DCT-AES Base Image Compression and Encryption Technique

Muslim Mohsin Khudhair

Abstract— With the fast evolution of digital data exchange, security of information becomes massively important in data storage and transmission. Due to the increasing use of images in an industrial process, it is essential to protect the confidential image data from unauthorized access. The current paper proposed an image encryption technique that is operated with advanced encryption standard (AES) and image compression using discrete cosine transform (DCT) to compress the encrypted image. The experimental results show that the current technique impressively outperforms other techniques. It is simple, efficient, and more secure.

Index Terms— advanced encryption standard (AES), discrete cosine transform (DCT), Encryption, Compression, quantization, Scaling, MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio)

1 Introduction

In recent years, the rapid growth in the demand of transmitting images via public networks has raised a lot of interest on image compression and encryption. On one hand, research on image compression has been carried out for a long time [1–3], with the goal of reducing the image size for easy storage and fast transmission. The need to apply both compression and encryption to digital images keeps rising in recent years. The traditional solution applies a data encryption algorithm such as Advanced Encryption Standard (AES) on the compressed image in JPEG format [4].

The AES algorithm has broad applications, including smart cards and cellular phones, WWW servers and automated teller machines (ATMs), and digital video recorders. Compared to software implementations, hardware implementations of the AES algorithm provide more physical security as well as higher speed [5]. In other hand, DCT is commonly used since it incorporates a strong energy compaction property which flavors compression [6]. The rest of the paper is organized as follows: Section 2 describes the Discrete cosine Transform and AES algorithm, Section 3 illustrates the Methodology of current technique , Section 4 presents the result and discussion. Finally, Section 5 concludes and future works the paper.

2 Background Study

2.1 Discrete Cosine Transform

The joint photographic expert group (JPEG) was developed in 1992, based on DCT. It has been one of the most widely used compression method [7]. Discrete cosine transform is an orthogonal transform method proposed by N. Ahmed et al. [8] in 1974. DCT has been widely applied in image processing research since it was proposed. Like Discrete Fourier Transform (DFT), it transforms a sequence of data from spatial domain to frequency domain. However, DCT deals with real numbers only, rather than complex numbers. The transformed sequence is expressed as the sum of cosine functions that oscil late at different frequencies. In other words, it decorrelates the image data into different frequency bands. After performing DCT, the block can be divided into two sub-bands: low frequency sub-band which contains most of the important visual parts of the image, and high frequency sub-band which contains details and textures of the image. Generally speaking, low frequency coefficients are more important than high frequency coefficients because the values of high frequency coefficients are usually closed to zero. Due to non-importance of high frequency sub-band, in general, the high frequency sub-band is usually removed for compression purpose. The following equations illustrated DCT and Inverse DCT function for two-dimensional matrices of an M by N input sequence [9, 10]:

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N}$$

$$I(x,y) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(u,v) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N}$$

where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}} & ,u = 0 \\ \sqrt{\frac{2}{M}} & ,1 \le u \le M-1 \end{cases} \quad ; \quad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}} & ,v = 0 \\ \sqrt{\frac{2}{N}} & ,1 \le v \le N-1 \end{cases} \tag{1}$$

The values C(u, v) are called the DCT coefficients of image I. The upper leftmost element is called discrete code (DC) coefficient and the rest are called arithmetic code (AC) coefficients. The input image is first divided into 8×8 blocks; then the 8-point 2-D DCT is performed. The DCT coefficients are then quantized using an 8×8 quantization table. The quantization is achieved by dividing each elements of the transformed original data matrix by corresponding element in the quantization matrix (Q) and rounding to the nearest integer value. After this, compression is achieved by applying appropriate scaling factor (SF). Then in order to reconstruct the data, rescaling and

Muslim Mohsin Khudhair: Master digree in computer science, Department of Computer Information Systems, College of Computer Science & Information Technology, University of Basrah, Basrah, IRAQ. Mobile: 009647801452456. E-mail : mos1970@yahoo.com.

de-quantization is performed. The de-quantized matrix is then transformed back using the inverse DCT (IDCT) [11, 12]. The whole procedure is shown in Fig. 1.

