Bitplane 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 3.125-12.5% of the original data is encrypted for four different images, resulting in a significant reduction in encryption and decryption time. In the compression step, the bitplane coding technique is used. In the encryption step the Advanced Encryption Standard (AES) cipher is used. The effect of the number of different bitplane levels on the performance of the proposed techniques is studied. The proposed partial encryption schemes are fast and secure, and do not reduce the compression performance of the underlying selected compression methods.

Keywords: Image, Partial encryption, AES cipher , Bitplane coding.

تقنيات مستوى البت للتشفير الجزئي معتمدة على التحويل المويجي للصور الرقمية المضغوطة

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

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

[**]قسم 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 تقوم خوارزمية التشفير بتشفير جزء من البيانات. وشفر بحدود (3.125-12.5%) من البيانات الأصلية المستخدمة (أربع صور مختلفة) للحصول على تقليل مهم في زمن التشفير وفك الشفرة. استخدمت في مرحلة الضغط، تقنيات ترميز مستوى البت. وفي مرحلة التشفير، استخدمت طرق تشفير متقدمة (التشفير القياسي المتقدم AES). درست تأثير مستويات بتات مختلفة على انجازية التقنيات المقترحة. أنظمة التشفير الجزئي المقترحة تكون سريعة وذات سرية عالية كما إن انجازية الضغط لا تقل ضمن طرق الضغط المختارة.**

الكلمات المفتاحية : صورة، تشفير جزئي، تشفير AES، ترميز مستوى البت.

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 and the nature of data (0..255) in image and characters in text. 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 DWT, the standard uses a 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 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 [wi], with i in the range 0 $\leq$ i < 44.

2.2 Wavelet Transform

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

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

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

These sets of functions are formed by dilation and translation of a single function ***ψ (x)***, called as the mother function or wavelet function in equation (1).The second function in equation (2) , ***ϕ (x)*** is called the scale function. Where $\boldsymbol{g_k}$'s and $\boldsymbol{h_k}$'s are analysis filters coefficients with ***h*** and ***g*** be the analysis filters [12, 13, 14, 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 $\uparrow\mathbf{2}$, and the downsampling process is indicated by $\downarrow\mathbf{2}$. 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 Bitplane Coding

This technique is used for removing coding redundancy and attaching inter pixel redundancy. It is based on the concept of decomposing a multilevel (monochrome or color) image into a series of binary images and compressing each binary image via one of several well–known binary compression methods. In order to be compress grayscale images with bitplane coding, the grayscale images are split into a bitplane representation (e.g. 8 bitplanes for a 8 bpp grayscale image as shown in Figure (2), subsequentialy the bitplanes are compressed independently.

In Figure (2), the eight bit planes corresponding to an 8-bit image are shown. Each bit plane is displayed as an image by using white if the corresponding bit is 1 and black if the bit is 0. Here, we see that the lower bit planes contain little information and can be eliminated with no significant information loss [17].

3. Bitplane-AES Partial Encryption Scheme (Bitplane-AES-PE)

In this scheme, a proposed method consists of bitplane coding, encryption of important part and coding of resultant image by using arithmetic coding will be presented.

Bitplane coding is splitting an 8bpp image into its 8 bitplanes as described in section (2.3).

In this method, only part of image (important part) is encrypted with AES cipher, while the remaining parts (unimportant parts) are transmitted without encryption. The important part of the bitstream of image is selected by two approaches:

a) One bitplane (i.e., bitplane 1) (Single-Bitplane-AES-PE)
b) Multi-bitplanes from any bitplane number to the last bitplane (i.e., 1-8 bitplanes) (Multi-Bitplane-AES-PE).

Single/Multi-Bitplane-AES-PE Algorithm:

1. Encryption key selection.

2. Bitplane number selection.

3. Entropy coding, here the bitplane coding is performed.

4. Partial encryption, here AES cipher is used.

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

In addition to these methods, we also suggest a method that uses wavelet transform called (**Wavelet-Bitplane-AES-PE**) as follows:

The method consists of wavelet transform (1 level), coding by bitplane coding, encryption of important part, then another coding of resultant image by using arithmetic coding.

