ISSN 1991- 8690 الترقيم الدولي ٨٦٩٠ ـ ١٩٩١

Website: http://jsci.utq.edu.iq Email: utjsci@utq.edu.iq

An Adaptive Algorithm for Image Encryption: Pseudo Random Generator with Crossover of Genetic Algorithm

Hazeem Baqer Taher

Computer Science Dept. - Science College - Thi-Qar University

Abstract

In this paper proposed an adaptive approach for image encryption. We used linear congruential random number generators to produce the pseudo random sequence. The input image is encrypted using pseudo random with crossover of genetic algorithm. This new encryption method can be used to encrypt an image with high secure, fast and lossless. It can be used to send the encrypted image through network and secure data storage (such as important documents). To validate our work, several experiments are executed on a number of different features (details) images. The proposed method reduces the weakness area in the encryption method and increasing the randomness of the encrypted image.

الخلاصة

في هذا البحث نقترح خوارزمية مطورة لتشفير الصور حيث نستخدم linear congruential random number generator من اجل انتاج pseudo random sequence بالاضافة إلى استخدام crossover of genetic algorithm.

حيث تم تطوير طريقة لتشفير انواع مختلفة من الصور لنحصل على صورة مشفره ذات درجة تعقيد عالية وسرعة تنفيذ كبيره وتكون الصوره الناتجه خالية من الاخطاء free of error . ومما يشار اليه إن الصور التي استخدمت كانت تحتوي على كميات مختلفه من التفاصيل. وقد حصلنا على نتائج جيده حيث قضت هذه الطريقة على نقاط الضعف التي كانت تظهر في حال استخدام طريقة pseudo random وكما ظهر في النتائج.

E.mail: Haze_comp792004@yahoo.com

1. Introduction

In the digital world, the security of digital images becomes more and more important since the communications of digital products over open network occur more frequently. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image communications, and confidential video conferencing, ect. In order to fulfill such a task, many image encryption methods have been proposed, but some of them have been known to be insecure [1].

Recently, with the greater demand in digital signal transmission and the big losses from illegal data access, data security has become a critical and imperative issue in multimedia data transmission applications. In order to protect valuable information from undesirable readers or against illegal reproduction and modifications, various types of cryptographic schemes are needed. There are two types of cryptographic schemes: symmetric cryptography [2] and asymmetric cryptography [3]. The symmetric scheme uses the same key for encryption and decryption. Two keys issued in asymmetrical cryptography, one for encryption, known as the public key, and the other for decryption, known as the private key. Asymmetric cryptography is often used in key distribution and digital signature for its slow processing speed. The symmetric cryptography is normally used to encrypt private data for its high performance. Moreover, none of the most used symmetrical ciphering systems like DES, IDEA and AES make use of the most recent developments in information processing technology. There have been various data encryption techniques [4,5] on multimedia data proposed in the literature. Genetic Algorithms (GAs) [6] are among such techniques. Generally, genetic algorithms contain three basic operators: reproduction, crossover and mutation where all three are analogous to their namesakes in genetics. Reproduction and crossover together give genetic algorithms most of their searching power.

2. Pseudo-Random Bit Generators

It is important to note that the use of pseudo-random sequence generator reduces but does not eliminate the need for a natural source of random bits, the pseudo-random sequence generator is a" randomness expander", but it must be given truly random seed to begin with. A classical techniques for pseudo-random number generation which are quite useful and effective for Monte Carlo simulations are typically unsuitable for cryptographic applications. For example, linear feedback shift registers are well-known to be cryptographically insecure, one can solve for the feedback pattern given a small number of output bits. Linear congruential random number generators are also insecure. These generators use the recurrence:

$$X_{i+1} = (a_n X_i^n + a_{n-1} X_i^{n-1} + \ldots\ldots\ldots + a_1 X_i + a_0) \bmod p$$

Where p is prime, $a_n, \ldots\ldots\ldots, a_1, a_0$ are integer number less than p, x_0 is initial value for generator. To generate an output sequence $\{X_1, X_2 \ldots\ldots\}$, and starting point X_0 . it is possible to enter the secret parameters given just a few of the X_i. even if only a fraction of the bits of each X_i are revealed.

