



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Finding the Best Key Stream by Using Genetic Algorithm for Image Encryption

Prasun Kumar Mitra¹, Partha Halder²

Lecturer, Department of Computer Science & Technology, Technique Polytechnic Institute, Hooghly,
West Bengal, India¹

Technical Assistant, Department of Computer Science & Technology, Technique Polytechnic Institute, Hooghly,
West Bengal, India²

ABSTRACT: Because of using images widely in industrial process, it is important to protect the confidential image data from unauthorized access. The RC4 algorithm is selected. The proposed algorithm is used with wavelet transform. The main idea of this paper is to show how genetic algorithm works to give the optimal keys and the influence of each key in the increasing security, several experiments were given to prove that.

KEYWORDS: Image, Encryption, RC4 algorithm, Wavelet Transform, Genetic Algorithm

I. INTRODUCTION

The Ciphering of image 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 very important factor for the image encryption [1]. Two levels of time are found, the first is the time to encrypt, and the other is the time to transfer images. To minimize it, the first step is to choose a robust and easy method to implement cryptosystem. Two approaches of select encryption where wavelet-based methods are used for compression [2]. 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 is keep secret. The use of genetic algorithm is very important tool to find more secure image, where genetic algorithm gives suitable key stream.

In the present work, the RC4 algorithm is developed to encrypt image with wavelet subband images and genetic algorithm.

II. RELATED WORK

II.1. ENCRYPTION

The basic idea of encryption is to modify the message in such away that its content can be reconstructed only by a legal recipient [3]. A discrete-valued cryptosystem can be characterized by:

- 1) A set of possible plaintexts (the original message), P .
- 2) A set of possible ciphertexts (the scrambled message), C .
- 3) A set of possible cipherkeys, K .

The basic model of the ciphering system is shown in Figure (1).

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017



Figure (1): The Encryption diagram of a cipher

Two classes of key based encryption algorithms, symmetric (or secret-key) and asymmetric (or public-key) algorithms [3].

Symmetric-Key Algorithms

Symmetric key encryption is a key based encryption algorithm in which the same key is used to encrypt sensitive data, used to decrypt the sensitive data. The key must be protected and secured. The key is often called a secret- key [4]. Symmetric-key algorithms are broken down according to the structure of the algorithm into stream cipher and block cipher.

Stream Cipher

It is symmetric key ciphers which process, the given message (plaintext) bit by bit (as a stream). So stream ciphers encrypt each bit of the input data individually before moving on to the next. In our work we used this type of ciphering.

II.2. 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 (2) [5]. A key stream generator (sometimes called a running-key generator) outputs a stream of bits: $K_1, K_2, K_3, \dots, K_i$. This key stream is XORed with a stream of plaintext bits, $P_1, P_2, P_3, \dots, P_i$ to produce the stream of ciphertext bits C_1, C_2, \dots, C_i .

$$C_i = P_i \oplus K_i \quad \dots (1)$$

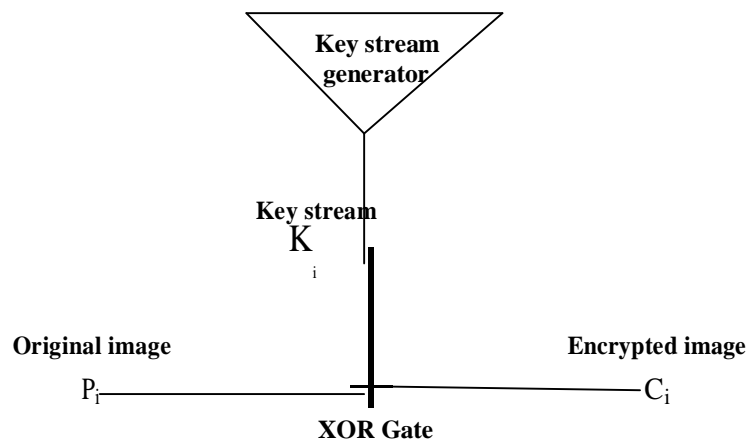


Figure (2): RC4 Structure

RC4 system consists of two main parts [6]:

- 1- Algorithm to generate key stream.
- 2- XOR gate.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Most algorithms which are used to generate the key streams are based on using the shift registers. Thus, the main component of the key stream generator is the shift register. A shift register can be represented by a sequence of bits. Each time a bit is needed; all of the bits in the shift register are shifted one bit to the right. The new left-most bit is computed as a function of the other bits in the register as shown in Figure (3) [7].

