Research Inventy: International Journal Of Engineering And Science
Vol.3, Issue 3(June 2013), Pp 45-49
Issn(E): 2278-4721, Issn(P):2319-6483, Www.Researchinventy.Com

Reversible Data Hiding In Encrypted Images Using Dct

[1]Vimal, [2]Mahendra Kumar Patil
[1]*(ECE Department, M. M. Engineering College, MMU, Mullana)*
[2]*(ECE Department, M. M. Engineering College, MMU, Mullana)*

ABSTRACT :*This letter proposes a method of reversible data hiding method in encrypted images using DCT.Reversible data hiding is a technique to embed additional message into some cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. The data extraction can be achieved by examining the block smoothness. This letter adopts a scheme for measuring the smoothness of blocks, and uses the closest match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over side match method. For example, when the block size is set to 8×8, the error rate of the Lena image of the proposed method is 0%, which is significantly lower than 0.34% of side match method.*

KEYWORDS : *DCT, closest match, image encryption, reversible data hiding, smoothness of blocks.*

I. INTRODUCTION

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. Many reversible data hiding methods have been proposed recently [1]–[5]. [1] Embeds data bits by expanding the difference of two consecutive pixels. [2] Uses a lossless compression technique to create extra spaces for carry data bits. [3] Shifts the bins of image histograms to leave an empty bin for data embedment. [4] Adopts the difference expansion and histogram shifting for data embedment. [5] Embeds data by shifting the histogram of prediction errors while considering the local activity of pixels to further enhance the quality of stego image.

As is well known, encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images. It may be also hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment [6]–[8]. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. A major recent trend is to minimize the computational requirements for secure multimedia distribution by "*selective encryption*" where only parts of the data are encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption.

II. PROPOSED METHOD

To enhance the quality of image after hiding some amount of data in it, here is to hide data in images using reversible data hiding algorithm with the use of DCT. A sketch of the proposed scheme is given in Fig. 1.

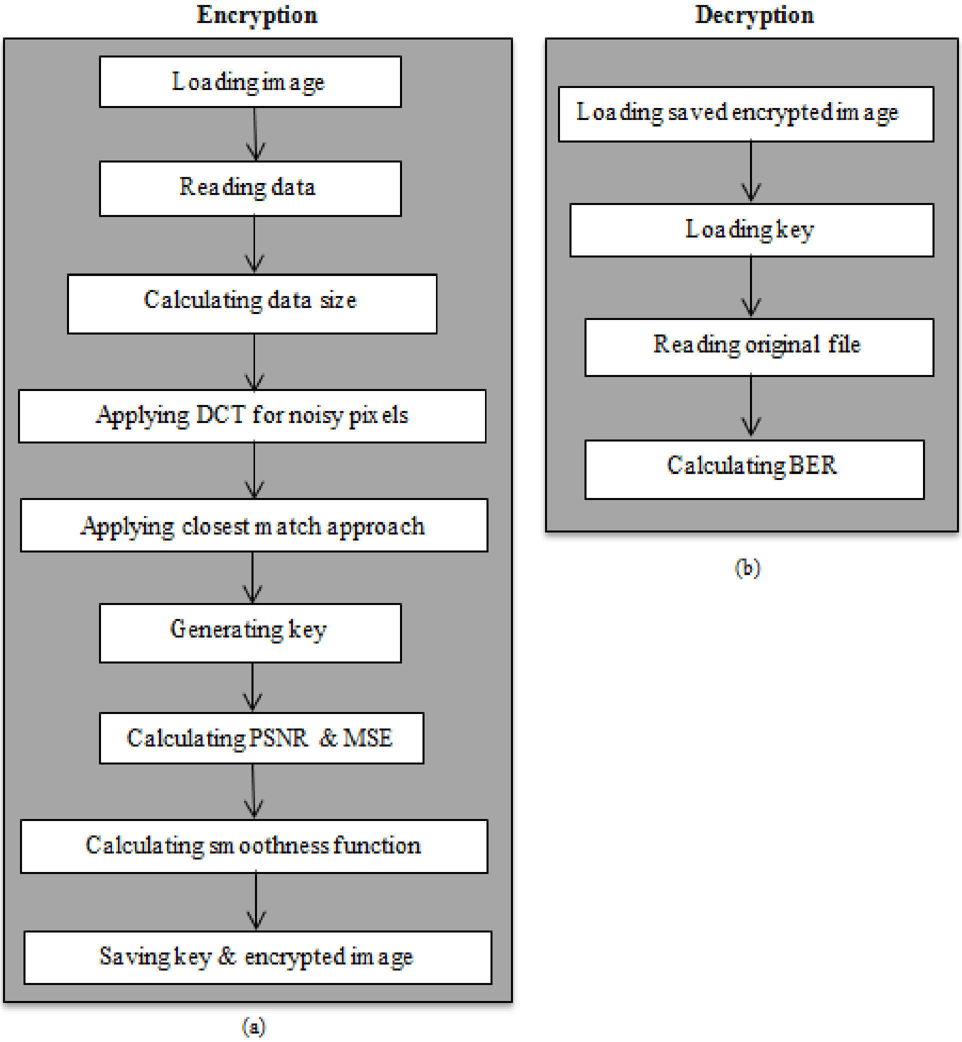

Fig.1. Sketch of proposed scheme (a) Encryption. (b) Decryption.