In this scheme, only part of image LL is coded by bitplane coding (one bitplane) (important part) is encrypted with AES cipher, while the remaining parts (unimportant parts) are transmitted without encryption.

Wavelet-Bitplane-AES-PE Algorithm:

1. Encryption key selection.

2. Bitplane number selection.

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

level) is used.

4. Entropy coding, here the bitplane coding is performed.

5. Partial encryption, here AES 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]:

1. **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.

2. **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.

3. **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. PSNR measures are estimates of the quality of a reconstructed image compared to an original image. Typical PSNR values ranges between 20 and 40 decibels (dB) [13].

4. **PSNR**

Peak signal-to-noise ratio (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:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad ...\ (3)$$

where the Mean Square Error (MSE) is defined as [18]:

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[x(m,n) - \hat{x}(m,n)\right]^2 \qquad ...\ (4)$$

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

5. **Compression Ratio (CR)**

The method of comparing the compressed and the original images is the compression ratio. It is defined as [19]:

$$Compression \quad Ratio = \frac{Compressed \quad File}{Uncompressed \quad File} \ldots (5)$$

Experiments

In these experiments, Bitplane-AES partial encryption is considered. Eight different bitplanes are chosen in these experiments. They are bitplane 1, bitplane 2, ……, bitplane 7 and bitplane 8.

We propose here to encrypt a selected part by using AES cipher by different methods:

a) **Single-Bitplane-AES-PE:**

We propose here to encrypt one bitplane. Results obtained by applying this method are presented in Table (1). Figure

(3) shows the result obtained for birds image.

In Table (1), the first column gives the encrypted bitplane. The second column gives the CR for each test image (Lena, house, birds and boys). The encryption key is “2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c”. Only 12.5% of the original data is encrypted for the test images. PSNR of the reconstructed Lena image is 33.9117 dB.

In this scheme, it is also suggested to improve the performance by using wavelet transform (1 level) (**Wavelet-based-Bitplane-AES-PE**). 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 3.125% of the original data is encrypted for the test images. PSNR of the reconstructed Lena image is 30.8867 dB.

b) Multi-Bitplane-AES-PE:

We propose here to encrypt more than one bitplane from any bitplane number to bitplane 8. Results obtained by applying this method are presented in Table (3). Figure (5) 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 12.5%, 25%, 37.5%, 50%, 62.5%, 75%, 87.5% or 100% of the original data is encrypted for the test images. PSNR of the reconstructed Lena image is 34.2369 dB.

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 Single-Bitplane-AES-PE results, we conclude that if the degree of importance of the bitplane increases, the CR increases as well. Figures (6 and 7) show CR versus encrypted plane for Lena image using Single-Bitplane-AES-PE and Wavelet-Bitplane-AES-PE, respectively.

Results of Multi-Bitplane-AES-PE indicate that as the number of planes increases, CR increases. Figure (8) shows CR versus the number of encrypted planes for Lena image using Multi-Bitplane-AES-PE.

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] **Baxes G. A.,**

“Digital Image Processing: Principles and Applications”, John Wiley & Sons, Inc., USA, 1994.]