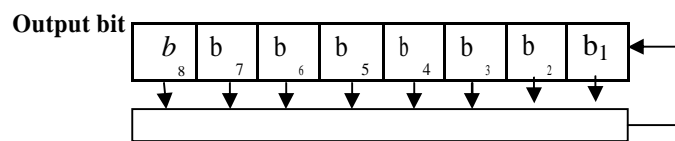


Figure (3): Feedback Shift Register

II.3. Wavelet Transform

Wavelet transform (WT) in the data processing can be considered as subband decomposition [8]. Figure (4) shows the image wavelet decomposition diagram. The original image $f_L(x, y)$ is firstly filtered on the row by applying filter H (high-pass filter) and G (low-pass filter) and down sampled by keeping one column out of two. Two resulting images, the low-pass $f_L(x, y)$ and high-pass $f_H(x, y)$ outputs are obtained. Then, both of them are filtered along the column and up sampled by keeping one row out of two. It can be obtained one low-pass subband image denoted by $f_{LL}(x, y)$ and three high-pass subband images denoted by $f_{LH}(x, y)$, $f_{HL}(x, y)$ and $f_{HH}(x, y)$, respectively.

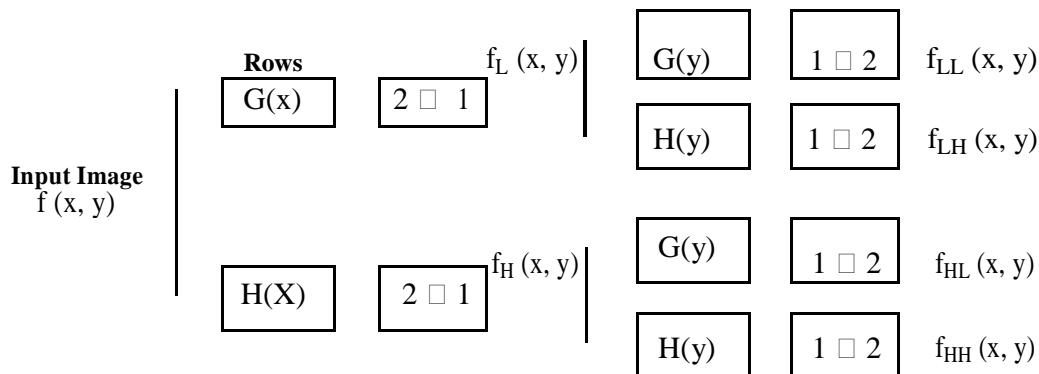


Figure (4): Image Wavelet Decomposition

$\begin{matrix} G(x) \\ x \end{matrix}$: Convolve (rows and Columns) with the filter x .

$\begin{matrix} 2 & \square & 1 \end{matrix}$: Keep one column out of two.

$\begin{matrix} 1 & \square & 2 \end{matrix}$: Keep one row out of two

II.4. Genetic Algorithms

Genetic algorithms are adaptive methods which may be used to solve search and optimization problems. They are based on the genetic process of biological organisms [9]. Genetic algorithms operate on encoded representations of the solutions, equivalent to those chromosomes of individuals in nature. Since a chromosome is a sequence of symbols and



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

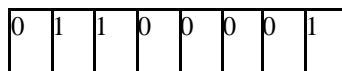
Vol. 5, Issue 11, November 2017

these symbols have been binary digits. Empirical studies have typically used chromosomes where each symbol represents an integer or a floating point number [10].

III. PROPOSED ALGORITHM

Binary Genetic Algorithm

Because the used of genetic algorithm in this paper is to find the best key stream, and these keys must be binary, therefore the encoding of genetic algorithm is binary. 1- Initialization The initial population of chromosomes is generated at random. The chromosomes in the population have a fixed length and represent the value of initial key stream shift register. Ten chromosomes are generated and each chromosome has eight genes. For example: There are many components of genetic algorithm that specified the work of this algorithm, where [10]:



Shift Register

It represents letter (a) with ASCII code (97).

