Middle-East Journal of Scientific Research 23 (5): 932-935, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.05.22222

An ETC System Using Advanced Encryption Standard and Arithmetic Coding

J. Subash Chandra Bose and Greeshma Gopinath

Computer Science and Engineering,
Professional Group of Institution, Palladam, Coimbatore, India

Abstract: Today, there is almost no area of technical endeavor that is not impacted in some way by digital image processing. The application areas of digital image processing are so varied that some form of organization is desirable in attempting to capture the breadth of this field. There is a need for secure and efficient transmission of images since the multimedia image is increasingly being used. So that the images are compressed and encrypted for transmitting through a network. In some situations image encryption has to be conducted prior to image compression. This has led to the problem of design of an encryption then compression system such that the encrypted image compression is still be efficiently performed.In this paper we design an encryption then compression (ETC) system. In this proposed system, image encryption is done over prediction error domain. For compressing the image efficiently, arithmetic coding based approach is used. For comparing the performance measure the PSNR values of the reconstructed images is used. The algorithm is implemented using MATLAB.

Key words: Encryption Then compression · Prediction error · Advanced Encryption Standard · Arithmetic coding

INRODUCTION

There is a need for secure and efficient transmission of images since the multimedia image is increasingly being used. Nowadays, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online bill images, albums, confidential archives, medical and military image databases. These images may contain confidential information so that they should be protected from third party during transmissions. At the same time they must be compressed efficiently. Recently, there are many methods have been proposed for securing image transmission, by merging both encryption and compression.

Most of the existing systems are image compression then encryption systems. But in some situations we need to reverse the order of applying compression and encryption.In a transmission the content owner is always interested in giving priority to protect the the privacy of the image data through encryption. Nevertheless, the owner has no incitation to compress the data, if the content owner is a limited resource mobile device. Instead of running a compression algorithm, the content owner simply forwards the encrypted source data to the channel provider. To maximize the network utilization the channel provider is interested in compression with their ample resources.The processing of encrypted signals has been receiving increasing attention in recent years.

Related Work: CALIC- Encryption Then Compression Technique [1] is a context based,adaptive lossless image codec, which obtains higher lossless compression of continuous tone images.CALIC employs a prediction /residual approach to reduce the model cost. In prediction by using a Gradient Adjusted Predictor is used to adjust prediction coefficient based on local gradient estimates.

Image Encryption Then compression Via prediction Error Clustering and Random Permutation proposes an ETC system[2],in which a permutation-based image encryption method conducted over the prediction error domain and an arithmetic coding (AC)-based approach to efficiently compress the encrypted image.

LOCO-I Lossless Image Compression Technique [3] proposes a lossless compression algorithm for continuous tone images. This algorithm contains two independent components namely modeling and coding. This algorithm is based on context modeling and it combines the simplicity of Huffman coding.

Corresponding Author: Greesha Gopinath, M.E. Student, Professional Group of Institution, Palladam, Coimbatore, India.

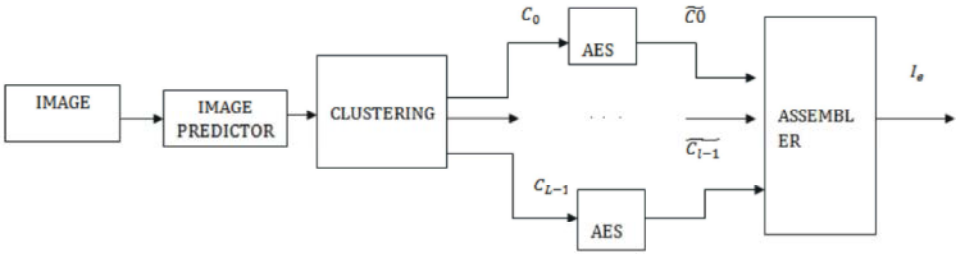

Fig. 1: Schematic diagram of mage Encryption

A scalable lossy coding framework of encrypted images via a multi-resolution construction [4] proposes an encryption then compression technique. In the encryption phase, the original image is decomposed into a sub-image and several layers of prediction errors. Then the sub-image and prediction errors are encrypted using an exclusive-or operation and a pseudo-random permutation, respectively. Finally the compression can be achieved by quantizing the permuted prediction errors on various layers and an optimization method.

Proposed System: In this section we present three different modules of the proposed system, namely image encryption conducted by the content owner Alice, image compression conducted by the channel provider Charlie and decryption and decompression conducted by the receiver Bob [5, 6].

Image Encryption using AES: The proposed system image encryption scheme operated over prediction error domanin. Figure 1 shows the schematic diagram of image encryption. Firstly for each pixel I (I, j) of the image to be encrypted the input image I is initially processed by using any image predictor; e.g. GAP [7] Then the prediction error is calculated by as follows:

$$e_{i,j} = I(imp) - \tilde{I}(i,j) \quad (1)$$

Instead of treating prediction errors as a whole, the prediction errors are divided in to clusters. Then each cluster is encrypted using AES (Advanced Encryption standard) to get the encrypted clusters. Finally the assembler concatenates all the encrypted clusters to get the encrypted image I_e.

