Multiple Image Steganography using LSB-DCT Technique

Devadath C Prabhu
Department of CS&E,
PESIT South Campus,
Bengaluru, India

S Ramya Nivedha
Department of CS&E,
PESIT South Campus,
Bengaluru, India

Ayush Kumar
Department of CS&E,
PESIT South Campus,
Bengaluru, India

Sajeevan K
Associate Professor,
Department of CS&E,
PESIT South Campus,
Bengaluru, India

Annapurna D
Professor,
Department of CS&E,
PESIT South Campus,
Bengaluru, India

***Abstract*— Steganography is an art of secret communication. The very existence of the data itself is hidden in steganography. Any little variation in pixels of the images has a low probability of being detected by the human eyes. Thus, data can be hidden in pixels of images. In this paper, a LSB-DCT based steganographic technique for hiding multiple images in a cover image is proposed. The data is embedded by altering least significant bits of quantized DCT coefficients of cover image. Hiding multiple images is achieved by embedding only higher bits of data in cover image. Experiments shows that imperceptibility is high for the stego image as well as PSNR values obtained for both stego image and extracted images are good.**

Keywords—Steganography, LSB, DCT, Cover Image, Stego Image, PSNR

I. INTRODUCTION

Secrecy of information is one of the most important factor in communication. There are two main methods by which secrecy of information can be obtained – Cryptography and Steganography. Cryptography is the process of using codes to ensure secrecy of information during communication. Cryptography has a long history. Its evolution and various methods are available in [1]. With advancement in technologies, it is not enough if the contents of information are kept secret as various Cryptanalysis techniques [2], [3] have been developed to detect the secret information. Thus, keeping the existence of the information secret is necessary. This is achieved using Steganography.

Steganography is the art and science of hiding messages in such a way that no one except the sender and intended recipient suspects the existence of the message. The existence of information is kept secret in Steganography by embedding the information in cover object. A basic block diagram of a Steganographic system is shown in Fig 1. The file used as cover object varies depending on type of media used for Steganography [4]. In our method, image is chosen as cover.

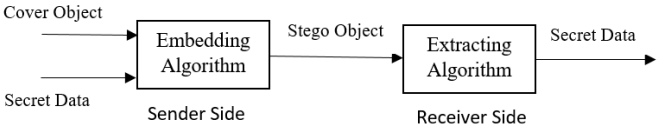


Fig 1. Steganographic system

There are different Steganographic techniques [4] each with their own advantages and disadvantages [5], [6], [7]. In this paper, the secret image is hidden in cover image using combination of LSB and DCT techniques. The cover image is transformed into frequency domain by applying DCT-II. Then pixel bits of secret image is hidden in LSB of quantized DCT co-efficients of cover image and is transformed back to spatial domain to construct the stego image. Few factors considered while designing the system are imperceptibility, payload capacity, PSNR and MSE which are discussed in detail in Section IV. The process of detecting the hidden messages without knowing the key and the algorithm used is Steganalysis [16].

The remainder of the paper is structured as follows. Section II has the overview of related existing works. In Section III, proposed technique is presented. Experimental results are presented in Section IV while Section V concludes the paper with future scope.

II. RELATED WORK

Steganographic embedding is not a new technique and has been used since very long. Many researches have carried various works in this field till date. We present an overview of few works carried out by others in this Section.

Requirements of Steganographic system and survey of various existing Steganographic systems are in [4], [8], [10]. Various existing techniques are analyzed in [11]. The transform domain Steganographic techniques such as DCT and DWT are discussed and analyzed in [12]. The security of few Steganographic approaches are compared and analyzed

in Shaveta Mahajan et al. [13]. The major topic of all these papers are various techniques that embed the data.

Least Significant Bit is one of the simple Spatial Domain techniques and is commonly used technique to embed the data. [14] uses LSB technique to embed the data. The data bits are embedded only in selected areas obtained using pixel selection filter. Immunity to noise and compression is poor using this method. Shailender Gupta et al. [15] uses one, two, three and four LSBs to embed the data once it is encrypted. But data embedded using this technique can be easily decoded. LSB techniques are simple and easy to detect. The robustness of these methods are low and hence other methods were explored.

Transform domain techniques are more immune to noise and variations. [17] proposes a DCT based technique where bits are embedded in DCT coefficients which are below certain threshold. Takeshi et al. [18] proposes a DCT based algorithm that embeds data with less distortion. A Shield algorithm based on DCT to embed the data is proposed in [19]. DCT, a transform domain technique is robust but the amount of information that can be embedded using this technique is less.