3. Genetic Algorithms

A genetic algorithm is a search technique used in finding true or approximate solutions to optimization and search problems. Genetic algorithms are categorized as global search heuristics. Genetic algorithms form a particular class of evolutionary algorithms that use techniques inspired by evolutionary biology such as inheritance, mutation, selection and crossover (also called recombination).Genetic algorithms are implemented as a computer simulation in which a population of abstract representations (called chromosomes or the genotype or the genome) of candidate solutions (called individuals, creatures, or phenotypes) to an optimization problem evolves toward better solutions. Traditionally, solutions are represented in binary strings of 0s and 1s,but other encodings are also possible. The evolution usually starts from a population of randomly generated individuals. Genetic algorithms form one of the best ways to solve a problem for which a little is known. They are very general algorithms that work well in any search space. A genetic algorithm is able to create a high quality solution [**7]**. The GA relies primarily on the creative effects of the Darwinian principle of survival and reproduction of the fitness. Mutation is a second operation in GA. The crossover operation involves the exchange (swap) between two selected bytes (i.e. string of bits) the crossover points are randomly chosen **[1].**

4. Structure of the Proposed Genetic Algorithm:

In this proposed method, the operations of GA (Crossover and mutation) are exploited to produce a new encryption method. This new method was applied to the candidate type of data in this work (i.e. Images). Many tests are performed to ensure the success of the new proposed encryption method. Some of them are listed in this paper. Then new encryption method is developed to satisfy the following goals, where the variable I be an image, E is the proposed encryption method and D is the proposed decryption method.

- Lossless: The encryption process has to be reversible, with perfect reconstruction of the image, D(E(I))=I.
- Secure: The cryptosystem has to be resistant to known attack such that corrections attack. Attacks specific to high redundant messages like images are to be taken into account.
- Complexity: the algorithm has to be based on low-cost operations.

The proposed encryption method consists of the following steps:

1. Initialize algorithm variable, Image I.
2. Initialize values of pseudo – random X_0 and P .
3. Generate pseudo random using spatial case depending **:**
$$X_n = ((X_{n-1})^{\wedge 2} + 5) \bmod p$$
4. $E(I_n) = I_n \oplus X_n$, $J_n = E(I_n)$
5. Using GA crossover for each pixel of Encryption Image J as shown bellow figure (1).

The proposed decryption method consists of the following steps:

1. Initial value of pseudo –random generator X_0 and P.

2. Generate pseudo –random using algorithm

$$X_n = ((X_{n-1})^{\wedge 2} + 5) \bmod p$$

3. Using GA crossover for each pixel of Encryption Image J as shown bellow figure(2).

4. Decryption using algorithm

$$D(J_n) = J_n \oplus X_n$$

$I_n=E(J_n)$

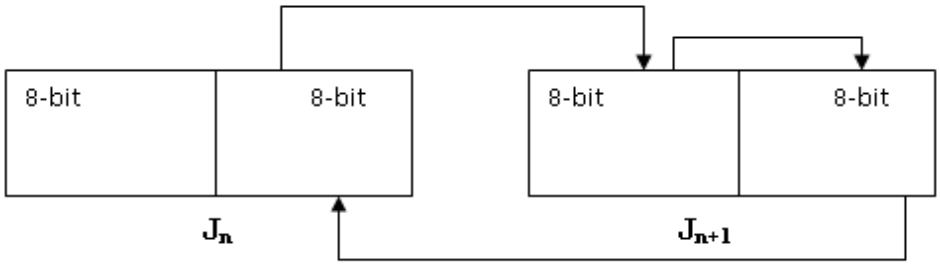


Figure (1):G.A. diagram for encryption.

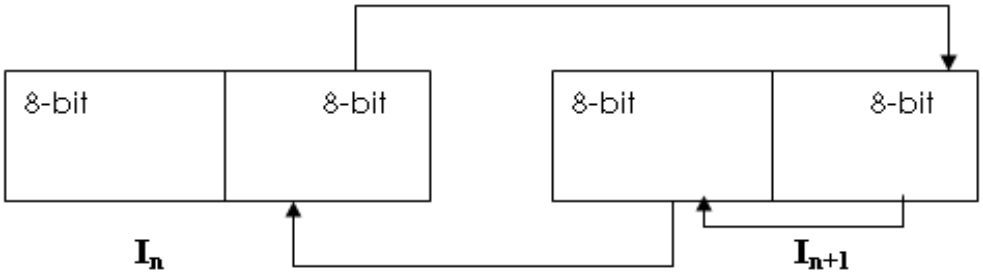


Figure (2):G.A. diagram for encryption.

5. statistical test

In this work, the proposed method pass four out of the five basic statistical tests to prove the randomness, these tests were:

1. Frequency test (Passed).
2. Serial test (Passed).
3. Poker test (Not Passed).
4. Runs test (Passed).
5. Autocorrelation test (Passed).

