IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IX (Sep-Oct. 2014), PP 49-54
www.iosrjournals.org

A Secure Data Hiding Scheme In Images Using Random Generated Key

Sobimol Mathew
(Dept. of Computer Science and Engineering Caarmel Engineering College,
, Mahatma Gandhi University, Kerala, India)

Abstract: *Data hiding is the process of transmitting images in a hidden manner, where as the message should be invisible to the unauthorized users. This technique is a good way to achieve the secret delivery of data, where the colour image acts as a popular cover media to send the secret. The commonly used data hiding technique are based on block truncation coding and complementary Error Diffused Block Truncation Coding. Block Truncation Coding is a type lossy image compression technique for grey scale images. It divide the original image into blocks and then use a quantizer to reduce the number of grey levels. The major issues associated with BTC are unnecessary blocking and false contouring effects. To overcome these issues a complementary Hiding Error Diffused Block Truncation Coding was developed by Jing-Min-Guo and Yun-Fu-Lin. This method overcomes the limitations of traditional BTC, ensure the image quality and highest processing efficiency. The existing system consists of an encoder and decoder and the encoder spreads the watermark into two marked images and the corresponding data security is also improved with the security sharing concepts. However the existing system uses a pseudo random key, which is not synchronized in between the encoder and decoder may leads to wrong extraction. Another problem associated with the existing system is Block size. Various block size can lead different bitmap through existing decoder and the system does not consider the bias limitation, number of water mark as keys and cannot protect the embedded data. The proposed system overcomes the limitations of existing CHEDBTC system without altering its advantages. Our system can yield high image quality and can with stand against various types of security attacks.*

Index Terms: *Block Truncation Coding (BTC),data hiding,CHEDBTC*

I. Introduction

Block Truncation Coding (BTC)[1], is a type of lossy image compression technique for grey scale images. It divides the original images into blocks and then uses a quantizer to reduce the number of grey levels. In BTC a 256X256 pixel image is divided into blocks of typically 4X4 pixels and mean and standard deviation are calculated for each block. These two values define what values are reconstructed or new blocks will have.BTC is efficient compression technique for images and the main advantage is its low computational complexity compared to the other compression mechanisms such as JPEG and MPEG.HoweverBTC[3] suffer from the disadvantages such as blocking and false contour effects. False contour effect occurs when color shows as distinct contour or edges where there should not be any.Due to these unnecessary factors BTC becomes less efficient and produce low quality images. Therefore to reduce the issues associated with BTC,several methods have been proposed by using the advantages of Halftoning.

Halftoning [3],is a process that simulates shades of grey by varying the size of tiny black dots arranged in regular pattern. When viewed from a distance by the low pass nature of Human Visual System,these halftone images can reassemble the original grey scale images. The various halftoning methods such as Error Diffused Block truncation Coding and Complementary Hiding Error Diffused BTC are developed to reduce the blocking and false contouring effect and thus provide high image quality, while the data can be hide in safe andData hiding technique is a good way to achieve secret delivery of data, thus the color image is a popular cover media used to send the secret.BTC is a lossy image compression technique, which can significantly reduce the size of the image and these compressed image can be sent to receiver and the receiver can decrypt and thus gets the information. However as we discussed earlier, BTC reduce the quality of the image.

Several methods have been proposed to improve the limitations of BTC, and one of the important method is Complementary Hiding Error Diffused Block Truncation Coding. However this method acquire more image quality and more data can be embedded along with this image ,also has the disadvantages such as the key is not synchronized in between the encoder and decoder and the transmitter and the receiver have to share the same pool for their communication, and here the block size used in this system is not identical to the encoder and thus various block size can lead different bitmap through the existing decoder.

