Image Steganography Using Block Level Entropy Thresholding Technique

Jagdish Mali[1], Viraj Sonawane[2], Prof. R.N.Awale[3]

[1,2] M.Tech Student, Department of Electrical Engineering, Veermata Jijabai Technological Institute, Matunga, Mumbai-19

[3]Professor, Department of Electrical Engineering, Veermata Jijabai Technological Institute, Matunga, Mumbai-19

ABSTRACT

Now days a lot of applications are Internet based and in some cases it is desired that the communication be made secret. The two most important aspects of any image based Steganographic system are the imperceptibility and the capacity of the stego image. In this paper, a novel Image Steganographic method using Block Level Entropy Thresholding Technique is proposed. This paper evaluates the performance and efficiency of using optimized Embedding tables within JPEG Steganography. After dividing cover image into 8X8 non overlapping blocks, DCT (Discrete Cosine Transform) is computed and based on Entropy Threshold (ET) scheme, these blocks are selected for information embedding decision. The secret message is hidden in the Valid Entropy Block of cover-image with its middle-frequency of the DCT coefficients. Finally, a JPEG stego-image is generated. DCT based Steganography scheme provides higher resistance to image processing attacks such as JPEG compression, noise, rotation, translation etc. we obtain that the proposed method has a larger message capacity, and the quality of the stego images of the proposed method is acceptable.

Keywords - Steganography, Discrete Cosine Transform (DCT), Data hiding, Entropy Thresholding, MSSIM.

I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. In image Steganography the information is hidden exclusively in images. Its main purpose is to hide the occurrence of communication over a public channel. In contrast to cryptography, Steganography tends to hide the very existence of the message or any communication form, whereas cryptography aims is to conceal the content of the secret message. Hiding the occurrence of communication can be done by embedding a secret message into an innocent cover medium, such as an image, which no one else than the sender and the recipient can suspect.

An information hiding system uses two algorithms to communicate: an embedding algorithm to produce the modified cover data (stego image) which results after embedding the secret message and an extraction algorithm to recover message from the stego image. Digital image that contains perceptually irrelevant or redundant information can be used as cover or carrier to hide secret messages. After embedding secret message into the cover image, so called stego image is obtained. The hidden data could be of various usages like copyright information, captions, time stamps, or movie subtitles, etc.

There are two kinds of image Steganographic techniques: *spatial domain* and *frequency domain* based methods. The schemes of the first kind directly embed the secret data within the pixels of the cover image such as Least Significant Bit (LSB) insertion [1]. The schemes of the second kind embed the secret data within the cover image that has been transformed such as DCT (discrete cosine transformation). The DCT coefficients of the transformed cover image are modified according to the secret data [2]. The capacity of spatial domain scheme (the amount of data embedded within a given image) is better than that of the transform based scheme. However, the frequency domain schemes are more robust than that of the spatial domain [4]. In this paper Data is directly embedded in the image and not into a header. Embedded data is self detectable. The modified image has good resemblance to the original image.

In JPEG compression, the image is divided into disjoint blocks of 8x8 pixels, a 2-dimensional DCT is applied to each block, and then the DCT coefficients of these blocks are coded. Most of the steganography techniques used for JPEG images adopt the standard JPEG compression. The cover image is divided into non-overlapping blocks of 8x8 pixels in order to perform DCT and provide compressed images [4] and [6]. Note that the secret image is embedded in the middle-frequency part of valid entropy block DCT coefficients in our method. The rest of this paper is organized as follows. Section II will review various data embedding techniques Section III will propose our data hiding method in JPEG. Section IV and Section V will propose Data Embedding Algorithm and Extracting Algorithm respectively. In Section VI experimental results will be listed. Finally, the conclusions will be presented in Section VII.

The Steganographic approaches for data hiding are divided into two types:

1) Spatial/Time domain

Spatial domain techniques embed messages in the intensity of the pixels directly. Least Significant Bit (LSB) is the first most famous and easy spatial domain Steganography technique. It embeds the bits of a message in a sequential way in the LSB of the image pixels but the problem of this technique is that if the image is compressed then the embedded data may be destroyed [1]. Thus, there is a fear for damage of the message that may have sensitive information. Moreover, these kinds of methods are easy to attack by Steganalysis techniques.

