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.

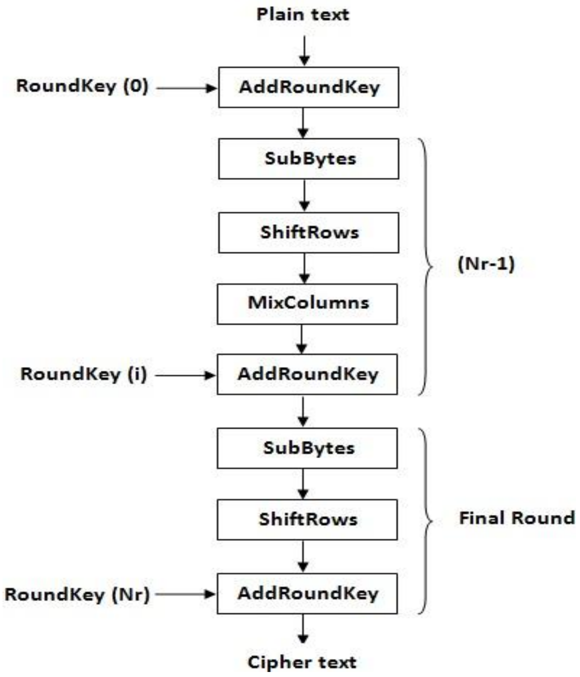


Fig 1: AES algorithm- Encryption structure.

The encryption procedure consists of several steps as shown by Figure 1. 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 [14].

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 Figure 2.

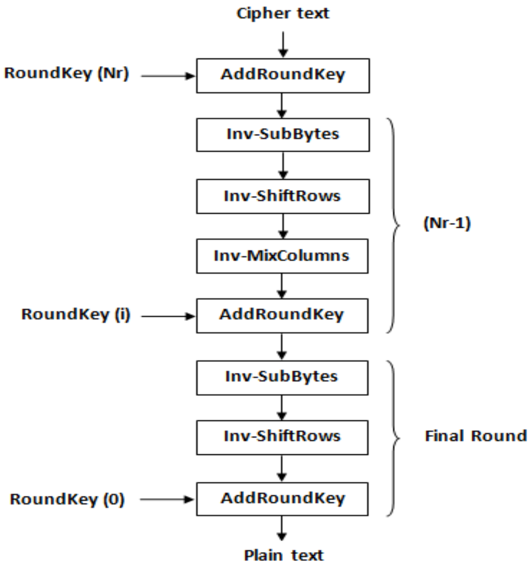


Fig 2: AES algorithm- Decryption structure.

2.3 Arnold Transform

The permutation techniques are very useful in the encryption process, because the advantages of using the permutation in cryptography (simple implementation speed, and universality for most image formats). The permutations will not change the coefficients values but their locations [15]. A permutation (rearrangement) can be described by assigning successive number to the objects to be permuted and then giving the order of the objects after the permutation is applied [16].

Arnold transform is commonly known as cat face transform. Apply Arnold transform in digital image, so it can change the layout of gray values by change the coordinates of pixels. Seen the digital image as a (NxN) matrix, then can achieve image pixels scrambling by formula [17]:

$$\begin{bmatrix} X_n \\ Y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} X \\ Y \end{bmatrix} \bmod N \qquad (1)$$

where (X, Y) is the location coordinates of the original image pixels, and (Xn, Yn) is the location coordinates of image pixel that after transform. Figure 3 shows the encryption image after applied Arnold transform over original image.

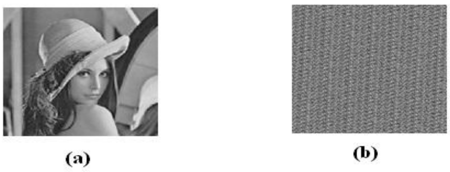


Fig 3 (a) Original image, (b) Encrypted image

3. THE CURRENT TECHNIQUE

In this paper, we have suggested an efficient technique for compressing and encrypting image. At the stage of compression, the original image is compressed by discrete wavelet transform(DWT). whereas, at the stage of encryption, the compressed image would be encrypted by (AES) algorithm and Arnold transform. The block diagram of this technique is shown in Figure 4.

