International Journal of Scientific & Engineering Research, Volume 6, Issue 11, November-2015 1060
ISSN 2229-5518

Improved Capacity Collage Steganography Using Discrete Cosine Transformation

Nidhi Antony

Abstract— Nowadays establishing secure communication has gained increasing relevance. One of the methods used for hidden communication is steganography, in which secret message is embedded into a carrier without attracting the attention of unintended recipients. Among the various steganography methods that have been proposed so far a new type of steganography, collage steganography hides the secret message in a more secure way. This paper presents an improved capacity collage steganography using DCT.The secret message, image pixels, coefficients, header files are embedded into cover image by using object images with transparent features and affine transformation parameters. Capacity analysis is used to select the cover image. The appearance of cover image is altered due to object image used for embedding. Template matching techniques are used to retrieve information.

Index Terms— Affine transformation, Capacity, Discrete cosine transform, Embedding, Secret Message, Steganography, Retrieving

1 Introduction

WITH the development of computer and its extensive usage in different aspects of work and daily life, secure communication has gained significant importance. For establishing secure communication various methods such as cryptography, steganography and watermarking have been used. Among these steganography is most commonly used during recent years.

Steganography is a data hiding technique used for transmitting cover media with secret message between sender and receiver without attracting the attention of unintended recipient in public channel**.** Steganography is a Greek word which means hidden writing. Text, image, video and audio are the possible cover media of secret message.

The main purpose of implementing this technique is to hide secret message in a cover media so that existence of data is not noticed by other persons.This is a major difference of this method over other traditional methods. In cryptography methods individuals receiving encoded data notice the existence of secret message but they cannot extract it. In steganography methods existence of data is not noticed by other persons. Depending upon different cover media used there are different types of steganography methods. If image is used as cover media then it is called image steganography. Among various steganography methods, the most common approach is to use image steganography because the redundancy of information in images is high.

This paper proposes collage steganography [1], [2], [3] which is a new type of steganography method in comparison to existing methods. The advantage of this method is that object image is used as the detractor, which avoids suspicion of secret message. Secret message bits are embedded in a cover image using affine transformation. The embedding of secret message is performed using a combination of iterative division and DCT embedding [4]

• *Nidhi Antony is currently pursuing masters degree program in Communication Engineering in Rajagiri School of Engineering and Technology, Mahatma Gandhi University, Kerala,India,E-mail: nidhian92@gmail.com*

2 Collage Steganography

This method hides secret message by altering the appearance instead of the features of image. Before embedding the secret message is converted to binary data. Two sets of image databases are needed cover image data base and object image database. Cover image database includes potential carriers whereas object image database includes directories of object images which are used to paste on top of cover image. The object images are of file type PNG or GIF containing transparent features. They have irregular shape and allows object image to be integrated into other images without visible rectangular outlines.

The main idea used in this paper is embedding object images into cover image so as not to be noticeable. Depending upon the location of object image on cover image and mode of object, the secret data is hidden in the image

3 Proposed Method

The proposed method basically consists of three steps

1. Capacity Analysis.
2. Embedding Algorithm.
3. Retrieving Algorithm.

3.1 Capacity Analysis

A proper cover image is selected by performing capacity analysis. Embedding capacity of cover image is analyzed before embedding process. The objective is to find the smooth regions with potential areas to incorporate an object image. Smooth regions are determined by performing self-similarity measurement method. In this method similar pixel areas are grouped together based on statistical calculation between pixel values.

ISSN 2229-5518

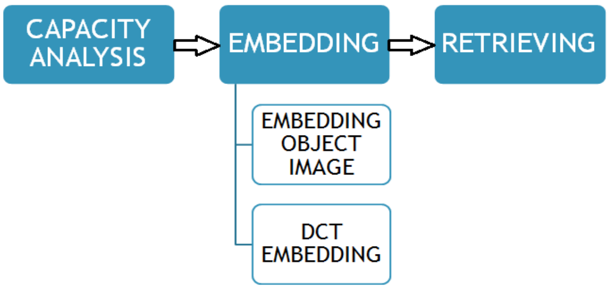

Fig. 1. Block Diagram of Improved Capacity Collage Steganography using Discrete Cosine Transformation

The embedding capacity of cover image is calculated based on smooth regions and average size of the possible object images. The capacity analysis algorithm is described as follows:

