Vector Quantization Techniques For Partial Encryption of Wavelet-based Compressed Digital Images

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

The use of image communication has increased in recent years. In this paper, new partial encryption schemes are used to encrypt only part of the compressed data. Only 6.25-25% of the original data is encrypted for four different images, resulting in a significant reduction in encryption and decryption time. In the compression step, an advanced clustering analysis technique (Fuzzy C-means (FCM)) is used. In the encryption step, the permutation cipher is used. The effect of number of different clusters is studied. The proposed partial encryption schemes are fast and secure, and do not reduce the compression performance of the underlying selected compression methods as shown in experimental results and conclusion.

Keywords: Image, Partial encryption, Compression, FCM, Wavelet transform..

تقنيات التكميم الاتجاهي للتشفير الجزئي معتمدة على التحويل الموجي للصور الرقمية المضغوطة

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

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

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

المستخلص:

ازداد الاهتمام في اتصالات الصور في السنوات الأخيرة.في هذا البحث، اقترحت طرقا جديدة للتشفير الجزئي، والتي فيها تقـوم خوارزميـة التشفير بتشفير جزء من البيانات المضغوطة. حيث تم تشفير بحدود (6.25-25%) من البيانات الأصلية المستخدمة لأربع صور مختلفـة والـتي أدت إلى تقليل مهم في زمن التشفير وفك الشفرة. استخدمت في مرحلة الضغط،تقنيات متقدمة للتحليل عنقودي مثـل FCM . وفي مرحلـة التشفير تم استخدام طرق التشفير الابدالي. درس تأثير عناقيد مختلفة على انجازية التقنيات المقترحة. إن أنظمة التشفير الجزئي المقترحة تكون سـريعة وذات سرية عالية كما إنا لا تقلل من انجازيه الضغط والذي يكون ضمن طرق الضغط المستخدمة كما مبين في النتائج التجريبية والاستنتاج.

الكلمات المفتاحية : صورة، تشفير جزئي، ضغط، FCM ، تحليل موجي.

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. Traditionally, an appropriate compression algorithm is applied to the multimedia data and its output is encrypted by an independent encryption algorithm. This process must be reversed by the receiver.

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 several approaches of partial encryption to reduce encryption and decryption time in image communication [7]. In these approaches, only part of the compressed data is encrypted

2. Basic Principles

2.1 Permutation Cipher

In this system, the position of the plaintext letters in the massage rather than the letters of alphabet are permuted, while the permutation is the key. For the digital image the position of pixels are rearranged for different algorithms according to a key, such as image reversal, row transposition, column transposition, and block or matrix transposition [8].

2.2 Fuzzy C-Means (FCM) Algorithm

Fuzzy c-means (FCM) is a method of clustering which allows one piece of data to belong to two or more clusters [9-10]. This method is frequently used in pattern recognition. It is based on minimization of the following objective function:

$$J = \sum_{i=1}^{C} J_i = \sum_{i=1}^{C} \sum_{j=1}^{N} U_{ij}^{\,m} . d_{ij}^{\,2} \quad \ldots (1)$$

where:

C : no. of clusters.

N : no. of input vector.

U_{ij} : membership matrix.

m : fuzzifier [0, ∞], (let m = 2).

d_{ij} : distance between vector i and vector j. During our work, we use Euclidean distance:

$$d_{ij} = d(x_i, y_j) = \left[\sum_{p=1}^{P} (x_{ip} - y_{jp})^2 \right]^{1/2} \quad \ldots (2)$$

where: P is the length of vectors x_i و y_j.

The algorithm is composed of the following steps:

FCM Algorithm

1-Initialize the membership matrix U to random values, such that:

$$\sum_{j=1}^{C} U_{ij} = 1 \qquad , \forall \, i = 1, 2, 3, \ldots, N$$

and $U_{ij} \in [0, 1]$

2-Calculate the cluster centres C_j using

$$C_j = \frac{\sum_{i=1}^{N} U_{ij}^{\,m} . x_i}{\sum_{i=1}^{N} U_{ij}^{\,m}} \qquad , \forall j = 1, \ldots, C \quad \cdots (3)$$

3- Calculate the distance measure,

d_{ij}=|| x_i – C_j ||, for all clusters j=1, …, C and vectors x_i , i=1, ..., N.

