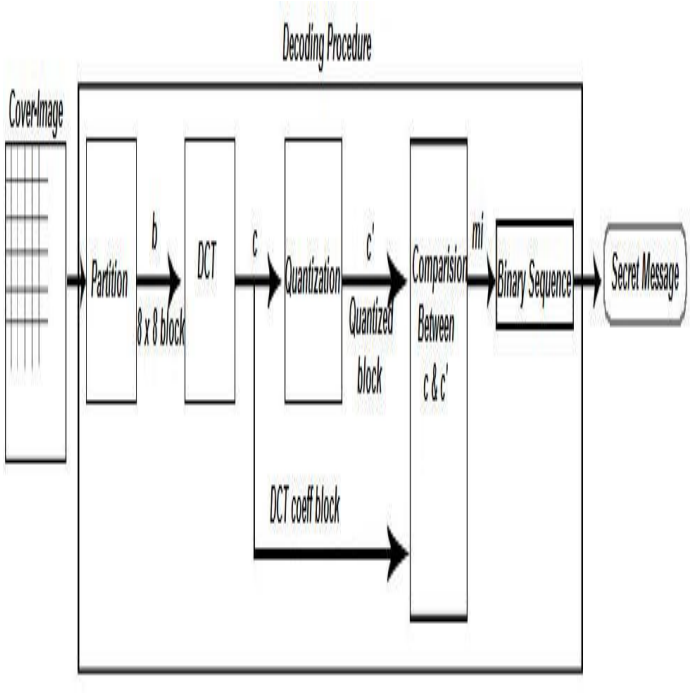


Fig- 7: Block diagram of DCT Steg Decoding process

6. RESULTS

Coding is done using Matlab and results are shown below. Mainly image is of size M X N (M rows and N columns). Images of formats like – tiff, jpeg, png are available. In Matlabrgb and indexed image is converted to grey scale image. RGB image does not have color image and we check for map variable in case of indexed image (2D).After the code is executed we run the program and there are 5 different modes. If we don't specify any mode (mode 0 fixed Thresholding is considered).
There are 5 different modes namely

- Fixed Thresholding
- Random noise Thresholding
- Ordered dithering
- Error diffusion by Floyd and Steinberg
- Error diffusion by sticky

Thresholding is an important approach to image segmentation. We assume that image falls in the range of 0 to 255.

Pixels of the digital image are processed. And we compare grey scale value of pixel to threshold (128). If pixel value is greater than threshold it's black else it's white.

Whenever color depth needs to be reduced we go for dithering. Dither is a form of noise used to minimize error.
There are 3 methods for dithering

- Add noise to image
- Use dithering matrix
- Diffuse error to neighboring pixels

In coding part we have used dithering matrix method.

Error diffusion is a technique in which quantization residual is distributed to neighboring pixels that are not yet processed. In case of error diffusion by Floyd and Steinberg error is distributed to neighboring pixels but in case of error diffusion by sticky – output tends to be clean and sharp.

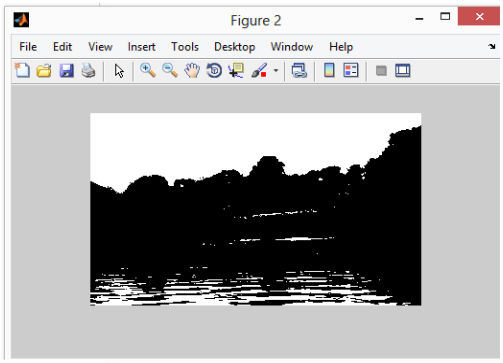


Fig8: output for fixed Thresholding of autumn.tif

The above figure shows the output for mode 0 (fixed Thresholding for image autumn.tif).In Matlab after running our program whenever we type Halftonedemofinal (3) we get output for ordered dithering of image autumn.tif which is shown in figure 8.

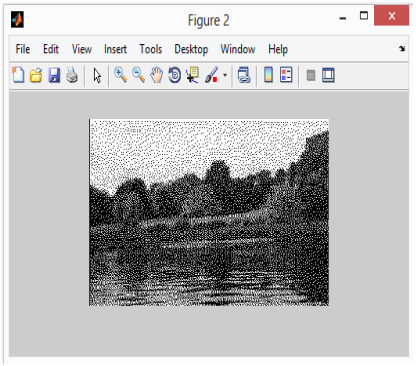
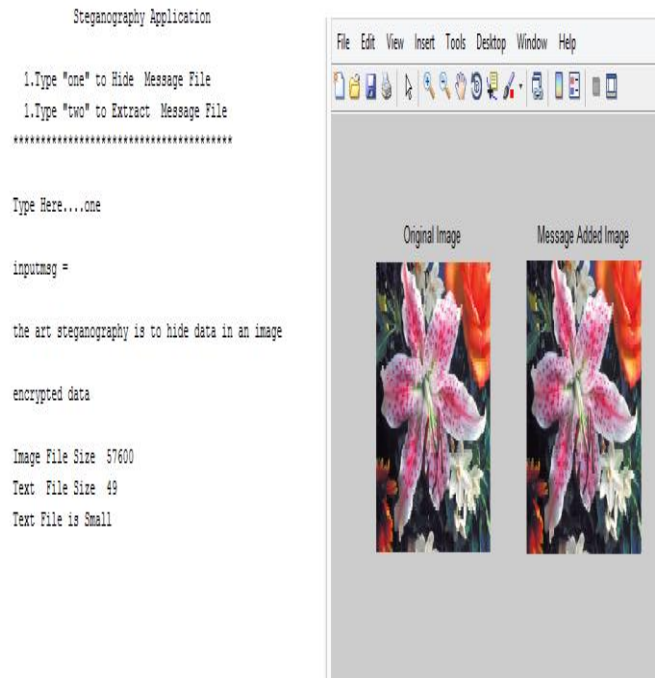


Fig8: output for ordered dithering of autumn.tif



The above figure shows output of steganography application. We can type input one or two in Matlab window. We need to type input message and it appears and also the size is displayed. For decoding the input message is shifted by 2 letters and the output (notepad version is created)

7. CONCLUSIONS

In this project we are going to hide the information by combining the features of both steganography and visual cryptography. The proposed system is used to overcome the difficulties faced in existing system and it has several advantages like 2 levels of security, requires computation time for single level of hiding and the proposed system can be used in applications like payment gateways, military, navy, business settlement contracts.

REFERENCES

[1].J.B.Krenn, “Steganography and Steganalysis” 2004.
[2].Dr.EktaWalia, “Analysis of LSB and DCT Based Steganography”, Vol 10, Issue1.
[3]. Digital image processing by Gonzalez and woods.
[4].Deshpande Neete, “Implementation of LSB steganography and its evaluation for various bits”.
[5].Zhi Zhou, “halftone visual cryptography”, IEEE transactions on Image processing, August 2006.
[6].George, saad, “image hiding using magnitude modulation on DCT coefficients”. Journal of applied Computer Sciences 2010
[7].Chandramati, Ramesh, “Overview of Various cryptography schemes,” 2010
[8]. Websites like Google, Wikipedia.