2) Transform domain

In this domain data embedding is done in the transform domain with a set of transform coefficients in the mid frequency bands as these are preserved better under compression attacks as compared to high frequency coefficients [7]. Transform domain technique performs well against attacks such as compression, cropping etc. and is imperceptible to human sensory system. Hence it is more undetectable.

In this paper, entropy property of an image block is considered for decision of data embedding. In order to robustly hide large volumes of data in images without causing significant perceptual degradation, hiding techniques must adapt to local characteristics within an image. The block level Entropy Threshold (ET) method decides whether or not to embed data in each block (typically 8X8) of transform coefficients depending on the entropy within that block. If a particular block fails this test, we keep it as it is and embed the same data in the next block that passes the test.

II. DATA EMBEDDING TECHNIQUES

The steganographic approaches for data hiding are divided into two types: 1) Spatial/Time domain and 2) Transform domain. Transform domain technique performs well against attacks such as compression, cropping etc. and is imperceptible to human sensory system. Hence it is more undetectable. Data embedding is done in the transform domain with a set of transform coefficients in the mid frequency bands as these are preserved better under compression attacks as compared to high frequency coefficients [7]. In this paper, entropy property of an image block is considered for decision of data embedding. In order to robustly hide large volumes of data in images without causing significant perceptual degradation, hiding techniques must adapt to local characteristics within an image. Two methods for applying local criteria which results in high volume data hiding are considered. First is the block level *Entropy Thresholding (ET) method* which decides whether or not to embed data in each block (typically 8X8) of transform coefficients depending on the entropy within that block. If a particular block fails this test, we keep it as it is and embed the same data in the next block that passes the test. The second is *selectively Embedding in Coefficients (SEC) method*, which decides whether or not to embed data based on the magnitude of the coefficient.

III. THE PROPOSED METHOD

Multimedia files are large in size and consume lots of hard disk space. So in order to reduce the image's file size, compression technique is used. Compression works by removing redundant data effectively summarizing the contents of a file in a way that preserves as much of the original meaning as possible. For these, different image file formats exist. Among all these file formats, JPEG file format is the most popular on the internet because of the small size of the images.

Tseng and Chang proposed a novel steganographic method based on JPEG. DCT for each block of 8x8 pixels was applied in order to improve the capacity and control the compression ratio [8]. Chang et al. developed a steganographic method based upon JPEG and modified 8x8 quantization table in order to improve the hiding capacity of Jpeg-Jsteg method. They utilized the middle frequency band for embedding in order to achieve better hiding capacity and acceptable stego image quality [4]. Since the energy of image is concentrated in the lower frequency coefficients, modifying such coefficients may cause a quality degradation of output image. However, high frequency coefficients will be discarded due to the quantization process. However, high frequency coefficients will be discarded due to the quantization process [Figure 1].

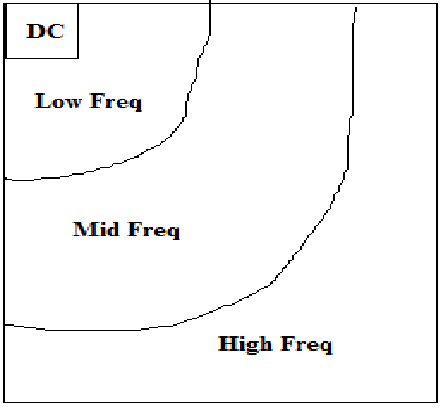


Figure-1 Frequency Distribution in a DCT Block

Fig. 2 shows the block diagram of the proposed Steganographic model. The proposed method uses the JPEG image preprocessing method upon the cover-image. We partition a cover-image C into non overlapping blocks of 8x8 pixels, and then we use DCT to transform each block into DCT coefficients. The corresponding 2-D (2 D) DCT, and the inverse DCT are defined as

$$S(u,v) = \frac{2}{N}C(u)C(v)\sum_{u=1}^{N-1}\sum_{v=1}^{N-1}F(x,y) * \left(\cos\frac{\pi u(2x+1)}{2N}\right)\left(\cos\frac{\pi v(2y+1)}{2N}\right)$$

$$F(x,y) = \frac{2}{N}\sum_{u=1}^{N-1}\sum_{v=1}^{N-1}C(u)C(v)S(u,v) * \left(\cos\frac{\pi u(2x+1)}{2N}\right)\left(\cos\frac{\pi v(2y+1)}{2N}\right)$$