4- Update the fuzzy membership matrix U according to d_{ij} so

if $d_{ij} > 0$ then

$$U_{ij} = \left[\sum_{k=1}^{C} \left(\frac{d_{ij}}{d_{ik}} \right)^{2/(m-1)} \right]^{-1} \quad \ldots(4)$$

If $d_{ij} = 0$ then

Vector x_i coincides with the cluster centre C_j, and so full membership can be set $U_{ij}=1$

5- Calculate J by using equation (1).

6- Repeat from 2 until the change in J is less than a given tolerance (tolerance here 0.01)

2.3 Wavelet Transform

Wavelet transform (WT) in the image processing can be considered as a subband decomposition [11-13]. Figure 3(a) shows the image wavelet decomposition diagram. The original image fL (x,y) is firstly filtered on the row by applying filter H (high-pass filter) and G (low-pass filter) and downsampled by keeping one column out of two. Two resulting images, the low-pass fL (x,y) and high-pass fH (x,y) outputs are obtained. Then, both of them are filtered along the column and upsampled by keeping one row out of two. It can be obtained one low-pass subband image denoted by fLL (x,y) and three high-pass subband images denoted by fLH (x,y), fHL (x,y) and fHH (x,y), respectively [14-19]. Finally, the image wavelet reconstruction is shown in Figure 3(b).

2.4 Wavelet Packet Transform (WPT)

The *wavelet packet* method [20-23] is a generalization of wavelet decomposition that offers a richer range of possibilities for signal analysis. In wavelet analysis, a signal is split into an approximation and a detail. The approximation is then itself split into a second-level approximation and detail, and the process is repeated. For an *n*-level decomposition, there are *n+1* possible ways to decompose or encode the signal as shown in Figure (2).

In wavelet packet analysis, the details as well as the approximations can be split. This yields equal to $2^{2^{n-1}}$ different ways to encode the signal. The *wavelet packet decomposition tree* is shown in Figure (3).

3. The Proposed Vector Quantization Partial Encryption Scheme (VQ-PE)

In this scheme, a method that consists of FCM vector quantization and Permutation cipher is proposed.

VQ process generates a codebook. Compression is achieved by

using the index of the codewords for the purpose of storage and transmission. FCM is described in section (2.2). Only the first part of codebook (important part) is encrypted with Permutation cipher, whereas the remaining parts (unimportant parts) are transmitted without encryption.

In the proposed scheme, a number of methods for partial encryption of compressed image are tested:

a) Vector Quantization-Permutation Partial Encryption Scheme (VQ-Permutation-PE)

VQ-Permutation-PE Algorithm:

1. Encryption key selection.

2. Quantization, here FCM vector quantization process is applied.

3. Partial encryption, here Permutation cipher is used.

b) Wavelet-based Vector Quantization-Permutation Partial Encryption Scheme (Wavelet-based-VQ-Permutation-PE)

This method consists of wavelet transform (1 level), quantization by FCM to the HL and LH subband images, Permutation cipher and arithmetic coding to the LL subband image. Finally, the HH subband image is given zeroes as shown in Figure (4).

In this method, only part of image (the LL subband image) (important part) is encrypted with Permutation cipher, whereas the remaining parts (unimportant parts) are transmitted without encryption.

Wavelet-based-VQ-Permutation-PE Algorithm:

1. Encryption key selection.

2. Wavelet filter selection.

3. Decomposition (filtering) the image, here discrete wavelet transform (1 level) is used.

4. Quantization, here FCM vector quantization process is applied.

5. Partial encryption, here Permutation cipher is used.

6. Entropy coding, here the arithmetic coding is adopted.

c) Wavelet Packet-based Vector Quantization-Permutation Partial Encryption Scheme (Wavelet Packet-based-VQ-Permutation-PE)

This proposed method consists of wavelet packet transform (2 levels), quantization by FCM to the HL and LH subband images, Permutation cipher and arithmetic coding to the LLLL subband image. Finally, the HH, HLHH and LHHH subband images are given zeroes as shown in Figure (5).

In this method, only part of image (the LLLL subband image) (important part) is encrypted with Permutation cipher, whereas the remaining parts (unimportant parts) are transmitted without encryption.

Wavelet Packet-based-VQ-Permutation-PE Algorithm:

1. Encryption key selection.

2. Wavelet filter selection.

3. Decomposition (filtering) the image, here wavelet packet transform (2

levels) is used.

