EFFICIENT GRAYSCALE IMAGE ENCRYPTION THEN COMPRESSION SYSTEM

[1]BHARATH K P, [2]PRABHAVATHI C

[1,2]Telecommunication Engineering Department SIT TUMAKURU INDIA
E-mail: [1]kpbharath93@gmail.com, [2]prabhachannaveer@gmail.com

Abstract— In secret communication, images are widely used and the major issues are how to protect the image and also reduce size of the image in order to maximize the network utilization. Various techniques are there in order to secure the image and to reduce the size of the image. In many practical scenarios, encryption of an image has to be conducted before the image compression. In proposed scheme, both image encryption and image compression system is designed efficiently. In order to get better network utilization, the encrypted images are compressed. An efficient image Encryption Then Compression(ETC) system is designed. In proposed scheme prediction error domain is used to encrypt the image in order to get high security.

Keywords— Encryption, Compression, Prediction error domain.

I. INTRODUCTION

Due to vast growth in multimedia applications memory, size and security are the major issues in communication. One of the way to secure the image is encryption and by using the compression techniques the size of the image can be reduced.

Consider the scenario in which the transmitter 'X' wants to send image I to receiver 'Y' with high security, through a channel provider 'C'. In traditional Compression Then Encryption (CTE) as shown in Fig.1(a) Transmitter 'X' wants to compress the image I into B and then encrypt the compressed image B into Ie with a secret key I_{ek}. The encrypted image Ie is then passed to 'C', who forwards simply to receiver 'Y'. After receiving the encrypted image Ie, decryption and decompression is sequentially performed by 'Y' in order to get reconstructed image $\hat{I}$. In distinction, the channel provider 'C' has interest to maximize the network utilization by compressing all the network traffic. It is therefore much preferred if the compression ratio can be delegated by 'C' who typically has rich computational resource. A huge task within such Encryption Then Compression (ETC) frame is that compression has to be done for encrypted data, as channel provider 'C' does not know the secret key to access the data. This form of ETC system is shown in the Fig.1(b).

The likelihood of dispensation encrypted data directly in the encrypted field has been receiving increased attention in recent years[3]-[6]. By relating LDPC codes in numerous bit planes and developing the inter/intra connection, Lazzeretti and Barni offered several technique for lossless compression for encrypted images[7]. Further, Kumar and Makur applied the method of[5] to the prediction error province and achieved improved lossless compression demonstration on the encrypted images[8]. The rest of this paper is organized as follows. Section 2 gives the aspectof ETC scheme, where lossless compression is considered. In Section 3 experimental results are reported. Finally Section 4 gives the conclusion.

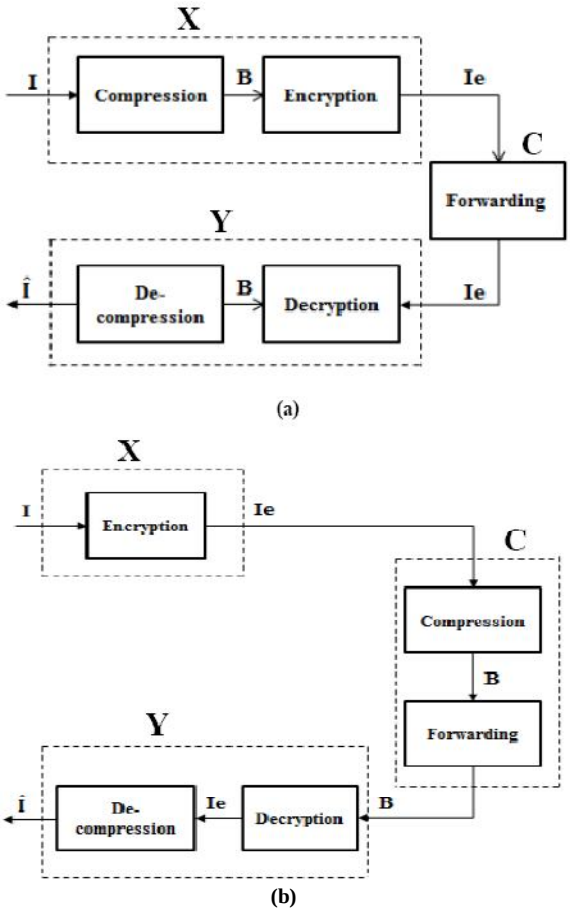


Fig.1.(a) Traditional Compression Then Encryption (CTE) system; (b) Encryption Then Compression (ETC) system.