1. Divide the cover image into non-overlapping blocks of size m×n.Each block is denoted as b_{ij},where i and j indicate the block index along rows and columns respectively.
2. Calculate the variance σ^2 for the image blocks.
3. Select the blocks using the constraint of mean values between blocks.

$$\sigma_{ij}^2 < \in_v \quad (1)$$

4. Calculate the number of pixels in the selected blocks. The number indicates the size of the feasible smooth region in a cover image and is denoted as a_s.
5. The embedding capacity C of the cover image is calculated as the ratio of the smooth region a_s from step 4 over the average size of object images a_o.

$$C = \frac{a_s}{a_o} \quad (2)$$

r_o can be the average size of either the entire object image database or the possible image directories in the database which are suitable for a cover image. The capacity can be calculated using only the feasible smooth regions which are greater than a specific size of area and the size of possible object images assigned by the users.

3.2 Embedding Algorithm

The Embedding Algorithm includes three stages

1. Affine Transformation.
2. Embedding the object image.
3. DCT Embedding.

1) Affine Transformation: The Affine transformation is a two dimensional geometric transformation representing a set of mapping operations such as scaling, rotation and translation. Given a pixel index represented as a vector, $p_o = [x_o; yo; 1]^T$. The pixel can be transformed to another location p_1 in the coordinate system using affine transformation matrix T given by,

$$T = \begin{bmatrix} s_x cos\theta & -s_y sin\theta & t_x \\ s_x sin\theta & s_y cos\theta & t_y \\ 0 & 0 & 1 \end{bmatrix} \quad (3)$$

where s_x and s_y are the scaling factors, tx and t_y are the translation factors, zooming and shifting along rows and columns respectively, and θ is a rotation of radians counterclockwise about the origin.

If θ=0, and $s_x=s_y=1$, a shape merely operates translation movement from one location to another in the coordinate space. The pixel values after transformation, especially scaling and rotation, are calculated using the inverse mapping approach.

p_1 can be obtained by matrix multiplication with T.

$$p_1 = T.p_o \quad (4)$$

2) Embedding the object image: The Steganographic message is represented by the binary bit stream. The generalized collage steganographic method converts the binary bit stream message recursively using the division operation where dd is the dividend, dv is the divisor, qt is the quotient and rd is the remainder.

$$\frac{dd}{dv} = qt \ldots\ldots\ldots.\ldots\ldots\ldots\ldots\ldots\ldots\ldots.rd \quad (5)$$

The steganographic message is hidden in translation, scaling, rotation factors in affine transformation matrix as well as in the cover image. Permissible area is determined from the smooth region. The corner location of object image is pasted into this area. The variables dv_i is considered as the divisors for embedding purpose. The five divisors are listed below,

1. dv_1: number of object images in object image database.
2. dv_2: number of rows in permissible area.
3. dv_3: number of columns in permissible area.
4. dv_4: number of feasible scaling factors.
5. dv_5:number of feasible rotation angles

The variables are not limited above, based on user requirement and specification it may vary. The number of binary bits b, which is allowed to be stored in permissible area is defined as:

$$b = \lfloor b1 \rfloor \quad (6)$$

where b1 is given by

$$b1 = log_2[\prod_{i=1}^{5} dv_i] \quad (7)$$

With the allowed bits $u_0u_1u_{b-1}$, hidden in permissible area, the decimal value is calculated as

$$d = \sum_{i=0}^{b-1} w_i u_i = \sum_{i=0}^{b-1} 2^i u_i \quad (8)$$

The range of d is $[0,2b^{-1}]$.Considering dv_1 to dv_5 as divisors and dd as dividend, the division operation as in (5) can be used recursively to derive set of quotients and remainders. For every iteration l,the dividend is the quotient obtained from the previous iteration l-1.The remainders from each iteration are the selected object image index, the translational factors t_x and t_y, the scaling factor for $s_x = s_y$, and rotation angle θ about the reference point as the centre of the object image. Hence the selected object image can be pasted into cover image within the permissible area and the derived affine transformation matrix. The corner indices of object image are used for hiding last four remainders.

The last quotient for each permissible area, either 0 or 1, and the object image indices need to be stored in order to retrieve the secret message. This is done by using DCT embedding [4].The divisors are stored in key file.

3) DCT Embedding: A combination of frequency domain by means of DCT and LSB technique of spatial domain steganography has been used to hide data. Two dimensional DCT converts the image block from spatial domain to frequency domain and then data bits are embedded by altering LSB of DCT coefficients.

