IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 4, Ver. I (Jul - Aug. 2014), PP 60-65
www.iosrjournals.org

A Comparison of Lossless Steganography Using I-AMBTC Technique for Various Block Sizes

[1]Gudapati Sri Kali, [2]Hema Chowdary
[1]*Member IEEE, Assistant Professor, Department of ECE, Saveetha School of Engineering Chennai, India*
[2]*Department of ECE, Saveetha School of Engineering Chennai, India*

Abstract: *Steganography is the art of hiding a message in an image and also the fact that there is a message inside the image. Steganography is a type of information hiding technique which embeds a secret message in a image,vedio,audio etc called the cover file. The main purpose of steganography is to provide security to personal or public data. In this paper Interpolative Absolute Moment Block Truncation Coding(I-AMBTC) is used for compressing the cover image and to embed the secret data into the cover. I-AMBTC compression is more than the AMBTC technique as only half of the number of pixels in the binary converted image are transmitted. Here a comparison of the I-AMBTC technique is done for 2x2, 4x4, 8x8 block sizes. I-AMBTC is a lossless technique as the cover image and the secret image can be recovered completely.*

Index Terms**:** *I-AMBTC, AMBTC, Information hiding , Steganography, Cryptography*

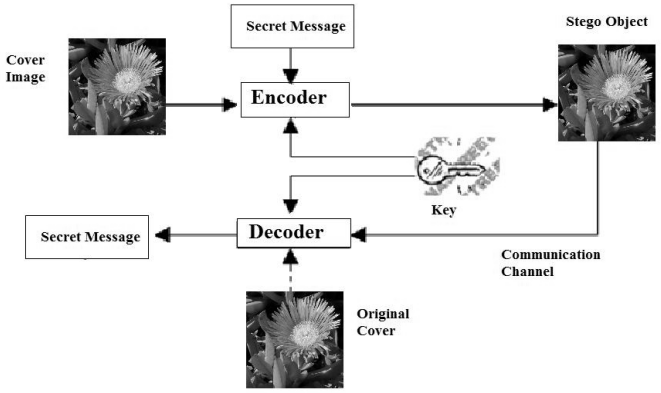
I. Introduction

In recent years, communication with images has become popular. The security of these images being transmitted is of great importance. One of the methods used for providing security is information hiding. Information hiding deals with hiding information in an image, audio file or in a video file. The concept of information hiding deals with steganography and cryptography.

Secured data transmission has started with cryptography. Cryptography is a form of secured data transmission where the contents of a message are kept secret(fig i) .Cryptography provides authentication and integrity.

Steganography is a popular technique in information hiding. Steganography embeds secret messages into digital content so that the secret messages are not detectable [1]. All digital media, such as digital images, videos and audio files, can be used to hide secret messages. However, digital images are often used for steganography. This is because nature images usually have higher degree of redundancy, which are suitable to embed information without degrading the visual quality of the images. Moreover, images are widely used throughout the internet, which usually arouse little suspicion than other digital media [2]

Images used for carrying data are called as cover images and images that embed data into them are termed as stego images fig(i). After embedding, pixels of cover images will be modified and distortion occurs. The distortion caused by data embedding is called the embedding distortion [3]. A good data- hiding method should be capable of evading visual and statistical detection [4] while providing an adjustable payload [5].



Fig(i): Block diagram of steganography

However, steganography, referred to as a process to hiding secret data of various types (message, image, information, etc.), called the cover , into another digital media (text, image, audio or video streams) can solve the problem of perception of the secret message. . The media that conceals the data is called “cover” or “host” media.

If this cover media is a digital image, it is called a cover image, and the altered cover image containing the secret information is called a stego-image (or stego-media)[6]

The major challenges of steganography are: embedding capacity, robustness and invisibility. The embedding capacity of steganographic scheme refers to the amount of the secret data that can be embedded into the cover image, and the term invisibility indicates how imperceptible is the cover image after it has been manipulated and turned to be a stego-image, to the eavesdroppers. Robustness is concerned with how well the technique withstands to the manipulations done by the intruders.

In 2008, Wien Hong and Tung-Shou Chen proposed Absolute Moment Block Truncation Coding (AMBTC) which compresses the image and performs the steganographic scheme. Moreover the stego-image preserves the same image quality as the original compressed images[7].