II. ETC SYSTEM

In this section ETC system is explained in detail with 3 main key components. Encrypting the image by 'X', compression of encrypted image by 'C', and sequential Decryption and Decompression by 'Y'.

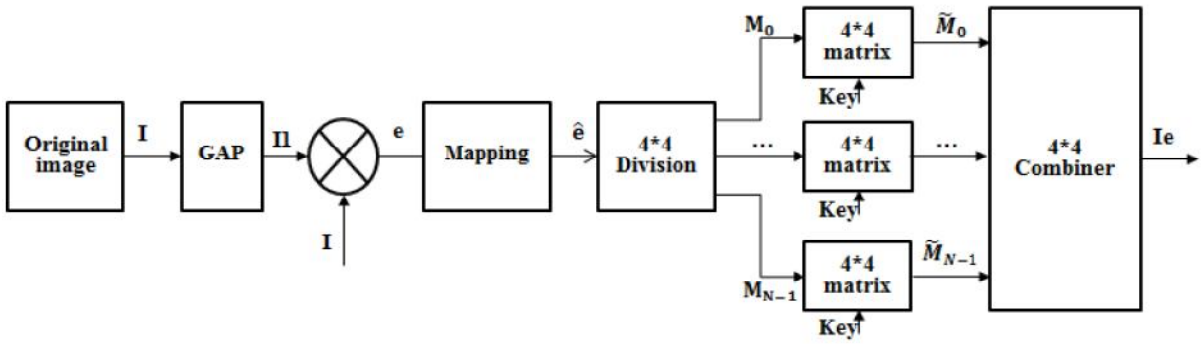


Fig. 2. Schematic diagram of image encryption.

2.1. Image Encryption Algorithm(Prediction error domain and Random keys)

From the perspective of the whole ETC system, the design of the encryption algorithm should simultaneously consider the security and the ease of compressing the encrypted data. By using the prediction error domain the proposed image encryption algorithm willoperate. The proposed image encryption scheme is as shown in Fig.2. Each and every pixels of an image I(i,j) to be encrypted, first pixel prediction I1(i,j) is done by using Gradient Adjusted Prediction(GAP)[9]. The pixel prediction I1(i,j) can be further refined to I2(i,j) by using context-adaptive , feedback mechanism[9].The prediction error related with I(i,j) can be calculated by

$$e(i,j) = I(i,j) - I2(i,j) \quad (1)$$

The problem with prediction error is, it has pixel values ranges between [-255, 255], so these pixel values are mapped into the range [0, 255], but the fact is decoding of image at receiver side is done by considering the predicted pixel values I2(i,j). So after mapping the prediction error it is denoted by e1(i,j), it has 256 distinct pixel values in the range of [0, 255][1].For encryption instead of taking all the mapped prediction error values, the whole mapped prediction error is divided into 4*4 matrices.

The image encryption algorithm procedure is as follows:

Step1: Apply GAP for input image.
Step2: Map the predicted values range [-255, 255] to [0,255].
Step3: Divide predicted error image into 4*4 matrices.
Step4: Apply two secret keys with cylical shift operation to the 4*4 matrixes.

Let keys be CS and RS which controls the columns shift and row shift operations respectively for each matrix. Here CSand RS keys are generated by stream cipher with a different key vectors. The key vector CS = [2 3 0 1] with all columns undergo a downward cyclical shift with the CS key. Same procedure is repeated for row shift operation using key RS = [1 3 1 2]. The operation is realized using circular shift which is easy to implement as shown in Fig.3.
Step5: By using 4*4 Combiner all the matrixes are concatenated and final encrypted image I_e is generated.