AES is a Block Cipher: This means that the number of bytes that it encrypts is fixed. The AES is flexible in supporting any combination of data and key size of 128, 192 and 256 bits. However, AES allows a 128 bit data length that can be divided into four basic operation blocks. AES operates on a 4×4 column-major order matrix of bytes, called as state. Most of the AES calculations are done in a special finite field. For complete encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [8- 10]. There are 4 different stages, one is permutation and other three are substitution:

- Substitute bytes: This stage uses an S-box to perform a byte-by-byte substitution of the block
- Shift Rows: This operation contains a simple permutation
- MixColumns: A substitution that makes a mixing operation which operates on the columns of the state and combines four bytes in each column.
- AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key

The AES algorithm is start with an initial addroundkey, Then a round function is applied to the data block.The round function consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively. Depending on the key length, It is performed iteratively (Nr times).

Compression of Encrypted Image via Arithmetic Coding: The diagram of compression is shown in Figure 2. Using the side information (length of each cluster), the De-assembler parses the encrypted image I_e in to L clusters as done in encryption stage.Then arithmetic coding is applied to each clusters to encode each prediction error sequence $\widetilde{ck}$ into binary bit stream B_K. In adaptive arithmetic coding random permutation is applied. This random permutation will not change values of prediction error but it changes the location. Then the assembler concatenates all B_K to produce the compressed bit streams B, namely [11],

$$B = B_0 B_1 ..... B_{L-1} \quad (2)$$

Reconstruction of the Image: The sequential decryption and decompression is done at receiver side.

