Crypto-Compression System for Secure Transfer of Grayscale Images

Dr. Hameed Abdul-Kareem Younis
Dept. of Computer Science, College of Science, University of Basrah, Basrah, Iraq.
E-mail: hameedalkinani2004@yahoo.com

Abstract

In this paper, the proposed partial encryption algorithm adopts secure encryption algorithm to encrypt only one part of the compressed data. Only 0.0031% of the original data is encrypted. This leads to reduction both encryption and decryption time.

Thus, a combination of encryption and compression is used in practical work. In the compression step, the advanced wavelet coding scheme, the Set Partition in Hierarchical Trees (SPIHT) algorithm is used while in the encryption step, stream cipher is applied.

The proposed partial encryption scheme is fast and secure; moreover, it never reduces the compression performance of the underlying selected compression method.

Keywords: Image, Partial Encryption, SPIHT, Compression.

نظام تشفير-ضغط للنقل الآمن للصور الرمادية

د. حميد عبد الكريم يونس

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

E-mail: hameedalkinani2004@yahoo.com

المستخلص

اقترح في هذا البحث خوارزمية للتشفير الجزئي، والتي تبنت خوارزمية تشفير سرية لتشفير جزء من البيانات المضغوطة. وشفر بحدود 0.0031% من البيانات الأصلية للصور المستعملة. يقود هذا إلى تقليل في زمن التشفير وفك الشفرة. وهكذا، جمع كل من التشفير والضغط استخدم في الجانب العملي. استخدمت في مرحلة الضغط، تقنية ترميز تحليل مويجي متقدمة (تقسيم المجموعة في أشجار هرمية (SPIHT)) بينما في مرحلة التشفير، استخدمت طريقة التشفير الانسيابي.

نظام التشفير الجزئي المقترح كان سريع وذات سرية عالية كما إن انجازية الضغط لا تقل ضمن طريقة الضغط المختارة.

الكلمات المفاتيح:

Image, Partial Encryption, SPIHT, Compression

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 [5]. 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.

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 [4]

Partial encryption (also called *selective encryption* or *soft encryption*) is a secure encryption algorithm which is used to encrypt only part of the data. It is used to reduce encryption and decryption time [5].

The aim of algorithm proposed here is to combine image compression with encryption. Many researchers have examined the possibility of combining compression and encryption: In 2002, Miaou S., Chen S., Lin C. [9] proposed a partially encrypting scheme combining SPIHT and AES. In this scheme, compressed SPIHT bit streams are identified based on their importance to signal quality. Then, AES is used to encrypt only the important part that can be defined and chosen by a user. In 2004, Borie J., Puech W., Dums M. [4] discuss the secure of transferring of medical images. They propose two cryptosystems, the first one is a very fast algorithm by block, the TEA (Tiny Encryption Algorithm) and the second is a stream cipher based on Vigenere's ciphering. They show differences existing between them, especially concerning the combination of the image encryption and the compression.

In the present work, only part of the compressed data is encrypted. Some compression algorithms have *important parts* that provide a significant amount of information about the original data, whereas the remaining parts may not provide much information without the important parts [6]. For simplicity, we consider all the important parts as one unit, and the remaining parts are grouped into one unimportant part. Since it is difficult to obtain information from the unimportant part alone, partial encryption approach encrypts only the important part. A significant reduction in encryption and decryption time is achieved when the relative size of the important part is small.

2. Basic Principles

2.1 Wavelet Transform

The wavelets transform have two terms, each one is a set of functions which takes the forms [1, 2, 3, 18]:

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

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

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 (1).The second function in (2) , ***ϕ (x)*** is called *the scale function*. Where g_k's and h_k's are analysis filters coefficients with ***h*** and g are the analysis filters [12, 16, 18]. Figure (1) shows the analysis and synthesis filters of a 2-D, 1-level of wavelet decomposition; where $\tilde{h}$ and $\tilde{g}$ are the synthesis filters. The upsampling process is indicated by ↑**2** , and the downsampling process is indicated by ↓**2**.

