http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

InformationTechnology Journal 5 (3): 516-519, 2006
ISSN 1812-5638

Image Encryption Using Genetic Algorithm

Mohammed A.F. Al-Husainy
Department of Computer Science, Faculty of Sciences and Information Technology,
Al-Zaytoonah University of Jordan, P.O. Box 130, Amman (11733), Jordan

Abstract: The security of digital images attracts much attention recently, especially when these digital images are stored in some types of memory or send through the communication networks. Many different image encryption methods have been proposed to keep the security of these images. Image encryption techniques tries to convert an image to another image that is hard to understand. In this proposed method, Genetic Algorithm (GA) is used to produce a new encryption method by exploitation the powerful features of the Crossover and Mutation operations of (GA). The proposed encryption method, in this study , has been tested on some known images and good results are recorded.

Key words: Transposition, substitution, crossover, mutation

INTRODUCTION

In the digital world nowadays, the security of digital images becomes more and more important since the communications of digital products over open network occur more and 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, etc. In order to fulfill such a task, many image encryption methods have been proposed, but some of them have been known to be insecure (Li and Zheng, 2002a).

Cryptographic systems for data security rely on the existence of large solution spaces to deter attack. Indeed, in the design of any cryptographic system it is an important point that the basic algorithm deter attempts to break it using so-called brute force attacks, involving simply running through all possible ways in which the algorithm could have encrypted the target data (Li and Zheng, 2002b; Shakir, 1997).

There are two classical techniques for encrypting data, which are used singly or in combination in virtually every cryptographic algorithm. Substitution involves the systematic replacement of bytes in the data by a cipher byte according to some algorithm. Being relatively easy to automate both mechanically and electronically, substitution has been very widely used in both government and commercial cryptographic systems. The second broad category of cryptographic algorithm is transposition, in which the relative order of bytes make up the data is permuted according to some rule. This is easy to automate, although the advent of microprocessors led to its being incorporated into a number of modern cryptographic systems, such as the Data Encryption Standard (DES) (Robert and Mathews, 1993).

The Genetic Algorithm (GA) relies primarily on the creative effects of sexual genetic recombination (Crossover) and the exploitative effects of the Darwinian principle of survival and reproduction of the fitness. Mutation is a second operation in Genetic Algorithm (GA). The crossover operation involves the exchange (swap) between two selected bytes (i.e., string of bits) the crossover points are randomly chosen. For example:

- Consider the data {64, 30, 230, 44, 0, 78}
- Consider crossing over at points 1 and 4 and swap the values at these positions to result {44, 30, 230, 64, 0,78}

The mutation operation is used to randomly alter the value at a single position in the data by applying a function. For example:

- Consider the data {64, 30, 230, 44, 0, 78}
- Consider the mutation operation applied at point 3 by using the function f(y)=255-x to result {64, 30, 25, 44, 0, 78}

It is clearly that (GA) based on both substitution (mutation) and transposition (crossover) operations (Cicirello and Smith, 2000; Al-Husainy, 2002; Koza, 1992).

The four major steps in preparing to use the conventional genetic algorithm on fixed length byte strings to solve a problem involve:

- Determining the representation scheme.
- Determining the fitness measure.

- Determining the parameters and variables for controlling the algorithm.
- Determining the way of designing the result and the criterion for terminating a run.

THE PROPOSED ENCRYPTION METHOD

In this study, 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. The new encryption method is developed to satisfy the following goals, where 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.

Opacity: Which is minimum when E(I)=I and maximum when E(I) is totally scrambled. So the variable opacity of the cryptosystem will allow the user of the system to decide on the degree of unrecognizability of the image.

Secure: The cryptosystem has to be resistant to any known attack. Attacks specific to high redundant messages like images are to be taken into account.

Low-complexity: The algorithm has to be based on low-cost operations.

The proposed encryption method consists of the following steps:

Step (1): Consider an image I(W×H), such that W and H are the width and height of I. Split the image I to a set of N vectors of length L (L = 64 bytes in this work).

Step (2): Then find R_1 and R_2 from the equations:

$$R_1 = \sum_{i=0}^{W-1}\sum_{j=0}^{H-1}(-1)^{(i+j)} * I(i,j) \Big/ 256 * L \quad (1)$$

$$R_2 = \sum_{i=0}^{W-1}\sum_{j=0}^{H-1}(-1)^{(i+j+1)} * I(i,j) \Big/ 256 * L \quad (2)$$

Assume the value $(R_1+R_2)/2$ as the start value of any known random number generation algorithm used that is used in this encryption method.

Step(3): Set x = R_1 and y = R_2.
For I = 0…N-1, set the following information for each vector Vi from the set of N vectors:

- CrossoverIndex = x
- CrossoverIteartion = $V_i(x)$
- MutationIndex = y
- MutationIteration = $V_i(y)$

x = x+1

y = y+1

if (x or y) >= L then set x = 0 and y = 0.