In order to overcome the limitations of the existing CHEDBTC system, we propose a 'Secure Data Hiding Scheme in Images Based on Improved BTC'.The proposed system also maintain the advantages of the existing system.Our system ensure a good balance between image quality and embedded capacity.The rest of

this paper is organized as follows. Section II introduces the existing CHEDBTC. Section III describes the proposed data hiding Scheme and finally Conclusions are drawn in section IV

II. Complementry Hiding Error Diffused Block Truncation Coding

Complementary Hiding Error Diffused Block Truncation Coding was proposed in order to overcome the blocking and false contouring effects of BTC. In this system, the concepts of secret sharing are employed and thus ensure the security of embedded data. The system mainly consists of an encoder and decoder and the working of the system can be explained as follows. One watermark w is embedded into two host images by the secret sharing scheme and for decoding the corresponding watermark,the receiver side require the two marked images. But this does not ensure the hundred percentage security of the watermark, while our proposed system employs an additional secret key to further improve the security of the watermark. Thus the watermark can be encrypted safely. The existing CHEDBTC can embed multiple watermark in order to increase the capacity of the transmitted information. The figure 1 shows the conceptual diagram for the existing data hiding.

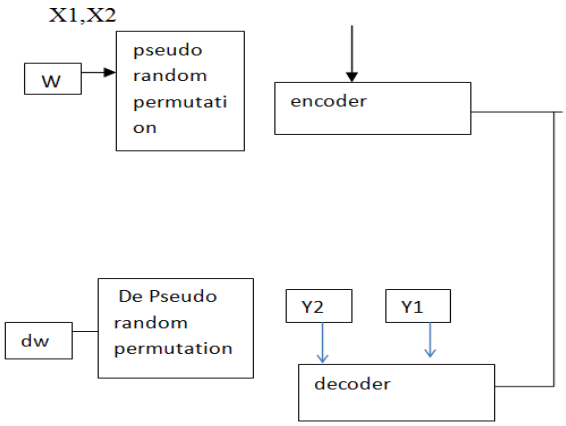

Fig 2.1conceptual diagram for the existing data hiding.

As we discussed earlier, the existing system consists of two main elements such as encoder and decoder.The encoder side manages the division of the images into a number of blocks, and embedding the message into the images and generating keys. The decoding side manages the retrieval of the embedded message from the respective image. The message can be retrieved from images by decrypting those using keys.The function of Encoder and Decoder are described in the following sections.

A. Encoder

As shown in figure 2, one water mark is embedded into two binary images and two corresponding marked images are generated .Each marked block involves two quantization levels and one bit map. To maintain a high quality images similar to the original image, the following processes are performed. The values in the bitmaps 0 and 1 are considered as black and white tones respectively and when the two bitmap from the compressed images are passed through an an exclusive NOR yield additional output and which can be considered as a watermark.

B. Decoder

In the decoder side, when two marked images Y1 and Y2 are received, each divided blocks are decrypted separately. Firstly the mean of a received block is calculated and it is denoted by y^-t and then the bitmap bi used to embedded the water mark is obtained. The hidden information can be obtained by applying the XNOR operations on the bitmap.

The existing system can embed multiple watermarking which cannot possible by the traditional BTC. Digital Watermarking is defined as invisible or in audible data permanently embedded in a graphic, video or audio for protecting authenticated data. Multiple watermarking is the process that embed more than one water mark in the cover image and this system allows embedding different marks at different stages into the host media. In order to solve the limitations of existing CHDBTC system 'A secure Data Hiding in Images using Random Generated Keys' is proposed. Instead of using symmetric keys as in the existing CHDBTC system, the proposed system uses random generated keys using one time padding key generator, thatis different key are used for different images.

III. A Secure Data Hiding In Images Usingrandom Generated Keys

The existing system offers high image quality without obviously damaging the image quality. However the system suffers from various problems as listed below. A pseudo random key is used in the existing system and which is not synchronized in between the encoder and decoder this may lead to wrong extraction. To address this problem we use an identical key instead of pseudo random key. Here the extraction will be in a good manner and security is also ensured. Another problem is regarding the size of the block. Various block size can yield different bitmaps through the existing system and this may leads to some encoding problem and our proposed system solve this issues by using an identical block size which is same as that of encoder. The threshold is affected by two parameters such as bias limitation and the number of embedded watermark. These two parameters can yield different correlation and can be considered as a key to protect the embedded data.