5. Experiments

To perform the proposed encryption method, MATLAB (2007a) was used to write it and applied on different features images, poor and rich details(information). comparing between the image encrypted using the pseudo random generator only, weakness area appear in the encrypted image as shown

in figure(3) with the proposed method PRGGA as shown in figure(4).

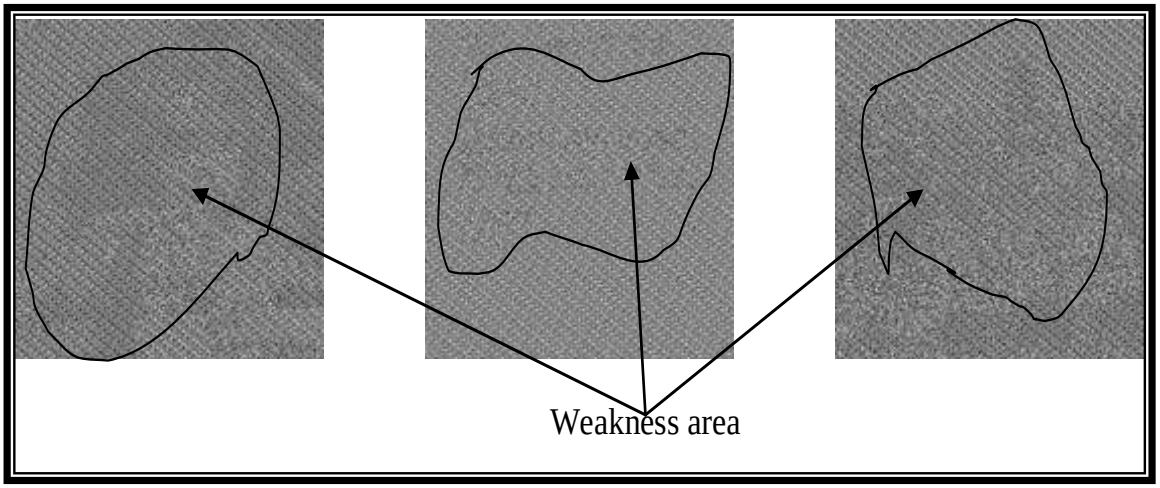
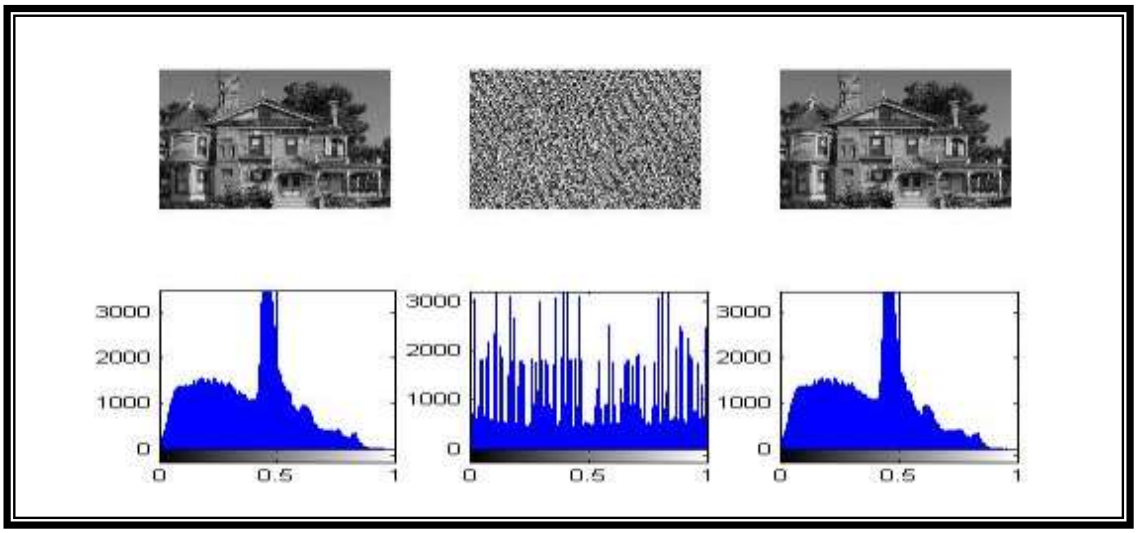
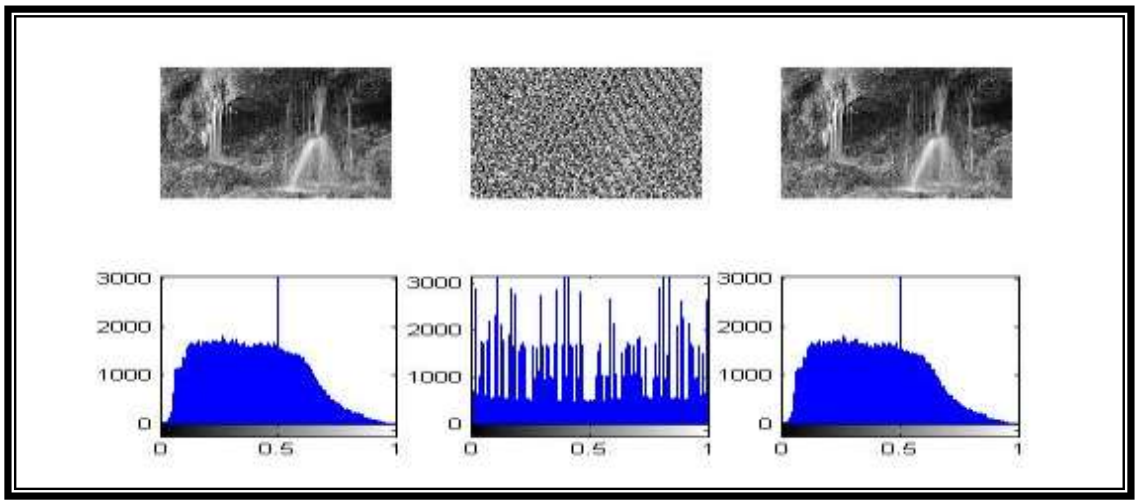
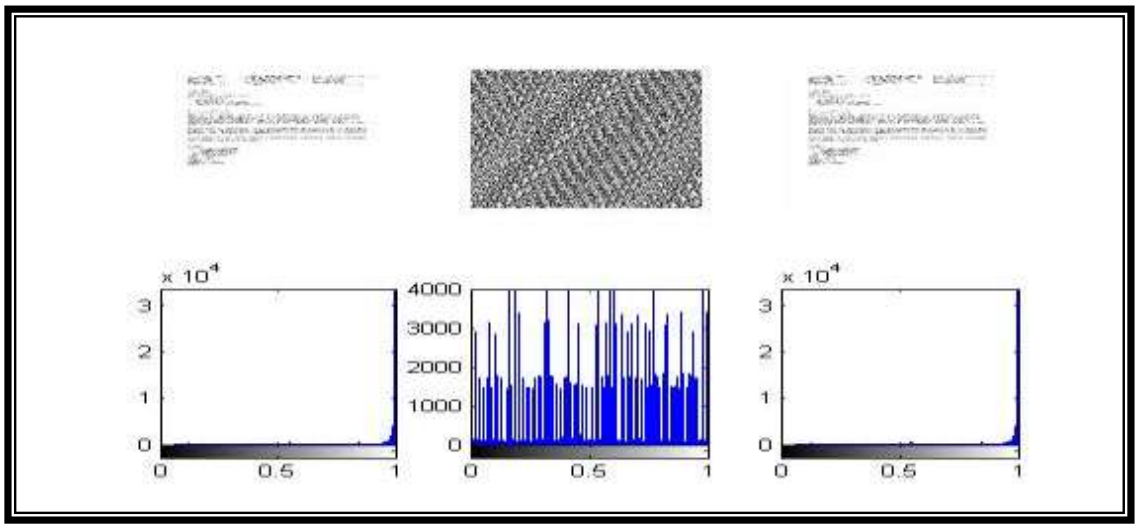
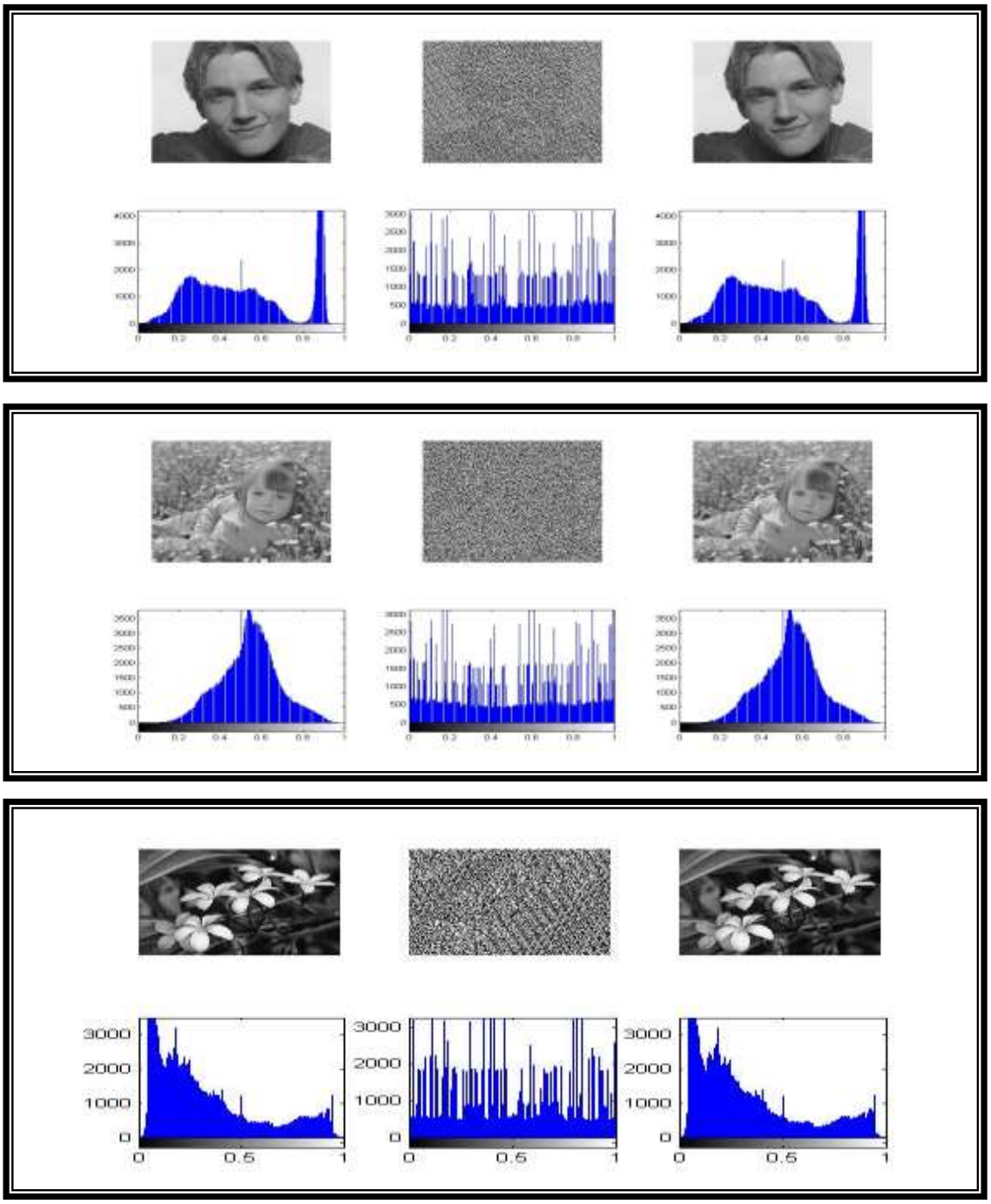