An embedding technique that uses both LSB and DCT is proposed in [20]. Analysis and results of LSB and DCT method is discussed in [21]. These methods use advantages of both LSB and DCT technique.

In [22], a method to embed multiple images with bit plane slicing is proposed. The imperceptibility of this algorithm goes on decreasing as the payload capacity is increased. DWT based method to hide multiple images is proposed in [23]. This approach is susceptible to noise. In general, DCT method is more robust and imperceptible compared to other methods proposed.

III. PROPOSED METHOD

The main aim of this work is to maximize the payload capacity without compromising imperceptibility. Proposed method targets grayscale images. Up to eight images can be embedded in a single image using the proposed technique which is discussed in this section. Selection of images (III-A) is discussed first, sub-sections III-B to III-F discusses the proposed LSB-DCT technique for embedding and finally extraction of hidden data is presented in III-G.

A. Image selection

When only one LSB of each DCT coefficients of cover image of size M×N is used to embed the data, the amount of information that can be embedded in the cover image is M*N bits. Considering each pixel is represented using eight bits, the ideal size of a single image that can be embedded is X×Y, where

$$1*X*Y*8=M*N \qquad \text{eq (1)}$$

To embed a single image, all eight bits of pixels in the secret image can be used. Embedding more than one secret image uses only the MSBs of pixels in secret image. The number of MSBs used depends on the number of images to be hidden. Four, two and one MSB(s) are selected to embed two, four and eight images respectively.

B. Discrete Cosine Transform

Discrete Cosine Transform (DCT) [25] is used to transform the image from spatial domain to frequency domain. The cover image of size M×N is first divided into 8×8 blocks and then DCT is applied on each block. DCT-II is used for two dimensional images of M×N. The equation for DCT-II is given by:

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{i=1}^{8}\sum_{i=1}^{8} f(x,y) \times Z \qquad \text{eq (2)}$$

where

$$C(i) = \begin{cases} 1/\sqrt{2} & \text{if } i = 0 \\ 1 & \text{else} \end{cases}$$

and

$$Z = \cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right]$$

for x=1 to 8 and y=1 to 8

On applying DCT on a block of image matrix I, a matrix K is obtained. Matrix I has pixels as its entries whereas matrix K has DCT coefficients as its entry. The obtained matrix K has higher values at the top left. This higher value indicates that it corresponds to lower frequencies and higher signal energies. The values other than that are very small enough such that it can be neglected with no or less distortion.

C. Quantization

Quantization [28] is done to compress the DCT coefficients obtained in previous step. Since human eyes are insensitive to high frequency components, these are made zero using standard Quantization matrix [24] which is

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Quantization is done by dividing each values in matrix K with corresponding values in quantization matrix Q. This will result in matrix P, which has the quantized DCT coefficients.

$$P(i, j) = K(i, j) / Q(i, j) \qquad \text{eq (3)}$$

D. Zigzag scanning

The matrix P, obtained in previous step may have intra-block correlation [9]. To remove this, zigzag scanning is done on matrix P which results in one-dimensional array A. The values in this array will be in ascending order which means that low frequency elements are in the beginning.

E. Embedding

Secret image is embedded by altering the LSB of the values in the array A. Value in A is made even if the data bit is even, else odd.

For embedding multiple images, LSBs of the data are neglected since it carries less information. To embed two images, four MSBs are considered and other four bits are neglected. Thus it satisfies eq (1) with 2*X*Y*4=M*N where 2 is the number of images and 4 is the number of bits. Four images can be embedded by considering only two MSBs, neglecting the remaining six bits. Thus eq (1) becomes 4*X*Y*2=M*N. Similarly 8 images can be embedded by considering only one MSB. Single image is embedded by using all bits in its pixels.

F. Image construction

After embedding, inverse zigzag is applied on array A to convert it back to the 8×8 matrix. Then this block is dequantized by multiplying each value in matrix with the corresponding value in quantization matrix Q and Inverse Discrete Cosine Transform (IDCT) is applied to transform it back to spatial domain. Finally all 8×8 blocks are combined to form the stego image S.

G. Extraction

Extraction of secret images from stego image requires the stego image to be broken into 8×8 blocks, transform it to frequency domain by applying DCT, quantize the coefficients, perform zigzag scanning and extract the data. The extracted bit is 0 if the value is even, else the extracted bit is 1. Concatenate 8 bits together to form a pixel.