Similar to the EDBTC,our proposed system also consists of both encoder and decoder. Here the original image is divided into two or more blocks of identical size and one watermark is embedded into original image. The resulting image consists of different marked image same as that of the block size. The figure3.2 illustrates the conceptual diagram. Here we use an identical secret key to encrypt each watermark in order to ensure the security of the transmitted data.An image consists of so many pixels and here we use an embedding scheme in which our secret image is embedded into one particular pixel of the image. The multiple water marking can be achieved by embedding the secret information into more than one pixel of the image.

In addition to the encoder and decoder, the proposed system consists of a secret key which is used for the encryption of the water mark. The secret key is used in some of the existing system has the disadvantage that once the key is hacked by an unauthorized user, the data or message can be encrypted by the third party, and which again loss the security of the embedded data .In order to prevent these type of attack, the proposed system uses a random generated key using a one-time padding key generator. In which different keys are generated for different messages and ensure the security of the embedded data while sending the message. Thus multiple message can be embedded in an image in a secure manner without losing the quality of the image.

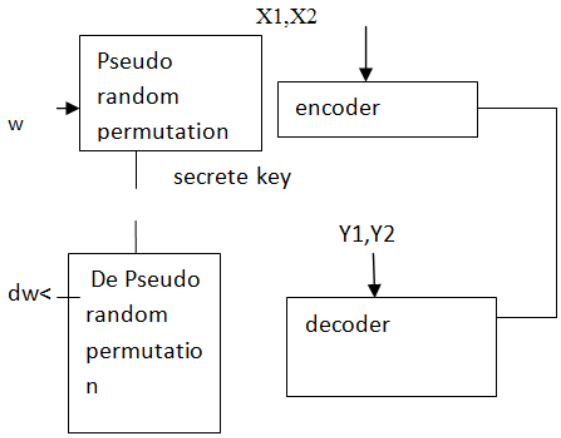

Fig 3.1conceptual diagram- proposed data hiding.

In our system we also use a pixel mapping method ,in addition to the traditional encoding and decoding method. This can be done by selecting a set of pixels and put the secret message into these selected pixels and put the secret message into these selected pixels according to some mapping rules. One of the main advantage is that ,it is difficult to find out the mapping rules and pixel to which the message is embedded, sincean image consists of so many pixels. This provide larger embedding capacity and also maintain high image quality.

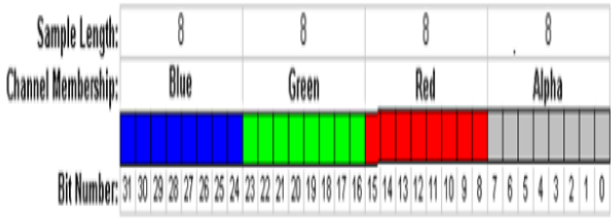

Fig 3.2Organization of pixel under ARGB system.

In our proposed method we determines the bit location of the RGBA pixel value you will embed your bit. Then find the total length of the image which is attached along with the image and send to the receiver and

then embed the message one by one into each bit of the pixel.A third party cannot find in which bit the data is embedded.

As shown in figure 3. 3,our while hiding data into the image, our proposed system can provide a better image quality as compared to the existing system such as Block Truncation Coding and CHDBTC methods. The figure 3.3 shows the original image into which the message should be embedded. Then the figure 3.3(b) shows an image in which data or message is embedded using the CHDBTC methodand it is clear from the figure that figure is blurred and a third party can easily understood that there is some message is attached inside the image. The third figure shows the data hiding scheme using the proposed method and it is clear from the figure that the proposed system maintains better image quality as compared to the existing data hiding method.

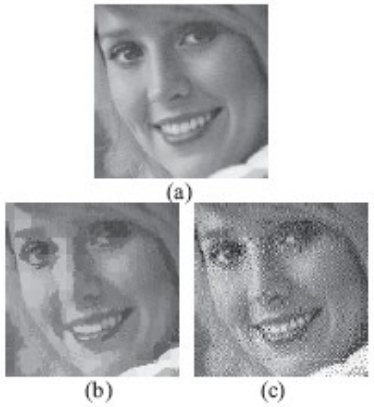

Fig3.3 (a) original images,3. 3 (b) data hiding using CHDBTC ,3. 3 (c) proposed method

In our system we use identical block size inorder to avoid the production of different bitmaps through the decoder.

