Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.153 – 157

SURVEY ARTICLE

Lossy Compression and Reconstruction for Encrypted Image

Prasanth P. S[1], Anusree L.[2]

Department of Electronics and communication Engg, Sree ChitraThirunal College of Engineering, Thiruvanthapuram, India

[1] prasanthsanthan25@gmail.com; [2] anusree_l@yahoo.co.in

Abstract— *This* ***paper introduces a novel scheme for Lossy compression of an encrypted image with flexible compression ratio. Usually we first compress an image, and then encrypt it. Here first encrypt the image, and then compress it. At the transmitter side compression of the original image is made by Discrete Cosine Transform (DCT).At the receiver side image reconstructed by Inverse Discrete Cosine Transform (IDCT). The novelty of this paper is reversing the order of steps usually preferred, that is first encrypting and then compressing.***

Keywords— Lossy compression; encryption; Discrete Cosine Transform; Inverse Discrete Cosine Transform; Compression

1. INTRODUCTION

Usually when we transmit redundant data, first we compress the data to reduce the redundancy and then to encrypt the compressed data to mask its meaning. At the receiver side the decryption and decompression operations are orderly performed to recover the original data and in this case it is insecure and bandwidth constrained channel. But in this paper we investigate the novelty of reversing the order of these steps that is first encrypting and then compressing [9]. As a result information remains confidential to network operator who provides channel resource for the transmission of the data. That means sender should encrypt the original data and the network

provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At the receiver side decoder integrating decompression and decryption function will be used to reconstruct the original data. Compared with previous lossless encrypted image compression approaches [1-8] proposed scheme have a slight degradation of encryption security and reconstruction quality with improvement on compression efficiency. The receiver can reconstruct the principal content of the original image by iteratively updating the values of the coefficients. The paper introduce novelty of reversing the order of steps usually preferred, i.e. first encrypting and then compressing. Higher compression ratio and the smoother original image, the better quality of the reconstructed image. Usually we first compress the data then encrypt it. In some application information should be confidential to the network operator is required, such cases we have to reverse the operation. Flexible compression ratio, Better quality of reconstructed image and improve compression efficiency.

2. ENCODING

In encoding a modification is used. For encoding Huffman coding is used i.e., compression is achieved by DCT followed by Huffman coding. For a given block size a technique called Huffman coding is the most efficient fixed to variable length encoding method

2.1 COMPRESSION AND DECOMPRESSION OF ENCRYPTED IMAGE

In this work DCT is used for the compression of the image and the IDCT is used for the decompression of the image. Transform coding constitutes an integral component of contemporary image/video processing adjacent pixels in consecutive frames show very high correlation. Consequently, these correlations can be exploited to predict the value of a pixel from its respective neighbors. A transformation is, therefore, defined to map this spatial (correlated) data into transformed (uncorrelated) coefficients. Clearly, the transformation should utilize the fact that the information content of an individual pixel is relatively small i.e., to a large extent visual contribution of a pixel can be predicted using its neighbors. A typical image/video transmission system [3] is outlined in Figure 1. The objective of the source encoder is to exploit the redundancies in image data to provide compression. In other words, the source encoder reduces the entropy, which in our case means decrease in the average number of bits required to represent the image. On the contrary, the channel encoder adds redundancy to the output of the source encoder in order to enhance the reliability of the transmission. Clearly, both these high-level blocks have contradictory objectives and their interplay is an active research area. However, discussion on joint source channel coding is out of the scope of this document and this document mainly focuses on the transformation block in the source encoder. Nevertheless, pertinent details about other blocks will be provided as required.