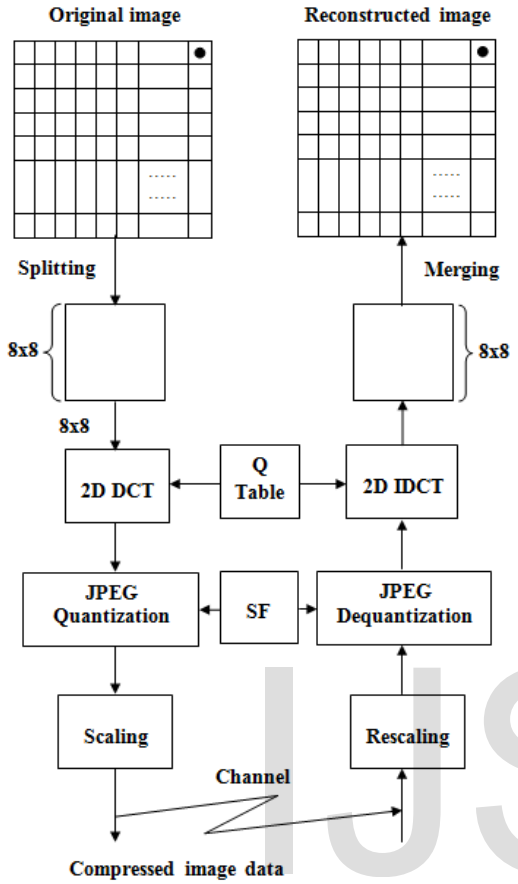

Fig. 1: Block diagram of the JPEG-based DCT scheme.

2.2 AES ALGORITHM

The AES algorithm is a symmetric block cipher that processes data blocks of 128-bits using a cipher key of length 128,192 or 256 bits each data block consist of a 4×4 array of bytes called the state, on which the basic operations of the AES algorithm are performed. The AES encryption procedure is shown in Fig.2. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [13, 14]. These rounds are governed by the following transformations:

- SubBytes transformation: is a nonlinear byte substitution that operates independently on each byte of the state using a substitution table (the SBox).
- ShiftRows transformation: is a circular shifting operation on the rows of the state with different numbers of bytes (offsets).
- MixColumns transformation: is equivalent to a matrix multiplication of columns of the states. It should be noted that the bytes are treated as polynomials rather than numbers.
- AddRoundKey transformation: is an XOR operation that adds a round key to the state in each iteration, where the round keys are generated during the key expansion.

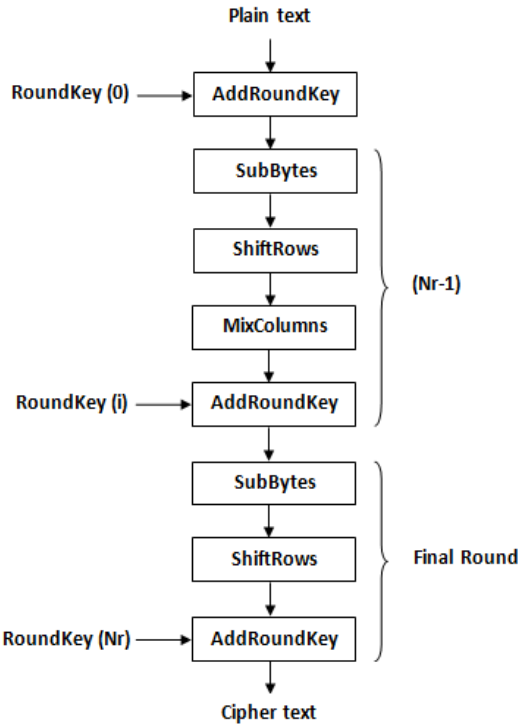

Fig. 2: AES algorithm- Encryption structure.