2.2. Lossless Compression of Encrypted Image

The encrypted image Ie can be compressed using lossless compression techniques. Two compression techniques are used. 1. Arithmetic coding (AC), 2. Huffman coding (HC).
Both the compression techniques are compared. Based on application a particular technique is used. The encrypted image Ie can be compressed via Adaptive Arithmetic coding/Huffman coding as shown in Fig.4. The channel provider 'C' doesn't know the secret key to access the data, channel provider 'C' simply compress the encrypted data and transmits via channel. The encrypted image Ie is divided into 4*4 matrix as in the same way exactly done during the encryption process. Now apply adaptive AC/HC to all 4*4 matrixes which converts the prediction errors into binary bit streams Bk. Finally all bit streams are concatenated and produces B. In order to improve the efficiency Bk will be done in parallel.B = B0,B1,B2,…….Bk.

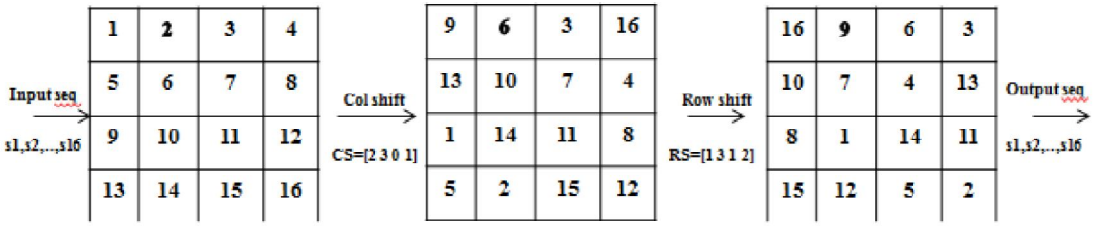


Fig. 3. An example of the cyclical shifts.

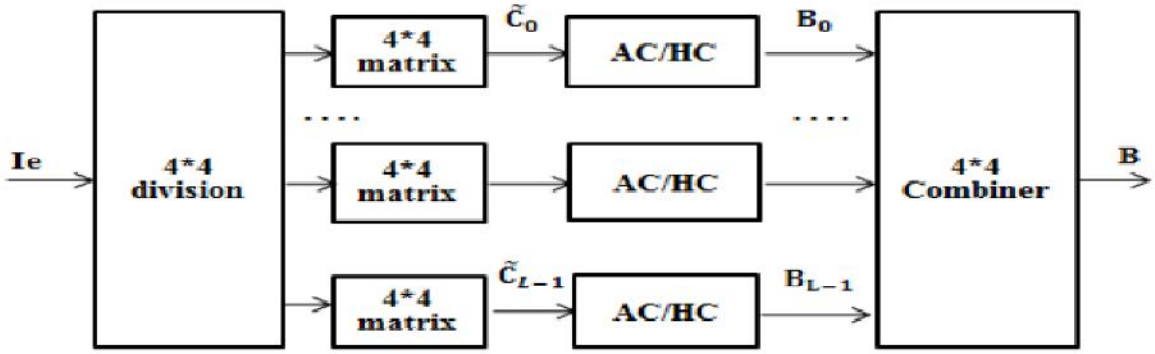


Fig. 4.Schematic diagram of compressing the encrypted image.

2.3. Consecutive Decompression and Decryption

After getting the encrypted image Ie and compressed image with binary bit stream B, goal of the receiver 'Y' is to retrieve the original image I as shown in Fig.5. The receiver 'Y' divides B into 4*4 matrices andfor each 4*4 matrix an adaptive arithmetic/Huffman decoding can be applied in order to gain the equivalent prediction error pixel values (Ck). k=0,1,…L-1

As the receiver knows the secret key, by applying the key for 4*4 matrixes original (Ck) can be retrieved.