The steps in DCT Embedding are as follows

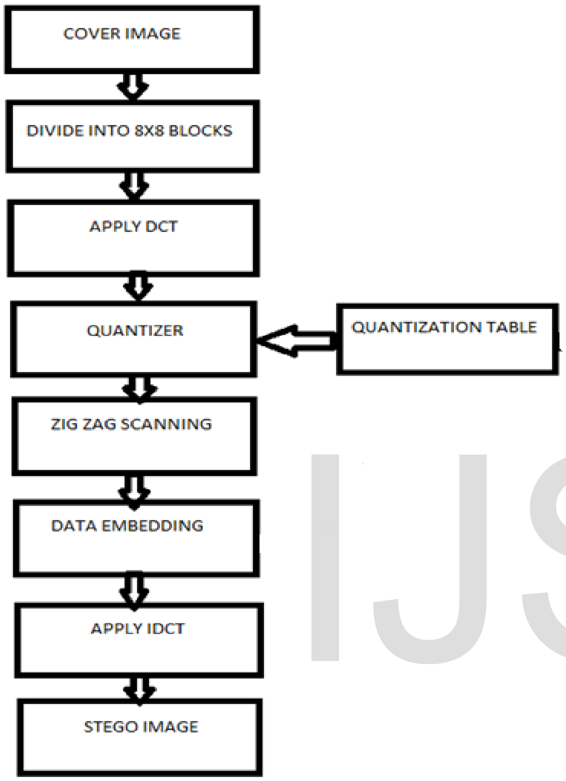

Fig. 2. DCT Embedding Block Diagram

162	40	20	72	30	2	-1	-1
30	108	10	32	27	5	8	-2
-94	-60	12	-43	-31	6	-3	7
-38	-83	-5	-22	3	5	-1	3
-31	17	-5	-1	4	-6	1	-6
0	-1	2	0	2	2	8	2
4	-2	2	6	8	-1	7	2
-1	1	7	6	2	0	5	0

Fig. 3. Discrete Cosine Transformation Coefficient Matrix.

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

Fig. 4. Discrete Cosine Transformation Quantization Matrix.

1. Discrete Cosine Transform: The image of size m×n is divided into 8×8 blocks and (2-D) DCT is performed on each block. In DCT block lower frequency coefficients are at upper left positions and higher frequency coefficients are at lower right positions. Low frequency coefficients are of larger value than high frequency coefficients. An example of 8×8 block of DCT coefficients is shown in Fig. 3.
2. Quantization: It compresses 8×8 block of DCT coefficients. A useful feature in this process is the image compression and the quality is obtainable through the selection of specific quantization table. The standard quantization matrix is shown in Fig. 4.Quantization is achieved by dividing each element in DCT coefficient block by corresponding value in the quantization matrix and the result is rounded to the nearest integer. As eye is not able to discern the change the high frequency components can be compressed to large extent. Lower right side components of quantization matrix are of high value so that after quantization high frequency components become zero. An example of quantized DCT block is shown in Fig. 5.

10	4	2	5	1	0	0	0
3	9	1	2	1	0	0	0
-7	-5	1	-2	-1	0	0	0
-3	-5	0	-1	0	0	0	0
-2	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Fig. 5. Quantized Discrete Cosine Transformation Block

3. Zigzag Scanning: After block DCT coefficients are arranged in zigzag scan pattern as in Fig. 6. dependencies among neighboring coefficients in both horizontal and vertical directions can be investigated. Zigzag scan [4] converts 8×8 blocks into 64 elements one dimensional array.

ISSN 2229-5518

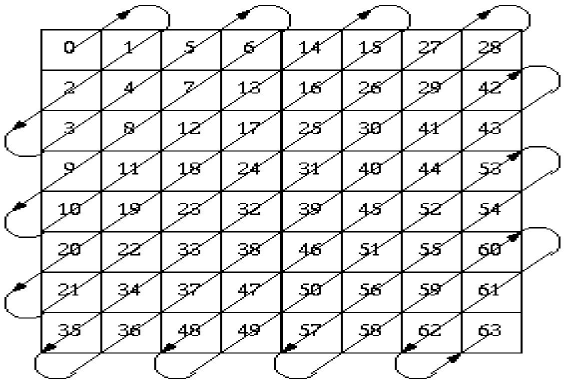

Fig. 6. Zigzag Scanning of Discrete Cosine Transform block coefficients.