The encryption procedure consists of several steps as shown by Fig. 2. After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length [5].

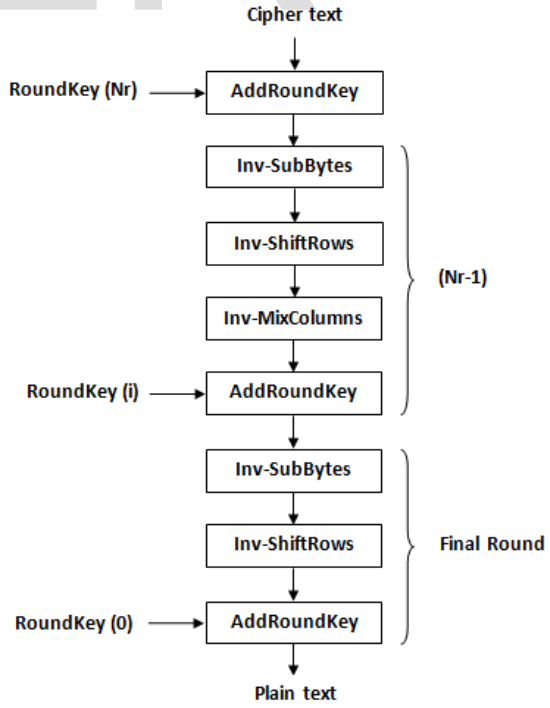

Fig. 3: AES algorithm- DEcryption structure.

The decryption procedure of the AES is basically the inverse of each transformation (Inv-SubBytes, Inv-ShiftRows, Inv-MixColumns, and AddRoundkey) in reverse order as shown in Fig. 3.

3 The Current Technique

In this paper, we propose an efficient image compression and encryption technique. The block diagram of this technique is shown in Fig. 4. It starts with divide the plain-image into blocks of size 8 × 8 pixels and apply DCT for each bock. Then, scramble the DCT coefficients of each block, except DC element, by 128-bit AES algorithm. The DC coefficient is not encrypted because it carries important visual information in an image. To decryption process, the process is done by applying inversed AES algorithm. Finally, The technique apply inverse discrete cosine transform (IDCT) for each block to get the reconstruct image.

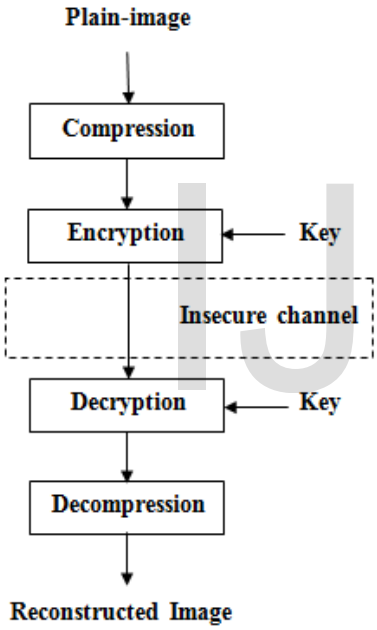

Fig. 4: General flowchart of current technique for encryption-compression image.

4 Experimental Results

The current technique was implemented with (MATLAB 2012) package. The implementation was done on a PC (DELL laptop) with 2.1 GHz core 2 due processor and 2GB main memory running with windows 7 operating system. The process was applied on greyscale image that has the size of (256×256 pixels). Two images that tested are (Lena) and (Barbara) as shown in Fig. 5.

Fig. 5: Test images

Fig. 6 illustrates the encrypted and reconstructed images obtained by applying this technique.

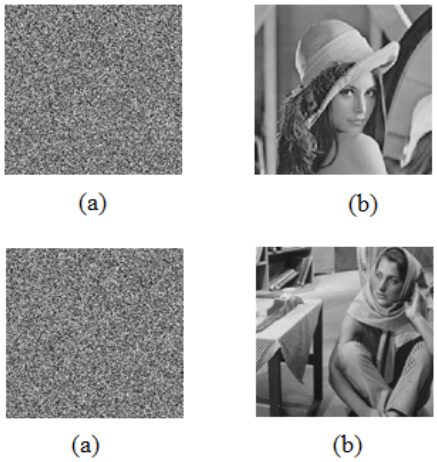

Fig. 6: (a) Encrypted images, (b) reconstruct images.