After getting all Ck values, the decrypting of the pixel values can be achieved in raster scan order. For each pixel value location (i,j), the related error energy estimator Δ(i,j) and the pixel prediction values I1(i,j) can be designed from the causal surroundings. That I1(i,j) has already known to the receiver. Providing Δ(i,j) cluster index as proposed in [1].The reassembled pixel values can be obtained by

$$\tilde{I}(i,j) = I1(i,j) + e(i,j) \qquad (2)$$

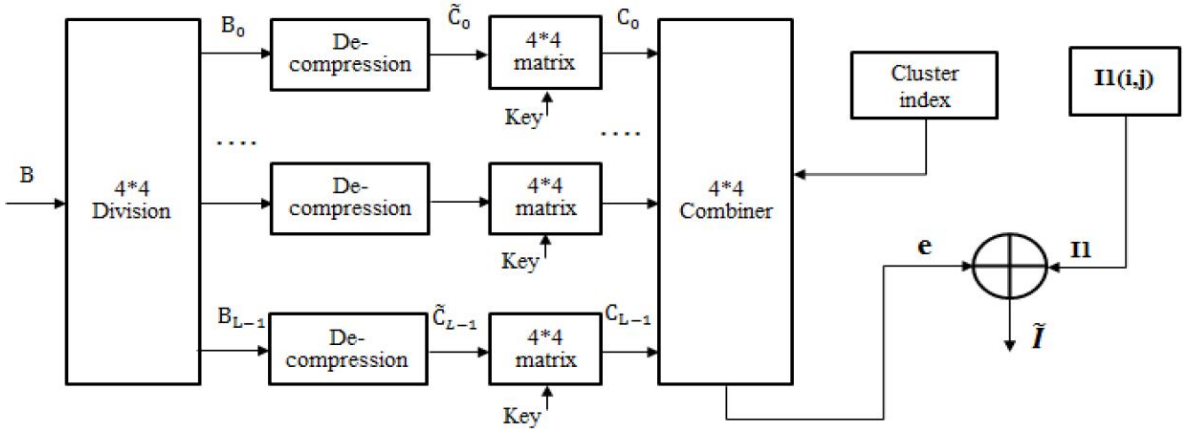
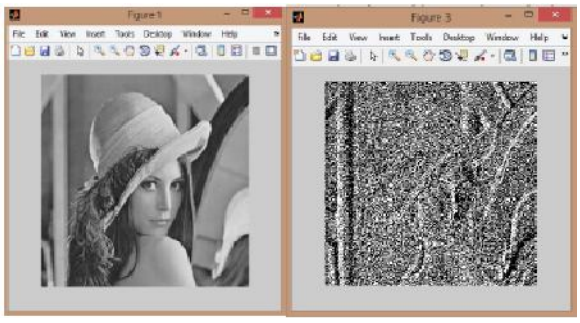


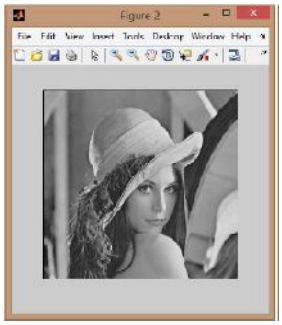
Fig. 5 Schematic diagram of sequential decompression and decryption.

III. EXPERIMENTAL RESULTS

In this section, Performance of the proposed scheme is estimated experimentally. Fig.6 demonstrates the original lena image, with its encrypted image and reconstructed image.



(a) **(b)**



(c)

Fig. 6.(a) original lena; (b) encrypted lena; (c) reconstructed lena.

A set of eight images with size of 512*512as shown in Fig.7 can be taken as test images. The compression ratio for all compressed test images is shown in the Table 1 and bar graph is shown in Fig.8. After comparing the compression ratio of both Adaptive

Arithmetic and Huffman coding, Adaptive AC is better than the Huffman coding, and also in terms of execution time Adaptive AC takes less time compared to the Huffman coding. The PSNR for decoded images is shown in Table 2. It can be observed that the PSNR values are little low it is due to padding of zeros while applying GAP for original image, hence for that reason errors can occur in first two rows and columns.