4. Quantization, here FCM vector quantization process is applied.

5. Partial encryption, here Permutation cipher is used.

6. Entropy coding, here the arithmetic 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.

To evaluate each of the proposed schemes, five aspects are examined [1]:

i. **Security**. Security in this work means confidentiality and robustness against attacks to break the images. It is obvious that the goal is not 100% security, but many advanced algorithms are adopted, such as AES, and Stream ciphers that make them difficult to cryptanalyze.

ii. **Speed**. Less data (important part) to encrypt means less CPU time required for encryption. So, in general partial encryption algorithms are used to reduce encryption and decryption time.

iii. **Compression Performance**. Compression performance of the selected compression methods is used to reduce bandwidth required for data transmission. The proposed encryption schemes do not reduce the compression performance of the underlying selected compression methods. Peak Signal to Noise Ratio (PSNR) measures are estimate of the quality of a reconstructed image compared to an original image. Typical PSNR values ranges between 20 and 40 decibels (dB) [15].

iv. **PSNR**

PSNR is the standard method for quantitatively comparing a compressed image with the original. For an 8-bit grayscale image, the peak signal value is 255. Hence, the PSNR of an M×N 8-bit

grayscale image x and its reconstruction $\hat{x}$ is calculated as:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad \ldots (5)$$

where the Mean Square Error (MSE) is defined as [25]:

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[x(m,n) - \hat{x}(m,n)]^2 \quad \ldots (6)$$

PSNR is measured in decibels (dB), M: height of the image, N: width of the image.

v. **Compression Ratio (CR)**

The method of comparing the compressed and the original images is the compression ratio. It is defined as [25]:

$$Compression\ \ Ratio = \frac{Compressed\ \ File}{Uncompressed\ \ File} \ldots (7)$$

Experiments

In these experiments, VQ partial encryption scheme is considered. Three different cluster numbers, which are 20, 50 or 256 clusters are chosen for these experiments. In these experiments, the proposed partial encryption algorithm will be performed as follows:

a) VQ-Permutation-PE:

We propose here to encrypt the important part by using Permutation cipher. Results obtained by applying this method are presented in Table (1). Figure (6) shows the results obtained for birds image.

In Table (1), the first column gives the number of clusters. The second column gives the CR. Finally, the third column gives the PSNR. The encryption key has positions of 8204 pixels randomly generated. Only 12.5% of the original data is encrypted for the test images.

b) Wavelet-based-VQ-Permutation-PE:

In this scheme, wavelet transform (1 level) is first made. The proposed encryption algorithm presented in section (2.2) is applied. Results of this method are presented in Table (2). Figure (7) shows the results obtained for birds image.

The encryption key contains positions of 16409 pixels randomly generated. Only 25% of the original data is encrypted for the test images.

c) c) Wavelet Packet-based-VQ-Permutation-PE:

I In this scheme, wavelet packet transform (2 levels) is first made, the proposed encryption algorithm presented in section (2.2) is applied. Results of this method are presented in Table (3). Figure (8) shows the result obtained for birds image.

The encryption key consists of positions of 4096 random pixels. Only 6.25% of the original data is encrypted for the test images.

5. Conclusion

In all experiments, 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.

Out of experiments, we conclude that as the number of clusters in the codebook increases, both PSNR value and execution time and CR increase as well. Figures (9, 10 and 11) show PSNR versus the number of clusters for Lena image using VQ-Permutation-PE, Wavelet-based-VQ-Permutation-PE and Wavelet packet-based-VQ-Permutation-PE, respectively.

As shown in Figure (10), the diagram for the case of Wavelet-based - VQ-Permutation-PE is more suitable because the PSNR of the reconstructed image is large.

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., and 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., and 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., and 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., and 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] **Stallings W.,**
"Cryptography and Network Security, Principles and Practice", Third Edition,

Pearson Education International, Inc., USA, 2003.

[9] **Hoppner F.,**
"Fuzzy Clustering", Advances in Intelligent Data Analysis V. Springer, Berlin, pp. 254-264, Oct. 2003.

[10] **T. Rashid,**
"A Tutorial on Clustering Algorithms: Fuzzy C-means Clustering", http://www.cs.bris.ac.uk/home/trl690/documentation/fuzzy_clustering_intial_report/node11.html

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

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

[13] **Varma K., and Bell A.,**
"JPEG2000-Choices and Tradeoffs For Encoders", IEEE Transactions on Image Processing Magazine, November 2004.