The proposed work is analyzed by using various parameters like MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) and [15].
The mean square error (MSE) is used as metric to measure the distortion between original and reconstructed image [16]. The equation that evaluating the MSE is:

$$MSE = \frac{1}{M * N} \sum_{x=1}^{N} \sum_{y=1}^{M} [I(x,y) - Irec(x,y)]^2 \quad (2)$$

where:
I : is the original image.
Irec: is the reconstructed image.
M: the height of the image.
N: the width of the image.
x and y: row and column numbers.

The peak signal to noise ratio (PSNR) , in decibels (dB), can be evaluated as follows [17]:

$$PSNR = 10.\log_{10}[(P_{ix})^2 / MSE] \quad (3)$$

where Pix is maximum possible pixel value, e.g. 256 in an 8-bit grey-level image.

4.1 Statistical Analysis

Shannon suggested different methods of diffusion and confusion in order to frustrate the powerful attacks based on statistical

analysis [18]. Statistical analysis has been performed on the AES, demonstrating its superior confusion and diffusion properties which strongly defend against statistical attacks. This is shown by a test on the histograms of the enciphered image.

Fig. 7 depicts the histograms of the plain-image (Lena) and the corresponding cipher-image. The histogram of the encrypted image is nearly uniformly distributed, which can well protect the information of the image to withstand the statistical attack [19].

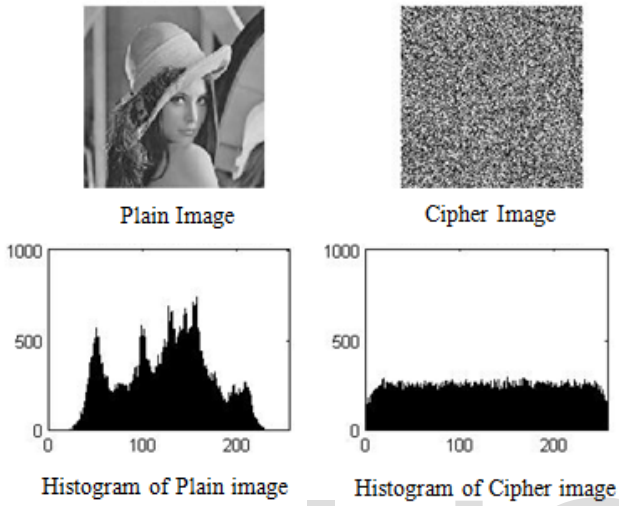

Fig. 7: Histograms of the plain image and cipher image.

4.2 JPEG Compression

Next we do some experiments to determine robustness of the cipher-images to common image processing such as JPEG compression [20]. JPEG compression causes the image size (in bytes) to be small and the image quality is reduced. The various compression qualities are 75%, 60%, 50%, 30%, 10%, and 5%. Fig. 8 shows the decrypted images of (Lena) after doing compression to the cipher-image. Quality of decrypted images (measured by PSNR) tends to decrease when quality of JPEG compression is reduced, but the decrypted image can be still recognized.

Fig. 8: The decrypted images of (Lena) when the corresponding cipher images is compressed by JPEG with various compression quality.

5 Conclusions and Future Works

In this paper, we present a joint image compression encryption scheme for Internet multimedia applications. The feature of the proposed method includes Discrete Cosine Transform (DCT) for image compression and advanced Encryption Standard (AES) for image encryption. These algorithms allow images can be compressed and the security of transmission process is enhanced. Experimental results show that the plain images are incomprehensible and the reconstructed images have acceptable quality. In future, the technique can be extended by modifying round key of AES algorithm to get high security.