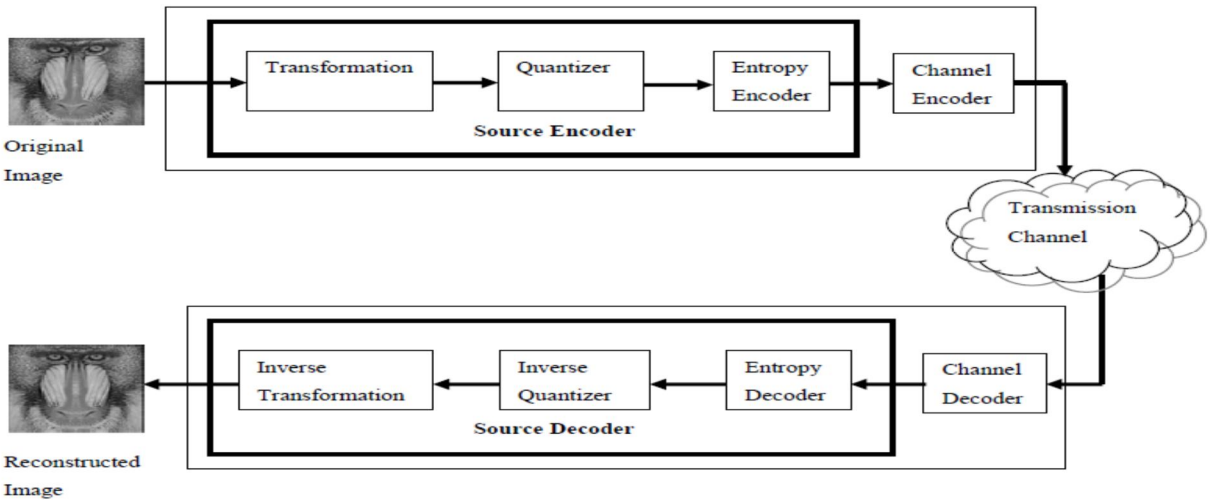

Fig. 1 A typical image/video transmission system

3. RESULTS AND DISCUSSION

For the testing image lena sized 512 x512 can be used in fig 2(a). After permuting the pixels encrypted data of the image is obtained. This encrypted pixel sequence is rearranged as a matrix of size 512 x 512 as in fig2 (a). Reconstructed image generated is also shown in fig. 2(a).A compressed image is obtained as in fig 2(b).

