Journal of Engineering and Applied Sciences 12 (Special Issue 9): 8679-8682, 2017
ISSN: 1816-949X

Data Encryption Employing Genetic Algorithm Based on a New Algorithm of Key Generator

Safa Saad A. Al-Murieb and Fryal Jassim Abd Al-Razaq
Information Technology College, University of Babylon, Hillah, Iraq

Abstract: Today's the data security is very necessary due to the wide uses of internet and the occurred development in communication media. So that, any data needs to be secured and protected by encrypted it to not be shown in its real form. In this study, the Genetic Algorithm (GA) was proposed for encryption any type of data file (image with any type-text, audio or video) with proposing a new algorithm to produce a key that was used in GA for encryption process using the operations of GA (crossover and mutation). The proposed encryption method can be used with watermarking and steganography, it is concerned the digital data integrity, security, confidentiality and authenticity.

Key words: Security, protection, data encryption and decryption, genetic algorithm and key generator, GA, confidentiality

INTRODUCTION

Data security: Todays, the basic concern includes providing security, protection and integrity for the digital data. To ensure the data security, either by watermarking it (concealing a visible watermark) or by encryption or cryptography process that is used to covert the original data form to non cleared form using secret keys (Stallings, 2011). Encryption operation encrypts the plain text with aiding of privet key this produces an intermediate cipher text, then, the last one will be decrypted to get the plain text after transmission of cipher text. The categories of cryptographic systems according to the used key are symmetric and asymmetric key. In the first type, the same key is used for both encryption and decryption operations (Dutta *et al*., 2014).

Genetic algorithm: John Holland conducted a technique for finding the solutions that are approximated to optimization problems of computer science, it is genetic algorithm which is a search algorithm that belongs to evolutionary algorithms which have operations like generation initial population, selection, recombination, mutation. There are three properties in GA, they are preproduction, recombination (crossover) and mutation whereas crossover operation corresponds to transposition process of cryptography while mutation operation corresponds to substitution process in cryptographic systems (Jhingran *et al*., 2015). GA begins with the first generation that is generated randomly, it represents a set of chromosomes (solutions). GA is used in many fields such as for optimization problems, scheduling of planning distributed network, problems of heuristic search in finding the optimum solutions, etc. (Matthews, 1993; Gondro and Kinghorn, 2007).

Literature review: There are many works of encryption and decryption the digital data using the genetic algorithms by Afarin and Mozaffari (2013), a method of two phases was proposed they were substitution and modification in the first phase the locations and values of image's pixels are changed in order to minimize the correlation between a pixel and its adjacent. While in the second phase the values were modified by encryption process. By Tragha *et al*. (2006), a cryptographic system was proposed with the aid of GA and physical model, the proposed schema could work on digital signal processing. Two schemas were worked they were GA that was used for symmetric cryptography system and RSA for asymmetric system whereas GA was used for key development (Hassan *et al*., 2014). By Singh *et al*. (2014), GA was used for providing security for images with the sequence of pseudorandom whereas nonlinear feedback shift register was used for generating that sequence. A function of self regression was proposed for encryption as by Bhowmik and Acharyya (2011). By Enayatifar and Abdullah (2011), the mixing of GA and chaotic function was proposed for encryption with high stability and efficiency achieving.

MATERIALS AND METHODS

Designing the suggested infrastructure: In this study, the genetic algorithm was used to achieve securing of digital data by encryption it, the data can be text file, audio, image or video file. The operation crossover and

Corresponding Author: Safa Saad A. Al-Murieb, Information Technology College, University of Babylon, Hillah, Iraq