References

[1] K.L. Chung, Y.W. Liu, and W.M. Yan, "A hybrid gray image representation using spatial and DCT based approach with application to moment computation," Journal of Visual Communication and Image Representation 17, pp. 1209-1226, June 2006.

[2] M. Zhang and X. Tong,"A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system," Multimedia Tools and Applications, Vol. 74, No. 24, pp. 11255-11279, Dec 2015.

[3] A. Kingston and F. Autrusseau, "Lossless image compression via predictive coding of discrete Radon projections," Signal Processing: Image Communication 23 (4), pp. 313–324, 2008.

[4] C. H. Yuen and K. W. Wong, "A chaos-based joint image compression and encryption scheme using DCT and SHA-1 ," Applied Soft Computing 11, pp. 5092-5098, 2011.

[5] X. Zhang and K. K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm," IEEE Trans. Verylarge Scaleintegration (VLSI) Systems , Vol. 12, No. 9, Sep 2004.

[6] Y.Q. Shi and H.F. Sun, "Image and Video Compression for Multimedia Engineering: Fundamentals, Algorithms, and Standards," CRC Press, Boca Raton, 2008.

[7] X. Zhou, Y. Bai, and C. Wang, "Image Compression Based on Discrete Cosine Transform and Multistage Vector Quantization," International Journal of Multimedia and Ubiquitous Engineering, Vol.10, No.6, pp. 347-356, 2015.

[8] K. R. Rao and P. Yip "Discrete cosine transform: Algorithms, advantages, applications," San Diego: Academic Press. 1990.

[9] K.W. Wong, B.S.H. Kwok, and W.S. Law, "A fast image encryption scheme based on chaotic standard map," Physics Letters A 37, pp. 2645–

2652, 2008.

[10] W.B. Pennebaker, J.L. Mitchell, "JPEG Still Image Data Compression Standard," Van Nostrand Reinhold, New York, 1993.

[11] M. M. Siddeq and M. A. Rodrigues, "A Novel Image Compression Algorithm for High Resolution 3D Reconstruction," 3DR Express, pp. 1-17, 2014, Doi: 10.1007/s13319-014-0007-6, (Springer.com).

[12] M. Gupta and A. Kumar Garg, "Analysis Of Image Compression Algorithm Using DCT," International Journal of Engineering Research and Applications, International Journal of Engineering Research and Applications, Vol. 2, Issue 1, pp. 515-521, Jan/Feb 2012.

[13] T. W. Cusick and P. Stănică, "Cryptographic Boolean Functions and Applications," San Diego, CA 92101-4495, USA, 2009.

[14] K.H. Chang1, Y. C. Chen, C. C.sieh, C. W. Huang, and C.J. Chang, " Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application," IEEE Xplore Digital Library, pp. 1922-1925, June 2009, Doi: 10.1109/ISCAS.2009.5118159.

[15] J. Singh and P. KAUR, "Image Encryption and Compression System Using Haar, Daubechies and Coiflet Wavelets," International Journal of Computer Science Engineering and Information Technology Research, Vol. 5, Issue 5, pp. 17-26, Oct 2015.

[16] Y. K. Chen, F. C. Cheng, and P. Tsai, "A gray-level clustering reduction algorithm with the least PSNR," Expert Systems with Applications 38, pp. 10183–10187, 2011.

[17] A. Tanchenko, "Visual-PSNR measure of image quality," J. Vis. Commun. Image R. 25, pp. 874–878, 2014.

[18] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption," International Scholarly and Scientific Research & Innovation, Vol. 1, No. 3, pp. 745-750, 2007.

[19] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics Communications 284 , pp. 2775-2780, 2011.

[20] R. Munir, "Robustness Analysis of Selective Image Encryption Algorithm Based on Arnold Cat Map Permutation," Proceeding of Makassar International Conference on Electrical Engineering and Informatics (MICEEI), pp. 1-5,Nov/Dec 2012.