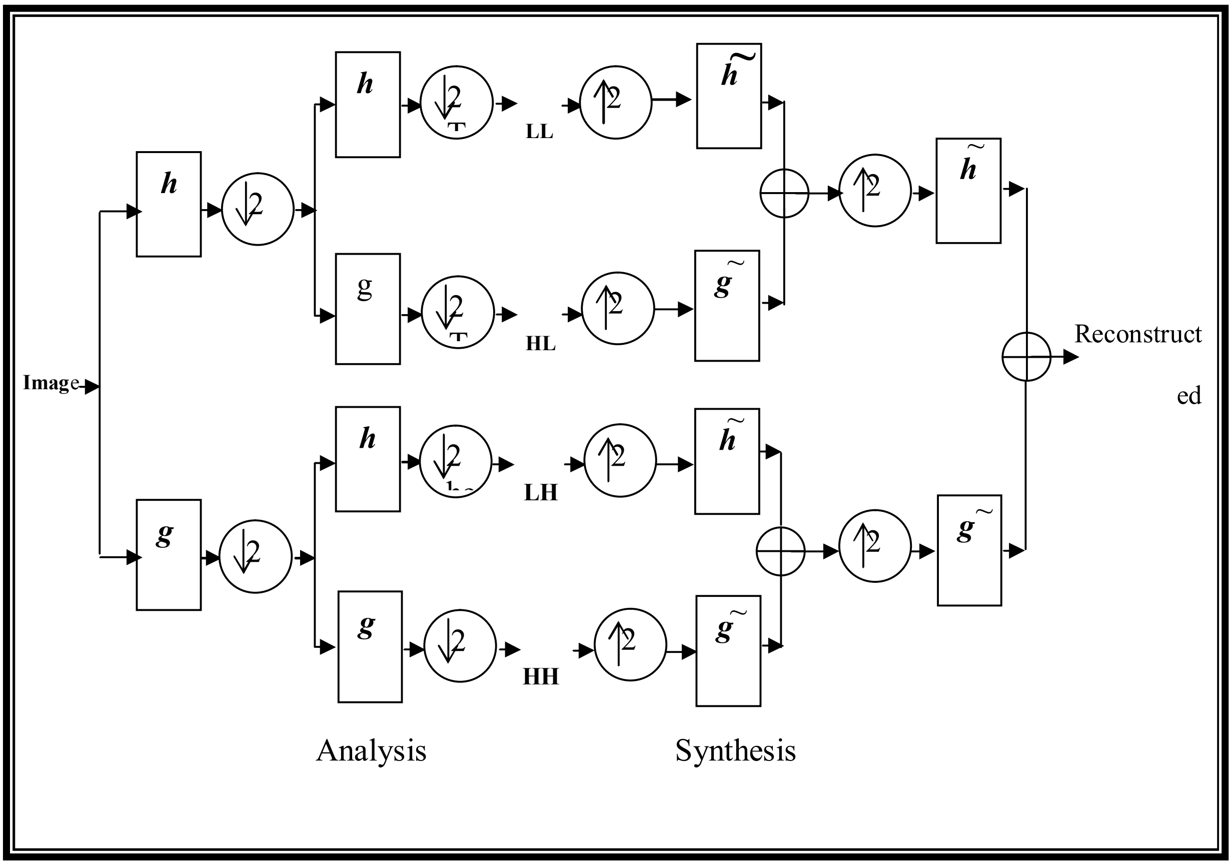


Figure (1): The analysis and synthesis of 2-D, 1-level discrete wavelet decomposition

2.2 SPIHT Algorithm

The quantization method used to generate some of the results in this thesis is the Set Partitioning In Hierarchical Trees ***(SPIHT)*** developed by Said and Pearlman [13]. Said and Pearlman have significantly improved the Sapiro's EZW algorithm [14]. The SPIHT quantizer is an embedded coder that achieves good performance by exploiting the spatial dependencies in the subbands of the wavelet decomposition [10, 14]. The SPIHT coder was chosen for the experiments in this thesis due to its good objective and computational performance.

For best understanding of how SPIHT works, the pixels relationship should be explained. In particular, each pixel in a smaller subband has four children in the next larger subband in the form of a 2×2 block of adjacent pixels. Each small square represents pixel and each arrow points from a particular parent pixel to its 2×2 group of children. The importance of the parent-child relation in quantization is described by the following statement: if the parent coefficient has a small value, then the children will most likely have small values.

Conversely, if the parent has a large value, one or more of the children may also have large value.