[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

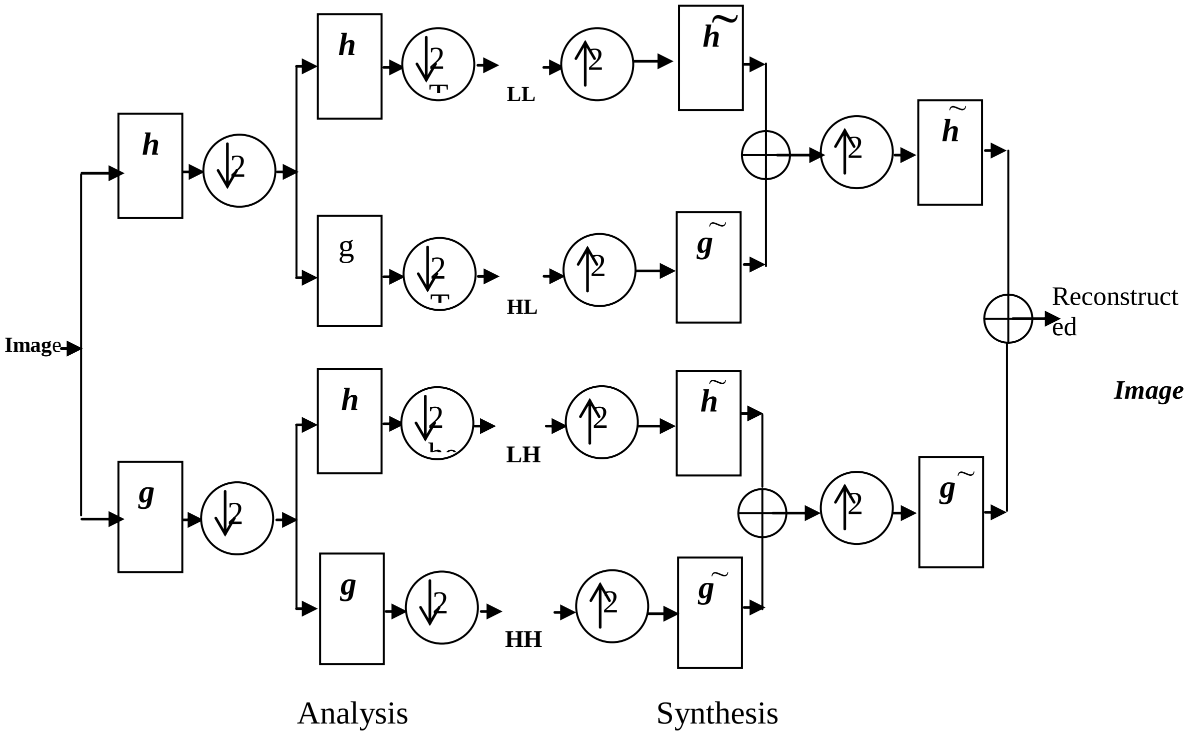
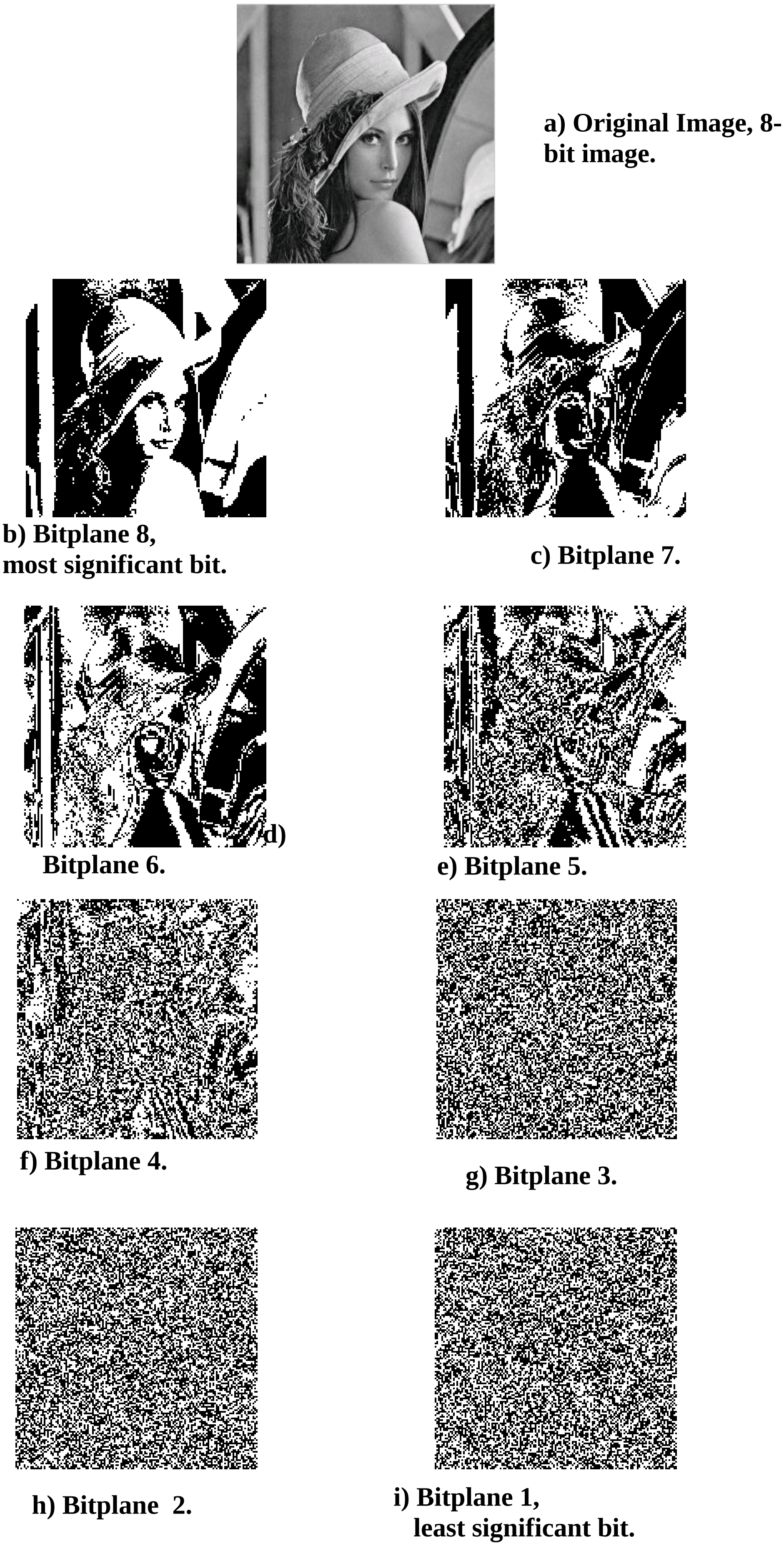


