Partial Encryption of Compressed Image Using Threshold Quantization and AES Cipher

Dr. Hameed A. Younis*, Dr. Abdulkareem Y. Abdalla*, Dr. Turki Y. Abdalla**

****Dept. of Computer Science, College of Science, University of Basrah, Basrah, Iraq.***
*****Dept. of Computer Engineering, College of Engineering, University of Basrah, Basrah, Iraq.***

Abstract

Cryptography is one of the technological means to provide security to data being transmitted on information and communication systems. When it is necessary to securely transmit data in limited bandwidth, both compression and encryption must be performed. Researchers have combined compression and encryption together to reduce the overall processing time.

In this paper, new partial encryption schemes are proposed to encrypt only part of the compressed image. Soft and hard threshold compression methods are used in the compression step and the Advanced Encryption Standard (AES) cipher is used for the encryption step. The effect of different threshold values on the performance of the proposed schemes are studied. The proposed partial encryption schemes are fast, secure, and do not reduce the compression performance of the underlying selected compression methods.

Keywords: Image, Partial encryption, AES cipher , Soft threshold quantization, Hard threshold quantization.

التشفير الجزئي للصور المضغوطة باستخدام تكميم العتبة وتشفير AES

د. حميد عبد الكريم يونس*، د. عبد الكريم يونس عبد الله*، د. تركي يونس عبد الله**

***قسم علوم الحاسبات، كلية العلوم، جامعة البصرة، البصرة، العراق.**

****قسم هندسة الحاسبات، كلية الهندسة، جامعة البصرة، البصرة، العراق.**

المستخلص:

التشفير يعتبر احد الوسائل التقنية التي تجهز البيانات المنقولة بالسرية عبر انظمة الاتصالات والمعلومات. عندما يكون من الضروري نقل البيانات بصورة سرية في عرض حزمة محدد, فانه يجب إنجاز كل من الضغط والتشفير معا. قام الباحثون بجمع الضغط والتشفير معا لتقليل زمن المعالجة الكلي.

في هذا البحث، اقترحت طريقة تشفير جزئي جديدة لتشفير جزء من الصورة المضغوطة. استخدمت في مرحلة الضغط، طريقة ضغط عتبة ناعمة وخشنة. وفي مرحلة التشفير، استخدمت طريقة التشفير القياسي المتقدم AES. ثم تمت دراسة تأثير قيم العتبة (threshold) المختلفة على انجازية التقنيات المقترحة. أنظمة التشفير الجزئي المقترحة كانت سريعة وذات سرية عالية كما إن انجازية الضغط لا تقل ضمن طرق الضغط المختارة.

الكلمات المفتاحية : صورة، تشفير جزئي، تشفير AES، تكميم عتبة ناعم، تكميم عتبة خشن.

1. Introduction

The use of image communication has increased dramatically in recent years. The World Wide Web and video conferencing are two examples. When communication bandwidth is limited, data is often compressed before transmission. If there is a need to protect the transmission from eavesdroppers, the transmission is also encrypted. For example, a wireless network often has limited bandwidth and its network traffic can easily be intercepted [1]. As a result, transmissions over a wireless network need to be compressed and encrypted.

Unfortunately, the processing time for encryption and decryption is a major factor in real-time image communication. In addition, the processing time required for compression and decompression of an associated image data is important. Encryption and decryption algorithms are too slow to handle the tremendous amount of data transmitted.

Ciphering of images is actually an important issue. One essential difference between text data and image data is that the size of image data is much larger than the text data. The time is a very important factor for the image encryption. We find it at two levels, one is the time to encrypt, the other is the time to transfer images. To minimize the time, the first step is to choose a robust, rapid and easy method to implement cryptosystem. The other important criterion concerns the method of compression is that to decrease the size of images without loss of image quality [2].

Wavelet Transform is one of the most powerful tools in digital signal processing. The image components are decomposed into different decomposition levels using a wavelet transform. These decomposition levels contain a number of subbands, which consist of coefficients that describe the horizontal and vertical spatial frequency characteristics of the original image component [3]. Power of 2 decompositions are allowed in the form of standard decomposition.

