A Modified Technique For Image Encryption

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 secure of transferring images is considered. A cryptosystem, which is a modified version of the RC4 algorithm is developed. The proposed algorithm is used with wavelet transform. Several experiments were given to illustrates the performance of the proposed scheme.

Keywords: Image, Encryption, RC4 algorithm, Wavelet.

تقنية معدلة لتشفير الصور

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 : Abstract

تعتبر نقل الصورة بصورة سرية ذات أهمية كبيرة. في هذا البحث، تم تطوير خوارزمية RC4. استخدمت خوارزمية RC4 المطورة مع التحليل المويجي (Wavelet) لتشفير الصور. طبقت العديد من التجارب على هذة التقنية الجديدة لحساب انجازيتها.

1. Introduction

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 factor very important for the image encryption [1]. Two levels of time are found, the first is the time to encrypt, the other is the time to transfer images. To minimize it, the first step is to choose a robust, rapid and easy method to implement cryptosystem. In pervious study, we have found some articles on image encryption: In 2000, Tarish [8] proposed image cryptographic system based on stream cipher as a tool for image encryption. In 2003, Pommer [3] two approaches of selective encryption where wavelet-based methods are used for compression. The first attempt was to hide the choice of filters, while the second approach of selective encryption was based on wavelet packets and the decomposition tree are keep secret.

In the present work, the RC4 algorithm is developed to encrypt image with wavelet subband images (LL, HL, LH or HH).

2. Basic Principles

2.1 RC4 Algorithm

A secret key cryptosystem encrypt image pixel by pixel, with the RC4 algorithm. RC4 convert original image to encrypted image one bit at a time. The simplest implementation of a RC4 is shown in Figure (1) [7]. 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.

$$C_i = P_i \oplus K_i \qquad \text{…(1)}$$

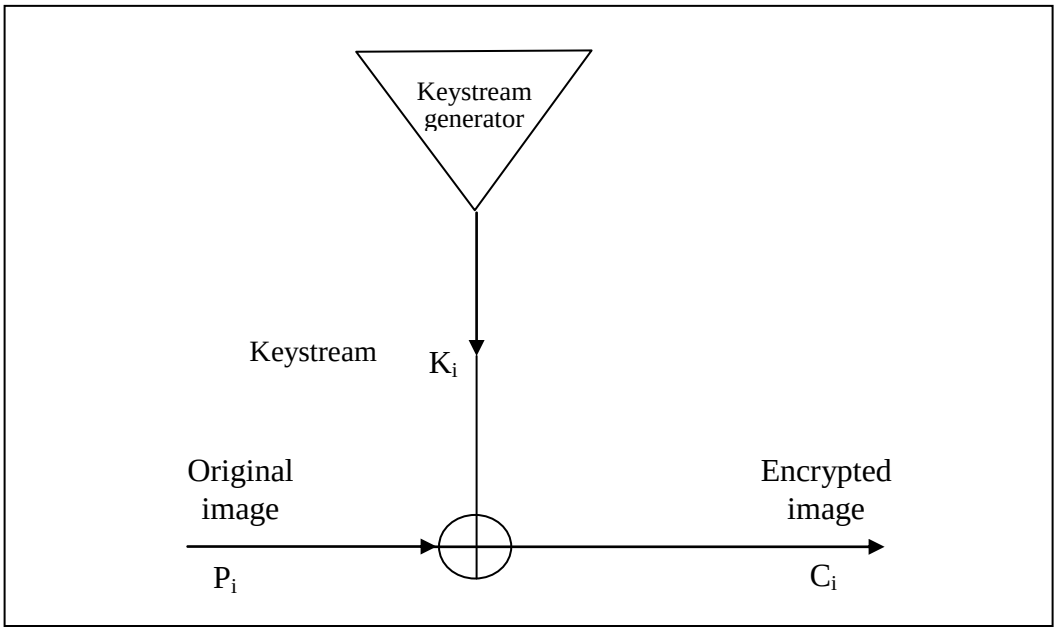


Figure (1): RC4 Structure

RC4 system consists of two main parts [5]:

1- **Algorithm to generate keystream.**

2- **XOR gate.**

In the next section a modified RC4 algorithm will be presented.