When multiple images are hidden, the number of embedded bits are extracted and is concatenated with 0 for remaining bits to form the pixel. If two images are hidden, four bits are extracted from stego image and is concatenated with four zeros to form the pixel. These pixels are arranged to reconstruct the secret image. Similarly four, eight images hidden can be extracted.

IV. EXPERIMENTAL RESULTS

There are many factors that decide how good a Steganographic system is. We consider few of these to analyze our method. Results with each of the factors considered are discussed in this section.

A. Imperceptibility

Imperceptibility is the invisibility of the hidden image to the human eye. This is the most important requirement of Steganographic system since Steganography deals with hiding data. The proposed method generates imperceptible stego image in which hidden image cannot be noticed by human eye. It is measured using PSNR which is discussed in IV-D.

B. Payload capacity

Payload capacity [28] is the amount of information that can be hidden in the cover image. The method we proposed hides up to eight images in a cover image. Simulations are carried out in MATLAB and obtained experimental results are shown in Fig 2 to 7.

C. Mean Squared Error

Mean Squared Error (MSE) [26] gives the average of the squares of errors between cover image and stego image. It is calculated by

$$MSE = \frac{1}{mn}\sum_{i=1}^{m-1}\sum_{i=1}^{n-1}||I(i,j) - S(i,j)||^2 \qquad \text{eq (4)}$$

where I is the cover image and S is the stego image.

MSE for various images with different payload capacity for embedded and extracted images are listed in Table 1 and Table 2.

D. Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) [27] is a measure of peak error. It is the ratio between the maximum possible power of a signal to the power of corrupting noise that affects the precision, in decibels (dB). PSNR measures the quality between two images. It is given by

$$PSNR = 10\log_{10}\left(\frac{MAX}{MSE}\right) \qquad \text{eq (5)}$$

where MAX is the maximum pixel value of image which is 255 for grayscale image.

PSNR values for various images with different payload capacity for embedded and extracted images are recorded in Table 1 and Table 2.

Table 1. PSNR values of stego image with different capacity for Fig 2.

Payload Capacity	MSE	PSNR (dB)
1	0.5778	50.5127
2	0.5732	50.5476
4	0.5677	50.5894
8	0.5836	50.4695

Table 2. PSNR values of extracted image for different capacity of cover image when Fig 3a is hidden.

Payload Capacity	MSE	PSNR (dB)
1	1.0000e-03	78.1308
2	77.4396	29.2412
4	1.3406e+03	16.8577
8	4.7548e+03	11.3595

Fig 2. Cover Image

a **b** **c** **d**

e f g h

Fig 3. (a)(b)(c)(d)(e)(f)(g)(h) Secret Images

a b

Fig 4. (a) Stego image with Fig 3a embedded

(b) Extracted image from Fig 4a

a

b c

Fig 5. (a) Stego image with fig 3a and 3b embedded

(b)and(c) Extracted images from Fig 5a

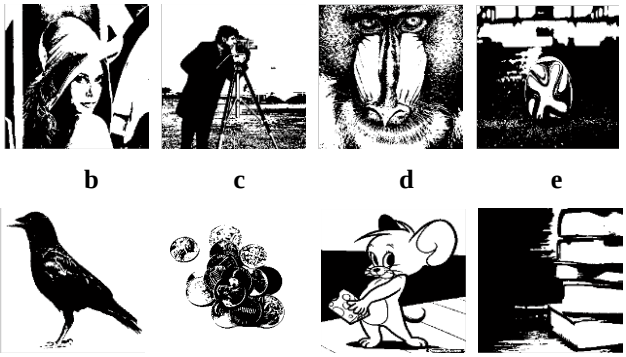
a

b c d e

Fig 6. (a)Stego image with Fig 3a to 3d embedded

(b)(c)(d)(e) Extracted images from Fig 6a

a



b c d e

f g h i

Fig 7. (a) Stego image with fig 3a to 3h hidden

(b)(c)(d)(e)(f)(g)(h)(i) Extracted images from Fig 7a

V. CONCLUSION AND FUTURE SCOPE

Steganography is a vast domain with its major application in watermarking and secret communication. It ensures that the data is invisible and is protected from the third person. There are various techniques of Steganography each with own advantages and disadvantages. LSB method embeds data directly in LSB of pixels of image whereas DCT method embeds data in DCT coefficients of the image. Our proposed method uses a mixture of both techniques to embed data which gives good results with respect to factors analyzed. The main task was increasing the payload capacity of the cover image. However, embedding more and more images decreases the quality of extracted images. When quality of extracted image is not a concern, the proposed method can be used.

