Steganography using Absolute Moment Block Truncation Coding

Dr.S.Vimala[1], Ms.M.Rajakani[2], Ms.Uma Poomi[3]

[1]Associate Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India
[2,3]M.Phil and Ph.D Scholars, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India

Abstract*—Steganography is a technique of hiding information in an image. The overhead in terms of increased transmission time is reduced by compressing the image. Absolute Moment Block Truncation Coding (AMBTC) technique is one of the lossy image compression techniques. In this paper, AMBTC technique is used to hide the information as part of compressed image. The performance of the proposed approach is analyzed in terms of Compression Ratio, Elapsed Time and PSNR. When tested with different images, the proposed method outperforms the few existing methods.*

Keywords— Steganography, Image compression, AMBTC, Compression ratio.

I. INTRODUCTION

1.1. Steganography

Steganography is a branch of Information Hiding method to hide secret data in the media such as audio, video and images [1]. Steganography aims at security of information to be passed. The transmission media must be robust enough to carry the secret information. Components of Steganography include components such as Cover Image, Stego-Image, Message and Key. Steganography is of many types such as Text-based, Audio, Image and Video Steganography [2]. In the proposed method, image has been taken as transmission media for carrying the secret message. Steganography is applied in fields such as Copyright Protection, Feature Tagging, Secret Communication, Digital Watermark, and even used by terrorists to hide their secret [3].

1.2. Image Compression

Image compression is used to minimize the size data required to represent the image without affecting the quality of the image. Image compression technique is very important and used for many applications [4]. Compression techniques are used to reduce the cost associated with storage and transmission of images. Image compression is familiar to most users of computers in the form of image file extensions, such as the jpg file extension used in the JPEG image compression standard [5]. The compression techniques are classified into two types such as lossless and lossy compression. With lossless techniques, the reconstructed images are exact replica of the original images but with lossy techniques, the reconstructed images are approximation of the original image with little loss in data. Two fundamental features that lead to compression are redundancy reduction and irrelevancy reduction [6]. Redundancy reduction aims at removing duplication from the signal source (image/video). Irrelevancy reduction omits part of the signal that will not be noticed by the Human Visual system (HVS).

A common characteristic used in image compression aims at reducing the number of bits needed to represent an image by removing the spatial and spectral redundancies as much as possible. Absolute Moment Block truncation coding (AMBTC) is one of the lossy image compression techniques [7]. The computational complexity involved is less and quality of the reconstructed images is appreciable and improves the coding efficiency [8]. In AMBTC, for each input block, a ***BitPlane*** of size 16 bits and two quantizing values ***high mean*** and ***low mean are*** preserved while storing or transmitting the images [9]. The remaining paper is organized as follows: in section 2, the proposed method is explained. Results are discussed in Section 3 and Conclusion is given in Section 4.

II. PROPOSED METHOD

In the proposed method, the input image is split up into blocks of size 4 x 4 pixels. For each block, Bitplane is generated by computing the Mean of the block. With Mean, the two quantizers Q1 and Q2 are computed. The input message (secret text file) is converted into its equivalent ascii form. The ascii value is then converted into its equivalent binary form. The result is a sequence of bits (0/1). Depending on the size of the bit sequence, either adjacent bitplanes or bitplanes at random positions are taken

for manipulation. If the current bit from the bit sequence is 1, the respective Bitplane is negated or left the same. The input bitstream is embedded as part of the compressed image as {BitPlane, Q1, Q2, 0/1}. The proposed method is combination of an Image Compression technique and a Steganography method. Image compression technique leads to efficient transmission of image and the staganography method helps us hide the secret text in the image. It is a simple and efficient way of transmitting the hidden text in the form of image without affecting the quality of the compressed image. In the decoding stage, wherever the bit in the bitstream is 1, the bitplane is negated and then decoded with Q1 and Q2 for 1 and 0 respectively.