Coders like SPIHT exploit this spatial dependence by partitioning the pixel values into parent-descendent groups. The coder starts with a threshold value that is the largest integer power of two. This power does not exceed the largest pixel value. Pixels are evaluated in turn to see if they are larger than the threshold; if not, these pixels are considered insignificant. If a parent and all of its descendents are insignificant, then the coder merely records the parent's coordinates. Since the children's coordinates can be inferred from those of the parent, those coordinates are not recorded, resulting in a potentially great savings in the output bit stream. After locating and recording all the significant pixels for the given threshold, the threshold is reduced by a factor of two and the process repeated. By the end of each stage, all coefficients that have been found to be significant will have their most significant bits (when considered as binary integers) recorded [10, 12].

2.3 Run Length Encoding (RLE)

This type of coding is based on transforming the sequence of image pixels along a scan line (row, column or diagonal) into a sequence of pairs (G_i,L_i), where G_i denotes the gray level and L_i is the run-length of the i^{th} run (i.e., adjacent pixels having approximately same gray level G_i) [7]. This type of mapping is suitable for those types of images showing a large areas of the same brightness. However, the run length encoding is a perfect reversible process, and its decoding process may lead to exact image reconstruction.

2.4 Stream Cipher

A secret key cryptosystem encrypt image pixel by pixel, with the stream cipher algorithm. stream cipher convert original image to encrypted image one bit at a time. The simplest implementation of a stream cipher is shown in Figure (2) [15]. A keystream generator (sometimes called *a running-key generator*) outputs a stream of bits: K_1, K_2, K_3,……, K_i. This keystream is XORed with a stream of plaintext bits, P_1, P_2, P_3,….,P_i to produce the stream of ciphertext bits C_1, C_2,……C_i.

$$C_i = P_i \oplus K_i \qquad \ldots(3)$$

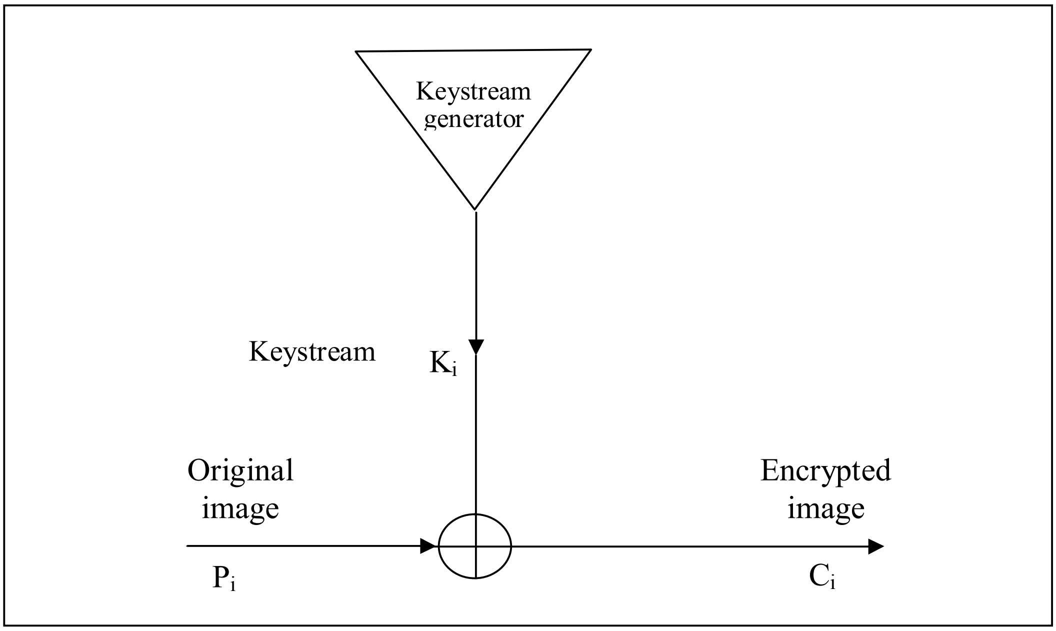


Figure (2): Stream cipher

Stream cipher system consists of two main parts [15]:

1- Algorithm to generate keystream.

2- XOR gate.