In this paper method called interpolative Absolute Moment Block Truncation Coding is proposed ,where the cover image is further compressed and the secret data is embedded using AMBTC. This paper gives the comparison of the I-AMBTC technique applied to block sizes of 2x2,4x4 and 8x8 and for different images. The Peak Signal to Noise Ratio for the images with different block sizes are compared.

The second section describes the Block Truncation Coding, III section describes the AMBTC technique and Section IV describes the I-AMBTC technique.

II. Block Truncation Coding

Block truncation coding (BTC) is fast and lossy compression technique with less complexity for digitized gray scale images. The BTC was introduced by Delp and Mitchell. The key idea of BTC is to preserve the quantization levels for blocks of pixels. By this the image quality remains satisfactory and the storage space also decreases. The next advanced technique of BTC is AMBTC that is proposed in the next section.

III. Ambtc

The concept of absolute moment block truncation coding (AMBTC) was introduced by Lema and Mitchell in 1984. The consideration of AMBTC is to maintain the mean and the first absolute moment of image blocks.

Algorithm

AMBTC Encoding

(i) Divide the image into blocks

(ii) Calculate the mean, lower and upper mean.

(iii) If the pixel value is less than mean value, it is replaced by zero otherwise it is replaced by one.

(iv) Embedding bit is obtained by XORing secret message and key

(v) If the embedding bit is zero, the trio generated consists of lower mean, upper mean and the sequence of bits of the image block

(vi) If the embedding bit is one, the trio generated consists of upper mean, lower mean and the not operation of the sequence of bits of the image block

AMBTC Decoding

(i). In the trio obtained if the first element of the trio is lesser than the second element, then the embedded bit is zero. Else the embedded bit is one.

(ii). If the embedded bit is zero, the sequence of bits of the image block remains same.

(iii). If the embedded bit is one, NOT operation is performed on the sequence of bits of the image block.

(iv). If the binary image consists of one, it is replaced by upper mean else it is replaced by lower mean obtained from the trio.

IV. I-AMBTC

In this section, a lossless steganography for I-AMBTC-compressed images is introduced and the performance of various block sizes is compared. For ,convenience, we define the notations used in this paper first. The original cover image is denoted as H and is a grayscale image. The I-AMBTC compressed code for H is represented by E, and the reconstructed AMBTC compressed image is denoted by R. Embedding is done by modifying E, and the result is an I-AMBTC compressed host-code E'. The receiver then uses the reconstruction procedure to obtain the IAMBTC-compressed stego-image R'.

The I-AMBTC compressed code E consists of a sequence of trios (two quantization level m_u and m_l, and a bit plane G). The bitplane G of the proposed method consists of the alternative values of the normal bitplane in AMBTC. Each trio (m_u, m_l, G) represents the compressed code for an image block. It is observed that if we interchange two quantization levels m_u and m_l, and perform Logical NOT operation on the bit plane G, the reconstructed I-AMBTC image blocks will remain the same.

Let F() denotes the reconstruction function for I-AMBTC compressed image blocks with 3 parameters m_u, m_l and G, then the equation given below always holds true for every trio (m_u, m_l, G) :
$F(m_u, m_l, G) \equiv F(m_u, m_l, G1)$-----(1)
where G1 is the resultant of the Logical NOT operation on the bit plane G. Equation 1 implies that the reconstructed image R and the recovered stego-image R' are exactly the same, i.e. $R \equiv R'$.

Since the interchange of the quantization levels along with logical NOT operation on bit the plane G does not change the value of decoded image blocks, we may use this property to embedded one bit into each trio without losing the quality of the image. The embedding procedures are described in the following section.

(i) The data embedding procedure

The process of generating a stego-image is described below. Suppose an I-AMBTC compressed code E, to be embedded, is composed of (NxN) trios. The embedding algorithm of the proposed method follows the steps given below:

Step 1. The secret data S (m bits where m = NxN) which has m-bits is first appended by 0's of size NxN-m , and is then XORed with a random binary sequence produced by a secret key k . The encrypted bit stream is denoted by

$$E_{bs} = \{e_1, e_2, \cdots, e_{N\times N} \mid e_i \in \{0,1\}, i = 1, 2, \cdots, N\times N\}$$.

Step 2. Sequentially embed secret data into I-AMBTC encoded blocks. For each I-AMBTC encoded block i with trio (m_{ui}, m_{li}, G_i), if the corresponding embedded bit e_i is 1, then thetrio (m_{ui}, m_{li}, G_i) is changed to(m_{ui}, m_{li}, G_i^1) . Otherwise, the trio (m_{ui}, m_{li}, G_i) remains unchanged.