Encoding Algorithm

Step 1: Convert the input secret text file into its equivalent binary form.
Step 2: Split the input image into blocks of size 4x4 pixels.
Step 3: Generate BitPlane, Q1, and Q2.
Step 4: Negate the respective Bitplane if the current bit in the Bitstream is 1.
Step 5: Transmit/Store the compressed image in the form of a set S = {B, Q1, Q2, b}

Decoding Algorithm

Step 1: Get the set S for each block.
Step 2: If b is 1, negate the Bitplane B.
Step 3: Code each 1 in B as Q1 and 0 as Q2.

III. RESULT AND DISCUSSION

The results obtained with the proposed method are given in Table 1. In Table 1, the time taken for both encoding and decoding with respect to the existing [9] and proposed techniques are computed for different images is given. When compared to that of the existing method, the time taken by the proposed method is lesser and reduced by a significant value. On average, the existing method takes 1.42 seconds and the proposed method takes 0.18 seconds which is a significant improvement. The input images taken for the study are given in Figure 1. For all the images, irrespective of the gray level distribution, the proposed method gives better results in terms of encoding and decoding time.

Table. 1 – Comparison of Encoding and Decoding Time with respect to existing and proposed methods.

IMAGE	Elapsed Time in Seconds	
	Existing	Proposed
Cameraman	1.23	0.19
Lena	0.54	0.18
Baboon	1.82	0.19
Airplane	0.88	0.14
Boats	1.98	0.19
Bridge	2.10	0.18
Average	**1.43**	**0.18**

a) Cameraman

(b) Lena

(c) Baboon

(d) Airplane

(e) Boats

(f) Bridge

Fig.1: Input images taken for the study

IV. CONCLUSION

The proposed method is a combination of AMBC and Steganography. The text that is to be hidden may be very short. But when embedding in an image, it takes lot of transmission time. Hence a simple image compression technique called AMBTC is used to compress the image and then the compressed image is manipulated to embed the text before transmission. When compared to the existing technique, the proposed method performs better in terms of decoding and encoding time. The time is reduced by 1.25 which is a significant improvement. It is something difficult to decode the text from the image as a compression technique is adopted and embedding of data can be done in n number of ways in the image.

REFERENCES

[1] Fariba Ghorbany Beram, "Effective Parameters of Image Steganography Techniques",International Journal of Computer Applications Technology and Research, volume-3, Issue 6, 361-363,2014, ISSN:2319-8656.

[2] Rashisingh and Gaurav chawla, "A Review on Image steganography", International Journal of Advanced Research in Computer Science and software Engineering, volume 4, Issue 5, may 2014, ISSN:2277 128X.

[3] Mahmud Hasan 1, Kamruddin Md. Nur 2, Tanzeem Bin Noor3,"A Novel Compressed Domain Technique of Reversible Steganography" International Journal of Advanced Research inComputer Science and Software Engineering Volume 2, Issue 3, March 2012 ISSN: 2277 128X .

[4] Vipul Sharma and Sunny Kumar, "A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN: 2277 128X .

[5] Harsh Prayagi, Tushar Srivastava, Gyanendra Ojha,and Sunil Chaurasia, "Information Hiding in an Image File: Steganography", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4216-4217.

[6] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S.Sruti, and M.Gomathymeenakshi, "An Improved Steganographic Technique Using LSB Replacement on a Scanned Path Image", International Journal of Network Security, Vol.16, No.1, PP.14-18, Jan. 2014 .

[7] N.Santoshi, B.Lokeswara Rao, B.Lokeswara Rao," A Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast", International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518 IJSER © 2012 http://www.ijser.org .

[8] Kamred Udham Singh, "A Survey on Image Steganography Techniques", International Journal of Computer Applications (0975 – 8887) Volume 97– No.18, July 2014.

[9] Pooja Rani and Apoorva Arora, "Image Security System using Encryption and Steganography", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, No. 6, pp. 3860-3869, June, 2015.