2.2 Modified RC4:

The following algorithm is a modification of the RC4. It is illustrated in Figure (2).

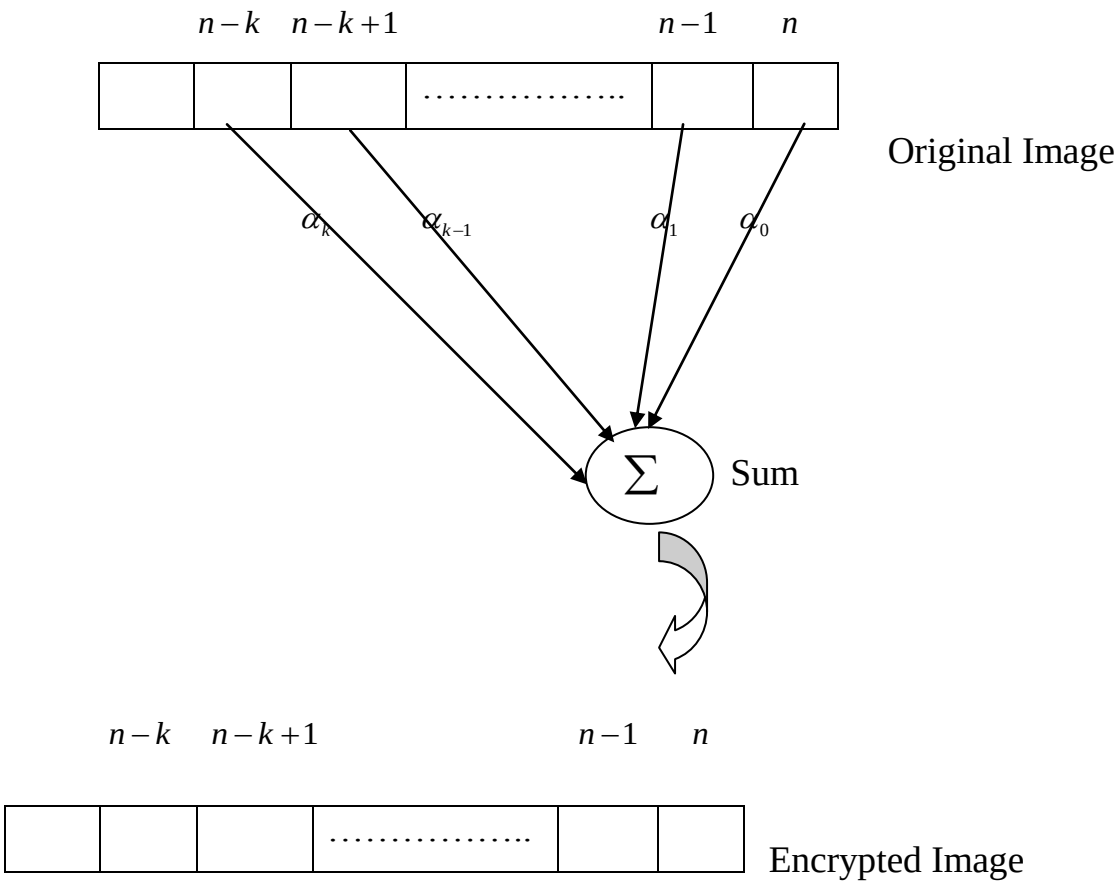


Figure (2) : Modified RC4 Algorithm.

If *p(n)* is a pixel of the original image, *p'(n)* the ciphered pixel is according to the next equation:

$$p'(n) = p(n) \oplus \alpha(1)\, p(n-1) \oplus \ldots\ldots\ldots \oplus \alpha(k)\, p(n-k) \qquad \ldots\ldots \quad (2)$$

where n∈[k,N] with k∈[1,n] and N the number of pixels. The coefficient α (k) are generated with the keystream. The equation (2) can be written:

$$p'(n) = p(n) + \sum_{i=1}^{i=k} \alpha(i).p(n-i) \qquad \ldots\ldots \quad (3)$$

where k is the order of recurrence corresponding to the length of the chosen key.