On the other hand, the process of image reconstruction is performed in reverse to the previous technique

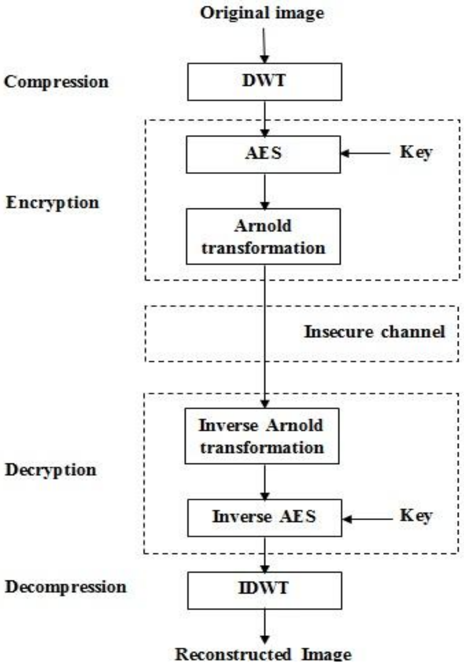


Fig 4: General flowchart of proposed technique for compression-encryption image.

3.1 Image Compression

Discrete Wavelet transform (DWT) is the first phase in the proposed Technique, to produces four sub-bands. The top-left corner is called LL, represents low-frequency coefficients, and the top-right called HL consists of residual vertical frequencies. The bottom-left corner LH, and bottom-right corner HH are represents residual horizontal and residual vertical frequencies respectively. The high-frequency components (LH1, HL1 and HH1) are zero or insignificant. This reflects the fact that much of the important information is contained in the LL sub-band. For this reason all the high frequency domains are discarded in this research (i.e. set all values to zero) [18, 19]. In particular, the Daubechies wavelet transform has the ability to reconstruct approximately the original image. This property allows higher compression ratios; this is because high frequencies from the first level can be ignored without loss of accuracy [8, 10]. Figure 5 shows the compression image by Daubechies wavelet transform.

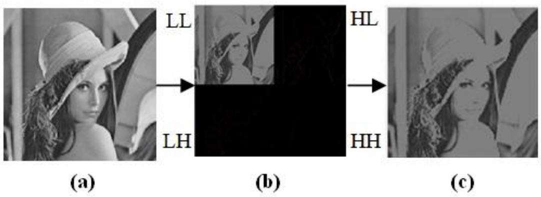


Fig 5: Compression Process: (a) Original image (b) Single stage DWT (c) Compressed image.

3.2 Encryption Image

The stage of encryption is composed of two processes for encrypting the compressed image which is produced by the previous stage. The compressed image would be passed to the 128-AES algorithm as it is shown in the Figure 6. Then, the image encrypted by means of Arnold transform which the image can be permuted for more security.

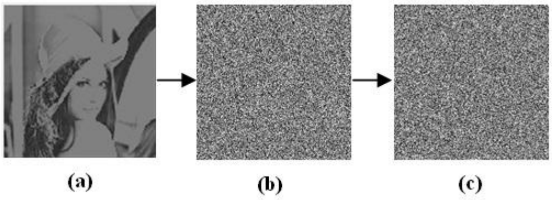


Fig 6: Encryption process: (a) Compressed image (b)Encrypted image by AES (c) Permuted image byArnold transform (Cipher image).

3.3 Reconstruction Image

The image can be reconstructed by using reverse proposed technique. The cipher image is passed to the inverse Arnold transform. Afterwards, the produced image passed to the inverse 128-AES algorithm which is called decryption process. Then, the process of decompression is performed by inverse discrete wavelet transform (IDWT) by means of which the image reconstructed. Figure 7 illustrates the process of the reconstructed image.

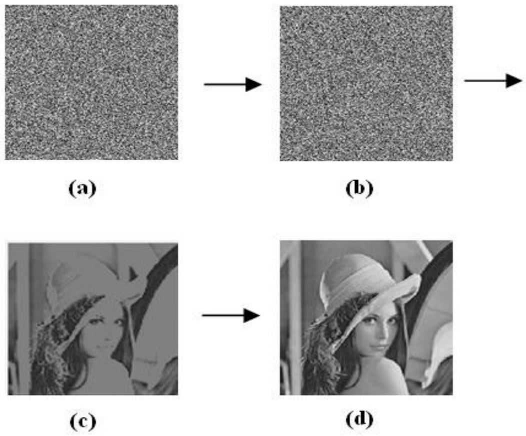


Fig 7: Reconstruction Process: (a) Cipher image (b)Decrypted image by Arnold transform (c)Decrypted image by AES (d) Decompressed imageby IDWT (Reconstructed image).