Figure (3): represent the weakness area when depending on the pseudo random generator only.


3000
2000
1000
0
0
0.5
1


3000
2000
1000
0
0
0.5
1


x 10^4
3
2
1
0
4000
3000
2000
1000
0
0
0.5
1



Figure(4):shows first row left column original image, center column encrypted image, right column decrypted image, second row left column original image histogram, center column encrypted image histogram, right column decrypted image histogram.

6. Conclusions

In this paper, we have presented a new scheme for image encryption method, the proposed method depending on merging Pseudo Random Generator with Crossover Genetic Algorithm, the new method is a lossless method and it has a high degree of the complexity with short time processing (few minutes). Additionally, using cryptography only the encrypted image has contain weakness area(contains information lead to break the image encryption) as shown in figure(3), but with G.A. produce high encrypted image as shown in figure(4).

References

1. M.A.F. Al-Husainy,2006, " image encryption using genetic algorithm", Information Technology Journal 5(3):516-519.

2. J.Daemen and V.Rijmen, 2002, "The Design of Rijndael, Advanced Encryption Standard", Springer-Verlag,Berlin.

3. R.L. Rivest, A. Shamir, and L. Adleman,1978, " A method for obtaining digital signatures and public key cryptosystems", Comm. ACM Vol. 21(2),pp.120-126.

4. R. Stinson, Douglas,1995," Theory and Practice", CRC Press.

5. M.Wenbo,2004,"Modren Cryptography: Theory and Practice", Publisher Hall PTR, Copyright: Hewlett Packard.

6. D.E. Goldberg, 1989, " Genetic algorithms in search optimization & Machine learning", Addison- Wesley.

7. Ibrahiem M.M. El-Emary and Mona M. Abd El-Kareem,2008 ,"On the Application of Genetic Algorithms in Finger Prints Registration" World Applied Sciences Journal 5(3):276-281.