To perform the forward Discrete Wavelet Transform (DWT), the standard uses a two dimension (2-D) subband decomposition of a 2-D set of samples into low-pass samples and high-pass samples. Low-pass samples represent a downsampled low-resolution version of the original set. High-pass samples represent a downsampled residual version of the original set, needed for the perfect reconstruction of the original set from the low-pass set. It is mainly used to de-correlate the image data, so the resulting wavelet coefficients can be efficiently coded. It also has good energy compaction

capability that results in a high compression ratio [4].

The aim of algorithm proposed here is to combine image compression with encryption. Many researchers have examined the possibility of combining compression and encryption [1, 2, 5, 6]. In this paper, we propose two approaches of partial encryption to reduce encryption and decryption time in image communication [7].

2. Basic Principles

2.1 Advanced Encryption Standard (AES) Cipher

The AES cipher described by Rijndael (called also *Rijndael encryption algorithm*) [8, 9], it is a block cipher that converts cleartext data blocks of 128, 192, or 256 bits into ciphertext blocks of the same length. The AES cipher uses a key of selectable length (128, 192, or 256 bits). This encryption algorithm is organized as a set of iterations called *round transformations*. In each round, a data block is transformed by series of operations. The total number of rounds depends on the largest of round *r* and key length kl, and equals 10, 12, and 14 for lengths of 128, 192, and 256 bits, respectively. All round transformations are identical, apart from the final one. The AES algorithm takes the cipher key, and performs a key expansion routine to generate a key schedule. For number of round = 10 and key length = 128 bits, the key expansion generates a total of 44 words. The resulting key schedule consists of a linear array of 4-byte words, denoted by $[w_i]$, with i in the range $0 \le i < 44$.

2.2 Wavelet Transform

The wavelets transform have two terms, each one is a set of functions takes the forms [10, 11]:

$$\psi(x) = \sqrt{2} \sum_{k=-\infty}^{\infty} g_k \psi(2x - k) \quad \ldots (1)$$

$$\phi(x) = \sqrt{2} \sum_{k=-\infty}^{\infty} h_k \phi(2x - k) \quad \ldots (2)$$

These sets of functions are formed by dilation and translation of a single function $\boldsymbol{\psi(x)}$, called as the mother function or wavelet function in equation (1). The second function in equation (2) , $\boldsymbol{\phi(x)}$ is called the scale function. Where $\boldsymbol{g_k}$'s and $\boldsymbol{h_k}$'s are analysis filters coefficients [12-15]. Figure (1) shows the analysis and synthesis filters of a 2-D, 1-level of wavelet decomposition; where $\boldsymbol{h}$ and $\boldsymbol{g}$ are the synthesis filters. The upsampling process is indicated by $\uparrow 2$, and the downsampling process is indicated by $\downarrow 2$. The wavelet transform performs an octave subband decomposition of an image. The output of the first analysis stage is the low-

low (LL) subband (an approximation of the original image); the high-low (HL) subband (the horizontal detail); the low-high (LH) subband (the vertical details); and, the high-high (HH) subband (the diagonal details).

Wavelet analysis allows the use of long time intervals where we want more precise low-frequency information, and shorter regions where we want high-frequency information [11]. The low-frequency content is the most important part. It is what gives the signal its identity. The high-frequency content, on the other hand, imparts flavour or nuance. Subband coding is a coding strategy that tries to isolate different characteristics of a signal in a way that collects the signal energy into few components. This is referred to as energy compaction. Energy compaction is desirable because it is easier to efficiently code these components than the signal itself [16].

2.3 Threshold Quantization (THR Q)

Threshold quantization performs a quantization process of an image by using wavelet transform. It restores a compressed version of input image obtained by wavelet transform. Coefficients thresholding using global positive threshold value THR is applied. Wavelet decomposition is performed for n levels [17].

There are two types of thresholding process. The first type is *soft thresholding*, which is calculated by the following equation:

$$Y = \begin{cases} Sign(X)(|X| - THR), & if \quad |X| > THR \\ 0 \quad , & if \quad |X| \le THR \end{cases} \quad \ldots(3)$$

The second type is *hard thresholding*, which is calculated by the following equation:

$$Y = \begin{cases} X, & if \quad |X| > THR \\ 0, & if \quad |X| \le THR \end{cases} \quad \ldots(4)$$

Where : X is the input vector or matrix.
THR is the threshold value.
The quantization procedure contains three steps [17]:

1. Decomposition.
2. Detail coefficient thresholding. For each level from 1 to n, a threshold is selected and soft or hard thresholding is applied to the detail coefficients.
3. Reconstruction.