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

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

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

[17] **Xiong Z., Ramchandran K., Orchard M. T., and 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.

[18] **Blelloch G. E.,**
"Introduction to Data Compression",
Computer Science Department, Carnegie Mellon University, October 2001.
E-mail: blelloch@cs.cmu.edu.

[19] **Umbaugh S. E.,**
"Computer Vision and Image Processing", Prentice-Hall, Inc., USA, 1998.

[20] **Fisch M. M., Stögner H., and Uhl A.,**
"Layered Encryption Techniques for DCT-Coded Visual Data", In Proceedings (CD-ROM) of the European Signal Processing Conference, EUSIPCO '04, Vienna, Austria, September 2004.

[21] **Pommer A., and Uhl A.,**
"Selective Encryption of Wavelet Packet Subband Structure for Secure Transmission of Visual Data", ACM

Multimedia System Journal, pp. 67-70, 2002.

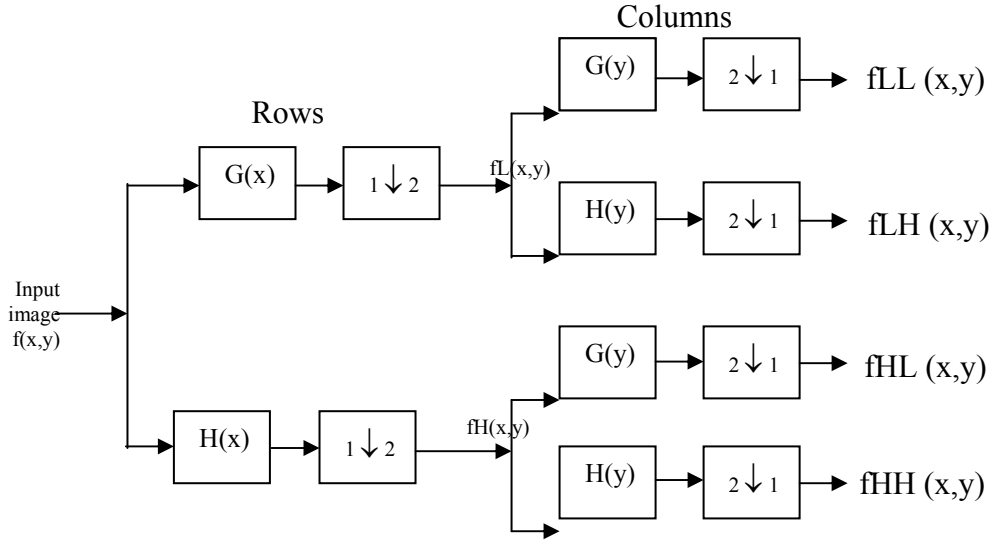
[22] **Pommer A., and Uhl A.,**
"Selective Encryption of Wavelet-packet Encoded Image Data- Efficiency and Security", ACM Multimedia Systems Journal, 9 (3), pp. 279-287, 2003.

[23] **Umbaugh S. E.,**
"Computer Vision and Image Processing", Prentice-Hall, Inc., USA, 1998.

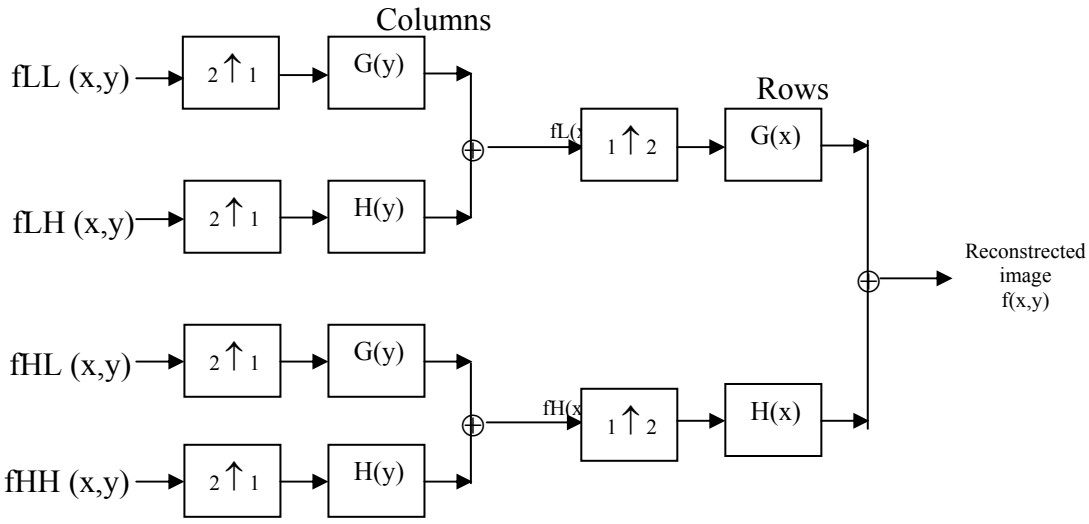
[24] **Beegan A. P.,**
"Wavelet-based Image Compression Using Human Visual System Models"
M.Sc. Thesis, Electrical Engineering Department, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, May 2001.