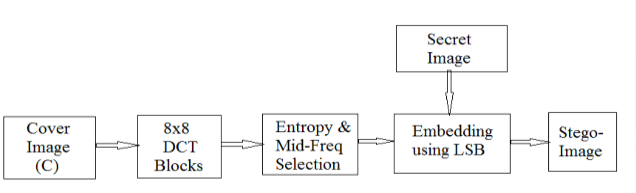


Figure – 2.Block diagram of Proposed Embedding Model

To find embedding region first Compute entropy (E) of all 8x8 DCT blocks. Entropy formula is shown in eq. 1.

E= $\sum_{i,j}$ ||Xi, j ||^2 (i,j) ≠(0,0) – (1)

Then calculate Mean Entropy (ME) from all blocks entropy. Now, to obtain the valid block (VB), compare the entropy of each block with mean entropy (ME). For embedding the information, we select block having entropy higher than the mean entropy value and is named as valid block. Further step is embedding by using K matrix. Middle coefficients of K Matrix are one's and other coefficients are zero this is because our secret message will be embedded in the middle-frequency part of the quantized DCT coefficients. In k matrix there are 26 coefficients located in the middle part that are set to be one.

$$K=\begin{bmatrix} 16 & 11 & 10 & 16 & 1 & 1 & 1 & 1 \\ 12 & 12 & 14 & 1 & 1 & 1 & 1 & 55 \\ 14 & 12 & 1 & 1 & 1 & 1 & 69 & 56 \\ 14 & 1 & 1 & 1 & 1 & 87 & 80 & 62 \\ 1 & 1 & 1 & 1 & 68 & 109 & 103 & 77 \\ 1 & 1 & 1 & 64 & 81 & 104 & 113 & 92 \\ 1 & 1 & 78 & 87 & 103 & 121 & 120 & 101 \\ 1 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Figure – 3.Quantization Matrix K

They are K[0,4],K[0,5], K[0,6], K[0,7], K[1,3], K[1,4], K[1,5], K[1,6], K[2,2], K[2,3], K[2,4], K[2,5], K[3,1],K[3,2], K[3,3], K[3,4], K[4,0], K[4,1], K[4,2], K[4,3],K[5,0], K[5,1], K[5,2], K[6,0], K[6,1], and K[7,0]. Here K[a,b] is the value of the ath row and bth column element of K [4]. Based on this table, the secret messages can be reserved and the reconstructed Image will not be too much distorted. The secret image S will be embedded in the middle frequency part of the DCT coefficients for valid block Vb. After embedding the secret image IDCT is taken to get Stego Image which will similar to the cover Image.

The procedure of embedding and extracting secret message in a cover image for JPEG based steganography approach is described below:

IV. DATA EMBEDDING ALGORITHM

1) First read input secret image file S which needs to be embedded.

2) RGB colour representation is first converted to a YUV representation. This step is required if the cover image is coloured. For JPEG, DCT is used but similar transforms can also be used for example the DFT (Discrete Fourier Transform).

3) Read cover image C (i, j) and divide it into disjoint blocks of 8×8 pixels. Each block is denoted by B. Now, for each block B (8, 8) which is in the range (0-255), the Discrete Cosine Transform (DCT) is calculated, producing 64 DCT coefficients. Let the ith DCT coefficient of the pth block as Cp(i), 0 ≤ i ≤ 63, p = 1… T, where 'T' is the total number of blocks in the image. Then make the DC coefficient of each block zero that is first coefficient of each 8x8 DCT block C(1,1).

4) Compute the entropy (E) of each 8 X 8 block as,

E=∑||Xij||2 (i,j) ≠(0,0)

5) Compute mean entropy (ME) of all T blocks. Now, to obtain the valid block (VB), compare the entropy of each block with mean entropy (ME). For embedding the information, we select block having entropy higher than the mean entropy value and is named as valid block [8].