Figure (1): The analysis and synthesis of 2-D, 1-level discrete wavelet decomposition



a) Original Image, 8-bit image.

b) Bitplane 8,
most significant bit.

c) Bitplane 7.

d) Bitplane 6.

e) Bitplane 5.

f) Bitplane 4.

g) Bitplane 3.

h) Bitplane 2.

i) Bitplane 1,
least significant bit.

Figure (2): Splitting an 8bpp image into its 8 bitplanes

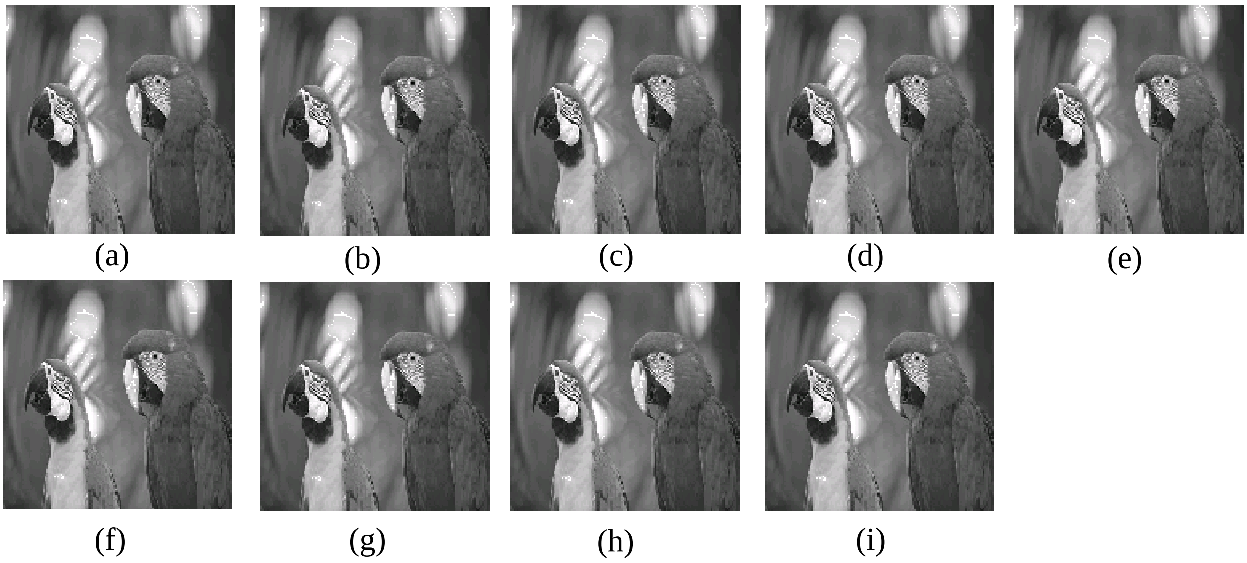


Figure (3): Results of Single-Bitplane-AES-PE
(a) Original birds image
(b) Reconstructed image at bitplane = 1
(c) Reconstructed image at bitplane = 2
(d) Reconstructed image at bitplane = 3
(e) Reconstructed image at bitplane = 4
(f) Reconstructed image at bitplane = 5
(g) Reconstructed image at bitplane = 6
(h) Reconstructed image at bitplane = 7
(i) Reconstructed image at bitplane = 8

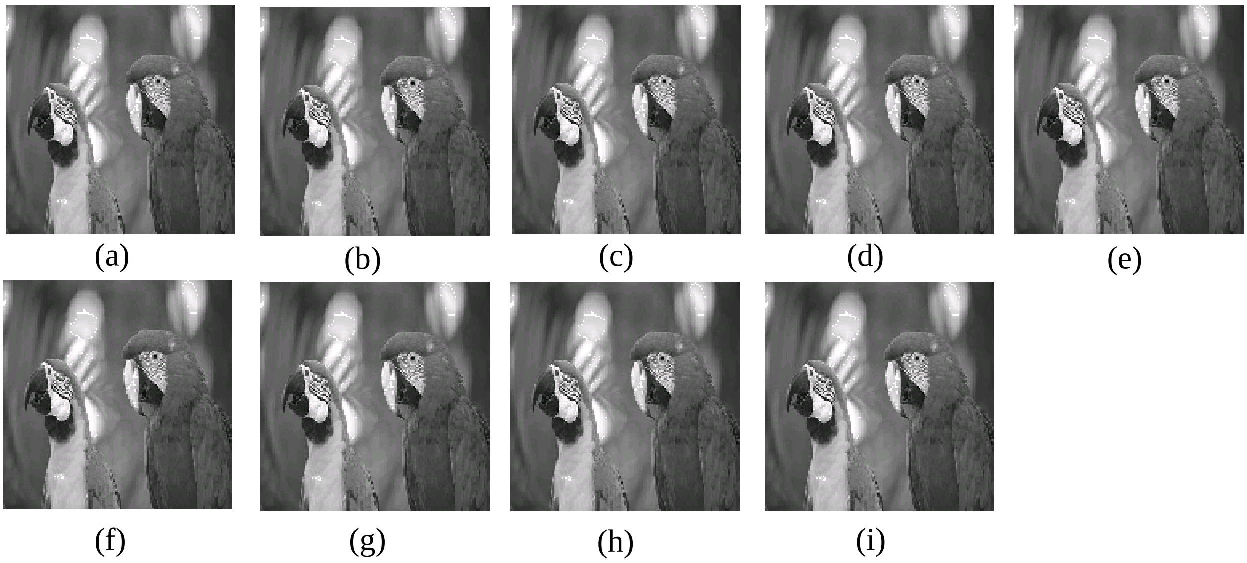


Figure (4): Results of Wavelet-based-Bitplane-AES-PE
(a) Original birds image
(b) Reconstructed image at bitplane = 1
(c) Reconstructed image at bitplane = 2
(d) Reconstructed image at bitplane = 3
(e) Reconstructed image at bitplane = 4
(f) Reconstructed image at bitplane = 5
(g) Reconstructed image at bitplane = 6
(h) Reconstructed image at bitplane = 7
(i) Reconstructed image at bitplane = 8