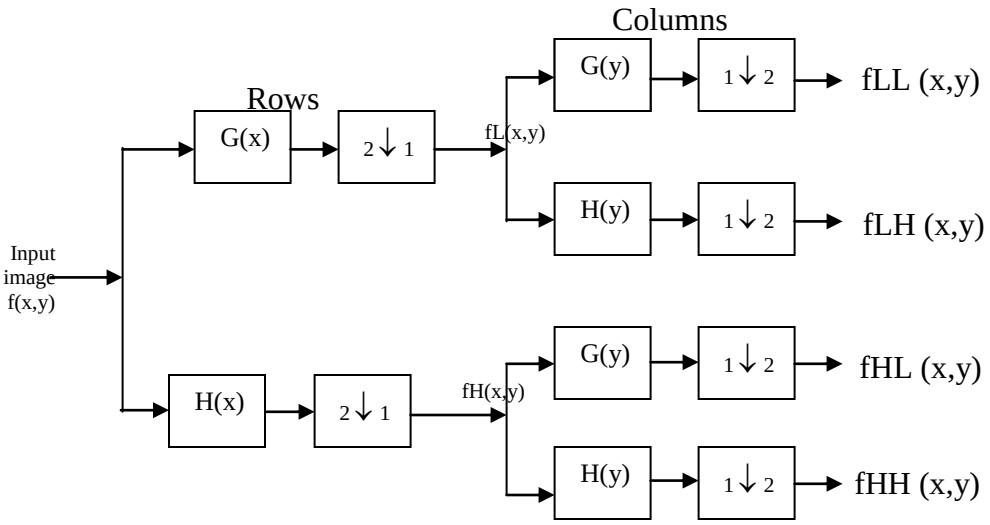
The particularity of the method resides in the fact that the encryption of each pixel depends on three elements, the pixel in clear, the keystream, and the k precedent pixels in the image. Moreover, our encryption system requires the introduction of k virtual pixels to encrypt the k first pixels. The α_i coefficients have been coded on two bits, we have chosen the following values (Table 1). During the binary lecture of the keystream, to the binary value 11 is associated alternatively the number +2 or -2. In this case, the effective length of the key to use is 2.k bits.

Table (1) : α_i coefficients.

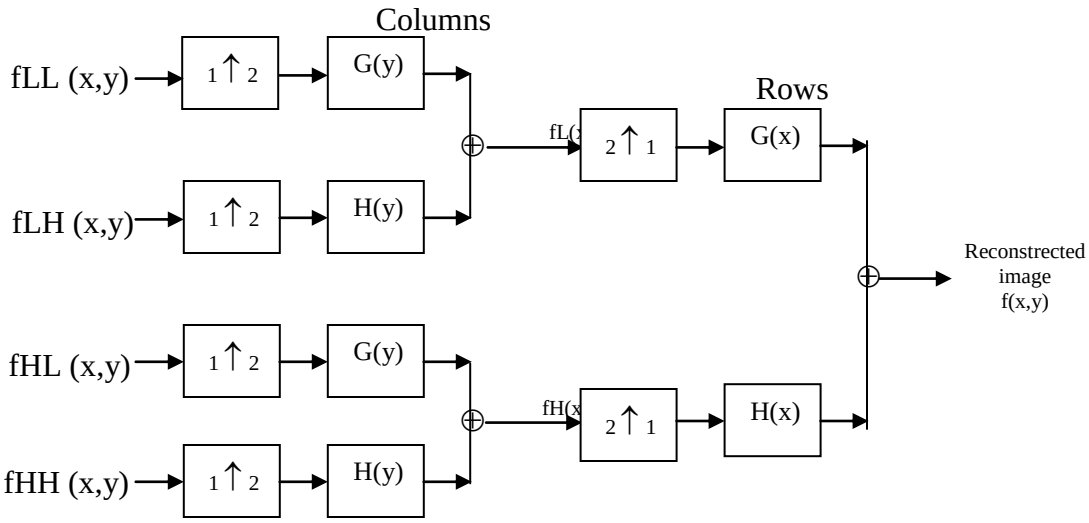
Two bits value	00	01	10	11
α_i	0	+1	-1	+/-2

2.3 Wavelet Transform

Wavelet transform (WT) in the image processing can be considered as a subband decomposition [2,4,6]. 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. Finally, the image wavelet reconstruction is shown in Figure 3(b).