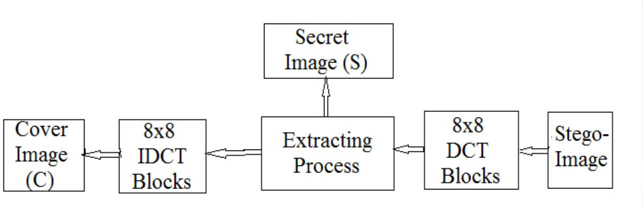
6) Further step is embedding using K matrix as follows,

Within each valid block, we choose the coefficients as, Select VB[a,b] to hide Secret data S respectively, where [a,b] equals to [0,4], [0,5], [0,6], [0,7], [1,3], [1,4], [1,5], [1,6], [2,2], [2,3], [2,4], [2,5], [3,1], [3,2], [3,3], [3,4], [4,0], [4,1], [4,2], [4,3], [5,0], [5,1], [5,2], [6,0], [6,1], and [7,0], respectively. Each VB [a,b] embeds one secret bit using LSB technique into it.

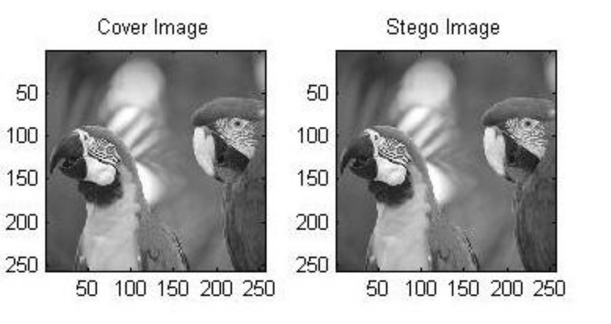
7) Compute Inverse Discrete Cosine Transform (IDCT) of all blocks. The blocks which are not used for embedding are taken as it is in stego image. At the end, add DC coefficient of each block in its respective block and organize all the blocks to get image, which is called stego image Stego (i, j).

V. Data Extraction Algorithm

While extracting the secret data, above Embedding steps are repeated for stego image. Extract 26 mid frequency Bit information (BI) from Valid Coefficient of all Valid Block in zigzag order of stego image. Then we order the extracted BI. Finally decode the image information and acquire input secret image file S.



VI. Simulation Results



Experiment was conducted in order to evaluate the efficiency of our method. Cover image of 256x256 pixels was used. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) criteria was used to measure the quality of image coding and compression. The PSNR for proposed algorithm was 61.15. Moreover, the improvement in robustness brought by this algorithm was considerably high.

VII. Conclusion

In this review, the secret message is embedded in the middle-frequency part of the DCT coefficients. Analysis based on DCT Steganography has been done on basis of parameters like PSNR. Grayscale images have been used for experiments. Peak signal to noise ratio is used to compute how well the methods perform. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality. Our experimental results show the proposed method provides acceptable image quality and highly robust system with high security system.

References

[1] Wang, R.Z., C.F. Lin and J.C. Lin. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 34, pp 671-683, 2001.

[2] Y. K. Lee and L.-H. Chen, “High capacity image steganographic model”, In IEE Proceedings on Vision, Image and Signal Processing, June, 147(3), 2000, pp. 288-294.

[3] Adel Almohammad, Gheorghita Ghinea, Robert M. Hierons. JPEG steganography: a performance evaluation of quantization tables International Conference on Advanced Information Networking and Applications 2009.

[4] Chang C.C., T.S. Chen and L.Z. Chung. A steganographic method based upon JPEG and quantization table modification. Information Sciences, 141, pp: 123-138, 2002.

[5] ISO DIS 10918-1 “Digital Compression and Coding of Continuous-Tone Still Images (JPEG)”, CCITT Recommendation T.81.

[6] Q. Li, C. Yu and D. Chu, “A Robust Image Hiding Method Based on Sign Embedding and Fuzzy Classification”, The Sixth World Congress on Intelligent Control and Automation, *2006. WCICA 2006*, June 21-23.2006, pp.10050-10053.

[7] Mansi Subhedar, Gajanan Birajdar, “Block Level Entropy Thresholding Technique for High Volume Image Adaptive Data Hiding” ICGST-GVIP Journal, Volume 11, Issue 3, June 2011.

[8] H.W.Tseng and C.C.Chang. Steganography using JPEG compressed images. The Fourth International Conference on Computer and Information Technology, CIT '04, 14-16 Sept, pp: 19-17, 2004.