Image Steganography using Block Level Entropy Thresholding Technique

Souma Pal  
Research Scholar  
Department of Computer Science & Engineering  
University of Calcutta, West Bengal, India

Prof. Samir Kumar Bandyopadhyay  
Professor  
Department of Computer Science & Engineering  
University of Calcutta, West Bengal, India

Abstract

Our modern civilization is based on Internet and sometimes it is required to keep the communication secret. It becomes possible by using two techniques: Cryptography and Steganography. The key concept behind both of two approaches is to hide information in anyway. There is little difference of these two approaches. Cryptography conceals the content of the secret message whereas Steganography is more advanced concept of the former. It embeds the secret message within a cover medium. Steganography is art and science in which the secret message is embedded into a cover medium so that no one else than the sender and the recipient can suspect it. So the third parties except the sender and receiver are imperceptible and unaware of the existence of the secret message. There are so many efficient Steganographic techniques like that text, image, audio, video and so on. This paper proposes only Image Steganographic method using Block Level Entropy Thresholding Technique.

Keywords: Steganography, Cryptography, Data hiding, Entropy

I. INTRODUCTION

The information hiding system uses two algorithms: embedding algorithm and extraction algorithm. The embedding algorithm hides the information which is to be kept secret within a cover image in such a way that no one else than the sender and receiver can understand the existence of the secret message and finally produces the stego-image. The extraction algorithm retrieves the original message from stego-image by omitting the irrelevant or redundant information presence in the cover image. There are two kinds of steganographic techniques: spatial domain and frequency domain.

A. 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.

B. Transform/Frequency Domain:

Transform domain technique is done with a set of transform coefficients(DCT,entropy ) 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 and robust than spatial domain.

This paper highlights the transform domain method. The cover image is split into non-overlapping 8x8 blocks and DCT (discrete cosine transforms) is computed for each block. 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. In this paper, entropy property of an image block is considered for decision of data embedding. 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.

II. REVIEW WORKS

Steganalysis is the art of how to detect the existence of hidden information or hidden message in a multimedia document, and to discriminate stego object and non-stego-object with little or no knowledge about the steganography algorithm. The goal of steganalysis is to collect any evidence about the presence of embedded message [1]. If the steganography is the art of hiding messages into multimedia documents; the steganalysis is the art of detecting such the hidden messages. A message can be hidden
in a document only if the content of a document has high redundancy [2]. Although the embedded message changes the characteristics and nature of the document, it is required that these changes are difficult to be identified by an unsuspecting user. On the other hand, steganalysis develops theories, methods and techniques that can be used to detect hidden messages in multimedia documents. The documents without any hidden messages or hidden information are called cover documents and the documents with hidden messages are named stego documents [3][4]. The multimedia document may be text, image, audio or video, this paper will concentrate on the image. Also stego document or stego object in this paper will be the stego image which is the image with hidden message or hidden information, and the cover document or cover object is the cover image which is the original image without and hidden message. The primary step of steganography and steganalysis process is to identify the image that the secret message will be hidden in, which will called cover image, then use any steganography algorithm to embed the message in the cover image, sometimes by the help of secret key, so the cover image become stego image as shown in Figure 1. After that steganalysis process determines whether that image contains hidden message or not and then try to recover the message from it. In the cryptanalysis it is clear that the intercepted message is encrypted and it certainly contains the hidden message because the message is scrambled. But this may not be true in the case of steganalysis. The stego image may or may not be with hidden message. The steganalysis process starts with a set of unknown information streams. Then the set is reduced with the help of advanced statistical methods [5]. Siva Jana Kiraman et.al [6] proposed a gray block embedding method, in this method the LSB bits are modified based on the MSB bit plane. In the embedding process the gray image is divided into the 4*4 blocks further this is divided into 2*2 blocks. The embedding process is done in 2 phase outer embedding and the inner embedding. In the outer a reference point is found in each of the 2*2 blocks and base on the reference point value are bought back and based on the reference point value the actual value are extracted from the stego image. The proposed scheme increases the embedding capacity and security by the complexity. Prabakaran G et.al [7] aims to develop a Steganography scheme to secure the medical digital images. The proposed method is based on the integer wavelet transform and the Arnold transform. In the embedding process the container image is taken and the flip left is applied, a dummy container image is obtained. The patient’s medical image is taken and the Arnold transform is applied and scrambled secret image is obtained. This scrambled secret image was embedded into the dummy container image and the inverse IWT was taken to get dummy secret image. This dummy secret image is embedded into the container image and transferred to receiver. The reverse with sub band subtraction is applied to get the actual data in extraction phase. The algorithm increases the capacity and the quality. Vn Mai et.al [8] proposed a Steganography scheme to have control over the access of the data stored in the ECG (Electrocardiogram). The scheme requires that the patient’s data to be stored in a tree structure which consists of leaf node and branch and each node represents a kind of data. Each leaf node or a branch is protected from access by Steganographic keys. The normal Steganography algorithm is used to embed data into ECG. Once data is embedded the data is stored in the public cloud and the data owner can upload some access keys and the interested users can request for keys to cloud server and retrieve some information and if there are some restricted data then the key has to be obtained from owner itself. In the extraction process the user key is compared with the key file on the cloud and only if the key matches the access is allowed. Confidentiality of the patient’s information is maintained.

III. PROPOSED METHOD

A. Embedding Procedure:
- At first, a cover image C (JPEG) is partitioned into non overlapping blocks of 8X8 pixels.DCT is computed for each block into DCT coefficients.
- To find embedding region first Compute entropy (E) of all 8x8 DCT blocks. Entropy formula is \[ E = \sum_{i,j} \log_2 (E_{i,j}) \]
- 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, a block having entropy higher than the mean entropy value is selected and is named as valid block.
- Middle coefficients of K Matrix for each valid block 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 matrix say k. In k matrix there are 26 coefficients located in the middle part that are set to be one. Here K[a,b] is the value of the ath row and bth column element of K.
- 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 computed for 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).

B. Extraction Procedure:
- While extracting the secret data, the said 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.

IV. Result

Several experiments are performed to evaluate our proposed methods. Eleven grayscale images with size 512 x 512 are used in the experiments as cover images namely ‘Lena’, ‘Baboon’, ‘Peppers’, ‘F16’, ‘Boat’, ‘Man’, ‘Tiffany’, ‘Barbara’, ‘Elaine’, ‘Couple’, ‘Splash’, and are shown in Fig. 1. The proposed schemes have been implemented using the MATLAB 7.8.0.347 (R2009a) program on Windows XP platform.

![Eleven cover images are used for the proposed schemes](image)

V. Conclusion

The cover image is taken as a grayscale image of 256X256 pixels for experiment. The secret message is embedded in the middle frequency part of the DCT coefficients. The PSNR (decibel format) and MSE are used as measurement of the quality of image coding and compression. If PSNR is high then images are best quality. This method provides acceptable image quality and highly robust system.

References