Figure (2) shows the threshold quantization.

3. Threshold Quantization-AES Partial Encryption Scheme (THR Q-AES-PE)

In this scheme, we propose a method for partial encryption of compressed image. The proposed method consists of wavelet transform (3 levels), quantization by soft or hard thresholding

to the detail coefficients, encryption of important part, then coding of resultant image by using run length.

In threshold quantization process, the detail coefficients (the LH, HL and HH subbands images) (unimportant parts) are thresholded, but the approximation coefficients are kept without thresholding as described in Section 2.3. In this scheme, only part of image (the LL subband image) (important part) is encrypted with AES cipher, whereas the remaining parts (unimportant parts) are transmitted without encryption.

In this scheme, a number of methods for partial encryption of compressed image will be used according to the threshold type:

a) Hard-Threshold Quantization-AES Partial Encryption Scheme (Hard-THR Q-AES-PE)

b) Soft-Threshold Quantization-AES Partial Encryption Scheme (Soft-THR Q-AES-PE)

Hard/Soft-THR Q-AES-PE Algorithm:

1. Encryption key selection.

2. Wavelet filter selection.

3. Threshold value selection.

4. Decomposition (filtering) the image, here discrete wavelet transform (3 levels) is used.

5. Quantization (here THR quantization process is applied).

6. Partial encryption, here AES cipher is used.

7. Entropy coding, here the run length coding is adopted.

4. Experimental Results

In this section, a number of experiments which are used to examine our proposed algorithms will be presented. The algorithms were programmed in MATLAB version 6.5 on a Pentium IV PC (2.4 GHz) using four grayscale images of (256×256) pixels.

Experiments

In these experiments, THR Q-AES partial encryption scheme is considered. Three different threshold values are chosen for these experiments, which are 20, 50 or 70.

The following proposed algorithms according to threshold type will be tested.

a) Hard-THR Q-AES-PE:

We propose here to quantize image by using hard threshold. Results obtained by applying this method are presented in Table (1). Figure (3) shows the results obtained for birds image.

In Table (1), the first column gives the threshold value. The second column gives the Compression Ratio (CR) for each test image (Lena, house, birds and boys).

Finally, the third column gives the Peak Signal-to-Noise Ratio (PSNR). The encryption key is "2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c". Only 1.5625% of the original data is encrypted for the test images.

b) Soft-THR Q-AES-PE:

We propose here to quantize image by using soft threshold. Results obtained by applying this method are presented in Table (2). Figure (4) shows the results obtained for birds image.

The encryption key is "2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c". Only 1.5625% of the original data is encrypted for the test images.

5. Conclusion

The attacker cannot obtain the original image unless he knows the encryption key. So, the proposed methods have good security since the keyspace is very large ($2^{128)}$.

Out of experiments, we find that as the threshold value is increased, both the CR and the PSNR are decreased. Figures (5 and 6) show PSNR versus the threshold value for Lena image by using Hard-THR Q-AES-PE and Soft-THR Q-AES-PE, respectively.

As shown in Figure (5), the diagram for the case of Hard-THR-Q-AES-PE is more suitable because the PSNR of the reconstructed image is large. When compared with results of other works such as [1, 2, 5, 6] , our approach gives an better security since it use small size of the original data is encrypted.

6. References

[1] Cheng H., *Partial Encryption for Image and Video Communication,* M.Sc. Thesis, Department of Computing Science, University of Alberta, Alberta, 1998.

[2] Borie J., Puech W., Dumas M., *"Crypto-Compression System for Secure Transfer of Medical Images",* 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.

[3] Uehara T., Safavi-Naini R., Ogunbona P.,*"Securing Wavelet Compression with Random Permutations",* In Proceedings of the 2000 IEEE Pacific Rim Conference on Multimedia, pp. 332-335, Sydney, 2000.

[4] Usevitch B. E., *"A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000",* IEEE Transactions on Image Processing Magazine, September 2001.

