# 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.*