4. EXPERIMENTAL RESULTS

The current technique is applied on six grayscale images labeled image 1 to image 6 as shown in Figure 8. Each of these images has size of (256×256 pixels) with 8-bit grey levels. It 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.

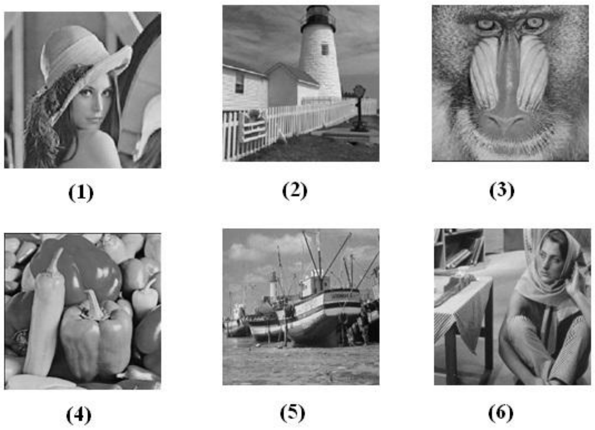


Fig 8: Test images

The proposed work is analyzed by using various parameters like MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) [20].

The mean square error (MSE) is used as metric to measure the distortion between original and reconstructed image [21]. The equation that evaluating the MSE is:

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

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 [22]:

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

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

Table (1) presents the PSNR, MSE values and execution time of whole process. We note higher value of PSNR is with more similarity between original image and Reconstructed image.

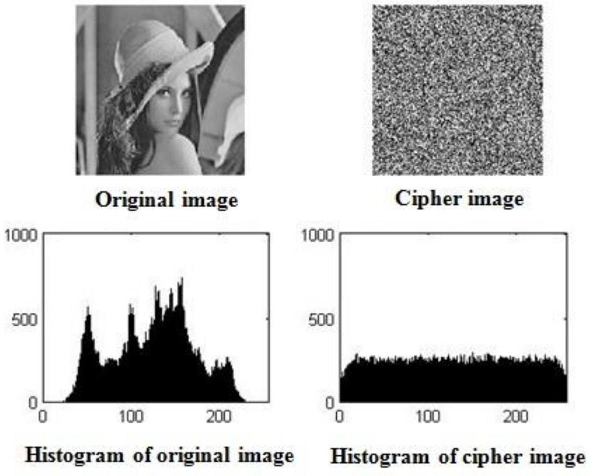
Table 1. PSNR, MSE and total time for six images tested.

Image No.	PNSR (dB)	MSE	Total Time
1	31.7501683	16.8658	4.781729
2	32.6091570	15.9654	4.452772
3	33.5867451	14.8750	4.293579
4	31.5535835	17.0296	4.823192
5	32.5689651	15.6013	4.400738
6	29.2351177	20.1309	4.979567

4.1 Statistical Analysis

Shannon suggested different methods of diffusion and confusion in order to frustrate the powerful attacks based on statistical analysis [23]. Statistical analysis has been performed on the AES and Arnold transform, 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.

Figure 9 depicts the histograms of the original 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 [24].



Original image

Cipher image

Histogram of original image

Histogram of cipher image

Fig 9: Histograms of the plain image and cipher image.

5. CONCLUSIONS

The feature of the proposed method includes Discrete Wavelet Transform (DWT) for image compression and advanced Encryption Standard (AES) with Arnold transform for image encryption. These algorithms allow images to compress and encrypt with high performance beside security. Experimental results show that the original images are incomprehensible and the reconstructed images have acceptable quality. In other words, the value of PSNR is high while the value of MSE is low this means our technique is effective. In future, the technique can be extended by modifying round key of AES algorithm to get high security.

6. REFERENCES

[1] Xinpeng Z. 2001. Lossy Compression and Iterative Reconstruction for Encrypted Image. IEEE Transactions On Information Forensics And Security. Vol. 6, No. 1, 53–58.

[2] Miao Z. and Xiaojun T. 2015. A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system. Multimedia Tools and Applications. Vol. 74, No. 24, 11255-11279.