[5] Li X., Knipe J., Cheng H., "*Image Compression and Encryption Using Tree Structures*", Pattern Recognition Letters, Vol. 18, No. 11-13, pp. 1253-1259, 1997.

[6] Norcen R., Podesser M., Pommer A., Schmidt H., Uhl A., *"Confidential Storage and Transmission of Medical Image Data",* Computers in Biology and Medicine 33, pp. 277-292, 2003.

[7] Younis, H. A., *New Techniques For Partial Encryption of Wavelet-based Compressed and Uncompressed Images*, Ph.D. Thesis, Department of Computer Science, College of Science, University of Basrah, Basrah, November 2006.

[8] National Institute of Standards and Technology, FIPS-197-Advanced Encryption Standard (AES), November 2001.

[9] Stallings W., *Cryptography and Network Security, Principles and Practice,* Third Edition, Pearson Education International, Inc., USA, 2003.

[10] Antonini M., Barlaud M, Daubechies I., *"Image Coding Using Wavelet Transform",* IEEE Transactions on Image Processing, Vol. 1, No. 2, pp. 1716-1740, April 1992.

[11] Baxes G. A., *Digital Image Processing: Principles and Applications,* John Wiley & Sons, Inc., USA, 1994.

[12] Gonzalez R. C., Woods R. E., *Digital Image Processing,* Addision-Wesley, Inc., USA, 1992.

[13] Saha S., *"Image Compression-From DCT to Wavelet: A Review",* ACM Crossroads Student Magazine, The ACM's First Electronic Publication, 2001.

[14] Tang L., "*Methods for Encryption and Decryption MPEG Video Data Efficiently",* Proceedings of the Fourth ACM International Conference on Multimedia, pp. 219-229, 1997.

[15] Xiong Z., Ramchandran K., Orchard M. T., Zhang Y., *"A Comparative Study of DCT-and Wavelet-Based Image Coding",* IEEE Transactions on Circuits and Systems for Video Technology, Vol. 9, No. 5, August 1999.

[16] Usevitch B. E., *"A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000",* IEEE Transactions on Image Processing Magazine, September 2001.

[17] DeVore R. A., Jawerth B., Lucier B. J., *"Image Compression Through Wavelet Transform Coding",* IEEE Trans. on Info. Theory, Vol. 38, No. 2, pp. 719-746, 1992.

[18] Beegan A. P., *Wavelet-based Image Compression Using Human Visual System Models,* M.Sc. Thesis, Electrical Engineering Department, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, May 2001.

[19] Salomon D., *Data Compression, The Complete Reference,* Springer-Verlag, Inc., New York, 1998.