Several further directions can be explored, including the Steganalysis for the proposed approach. Further, payload capacity can be increased if more LSBs are considered for embedding. It would also be interesting to try embedding images and texts together in a cover image using proposed approach. Lastly, exploring the audio and video steganography with this technique is suggested.

REFERENCES

[1] Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security," 4th Edition.

[2] Ashish Kumar Kendhe, Himani Agarwal, "A Survey Report on Various Cryptanalysis Techniques," *IJSCE*, vol 3, Issue 2, 2013.

[3] Vinod Saroha, Suman Mor, Jyoti Malik, "A Review of Various Techniques of Cryptanalysis," *IJARCSSE*, vol 2, Issue 10, 2012.

[4] Jasleen Kour, Deepankar Verma, "Steganography Techniques – A Review Paper," *IJERMT*, vol-3, Issue 5, 2014.

[5] Pooja Rai, Sandeep Gurung, M.K. Ghose, "Analysis of Image Steganography Techniques: A Survey," *International Journal of Computer Applications* (0975-8887), vol 114, No. 1, 2015.

[6] S.G.Shelke, S.K.Jagtap, "Analysis of Spatial Domain Image Steganography Techniques," *IEEE International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2015.

[7] Falesh M. Shelke, Ashwini A. Dongre, Pravin D. Soni, "Comparision of different Techniques for Steganography in Images," *IJAIEM*, vol 3, Issue 2, 2014.

[8] Nan-I Wu, Chung-Ming Wang, Min-Shiang Hwang, "Data Hiding: Current Status and Key Issues," *International Journal of Network Security*, vol 4, No. 1, pp. 1-9, January 2007.

[9] Chengjie Tu, Trac D. Tran, "Context-Based Entropy Coding of Block Transform Coeffiecients for Image Compression," *IEEE Transactions on Image Processing*, vol 11, No. 11, 2002.

[10] R Poornima, R J Iswarya, "An Overview of Digital Image Steganography," *IJCSES*, vol 4, No. 1, 2013.

[11] C.P.Sumathi, T.Santanam, G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *IJCSES*, vol 4, No. 6, 2013.

[12] Gurmeet Kaur, Aarti Kochhar, "Transform Domain Analysis of Image Steganography," *IJSETT*, 6(1): 29-37, 2013.

[13] Shaveta Mahajan, Arpinder Singh, "A Review of Methods and Approach for Secure Stegnography," *IJARCSSE*, vol 2, Issue 10, 2012.

[14] Rahul Joshi, Lokesh Gagnani, Salony Pandey, "Image Steganography With LSB," *IJARCET*, vol 2, Issue 1, 2013.

[15] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," *IJMECS*, 6, 27-34, 2012.

[16] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", *Morgan Kaufmann Publishers*, 2nd Edition, 2008.

[17] Hardik Patel, Preeti Dave, "Steganography Technique based on DCT Coefficients," *IJERA*, vol. 2, Issue 1, 2012.

[18] Takeshi Ogihara, Daisuke Nakamura, Naokazu Yokoya, "Data Embedding into Pictorial Images with Less Distortion Using Discrete Cosine Transform," *IEEE Proceedings of ICPR*, 1996.

[19] Deepika Bansal, Rita Chhikara, "An Improved DCT based Steganography Technique," *IJCA*, vol 102, No. 14, 2014.

[20] Deepak Singla, Rupali Syal, "Data Security Using LSB & DCT Steganography In Images", *IJCER*, vol 2, Issue 2, 2012.

[21] Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography," *GJCST*, vol 10, Issue 1, 2010.

[22] H Faheem Ahmed, U Rizwan, "Embedding Multiple Images in an Image Using Bit Plane Slicing", *IJARCSSE*, vol 3, Issue 1, 2013.

[23] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "A secure and high capacity Image Steganography technique," *SIPIJ*, vol 4, No. 1, 2013.

[24] Andrew B. Watson, "Image Compression Using the Discrete Cosine Transform," *Mathematica Journal*, 4(1), 1994.

[25] https://en.wikipedia.org/wiki/Discrete_cosine_transform.

[26] https://en.wikipedia.org/wiki/Mean_squared_error.

[27] https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[28] Jessica Fridrich, "Steganography in Digital Media", *Cambridge University Press*, 2010.