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

Figures and Tables



(a) Image Wavelet Decomposition



(b) Image Wavelet Reconstructed.

x	: convolve (rows and colomns) with the filter x
1↓2	: keep one column out of two
2↓1	: keep one row out of two
1↑2	: put one column of zeros between each column
2↑1	: put one row of zeros between each row

Figure (1): Image Wavelet Transform and Its Inverse

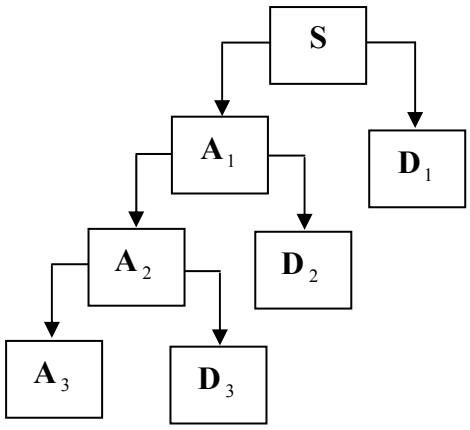


Figure (2): Wavelet Tree

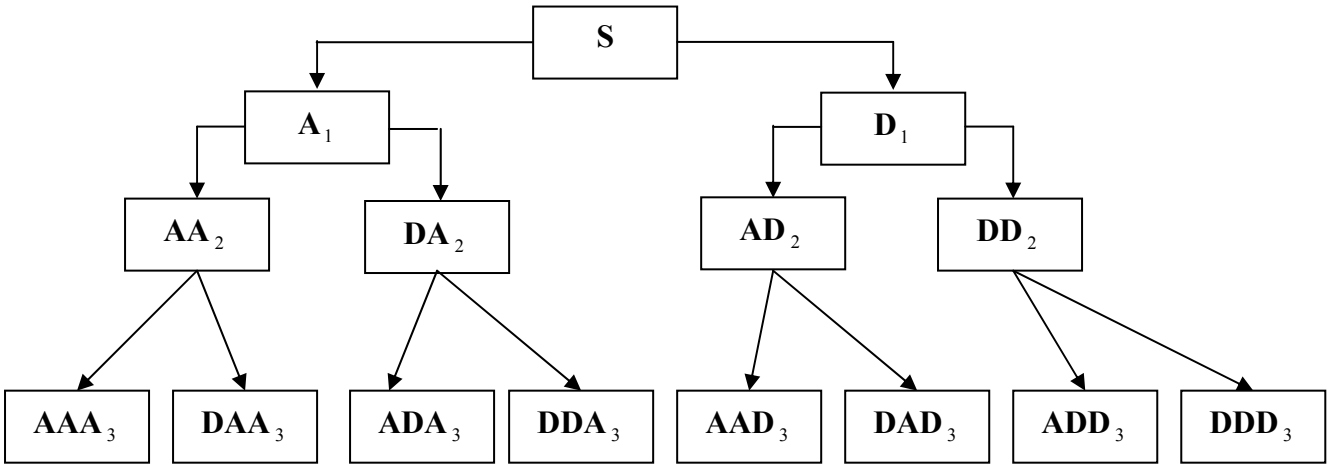


Figure (3): Wavelet Packet Decomposition Tree

LL	HL
LH	HH

Figure (4): Wavelet subband images of 2-D, 1-level.