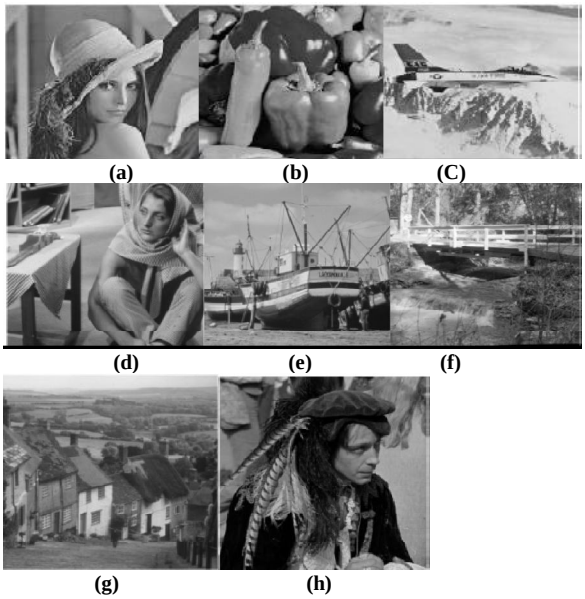


Fig.7. Eight test images (512*512), each of which is assigned with an ID range from 1-8, in raster scan order. (a) Lena.(b) Peppers. (c) Airplane. (d) Barbara. (e) Boat. (f) Bridge. (g) Gold hill. (h) Man.

Table 1: The compression ratio obtained with the Arithmetic coding(AC) and Huffman coding (HC).

Test images	Compression ratio for Arithmetic coding	Compression ratio for Huffman coding
Lena	11.23	11.09
Peppers	11.26	11.12
Airplane	11.39	11.24
Barbara	11.32	11.17
Boat	11.36	11.22
Bridge	11.42	11.27
Gold hill	11.33	11.18
Man	11.42	11.25

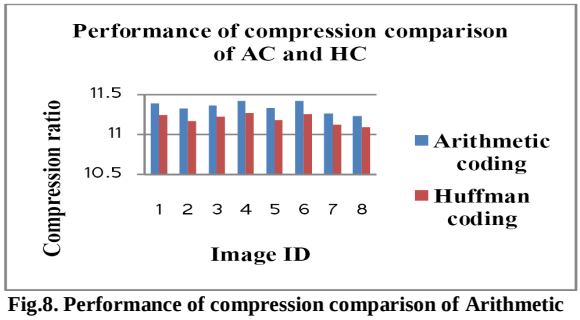


Fig.8. Performance of compression comparison of Arithmetic coding(AC) andHuffman coding (HC).

Table 2: The PSNR Values obtained for reconstructed images.

Test images	PSNR in dB
Lena	26.35
Peppers	26.39
Airplane	24.93
Barbara	21.98
Boat	24.84
Bridge	23.42
Gold hill	25.95
Man	24.65

CONCLUSION

In the proposed schemean efficient grayscale image Encryption Then Compression system (ETC system) is developed. Here the encryption of an image is accomplished via pixel prediction and secret key. Extreme compression of the encrypted image is done by using two techniques, Arithmetic and Huffman coding. Upon comparing the compression ratio Arithmetic coding is found to be better. Both experimental and theoretical results have shown the high level security and the reconstructed image is nearly equal to the original image.

REFERENCES

[1] J. Zhou, X. liu, and O. C. Au,"Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation," in IEEE Transaction on information forensics and security, vol. 9, No. 1, 2014.

[2] J. Zhou, X. liu, and O. C. Au, "On the design of an efficient encryption-then-compression system," in Proc. ICASSP, 2013, pp. 2872-2876.

[3] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86-97, Mar.2009.

[4] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphiccryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.

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

[6] D. Schonberg, S. C. Draper, and K. Ramachandran, "On compression encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269-272

[7] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in Proc. 16th Eur. Signal process. Conf.,Aug. 2008, pp.1-5.

[8] A. Kumar, A. Makur, "Distributed source coding based encryption and Lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760-764.

[9] X.Wu and N. Memon, "Context-based adaptive lossless image codec,"IEEE Trans. Commun., vol. 45, no. 4, pp. 437-444, April 1997.

[10] M.J. Wienberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and Standardization into JPEG-LS," IEEE Trans. Imag. Process., vol. 9, no. 8, pp. 1309-1324, Aug. 2000.

★★★