(a) Image Wavelet Decomposition.



(b) Image Wavelet Reconstructed.

LL (Low-Low)	HL (High-Low)
LH (Low-High)	HH (High-High)

(c) : Wavelet Subband Images.

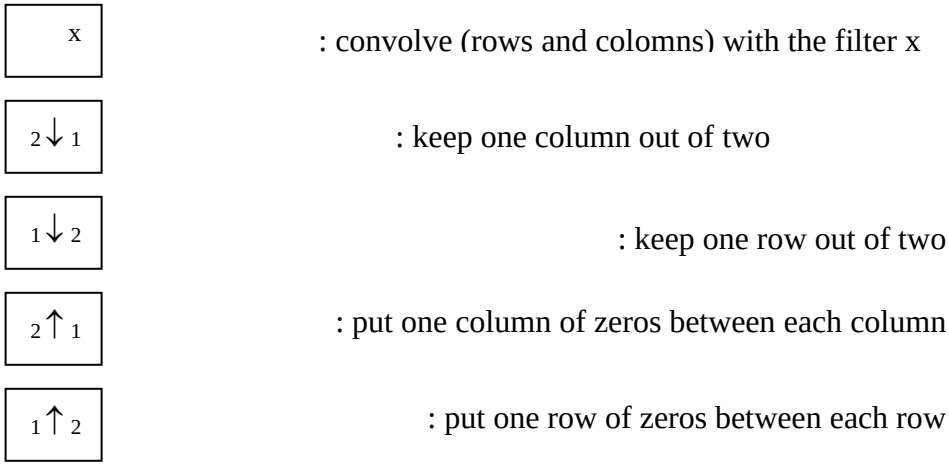


Figure (3) : Image Wavelet Transform and Its Inverse.

3. The Proposed Technique

The proposed technique consists of two steps. In the first step, the wavelet decomposition is applied to the original image and resulted wavelet subband images are enciphered using modified RC4 algorithm in two different approaches:

(1) Full Encryption

In this approach, original image is encrypted using the modified RC4 algorithm. The result is the encrypted image.

(2) Partial Encryption

In this approach, only one of the wavelet subband images is encrypted using the modified RC4 algorithm as follows:

(a) the subband image LL.

(b) the subband image HL.

(c) the subband image LH.

(d) the subband image HH.

In the second step, wavelet subband images are collected to form the enciphered image. The main principle of this technique is to reduce time. The time is a very important factor for the image encryption. Also, the subband image LL is an important subband since it given better result.

4. Experimental Results

Peak signal-to-noise ratio (PSNR) is the standard method for quantitatively comparing a reconstructed 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:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad \text{……(4)}$$

where the mean square error (MSE) is defined as:

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[x(m,n) - \hat{x}(m,n)\right]^2 \qquad \text{……(5)}$$

Two 128*128 images, Lena and boat, grayscale images are used in this experiment. Figure (4) and Figure (5) show the encrypted images using the modified RC4 method. The encryption results show that the proposed method gives less time when we encrypt subband image instead of the full image. Also, the subband image LL is an important subband through encryption. Thus, it gives less PSNR. This can confirm by the following table.

Table (2) : Encryption Results.

	Full Encryption		Partial Encryption							
	Time (sec)	PSNR	LL		HL		LH		HH	
			Time (sec)	PSNR	Time (sec)	PSNR	Time (sec)	PSNR	Time (sec)	PSNR
Lena	36.562	5.255	9.797	5.279	4.859	14.729	4.531	11.799	4.406	15.325
boat	37.797	5.605	8.406	5.616	4.75	11.755	4.625	11.939	4.563	14.118

5. Conclusion

The experimental result shows that the image encryption using modified RC4 in the proposed method can reduce time and PSNR. Therefore this technique is useful for achieving the secure of transferring of images. The conclusion that subband image LL is the important subband compared with the other subband images. The less PSNR leads to the best encryption.