This technique is based on encryption as well as decryption.Encryption is the process of encoding messages (or information) shown in fig. 1(a) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm shown in fig. 1(b), which usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys. In this technique, here is to hide data in images using reversible data hiding algorithm with the use of DCT to match the closest data hiding pixel for every symbol to be hide. Basically the purpose of this method is to find out the noisy pixels and then hiding the data in it. This can be done in encryption process and then generating the key for decryption. PSNR and MSE are then calculated to check the changes in quality of image. Then by saving the key and the encrypted image, the decryption process is done. Then calculation of bit error rate is done to check the changes in extracted data.

2.1 Calculation of PSNR and MSE

PSNR is most easily defined via the mean squared error (*MSE*). Given a noise-free $m \times n$ monochrome image*I* and its noisy approximation *K*, *MSE* is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (1)$$

PSNR is defined as:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20.\log_{10}\left(\frac{MAX_I}{MSE}\right)$$

$$= 20.\log_{10}(MAX_I) - 10.\log_{10}(MSE) \qquad (2)$$

2.2Calculation of block smoothness

The smoothness of an image block can be evaluated by calculating the absolute difference of neighboring pixels. The larger the summation of absolute differences, the more complex the image blocks is. Therefore, the block smoothness calculated by taking the summation of the vertical absolute differences and horizontal absolute differences of pixels in image blocks using the following equation:

$$f = \sum_{u=1}^{s_2}\sum_{v=1}^{s_1-1}|p_{u,v} - p_{u,v+1}| + \sum_{u=1}^{s_2-1}\sum_{v=1}^{s_1}|p_{u,v} - p_{u+1,v}| \qquad (3)$$

Were $p_{u,v}$ represents the pixel values located at position (u,v) of a given image block of size $s_1 \times s_2$. This equation fully exploits the absolute difference between two consecutive pixels in both vertical and horizontal directions and thus, the smoothness of blocks can be better estimated.

2.3Bit Error Rate

The number of bit errors is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors. Bit error rate can be calculated by taking the difference between the decrypted data and original data.

III. EXPERIMENTAL RESULTS

We used two images and then convert these images into gray level images of size 512×512, including Baboon, and Splash as the test images, as shown in fig.1.

(a) (b) (c) (d)

Fig.2. Four test images (a) Lena (b) Baboon (c) Sailboat (d) Splash

To demonstrate the performance of the proposed method, we take Lena image as an example. The test image Lena sized 512×512 shown in Fig. 2(a) was used as the original cover in the experiment. After image encryption, the 8 encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig. 3(a). Then, we embedded 256 bits into the encrypted image by using the side length of each block shown in fig. 3(b). The decrypted image is given as Fig. 3(c). At last, the embedded data were successfully extracted and the original image was perfectly recovered from the decrypted image. In the proposed scheme, the smaller the block size, larger will be the PSNR, and BER comes to be less.

(a) (b) (c)

Fig. 3 (a) Original Lena (b) its encrypted version and (c) a decrypted version containing data.

Fig.4 reveals that the proposed method of all given images, offers lower error rates than that of [10]. For example, for the Lena image at block size 8×8, the error rate of the proposed method is 0% whereas the error rate of [10] is 0.34 %, which is less than that of [10] and at block size 14×14 the error rate is 0% and peak signal noise ratio(psnr) is 93.8652 dB. For Lena image at block size 64×64 the error rate changes from 0 to 7.3750% as shown in fig. 5(a) and psnr is 48.0655 dB which shows that as the block size increases, error rate also increases, and psnr decreases as shown in fig. 5 (b).

For the complex image, such as Baboon, the error rate of proposed method at block size 8×8 is 0, however,[10] has not found this result at block size 8×8. Fig. 4 shows the extracted-bit error rate with respect to block sizes when four test images Lena, Baboon, Sailboat and Splash sized 512×512 were used as the original covers. Note that this method is also useful for large data size.