Evaluation

In Evaluation step, we will find the fitness function, the fitness function is very important in order to obtain good encryption results. The evaluation function used in this work is based on correlation (corr) that measures the similarity between the original image and encryption image, it is between 0 and 1, and then the correlation can be defined as [3]:

$$\text{corr (fitness function)} = \frac{\sum_{r=1}^N \sum_{c=1}^M (I_1(r, c) - \bar{I}_1)(I_2(r, c) - \bar{I}_2)}{\sqrt{\sum_{r=1}^N \sum_{c=1}^M (I_1(r, c) - \bar{I}_1)^2 \sum_{r=1}^N \sum_{c=1}^M (I_2(r, c) - \bar{I}_2)^2}} \quad \dots(2)$$

where:

$I_1(r, c)$: is the value of pixel at (r, c) of the original image.

\bar{I}_1 : is the mean of the original image that

$$\bar{I}_1 = \frac{1}{NM} \sum_{r=1}^N \sum_{c=1}^M I_1(r, c) \quad \dots(3)$$

$I_2(r, c)$: is the value of the pixel at (r, c) of encryption image.

\bar{I}_2 : is the mean of the encryption image that

$$\bar{I}_2 = \frac{1}{NM} \sum_{r=1}^N \sum_{c=1}^M I_2(r, c) \quad \dots(4)$$



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

$$M^N \quad r \quad c$$

M-height of the image.

N-width of the image.

r and c : row and column numbers.

Selection Operator

Selection is the process of choosing two strategy that is used here is Roulette Wheel parents from the population for crossing. The Selection.

Crossover Operator

Crossover is the main genetic operator. It operates on two individuals at a time and generates two offsprings. 1-point crossover (1X) used in our work as in Figure (5).

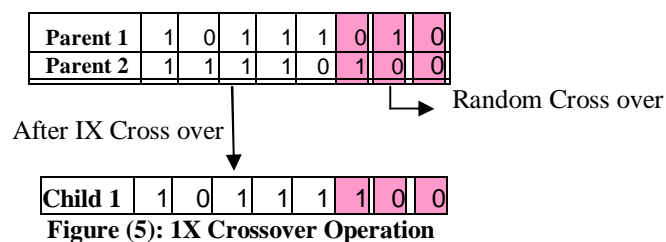


Figure (5): 1X Crossover Operation

Mutation Operation

Mutation is a random change of one or more genes. Every chromosome is simply scanned gene by gene and with a mutation rate (P_m) a gene is changed/swapped, i.e.

$0 \Rightarrow 1$ and $1 \Rightarrow 0$ [11].

Elitism

During our study, we used Holland technique in which offspring are replaced with poor chromosomes in population [12]. The child replaces the parent after applying crossover and mutation.

Proposed Model Operation

The operation of the system is as follow: Input the original image to the system, by using switches S_0 and S_1 will get two cases:

Case 1: if the S_0 is close and S_1 is open, then the original image will be transform by wavelet transform to approximation and details images. After that the transformer image convert to stream of bits and XORed with key stream bits, and result the encrypted image, this encrypted image may be not the best, therefore; this will again convert to pixels and correlated with the original image to give the fitness function of the genetic algorithm that gives another key stream and after that another encrypted image this process will stop directly after we get the good encryption.

Case 2: if the S_0 is open and S_1 is closed, the same procedures above but without wavelet transform. The full diagram is shown in Figure (6).

Two 256×256 images, boat and birds, 8-bit grayscale images are used in these experiments.

As shown in table (1), in the two images the encryption was taken on the image without

the number of cycles is zero (no genetic algorithm) and, second, the number of cycles is 5 (5 genetic cycles). Figure (7) and Figure (8) explain these procedures. The parameters of

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

wavelet transform (Full encryption) and with 1-level wavelet transforms (partial encryption). In the full encryption we used the genetic algorithm for 5 cycles but in partial encryption, there are two cases of genetic algorithm, first,

genetic algorithm are as follow:
Pc=0.83
Pm=0.23
No.of cycle=5.