6.References

[1] 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.

[2] P.M. Bentley and J.T.E. McDonnell,
"Wavelet Transform: an Introduction,"
Electronics & Communication Engineering Journal, August 1994.

[3] Pommer A.,
"Selective Encryption of Wavelet-compressed Visual Data",
Ph.D. Thesis, Department of Scientific Computing, Salzburg University, Austria, June 2003.

[4] R.K. Young,
"Wavelet Theory and Its Application",
Kluwer Academic Publishers, 1993.

[5] Schneier B.,
"Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C",
John Wiley & Sons, Inc., USA, 1996

[6] S. Mallat,
"A Theory for Multiresolution Signal Decomposition: The Wavelet Representation,",
IEEE Trans. On Patt. Anal. Machine Intell., Vol.11, No.7, pp. 674-693 1989.

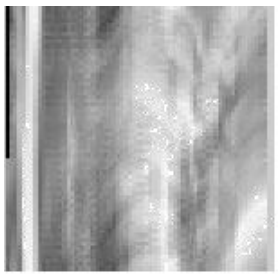
[7] Stallings W.,
"Cryptography and Network Security, Principles and Practice",
Third Edition, Pearson Education International, Inc., USA, 2003.

[8] Tarish A.H.,
"Designing and implementation a stream cipher cryptography system",
M.Sc. Thesis, Computer Science Department, University of Technology, 2000.

(a) Original imag

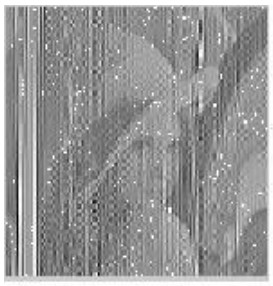
(b) wavelet subband

(c) encryption of full image, Time=36.562 sec,



(d) encryption of subband image LL, Time=9.797 sec,

(e) encryption of subband image HL, Time=4.859 sec,

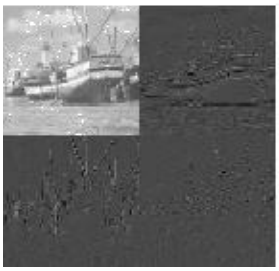


(f) encryption of subband image LH, Time=4.531 sec,

(g) encryption of subband image HH, Time=4.406 sec,

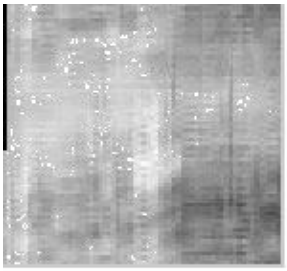
(h) reconstructed

Figure (4): Resulting image of Lena.

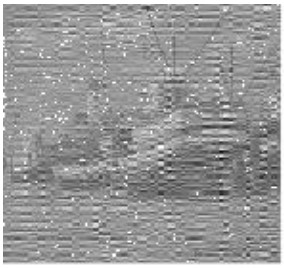


(b) wavelet subband images

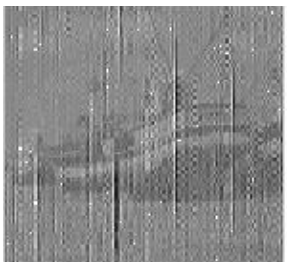
(c) encryption of full image,
Time=37.797 sec, PSNR=5.605



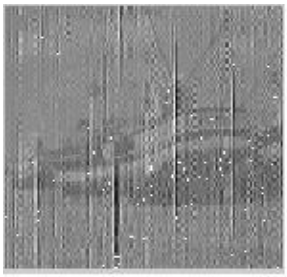
(d) encryption of subband image
LL, Time=8.406 sec, PSNR=5.616



(e) encryption of subband image HL,
Time=4.75 sec, PSNR=11.755



(f) encryption of subband image
LH, Time=4.625 sec,



(g) encryption of subband image
HH, Time=4.563 sec,

(h) reconstructed

Figure (5): Resulting image of boat.