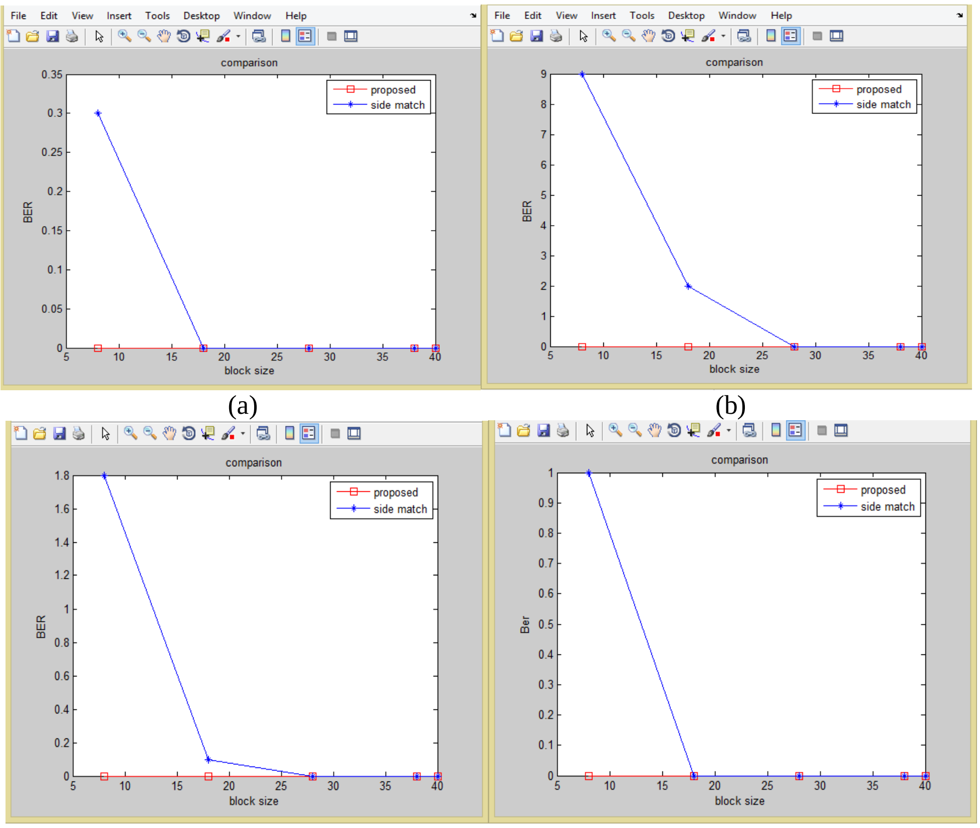

Fig. 4 Error rate comparison. (a) Lena (b) Baboon (c) Sailboat (d) Splash

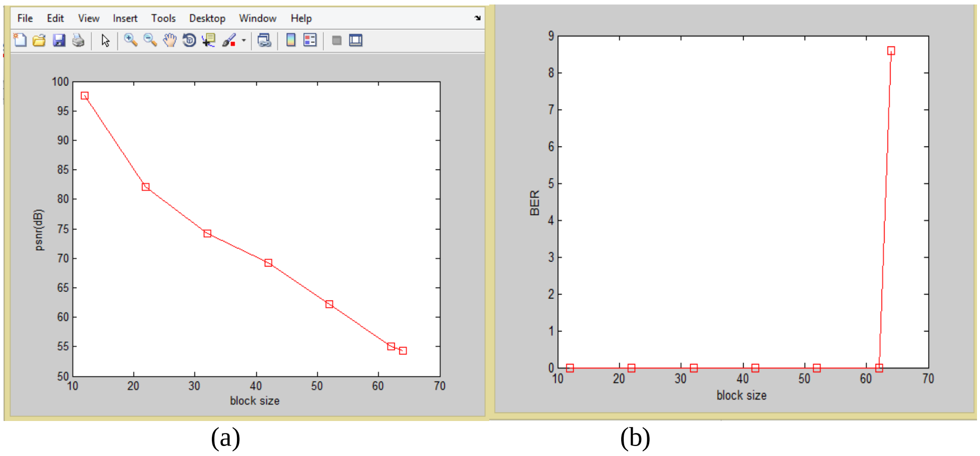

Fig. 5(a) Block size v/s PSNR (b) Block size v/s Ber of Lena image for different blocks

IV. CONCLUSION

This letter proposes improved data extraction with less BER, based on DCT method. We used a new algorithm better estimate the smoothness of image blocks. The extraction of data is performed according to the descending order of the absolute smoothness difference between two candidate blocks. The closest match technique is employed to further reduce the error rate. The experimental result shows that the proposed method effectively improves Side Match method. This method is also applicable for large data size.

REFERENCES

[1] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, 2003.
[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized- LSB data embedding,” *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, 2005.
[3] Z. Ni, Y. Q. Shi, N. Ansari, andW. Su, “Reversible data hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 8, pp. 354–362, 2006.
[4] D.M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, 2007.
[5] W. Hong and T. S. Chen, “Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism,” *J. Vis. Commun. Image Represent*,vol. 22, no. 2, pp. 131–140, 2011.
[6] D.Kundur andK.Karthik, “Video fingerprinting and encryption principles for digital rights management,” *Proc. IEEE*, vol. 92, pp. 918–932, 2004.
[7] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,” *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, 2007.
[8] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, “A commutative digital image watermarking and encryption method in the tree structured haar transform domain,” *Signal Process.:Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.
[9] X. Zhang, “Reversible data hiding in encrypted images,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, 2011.
[10] Wien Hong; Tung-Shou Chen; Han-Yan Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," *Signal Processing Letters, IEEE* , vol.19, no.4, pp.199,202, April 2012
[11] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Trans. Inf. Forensics Security*, 10.1109/TIFS.2011.2176120.