Step 3. Repeat step 1 and step 2 until the entire encrypted bit stream E_{bs} is embedded.

(ii) The data extraction procedures

The data extraction procedure is similar to that of the embedding procedure. For each AMBTC compressed block i, if $m_{ui} < m_{li}$, then the embedded secret bit e_i is extracted. Otherwise, e_i is extracted. If e_i is 1 the trio consists of (m_{ui}, m_{li}, G_i) else it consists of (m_{ui}, m_{li}, G_i^1). If the binary image extracted contains one,it is replaced by the upper mean value else it is replaced by lower mean value. The excluded pixel values in the I-AMBTC compressed image are obtained by averaging the neighborhood pixels. This procedure is repeated until all the encrypted secret data E_{bs} have been extracted, and then decrypted using the secret key k to obtain the original secret data S.

V. Results

The PSNR values of the cover image and the reconstructed image is calculated and tabulated for different block sizes.

image	2x2	4x4	8x8
cat	32.0407	31.0162	24.3087
bird	33.8655	32.975	25.1356

The output images of cat and bird are shown in figures below

Figure (a): input Bird image

Figure(b): Reconstructed image for 2 X 2

Figure(c): Reconstructed image for 4X4

Figure(d): Reconstructed image for 8X8

Figure (e): Input Cat image

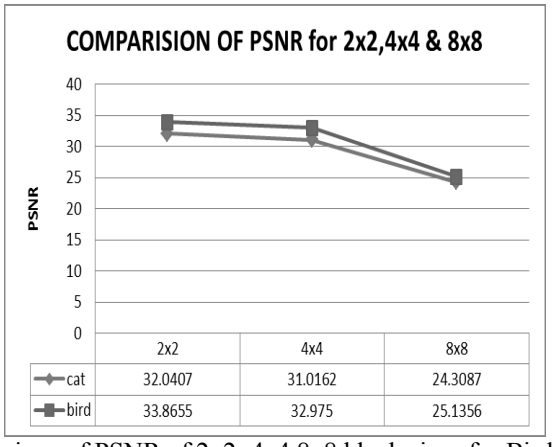
Figure(f): Reconstructed image for 2 X 2

Figure (g): Reconstructed image for 4X4

Figure(h): Reconstructed image for 8X8

The result in the tabular column shows that the PSNR is high and the cover image can be reconstructed efficiently using I-AMBTC. The comparision chart of the PSNR values for different PSNR values for cat and bird images is shown in chart1. Figures (a) and (e) are the two input images. Figures (b) and (f) are the output images after the retrieval of the secret data for 2x2 block size. Figures (c) and (g) are the output images after the retrieval of the secret data for 4x4 block size.

Figures (d) and (h) are the output images after the retrieval of the secret data for 8x8 block size. From the figures it is noted that the quality of the 2x2 block size output images has more quality than the 4x4 and 8x8 block sizes.



Fig(ii) : Comparison of PSNR of 2x2 ,4x4,8x8 block sizes for Bird and Cat image

VI. Conclusion

In this paper, we present a lossless data hiding technique that hides the secret data in an interpolative-AMBTC technique. Even though the AMBTC technique uses compression technique, the compression ratio is further increased using the I-AMBTC technique. This technique is lossless as the secret data can be completely recovered without any loss. The data extraction procedure is simple and the computational cost is less for the proposed method. Future works may include trying to increasing the payload and the level of security.

References

[1]. Wien Hong. Tung-Shou Chen. Chih-Wei Shiu," Lossless Steganography for AMBTC-Compressed Images" Image and Signal Processing, 2008. CISP '08. Congress on(Volume:2)

[2]. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding—A Survey," Proceedings of the IEEE, special issue on protection of multimedia content, 7(7), 1999, pp. 1062–1078

[3]. A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital imag steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752, 2010.

[4]. T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact insteganography using trellis-coded quantization," in Proc. SPIE, MediaForensics and Security, 2010, vol. 7541, DOI: 10.1117/12.838002.

[5]. S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vo1, no. 1, pp. 111–119, Mar. 2006.

[6]. R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[7]. Wien Hong and Tung-Shou Chen and Chih-Wei Shiu, "Lossless Steganography for AMBTC-Compressed Images, " 2008 Congress on Image and Signal Processing.