LLLL	LLHL	HLLL	HLHL
LLLH	LLHH	HLLH	HLHH
LHLL	LHHL	HHLL	HHHL
LHLH	LHHH	HHLH	HHHH

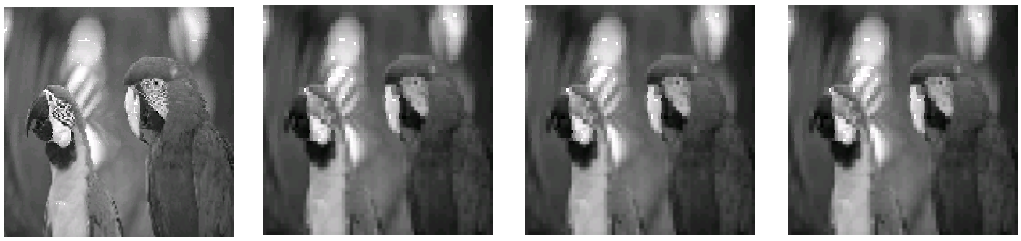
Figure (5): Wavelet packet subband images of 2-D, 2-levels.

(a) (b) (c) (d)

Figure (6): Results of VQ-Permutation-PE.
(a) Original birds image
(b) Reconstructed image at number of clusters = 20, PSNR = 27.4190 dB
(c) Reconstructed image at number of clusters = 50, PSNR = 27.6315 dB
(d) Reconstructed image at number of clusters = 256, PSNR = 27.5957 dB

(a) (b) (c) (d)

Figure (7): Results of Wavelet-based-VQ-Permutation-PE.
(a) Original birds image
(b) Reconstructed image at number of clusters = 20, PSNR = 27.7545 dB
(c) Reconstructed image at number of clusters = 50, PSNR = 27.7550 dB
(d) Reconstructed image at number of clusters = 256, PSNR = 27.7600 dB



(a) (b) (c) (d)

Figure (8): Results of Wavelet packet-based-VQ-Permutation-PE
(a) Original birds image
(b) Reconstructed image at number of clusters = 20, PSNR = 25.4427 dB
(c) Reconstructed image at number of clusters = 50, PSNR = 25.4431 dB
(d) Reconstructed image at number of clusters = 256, PSNR = 25.445

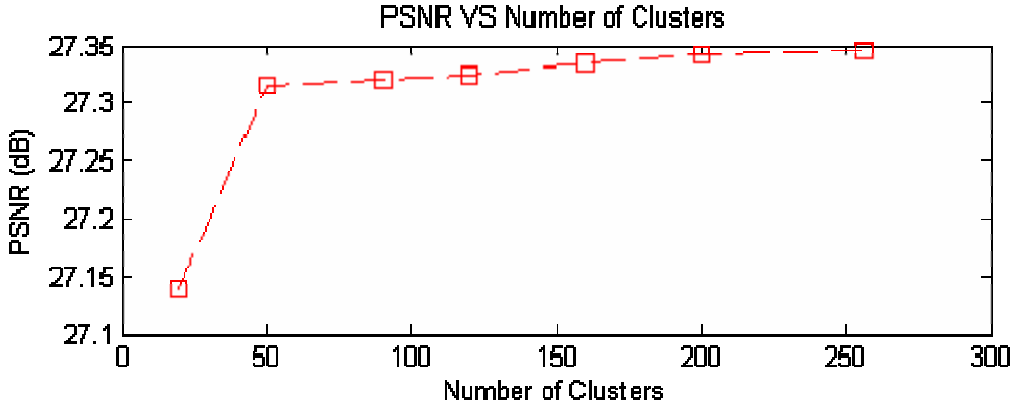


Figure (9): PSNR versus number of clusters for Lena image using VQ-Permutation-PE

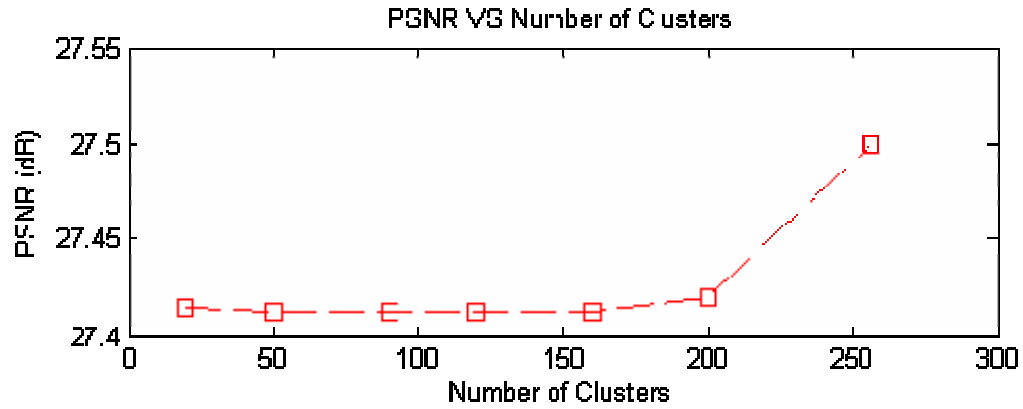


Figure (10): PSNR versus number of clusters for Lena image using Wavelet-based-VQ-Permutation-PE