4. Data Embedding: Data bits are concealed by altering the LSB of elements of zigzag array. If data bit is 0 then make DCT coefficient even or if data bit is 1 then make DCT coefficient odd.
5. Dequantization and Inverse DCT: After embedding data zigzag array is again converted into 8×8 block. These blocks are dequantized and inverse DCT is performed. The entire 8×8 blocks are combined to form the stego image as shown in Fig. 9. which is then sent to the receiver.

3.3 Retrieving Algorithm

For retrieval the receiver must have object image database as well as key file containing divisors and steganographic image. The object image indices and last quotient are retrieved by performing DCT retrieving. The steps in DCT retrieving are as follows:

1. Divide the stego image into 8×8 blocks.
2. Perform 2-D DCT on each block.
3. Perform Quantization on each block.
4. Perform zigzag scan to convert 8×8 block into one dimensional array.
5. Check the DCT coefficient. If DCT coefficient is even then data bit is 0 or, if DCT coefficient is odd then data bit is 1.
6. Concatenate the bits to obtain secret message.

With the knowledge of incorporated object image index in a certain directory, each remainder, the divisors from the key file and the quotient for each permissible area, the hidden data is retrievable as

$$qtdv + rd = dd \qquad (9)$$

4 Experimental Results

The object image database is created by gathering images from various websites. The image size can be altered using image preprocessing methods based on cover image size and other user specification

Suppose a secret message is to be transmitted with collage steganographic method. The appropriate cover image will be chosen according to capacity analysis. The selection of object image directory is also required. For example if the smooth region in the image is the sky, only flying objects such as birds,airplanes,baseballs etc. can be pasted onto cover image. Appropriate selection of object image allows image to appear as natural as possible.

The implementation of proposed method was done using MATLAB software. A cover image as shown in Fig. 7. was chosen by performing capacity analysis on 10 different cover images. The permissible area is selected of size 15×23 within the smooth region at the lower right part of image. In other words dv_2=15 and dv_3=23.The chosen object image directory is Cow having 11 cow images,dv_1=11.One among them is chosen as object image to be pasted onto cover image. The number of feasible scaling factor is 2,dv_4=2,which includes the potential $s_x=s_y$=1 or 0.8.The number of feasible rotation angles is 3,dv_5=3,which includes possible θ=0 or $\pm\pi/4$.

Consider the secret message 001001110110101.The corresponding decimal value is 5045 and recursively dividing using dv_1 to dv_5 as dv, the remainders are 7, 8, 7, 1, 0.This designates object image index 7 in the directory is selected as shown in Fig. 8.The affine transformation factors are t_x=8, ty=7, $s_x=s_y$=1 and θ=0.The last quotient value 0 and the object image indices are hidden in the cover image itself using DCT embedding. The retrieved message is 1001110110101

Fig. 7. Cover Image selected after performing capacity analysis.

Fig. 8. Object Image selected for incorporating into cover image.

Fig. 9. Steganographic Image obtained after incorporating object image into cover image.

4 Conclusion

This paper proposes Improved capacity collage steganography using Discrete Cosine Transformation, an extension to Generalized Collage Steganography[1] which is different than existing steganographic methods. In order to select proper cover image according to secret message the capacity of cover images in database are analyzed in advance by determining smooth regions. The secret messages were hidden into cover image by incorporating object image which are displayed directly. Using the combination of iterative division and DCT embedding secret messages were hidden. This method has high capacity over other collage steganographic method [2], [3].The proposed method can be used in military applications, mobile phones via MMS sevices, e-governance

Acknowledgment

The author would like to thank God, the Almighty for his immense blessings on the successful completion of the paper. The author would also like to thank Krishnapriya M, Niya Francis, and R.Nimmy for their valuable support throughout the implementation and background studies.

References

[1] M.-C. Chen, S.S. Agaian, and C.L.P. Chen,"Generalized Collage Steganography on Image", IEEE International Conference on Systems, Man and Cybernetics, 2008.

[2] S. Shirali-Shahreza and M. Shirali-Shahreza,"Improved Collage Steganography", International Conference on Emerging Technologies, 2008.

[3] M. Shirali-Shahreza and S. Shirali-Shahreza, "Collage Steganography", Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse ,2006.

[4] D. Singla and R. Syal, "Data Security Using LSB and DCT Steganography In Images", International Journal Of Computational Engineering Research,ISSN:22503005,IJCER