A.DECODER

At the decoder or the receiver side the following operations are performed. Receiver side consists of two marked images Y1, Y2 and the corresponding blocks are decrypted independely using the keys. For that the receiver has to find out the bit in which the message is embedded. The bitmap can be obtained as follows

Bit map bij={1,if yij>yt

{0, if ytj,<yt

Where yt is the mean of each block.

The hidden information can be obtained by decrypting using the key.

Even though, the message is send in a secure way, there is some chance of losing the data, and the problem is that the receiver is eagerly waiting for a particular message without knowing the loss of data and the sender or the encoder side continues its work without knowing that the data is not reached at the receiver safely.The existing system does not offer any method to solve these types of issues, and the proposed data hiding scheme offer a timer to solve these issues. That is, if the message is not received within a particular time period, the decoder side generate 'message not received' message and it is send to the sender, on getting this message from the receiver,the sender again send the message. Thus the proposed system offer high image quality , high data security and with stand against various types of security attacks.

IV. Experimental Results

The main security attacks which affect images are cropping and salt and pepper attacks.Cropping refers to cutting a portion of the image and salt and pepper attack is blurring the image.The following experiment shows that our proposed system can withstand against various attacks such as cropping, salt and pepperattacks. Croppingfifty percentage ofthe image may cause loss of data, since the major portion of the image is lost. The analysis shows that our system can with stand against these types of attacks and provide higher security. Similarly salt and pepper attack effectsto the losing the clarity of the imageby adding unnecessary signals or noise.Our system can also withstand against these type of security attacks.

Fig 4.1(a) Cropping 50%.

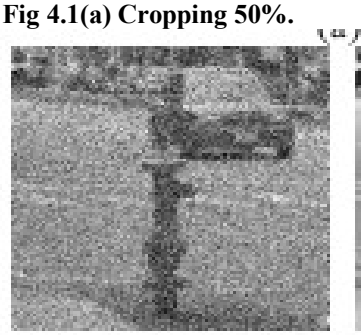

Fig4.1(b) salt and pepper attacks

V. Conclusion

The existing system offers high image quality without obviously damaging the image quality. However the system suffers from various problems as listed below. A pseudo random key is used in the existing system and which is not synchronized in between the encoder and decoder this may lead to wrong extraction.

To address this problem we use anrandom generated keys instead of pseudo random key. That is different keys are used for different images and the encryption will be done in a secure way.Here the extraction will be in a good manner and security is also ensured. Another problem is regarding the size of the block. Various block size can yield different bitmaps through the existing system and this may leads to some encoding problem and our proposed system solve this issues by using an identical block size which is same as that of encoder. The threshold is affected by two parameters such as bias limitation and the number of embeddedwatermark. These two parameters can yield different correlation and can be considered as a key to protect the embedded data. This system also maintain a message resending mechanism ,even if the message is lost while sending.

The experimental results show that our system has a very good embedding capacity. That is more than one watermark can be embedded without losing the quality of the image. Even though forty percentageof the original image contents are changed, correct extract ratio is still higher than ninety percentage .This shows that our system can withstand against various types of security attacks.

References

[1] E. J. Delp and O. R. Mitchell, "Image compression [using [block truncationcoding,"
[2] "BTC image coding using vector quantization,"
[3] "Digital halftones by dot diffusion,"
[4] "Multiple images embedding scheme based on moment preserving block truncation coding, "FundamentalInform.,

Author
Sobimol Mathew
Dept.Of Computer Science and Engineering
Caarmel Engineering College,Perunnad Ranni,
Mahathma Gandhi University,Kerala
Guided By,
Josy Elsa Varghese
Asst.Prof. Dept.Of Computer Science and Engineering
Caarmel Engineering College,Perunnad Ranni,
Mahathma Gandhi University,Kerala