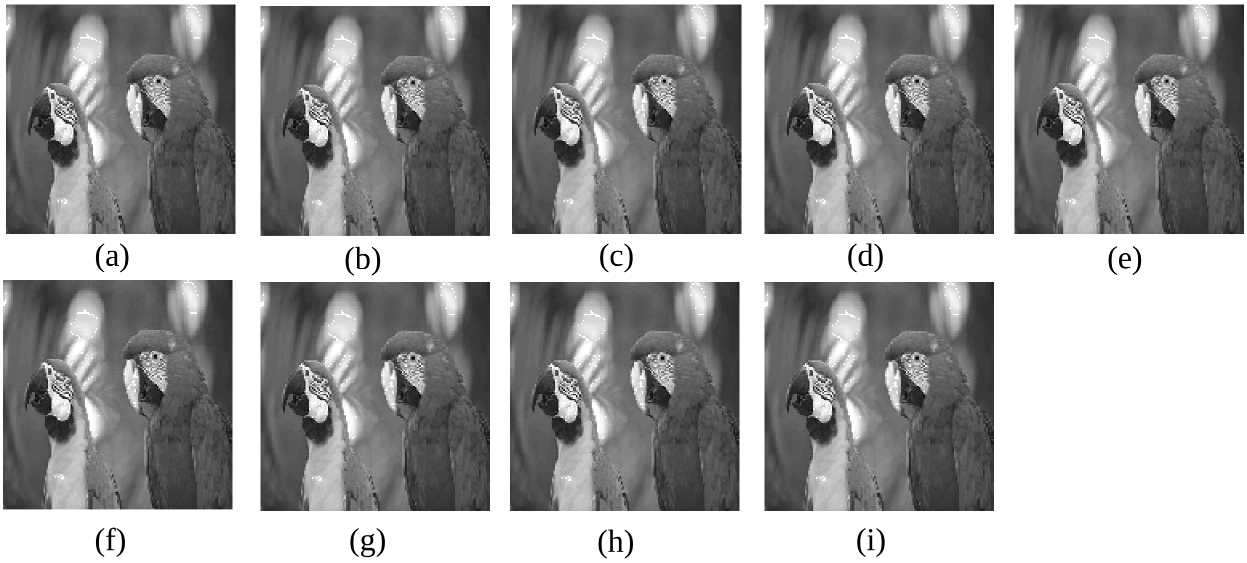


Figure (5): Results of Multi-bitplane-AES-PE

(a) Original birds image
(b) Reconstructed image at bitplanes = 8-8
(c) Reconstructed image at bitplanes = 7-8
(d) Reconstructed image at bitplanes = 6-8
(e) Reconstructed image at bitplanes = 5-8
(f) Reconstructed image at bitplanes = 4-8
(g) Reconstructed image at bitplanes = 3-8
(h) Reconstructed image at bitplanes = 2-8
(i) Reconstructed image at bitplanes = 1-8