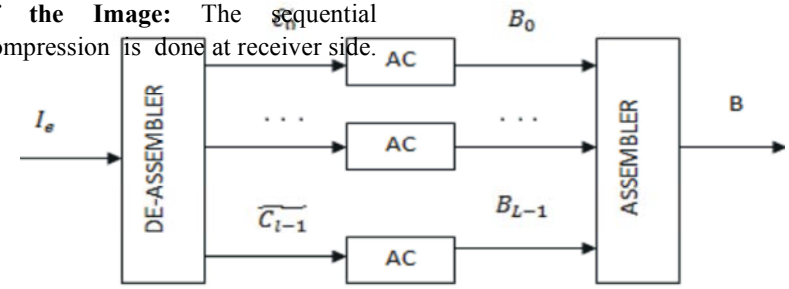

Fig. 2: Schematic diagram of image compression

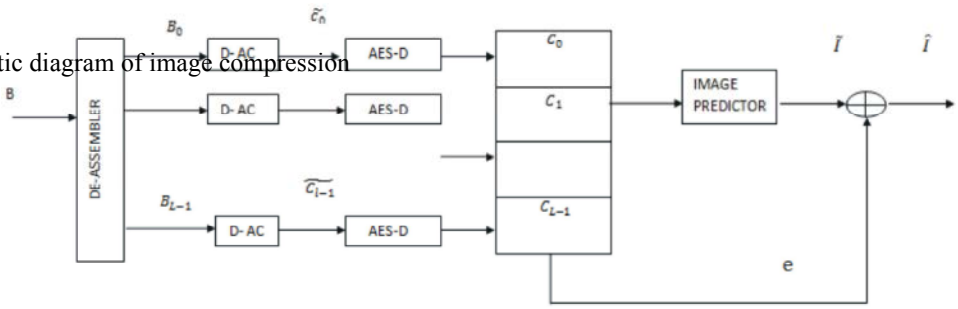

Fig. 3: Schematic diagram of decryption and decompression

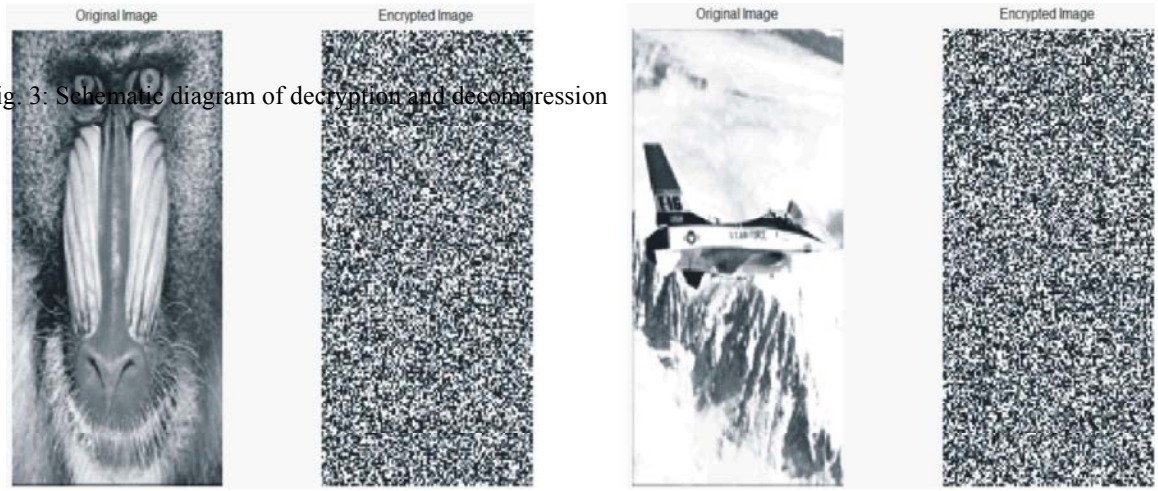

Fig. 4: a). Original and encrypted version of Baboon Image b). Original and encrypted version of Airplane

Schematic diagram of decryption and compression is depicted in Figure 3. Shown in figure. The compressed image B is sequentially decompressed and decrypted. The reconstructed pixel value is computed by the as follows:

$$\hat{I} = \tilde{I}_{i,j} + e_{i,j} \quad (3)$$

Security and Performance Analysis: In this section we evaluate the security of our proposed image encryption and compression performance.Following Figure illustrates the test images and their encrypted versions. From the figure we can see that proposed image encryption destroys the semantic meaning of the original images.

The brightness of the encrypted images varies based on texture region that it contains.

PSNR is most commonly used to measure the quality of reconstruction compressed image.PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{M\,N}\sum_{1=0}^{M-1}\ \sum_{j=0}^{N-1}\ [I(i,j)-k(i,j)]^2$$

The PSNR (in dB) is defined as:

$$\begin{aligned} PSR &= 10.\ log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20.\ log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20.log_{10}(MAX_I) - 10log_{10}(MSE) \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. Table 1 shows PSNR values of diffent test images.

Table 1: Quality Measure of reconstructed image

Image	PSNR
Baboon	16.7531
Airplane	14.0330
Lena	15.6732

CONCLUSION

In this paper we have designed an ETC (Encryption then Compression system) system,using AES (Advanced Encryption Standard) and arithmetic coding. Within the proposed work, the image encryption has been achieved using prediction error clustering and AES. Compression of the encrypted data has then been done by arithmetic coding scheme. By arithmetic coding, we encode the data into a number in the unit interval [0,1]. This method is implemented by separating the unit interval into different clusters according to the number of distinct symbols. The experimental results have shown that the security of our proposed method is reasonably high. The reconstructed image quality is measured in terms of PSNR.

REFERENCES

1. Wu, X. and N. Memon, 1997. Context-based, adaptive, lossless image codec,IEEE Trans. Commun., 45(4): 437-444.
2. Zhou Jiantao, Xianming Liu, Oscar C. Au and Yuan Yan Tang, 2014. Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation,IEEE Transactions On Information Forensics And Security, 9(1): 00-00.
3. Weinberger, M.J., G. Seroussi and G. Sapiro, 2000. The LOCO-I loss- less image compression algorithm: Principlesand standardization into JPEG-LS, IEEE Trans. Imag. Process., 9(8): 1309-1324.
4. Zhang Xinpeng, Guorui Feng, Yanli Ren and Zhenxing Qian, 2012. Scalable Coding of Encrypted Images, Image Processing, IEEE Transactions on, 21(6): 3108-3114.
5. Zhou, J., X. Liu and O.C. Au, 0000. On the design of an efficient encryption then-compression system.
6. Bianchi, T., A. Piva and M. Barni, 2009. On the implementation of the discrete Fourier transform in the encrypted domain, IEEE Trans. on Inf. Forensics Security, 4(1): 86-97.
7. Johnson, M., P. Ishwar, V.M. Prabhakaran, D. Schonberg and K. Ramchandran, 2004. On compressing encrypted data, IEEE Trans. On Signal Process., 52(10): 2992-3006.
8. Liu, W., W.J. Zeng, L. Dong and Q.M. Yao, 2010. Efficient compression of encrypted grayscale images, IEEE Trans. on Image. Process, 19(4): 1097-1102.
9. Zeghid, M., M. Machhout, L. Khriji, A. Baganne and R. Tourki, 2007. A Modified AES Based Algorithm for ImageEncryption" World Academy of Science, Engineering and Technology International Journal of Computer, Control, Quantum and Information Engineering, 1(3): 00-00.
10. Daemen, J. and V. Rijmen, 2000. The block cipher Rijindael, Proceedings of the Third International Conference on smart card Research and Applications, CARDIS'98, Lecture Notes in computer Science, Springer, Berlin, 277-284,1820.
11. Federal Information Processing Standards Publications (FIPS 197), 2001. Advanced Encryption Standard (AES).