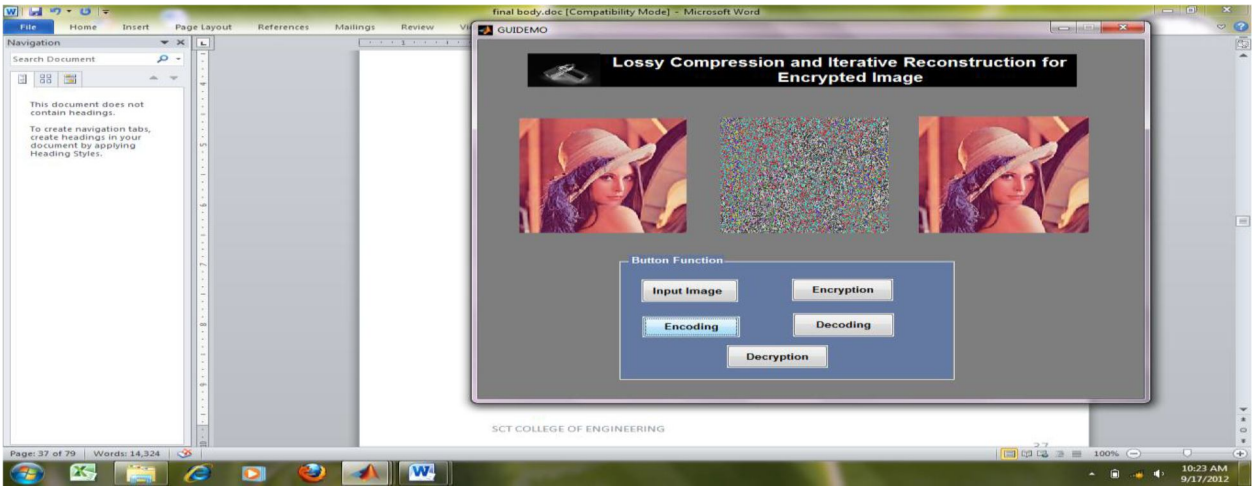

Fig 2.a. Input image, Encrypted Image and Reconstructed Image

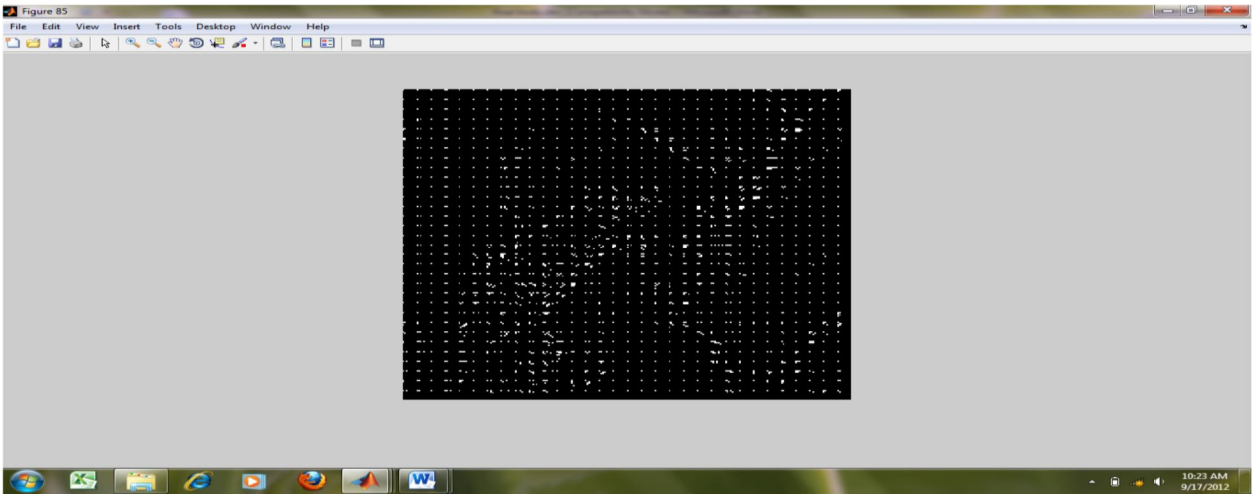

Figure 2.b.compressed image(DCT)

4. COMPARISON TABLE OF PARAMETERS BETWEEN DAUBACIUS WAVELET COMPRESSION AND DCT

TABLE I

Parameters	DCT	Daubacius Wavelet
PSNR	16.5708	26.9976
MSE	1432.2	129.812
CR	1.2593	1.2426
ENCRYPTION TIME	3.8007	3.63475
DECRYPTION TIME	1.5199	1.82448

5. CONCLUSION

This paper introduces a novel idea for compressing an encrypted image and made a practical scheme for image encryption, lossy compression and reconstruction. The original image is encrypted by pseudo random permutation. The higher compression ratio and smoother the original image, the better quality of reconstructed image. In encryption phase only pixel positions are shuffled, pixels values are not masked. But it has some disadvantage also. Security of encryption used is weaker than that of standard stream cipher. Future scope of this work is, the lossy compression of image can be encrypted by more secure methods. Here compress the image with wavelet compression and DCT. Compare the parameters of wavelet compression and DCT. Smaller value of Compression Ratio (CR) obtained in wavelet compression, and hence better

compression can be achieved. PSNR is better in wavelet compression. So we can conclude that wavelet compression is better than DCT.

REFERENCES

[1] J.C. Yen and J.I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realization," Proc. Inst. Elect. Eng., Vis. Image Signal Process. vol. 147, no. 2, pp. 167-175, 2000.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramachandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pt. 2, pp. 2992-3006, Oct. 2004.

[3] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097-1102, Apr. 2010.

[4] D. Schonberg, S. C. Draper, and K. Ramachandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., Allerton, IL, 2005.

[5] D. Schonberg, S.C. Draper, C. Yeo, and K. Ramachandran, "Toward compression of encrypted images and video sequences," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749-762, Dec. 2008.

[6] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," in Proc. IEEE Region 10 Conf. (TENCON 2009), 2009, pp. 1-6.

[7] R. G. Gallager, ―Low Density Parity Check Codes, Ph.D. dissertation, Mass. Inst. Technol., Cambridge, MA, 1963.

[8] A. Kumar and A. Makur, ―Lossy compression of encrypted image by compressing sensing technique, in *Proc. IEEE Region 10 Conf.(TENCON 2009)*, 2009, pp. 1–6.

[9] T. Bianchi, A. Piva, and M. Barni, ―Composite signal representation for fast and storage-efficient processing of encrypted signals, *IEEETrans. Inf. Forensics Security*, vol. 5, no. 1, pp. 180–187, Mar. 2010