3. Proposed Partial Encryption Scheme

In this scheme, we propose a method for partial encryption of compressed image. The proposed method consists of wavelet transform (8 levels), quantization by SPIHT, encryption of important part then coding of resultant image by using run length encoding.

The encryption step in this algorithm can be preformed by using any standard encryption algorithm. In the proposed scheme, a stream cipher is tested.

During the compression step, the SPIHT image coding algorithm is used, which can achieve a reasonably good compression rate. Among all wavelet-based image compression schemes, SPIHT quantization shows its remarkable performance not only in terms of efficiency but also in its low computational cost and progressive coding characteristics. Progressive coding (also called *embedding coding*) refers to the way that the most significant bits representing an image are placed at the beginning of the code, and the code bits are arranged according to their importance relative to the representation of the image. SPIHT quantizer is an embedded coder that the pixels are sorted descendently in the output bit stream according to the information importance. The important part is the first part of bitstream.

In this scheme, only the important part of bitstream of image of SPIHT quantization is encrypted whereas the remaining parts (unimportant parts) are transmitted without encryption. The important part of the bitstream is encrypted with the stream cipher.

SPIHT-Stream –SE-Algorithm:

1. Encryption key selection.
2. Wavelet filter selection.
3. Decomposition (filtering) the image, here discrete wavelet transform (8 levels) is used.
4. Quantization, here SPIHT quantization process is applied.
5. Partial encryption, here stream cipher is used.
6. Entropy coding, here the run length encoding is adopted.

4. Experimental Results

To evaluate each of the proposed wavelet based image encryption schemes, three aspects are examined [8, 11]:

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 algorithm is adopted, such as stream cipher 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) [12].

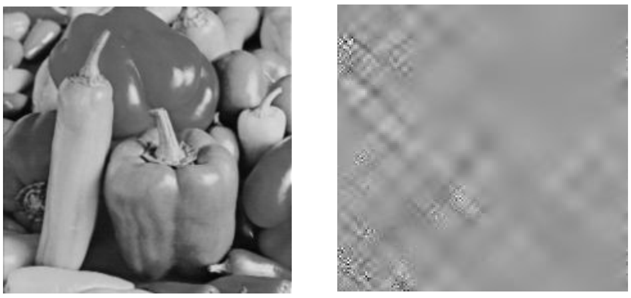
In this experiments, four different Compression Ratios (CRs) are chosen for this experiment, which are 1, 0.5, 0.25 or 0.125. The important part of bitstream of SPIHT quantization image is encrypted by using stream encryption algorithm as follows:

We propose here to encrypt important part by using stream cipher. The proposed system is very high security because of the security of stream cipher. Results obtained by applying this method are presented in Table (1). Figure (3) shows resulting after encryption. Figure (4) shows the results obtained for grayscale Peppers image.

In Table (1), the first column gives the CR. The second column gives the PSNR for each test grayscale image (Boys, Peppers, Map or Barco). The encryption key is 16! . Only the first 16 bits (0.0031%) of the original data is encrypted for the test grayscale images.

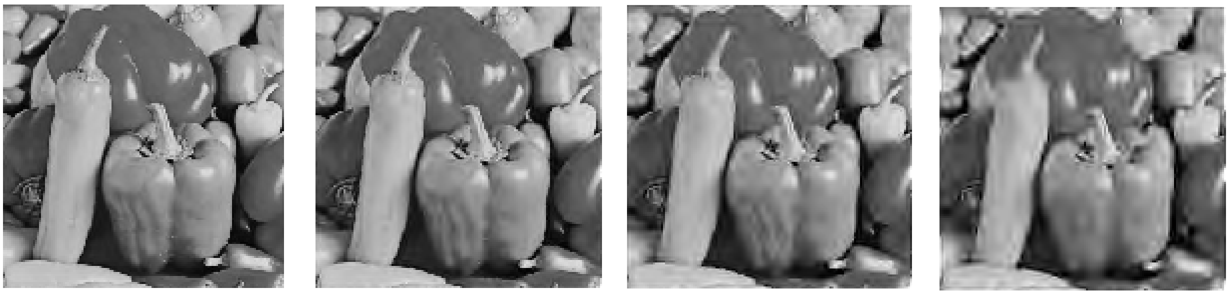
CR	PSNR (dB)			
	Boys	Peppers	Map	Barco
1	36.6080	36.6182	32.0934	37.3310
0.5	32.8733	31.9364	28.9277	32.5922
0.25	30.2179	27.7008	26.7265	28.9967
0.125	27.9773	24.2079	25.1105	26.4371

Table (1): Experimental results for different CRs of grayscale images.