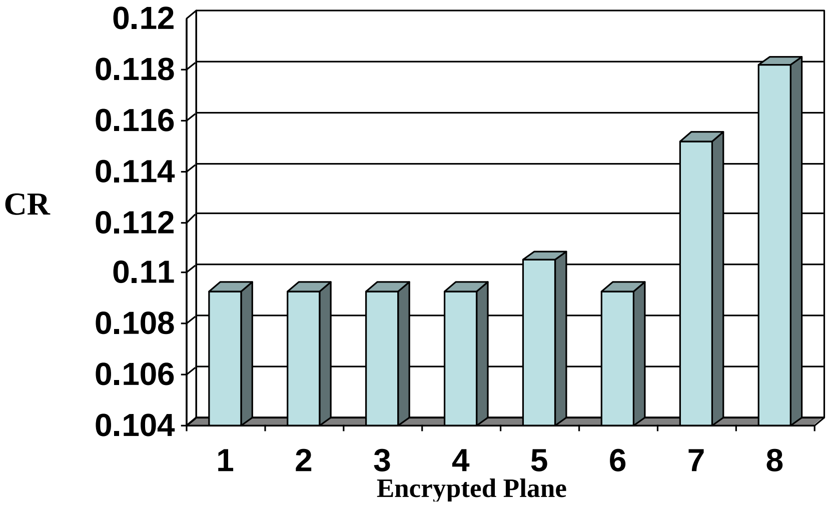


Figure (6): CR versus encrypted plane for Lena image using Single-Bitplane-AES-PE

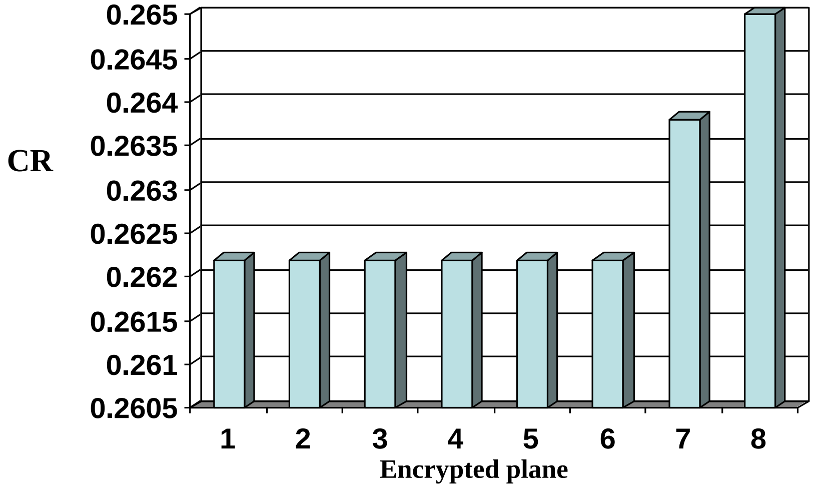


Figure (7): CR versus encrypted plane for Lena image using Wavelet-based-Bitplane-AES-PE

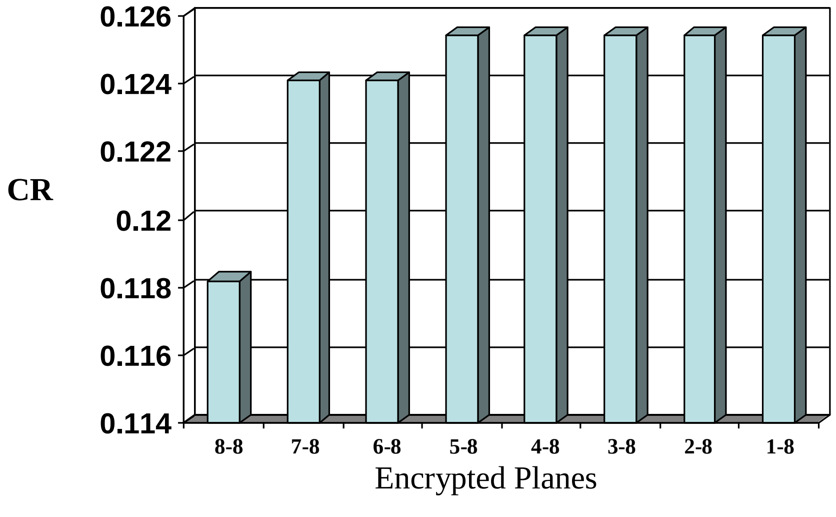


Figure (8): CR versus encrypted plane for Lena image using Multi-Bitplane-AES-PE

Bitplane	CR	PSNR (dB)
1	0.1093	33.9117
2	0.1093	33.9117
3	0.1093	33.9117
4	0.1093	33.9117
5	0.1105	33.9117
6	0.1093	33.9117
7	0.1152	33.9117
8	0.1182	33.9117