Figures and Tables

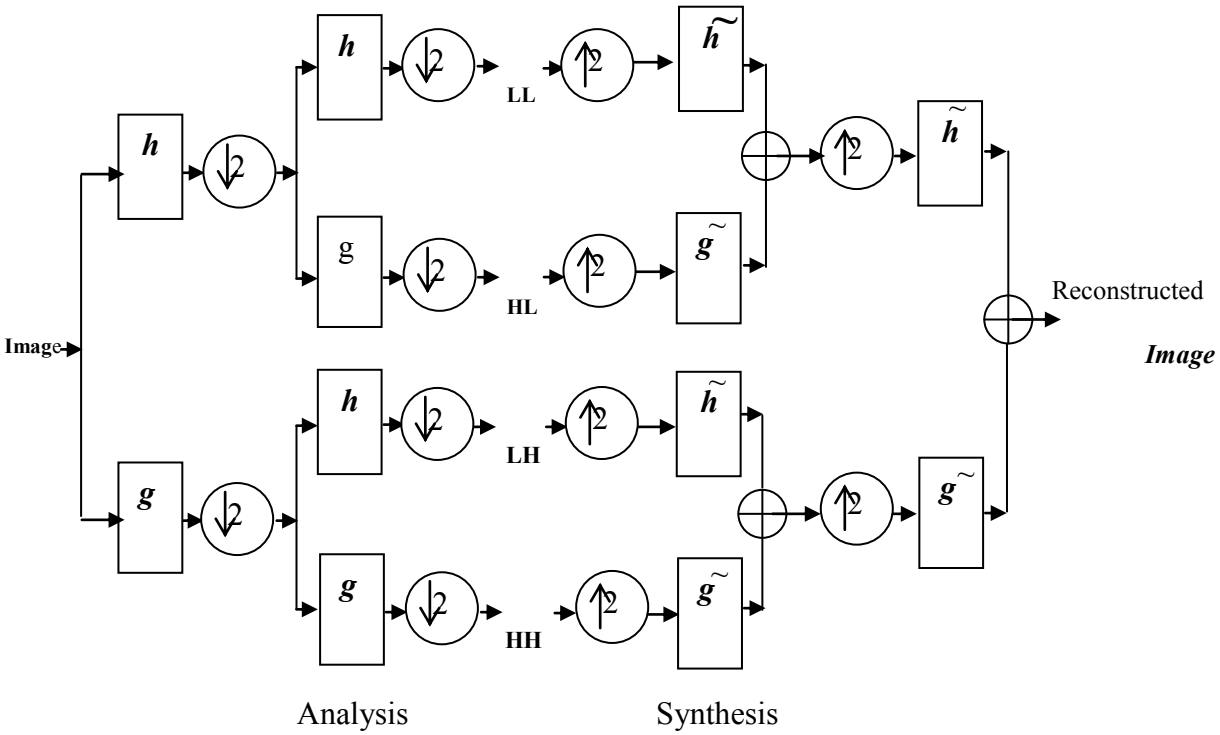

Figure (1): The analysis and synthesis of 2-D, 1-level discrete wavelet decomposition

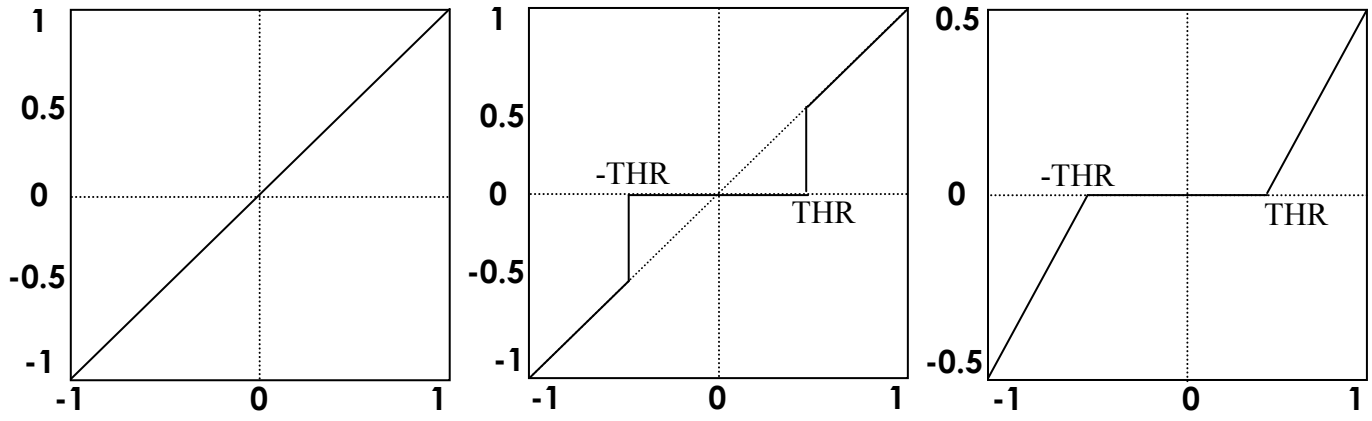

Figure (2): Shape of the Original Signal, its Hard, and its Soft, Thresholding.

Figure (3): Results of Hard-THR Q-AES.
(a) Original birds image
(b) Reconstructed image at threshold value = 20, PSNR = 34.0366 dB
(c) Reconstructed image at threshold value = 50, PSNR = 29.1742 dB
(d) Reconstructed image at threshold value = 70, PSNR = 27.5272 dB

Figure (4): Results of Soft-THR Q-AES-PE
(a) Original birds image
(b) Reconstructed image at threshold value = 20, PSNR = 30.6795 dB
(c) Reconstructed image at threshold value = 50, PSNR = 26.7930 dB
(d) Reconstructed image at threshold value = 70, PSNR = 25.6514 dB