(a) (b)

Figure (3): (a) Original grayscale Peppers image.
(b) Encrypted Peppers image.



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

Figure (4): Results of experiment:
(a) Reconstructed image at CR = 1, PSNR = 36.6182 dB
(b) Reconstructed image at CR = 0.5, PSNR = 31.9364 dB
(c) Reconstructed image at CR = 0.25, PSNR = 27.7008 dB
(d) Reconstructed image at CR = 0.125, PSNR = 24.2079 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 the results of experiments, one can notice that as the CR increases (low compression), PSNR value of the reconstructed image will increase. The average one can take is the second case (CR = 0.5). It is an acceptable one since it gives an acceptable PSNR and a reasonable time. Figure (5) shows PSNR versus CR for grayscale Peppers image.

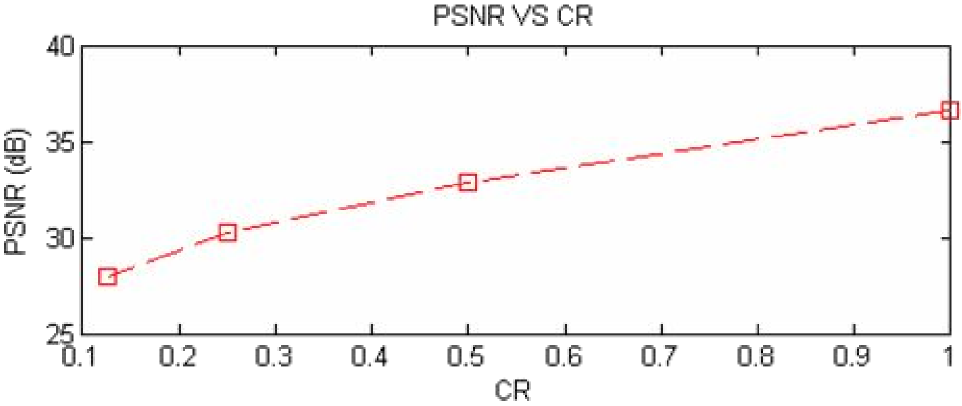


Figure (5): PSNR versus CR for grayscale Peppers image.

6. References

[1] **Al-Obaidi H. H.,**

“***Encryption Using Wavelet Coded Image Data”,***

M.Sc. Thesis, Computer Engineering Department, College of Engineering, Basrah University, June 2004.

[2] **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.

[3] **Baxes G. A.,**

“Digital Image Processing: Principles and Applications”,

John Wiley & Sons, Inc., USA, 1994.

[4] **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.

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

[6] **Cheng H., Li X.,**
"Partial Encryption of Compressed Images and Videos",
IEEE Transaction Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000.

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

[8] **Li S., Li C., Lo K.T., Chen G.,**
"Cryptanalysis of an Image Encryption Schemes",
Journal of Electronic Imaging, 2006.

[9] **Miaou S., Chen S., Lin C**.,
"An Integration Design of Compression and Encryption for Biomedical Signals",
Journal of Medical and Biological Engineering, Vol. 22, No. 4, pp. 183-192, 2002.

[10] **Morales A., Agili S.,**
"Implementing the SPIHT Algorithm in MATLAB",
In Proceedings of the 2003 ASEE/WFEO International Colloquium, 2003.

[11] **Öztürk Ï, Sogukpinar Ï,**
"Analysis and Comparison of Image Encryption Algorithms",
IEEE Transactions on Engineering, Computing and Technology, Volume 3, ISSN 1305-5313, December 2004.

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

[13] **Said A., Pearlman W. A.,**
"A New Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees",
IEEE Transactions on Circuits and Systems for Video Technology, Vol. 6, No. 3, pp. 243-249, June 1996.

[14] **Shapiro J. M.,**

"Embedded Image Coding Using Zerotrees of Wavelet Coefficients",
IEEE Transactions on Image Processing, Vol. 41, No. 12, pp. 3445-3462,
December1993.

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

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

[18] **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.