(a)

Bitplane	CR	PSNR (dB)
1	0.1120	34.5113
2	0.1120	34.5113
3	0.1120	34.5113
4	0.1121	34.5113
5	0.1120	34.5113
6	0.1151	34.5113
7	0.1123	34.5113
8	0.1216	34.5113

(b)

Bitplane	CR	PSNR (dB)
1	0.1061	33.9066
2	0.1061	33.9066
3	0.1063	33.9066
4	0.1061	33.9066
5	0.1061	33.9066
6	0.1117	33.9066
7	0.1079	33.9066
8	0.1177	33.9066

(c)

Bitplane	CR	PSNR (dB)
1	0.1055	33.9091
2	0.1058	33.9091
3	0.1059	33.9091
4	0.1056	33.9091
5	0.1056	33.9091
6	0.1089	33.9091
7	0.1112	33.9091
8	0.1150	33.9091

(d)

Table (1): Results of different bitplanes for images using Single-Bitplane-AES-PE.
(a) Lena (b) House (c) Birds (d) Boys

Bitplane	CR	PSNR (dB)
1	0.2622	30.8867
2	0.2622	30.8867
3	0.2622	30.8867
4	0.2622	30.8867
5	0.2622	30.8867
6	0.2622	30.8867
7	0.2638	30.8867
8	0.2650	30.8867

(a)

Bitplane	CR	PSNR (dB)
1	0.2549	30.8611
2	0.2549	30.8611
3	0.2549	30.8611
4	0.2549	30.8611
5	0.2550	30.8611
6	0.2550	30.8611
7	0.2555	30.8611
8	0.2574	30.8611

(b)

Bitplane	CR	PSNR (dB)
1	0.2325	30.9844
2	0.2325	30.9844
3	0.2325	30.9844
4	0.2325	30.9844
5	0.2326	30.9844
6	0.2331	30.9844
7	0.2339	30.9844
8	0.2361	30.9844

(c)

Bitplane	CR	PSNR (dB)
1	0.2457	30.9875
2	0.2457	30.9875
3	0.2457	30.9875
4	0.2458	30.9875
5	0.2458	30.9875
6	0.2464	30.9875
7	0.2471	30.9875
8	0.2484	30.9875

(d)

Table (2): Results of different bitplanes for images using Wavelet-based-Bitplane-AES-PE.
(a) Lena (b) House (c) Birds (d) Boys

Bitplanes	CR	PSNR (dB)
8-8	0.1182	34.2369
7-8	0.1241	34.2369
6-8	0.1241	34.2369
5-8	0.1254	34.2369
4-8	0.1254	34.2369
3-8	0.1254	34.2369
2-8	0.1254	34.2369
1-8	0.1254	34.2369

(a)

Bitplanes	CR	PSNR (dB)
8-8	0.1216	34.2827
7-8	0.1219	34.2827
6-8	0.1251	34.2827
5-8	0.1253	34.2827
4-8	0.1254	34.2827
3-8	0.1254	34.2827
2-8	0.1254	34.2827
1-8	0.1254	34.2827

(b)

Bitplanes	CR	PSNR (dB)
8-8	0.1177	34.0975
7-8	0.1195	34.0975
6-8	0.1252	34.0975
5-8	0.1252	34.0975
4-8	0.1252	34.0975
3-8	0.1254	34.0975
2-8	0.1254	34.0975
1-8	0.1254	34.0975

(c)

Bitplanes	CR	PSNR (dB)
8-8	0.1150	33.6355
7-8	0.1208	33.6355
6-8	0.1242	33.6355
5-8	0.1243	33.6355
4-8	0.1245	33.6355
3-8	0.1249	33.6355
2-8	0.1253	33.6355
1-8	0.1254	33.6355

(d)

Table (3): Results of different bitplanes for images using Multi-bitplane-AES-PE.
(a) Lena (b) House (c) Birds (d) Boys