[3] Andrew K. and Floren A. 2008. Lossless image compression via predictive coding of discrete Radon projections. Signal Processing: Image Communication. Vol. 23, No. 4, 313–324.

[4] Woods, R. C. 2008. Digital Image processing, 3rd (Ed.), Pearson Prentice Hall.

[5] Ping S. T. and Ricardo S. 2008. Graphics Image Compression Using JPEG2000. IEEE computer society Congress on Image and Signal Processing.

[6] Charilaos C., Athanassios S., and Touradj E. 2000. The JPEG 2000 still image coding system: an overview. IEEE Transactions on Consumer Electronics. Vol. 46, No. 4, 1103-1127.

[7] Diego, S. C. and Touradj E. 2000. An Analytical Study of JPEG2000 Functionalities. In Proc. of the IEEE International Conference on Image Processing. Vol. 2,49-52.

[8] Sayood, K. 2000. Introduction to data compression, 2nd (Ed.), Morgan Kaufman Publishers, Academic Press.

[9] Sana K., Kaıs O., and Noureddine E. 2009. A novel compression algorithm for electrocardiogram signals based on wavelet transform and SPIHT. International Scholarly and Scientific Research & Innovation. Vol. 3, NO. 11, 342-347.

[10] Marc A., Michel B., Pierre M., and Ingrid D. 1992. Image Coding Using Wavelet Transform. IEEE Transactions on Image Processing, Vol. 1 , No. 2, 205–220.

[11] Acharya T., and Tsai P. S. 2005. JPEG2000 standard for image compression: Concepts, algorithms and VLSI architectures. New York: Wiley.

[12] Thomas W. C. and Pantelimon S. 2009. Cryptographic Boolean Functions and Applications. San Diego, CA 92101-4495, USA.

[13] Kuo H. C., Yi C. C., Chung C. H., Chi W. H., and Chi J. C. 2009. Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application. IEEE Xplore Digital Library. 1922-1925.

[14] Xinmiao Z. and Keshab K. P. 2004. High-Speed VLSI Architectures for the AES Algorithm. IEEE TRANSACTIONS on Very large Scale integration (VLSI) Systems. Vol. 12, No. 9, 957-967.

[15] Muslim M. K. 2016. An Efficient Image Encryption Technique by Using Cascaded Combined Permutation. International Journal of Computer Science and Information Security (IJCSIS). Vol.14, No. 6, 576-588.

[16] Shujun L., Chengqing L., Guanrong C., Nikolaos G. B., and Kwok T. L.o. 2008. A General Quantitative Cryptanalysis of Permutation-only Multimedia Ciphers Against Plaintext Attacks. Signal Processing: Image Communication. Vol. 23, NO. 3, 212–223.

[17] Guanrong C., Yaobi M., and Charles K. C. 2004. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps. Chaos, Solitons and Fractals, Vol. 21, Issue 3, 749–761.

[18] K. S. Thyagarajan. 2011. Still Image and Video Compression with Matlab. John Wiley & Sons, Inc., Hoboken, New Jersey.

[19] Aatthew C. S., and K. J. Ray . 2010. Wavelet-Based Image Compression Anti-Forensics. In Proceedings of IEEE 17th international conference on image processing, Hong Kong, 1737–1740.

[20] Jaspreet S. and Prabhjot K. 2015. Image Encryption and Compression System Using Haar, Daubechies and Coiflet Wavelets. International Journal of Computer Science Engineering and Information Technology Research. Vol. 5, No. 5, 17-26.

[21] Yu K. C., Fan C. C., and Pohsiang T. 2001. A gray-level clustering reduction algorithm with the least PSNR. Expert Systems with Applications. Vol. 38, No.8, 10183–10187.

[22] Alexander T. 2014. Visual-PSNR measure of image quality Journal of Visual Communication and Image Representation. Vol. 25 No.5, 874–878.

[23] Medien Z., Mohsen M., Lazhar K., Adel B., and Rached Ti. 2007. A Modified AES Based Algorithm for Image Encryption. International Scholarly and Scientific Research & Innovation. Vol. 1, No. 3, 745-750.

[24] Guoji Z. and Qing L. 2011. A novel image encryption method based on total shuffling scheme. Optics Communications. Vol. 284 , No.12, 2775-2780.