Step(4): For i = 0…N-1, perform Step(5) and Step(6) for each vector Vi from the set of N vectors. Note that both values in Vi (CrossoverIndex) and Vi (MutationIndex) are not participate in the crossover and mutation operation.

Step (5): (crossover operation)

- Set CrossoverIndex of vector Vi as a new start value of the adopted random number generation algorithm.
- For j from 0 to CrossoverIteartion of vector Vi, generate two random numbers N_1 and N_2 with values between (0..L-1), then perform $Vi(N_1) \leftrightarrow Vi(N_2)$

Step (6): (mutation operation)

- Set MutationIndex of vector Vi as a new start value of the adopted random number generation algorithm.
- For j from 0 to MutationIteartion of vector Vi, generate one random number N_1 with values between (0..L-1), then perform $Vi(N_1) = 255-Vi(N_1)$.

Step (7): Construct an encrypted image from the set of N encrypted vectors that are produced from the Step(4). Then hide the values R_1 and R_2 in the encrypted image.
Certainly, the proposed decryption method is done in the reverse form of the above encryption method.

EXPERIMENTS

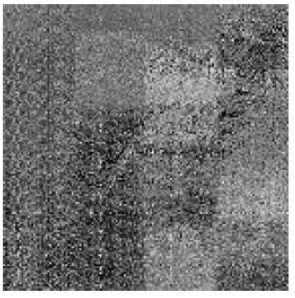
To test this proposed encryption method, the programs are written using Visual C++ 6.0 programming

Original image

After finished crossover operation

After finished mutation operation

After performed some crossover operations



After performed some mutation operations

Decrypted image

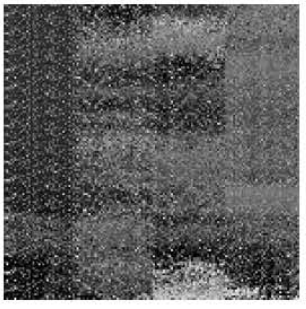
Experiment 1: Lena (256×256)

Original image

After finished crossover operation

After finished mutation operation

After performed some crossover operations



After performed some mutation operations

Decrypted image

Experiment 2: Girl (256×256)

language and applied this encryption method on some known images, the behavior of the method through the encryption and decryption phase showed as:

RESULTS AND DISCUSSION

Now, from the above experiments figures we can note that the first goal lossless was satisfied by this method because that the decrypted image is exactly similar to the original image without any loss of data through the encryption and decryption operations in this method. In other words, the recorded noise in the decrypted image is 0%.

It is clear that the opacity of between the encrypted images and he original images is very low. On the other side, the distortion between the original and the encrypted images that are shown in the above experiments is very high.

The secure of the proposed encryption method comes from the ability to use different vector lengths and from performing different number of crossover and mutation operations for each vector in the data of image. The number of crossover and mutation operations that are done in each vector depend on nature of the data in that vector.

To assessment the complexity of the proposed encryption method, the time in milliseconds for doing the encryption and decryption operations for each of the above experiments was recorded in the following table. These measures is done on the computer with microprocessor 2.40 GHz.

	Size of data	Encryption operation	Decryption operation
Experiment (1)	128KB	390	328
Experiment (2)	128KB	360	297

CONCLUSIONS AND FUTURE WORKS

After the experiments of the proposed encryption method in this paper, it is clearly that this encryption method was satisfied the goals that are required in any encryption method for encrypt images. The research in this study will be expanded to apply this method on the text data and multi-media data.

REFERENCES

Li, S. and X. Zheng, 2002a. Cryptanalysis of a chaotic image encryption method. The 2002 IEEE Intl. Symp. on Circuits and Systems (ISCAS 2002), Scottsdale, Arizona, Proceedings of ISCAS, 2: 708-711.

Li, S. and X. Zheng, 2002b. On the security of an image encryption method. The 2002 IEEE Intl. Conf. Image Processing (ICIP 2002), Rochester, New York, Proceedings of ICIP, 2: 925-928.

Shakir, M.H., 1997. A new feedback symmetric block cipher method. Ph.D Thesis in Computer Science at the University of Technology, Iraq.

Robert, A. and J. Mathews, 1993. The Use of Genetic Algorithms in Cryptanalysis. Cryptologia, 17: 187-201.

Cicirello, V.A. and S.F. Smith, 2000. Modeling GA Performance for Control Parameter Optimization. book title. Proceedings of the Genetic and Evolutionary Computation Conference ({GECCO}-2000), Morgan Kaufmann Publisher, Las Vegas, Nevada, USA, Internet Paper, URL: http://www.citeseer.nj.nec.com/cicirello00modeling.html, pp: 235-242.

Al-Husainy, M.A., 2002. Multi Media Data Processing Using Genetic Algorithm. Ph.D Thesis, E-mail: dralhusainy@yahoo.com.

Koza, Jr., 1992. Genetic Programming: On Programming of Computers by Means of Natural Selection. Bradford book. MIT Press, Cambridge, Massachusetts, London England.