Table (1): Encryption Results

Boat	Full Encryption		Partial Encryption		Partial Encryption	
No. of Genetic Cycle	5		0		5	
Initial Key stream	(11110101)		(01110011)		(10000010)	
	Time (sec)	corr	Time (sec)	corr	Time (sec)	corr
	152.844	0.0012	5.1	0.5932	32.672	0.0282
Birds	Full Encryption		Partial Encryption		Partial Encryption	
PDF Created with	deskPDF PDF		Writer - Trial ::		http://www.docudesk.com	
No. of Genetic Cycle	5		0		5	
Initial Key stream	(10011110)		(01110011)		(00010001)	

IV. SIMULATION RESULTS

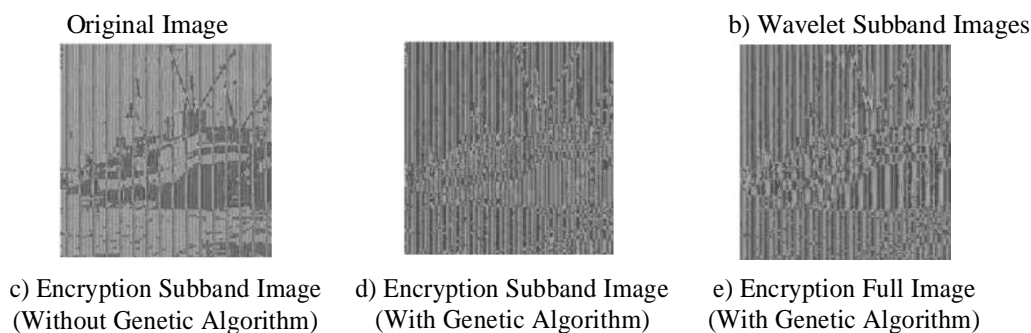
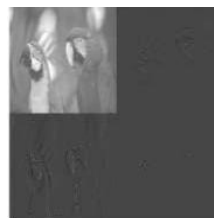


Figure (7) Resulting Images of Boat



a) Original Image



b) Wavelet Subband Images



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017



c) Encryption Subband Image d) Encryption Subband Image (With Genetic Algorithm) e) Encryption Full Image

Figure (8) Resulting Images of Birds

V. CONCLUSION AND FUTURE WORK

The experimental results shows that the type of image and the wavelet transform as well as the suitable keystream all these factors influence the encryption process. The genetic algorithm gives here the best encryption, although in the full image the genetic algorithm finds the best initial key stream that makes the correlation approach to zero (high encryption), but it takes more time. In the partial image (after wavelet transform) reduces the time but the correlation will be larger than the previous state, the last case is the partial image with manually selection of initial key stream (without genetic algorithm) this case reduces the time, with bad encryption. Without genetic algorithm we may take initial key that is not good to encrypt the image, but the use of genetic algorithm gives always suitable results. The much smaller correlation leads to more difference between the two images and then more secure.

The proposed algorithm may be used in many future works, one of these works is the modified RC4 with wavelet transform

REFERENCES

- [1] J. Borie, W. Puech, and M. Dumas, "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] A. Pommer, "Selective Encryption of Wavelet Compression Visual Data", Ph.D. Thesis, Department of Scientific Computing, Salzburg University, Austria, June 2003.
- [3] A. S. Yaseen, "Chaos Encryption Methods for Partial Encryption of Wavelet-based Compressed Images", M.Sc. Thesis, Computer Engineering Department, University of Basrah, 2005.
- [4] H. H. Al-Obaidi, "Encryption Using Wavelet Coded Image Data", M.Sc. Thesis, Computer Engineering Department, College of Engineering, Basrah University, June 2004.
- [5] W. Stallings, "Cryptography and Network Security, Principles and Practice", Third Edition, Pearson Education International, Inc., USA, 2003.
- [6] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C", John Wiley & Sons, Inc., USA, 1996.
- [7] S. A. Al-Agelee, "Use of Genetic Algorithm in the Cryptanalysis of Stream Cipher System", Ph.D. Thesis, Technology University, Baghdad, 1998.
- [8] 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.
- [9] D. Beasley, D. Bull, and R. Martin, "An Overview of Genetic Algorithms: Part1 and 2, Fundamentals", University Computing, 15(2), pp. 58-69, 1993. S. Behnam, "Image Filtering Based on Soft Computing Techniques", Ph.D. Thesis, Computer Science Department, College of Science, Basrah University, August 2006.
- [11] M. A. Al-Bayati, "Genetic Algorithm Based Path Planner", Ph.D. Thesis, Technology University, Baghdad, 1998.
- [12] E. J. Goldberg, "Genetic Algorithm in Search, Optimization, and Machine Learning", Addison-Wesley Publishing Company, Inc., USA, 1989.