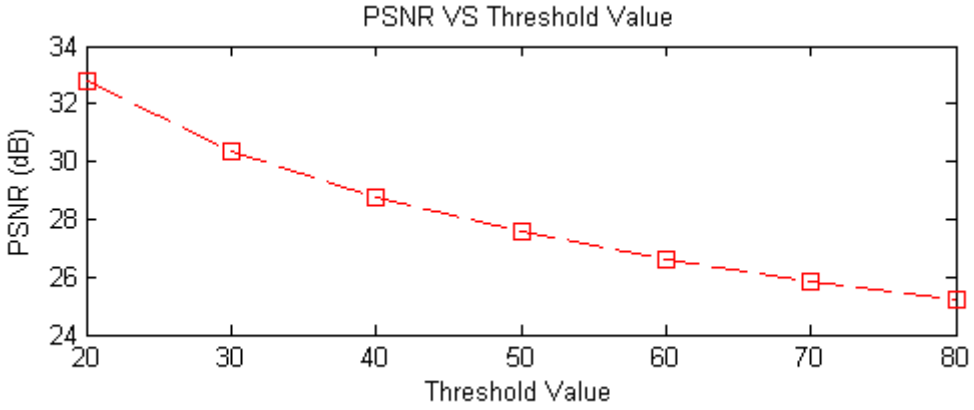

Figure (5): PSNR versus threshold value for Lena image using Hard-THR Q-AES-PE

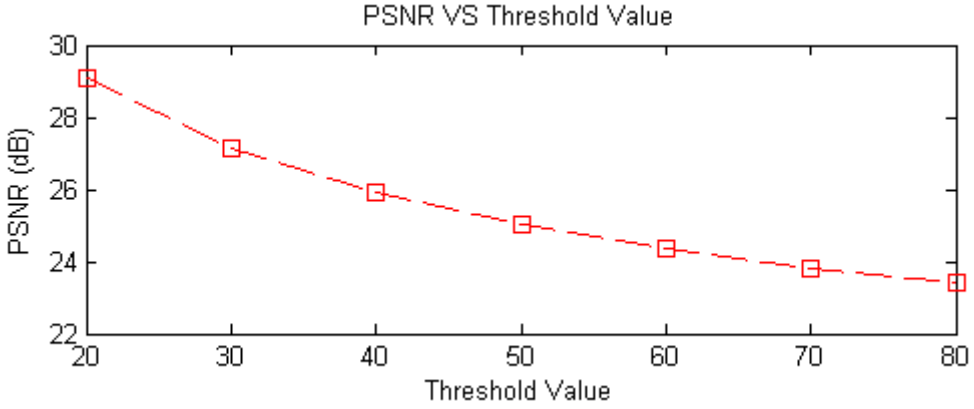

Figure (6): PSNR versus threshold value for Lena image using Soft-THR Q-AES-PE

Threshold Value	CR	PSNR (dB)
20	0.0993	32.8027
50	0.0391	27.5537
70	0.0259	25.8069

(a)

Threshold Value	CR	PSNR (dB)
20	0.0909	34.1044
50	0.0389	28.2790
70	0.0262	26.3141

(b)

Threshold Value	CR	PSNR (dB)
20	0.0650	34.0366
50	0.0275	29.1742
70	0.0193	27.5272

(c)

Threshold Value	CR	PSNR (dB)
20	0.0784	33.2195
50	0.0287	28.5604
70	0.0198	27.1585

(d)

Table (1): Experimental results for different threshold values of images using Hard-THR Q-AES.
(a) Lena (b) House (c) Birds (d) Boys

Threshold Value	CR	PSNR (dB)
20	0.0977	29.0964
50	0.0387	25.0146
70	0.0257	23.8283

(a)

Threshold Value	CR	PSNR (dB)
20	0.0897	29.8498
50	0.0386	25.3136
70	0.0260	23.9921

(b)

Threshold Value	CR	PSNR (dB)
20	0.0640	30.6795
50	0.0273	26.7930
70	0.0192	25.6514

(c)

Threshold Value	CR	PSNR (dB)
20	0.0773	30.0757
50	0.0284	26.5054
70	0.0196	25.4786

(d)

Table (2): Experimental results for different threshold values of images using Soft-THR Q-AES-PE.
(a) Lena (b) House (c) Birds (d) Boys