Crypto-Compression Image Scheme using DWT and AES-Arnold Transforms

Asaad Abdul-Kareem Al-hijaj
Department of Computer Information Systems, College of Computer Science & Information Technology, University of Basrah, Basrah, IRAQ.

Muslim Mohsin Khudhair
Department of Computer Information Systems, College of Computer Science & Information Technology, University of Basrah, Basrah, IRAQ.

Luay Abdulwahid Shihab
Department of Branch of Basic Science, College of Nursing, University of Basrah, Basrah, IRAQ.

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 different process, it is essential to protect the confidential image data from unauthorized access. If encryption is not well performed then there may be possibility of stealing the information. Image compression is also essential where images need to be stored, transmitted or viewed quickly and efficiently. The current paper proposes an efficient technique to compress image by using Daubechies wavelet transforms. Moreover, it uses two algorithms which are advanced encryption standard (AES) and Arnold transform method for encryption the image. Experimental results show efficient technique that is simple in implementation and has high degree of security.

Keywords
encryption, compression, Daubechies, AES, Arnold transform.

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. The need to apply both compression and encryption to digital images keeps rising. Hence, image security/protection from unauthorized access becomes very important [1–3]. Image compression consists of processes leading to compact representation of an image, so as to reduce total storage/transmission requirements. While image encryption refers to converting an image to such a format, so that it becomes unreadable to unauthorized access and can be transmitted securely over the internet. On the other hand, image decryption means to convert the unreadable format of an image to an original image [4].

This paper is a step forward in this regards. The rest of this paper is organized as follows: Section 2 describes the Discrete Wavelet Transform and AES algorithm besides to Arnold transform, Section 3 illustrates the Methodology of current technique, Section 4 presents the result and discussion. Finally, Section 5 concludes of the current paper.

2. PRELIMINARY

2.1 Discrete Wavelet Transform (DWT)
At the beginning of 2000, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) made the core of JPEG2000 [5, 6] which adopts Discrete Wavelet Transform (DWT) as the standard compression tool. The DWT has been used successfully in many image processing applications including noise reduction, edge detection, and compression [7]. Currently, there's an increase role of utilization wavelet in image compression due to the fact that it provides high image quality with high compression ratios [8]. The DWT exploits both the spatial and frequency correlation of data by dilations (or contractions) and translations of the mother wavelet on the input data. It supports multi-resolution analysis of data (i.e. it can be applied to different scales according to the details required, which allows progressive transmission and zooming of the image without the need for extra storage) [9]. Another useful feature of a wavelet transform is its symmetric nature meaning that both the forward and the inverse transforms have the same complexity, allowing building fast compression and decompression routines. Wavelet transform divides the information of an image into an approximation (i.e. LL) and detail sub-band [10, 11].

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 (4x4) array of bytes called the state, on which the basic operations of the AES algorithm are performed. The AES encryption procedure is shown in Figure 1. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [12, 13]. 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.