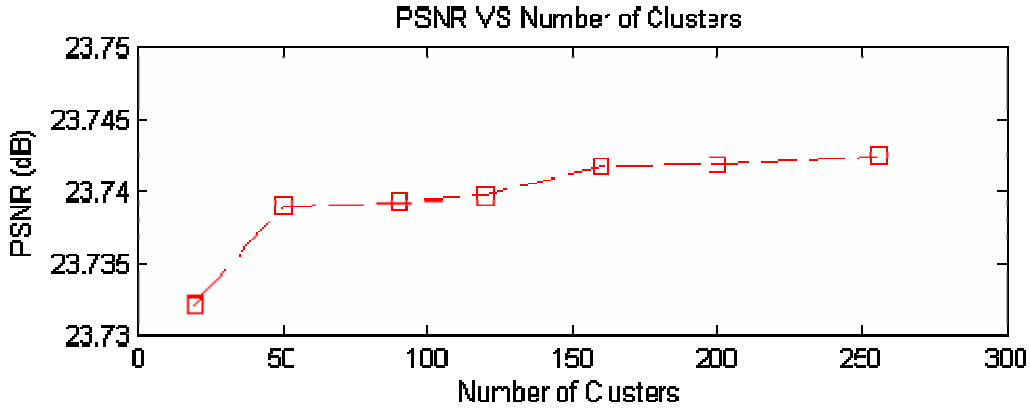


Figure (11): PSNR versus number of clusters for Lena image using Wavelet packet-based-VQ-Permutation-PE

Table (1): Experimental results for different clusters numbers of images using VQ-Permutation-PE.

(a) Lena (b) House (c) Birds (d) Boys

Number of Clusters	CR	PSNR (dB)
20	0.2512	27.1397
50	0.2531	27.3162
256	0.2656	27.3361

(a)

Number of Clusters	CR	PSNR (dB)
20	0.2512	25.7261
50	0.2513	26.0146
256	0.2656	26.0228

(b)

Number of Clusters	CR	PSNR (dB)
20	0.2512	27.4190
50	0.2531	27.6315
256	0.2656	27.5957

(c)

Number of Clusters	CR	PSNR (dB)
20	0.2512	29.5933
50	0.2531	29.9258
256	0.2656	29.9262

(d)

Table (2): Experimental results for different clusters numbers of images using Wavelet-based-VQ-Permutation-PE.
(a) Lena (b) House (c) Birds (d) Boys

Number of Clusters	CR	PSNR (dB)
20	0.6267	27.4154
50	0.6414	27.4200
256	0.7419	27.5000

(a)

Number of Clusters	CR	PSNR (dB)
20	0.6455	26.1168
50	0.6602	26.1170
256	0.7607	26.1180

(b)

Number of Clusters	CR	PSNR (dB)
20	0.6095	27.7545
50	0.6241	27.7550
256	0.7247	27.7600

(c)

Number of Clusters	CR	PSNR (dB)
20	0.6665	30.0871
50	0.6812	30.1000
256	0.7817	30.1500

(d)

Table (3): Experimental results for different clusters numbers of images using Wavelet packet-based-VQ-Permutation-PE.
(a) Lena (b) House (c) Birds (d) Boys

Number of Clusters	CR	PSNR (dB)
20	0.1196	23.7322
50	0.1819	23.7392
256	0.6094	23.7396

(a)

Number of Clusters	CR	PSNR (dB)
20	0.1196	22.7771
50	0.1819	22.7798
256	0.6094	22.7800

(b)

Number of Clusters	CR	PSNR (dB)
20	0.1196	25.4427
50	0.1819	25.4431
256	0.6094	25.4450

(c)

Number of Clusters	CR	PSNR (dB)
20	0.1196	26.2787
50	0.1819	26.2789
256	0.6094	26.2900

(d)