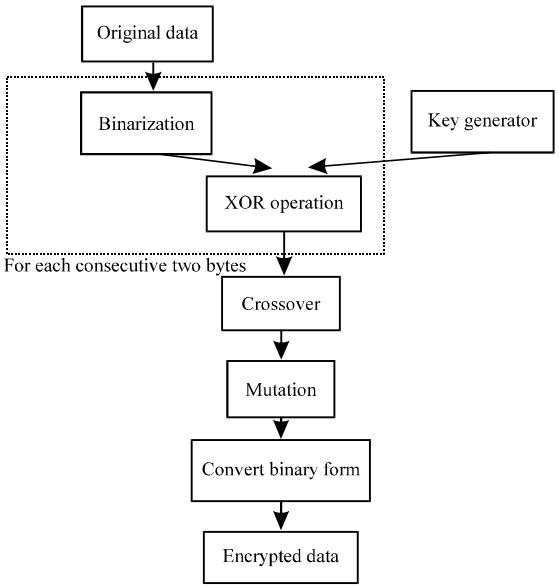

Fig. 1: Encryption process

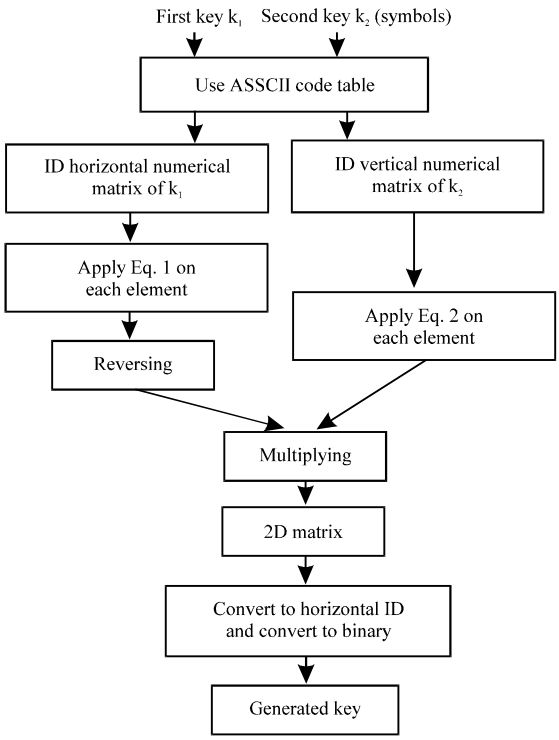

Fig. 2: Key generator process

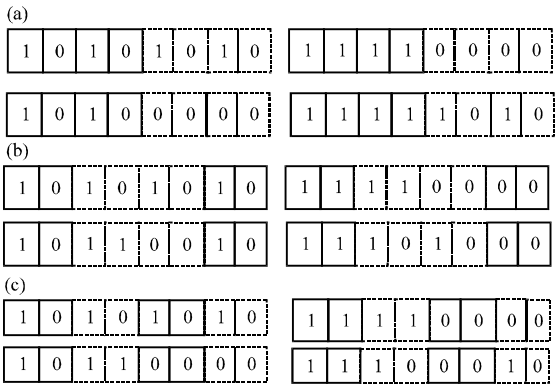

Fig. 3: Crossover types: a) Single point; b) Two points and c) Multipoint

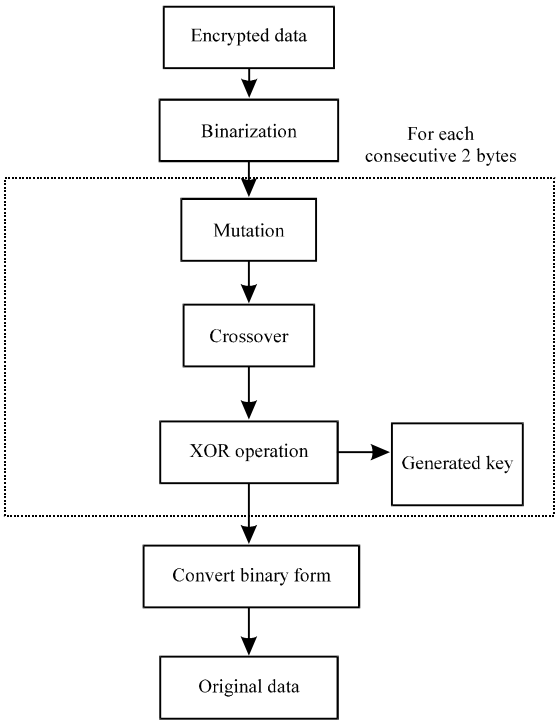

Fig. 4: Decryption process

mutation of GA were used. Figure 1 explains the main block diagram of the encryption process while Fig. 2-4 explains the steps of decryption diagram of the proposed research.

Where the proposed research encrypt any type of digital data whereas in the preprocessing it should be converted to the binary form such that if the data file of text, the contains are converted according to the ASCII code table to the binary form. If the file is for image (with any type) which represents each pixel with 8 bits, then, each pixel value is converted to binary and if it is RGB, each band of three bytes is converted to binary form.

The main idea of the encryption block diagram after get the binary form of the original (plain) data is working in each two consecutive bytes whereas each byte of them is input to the XOR gate with the generated key. Then,

apply the crossover between the results of XOR gate on $byte_i$ and on $byte_{i+1}$. The apply mutation operation on each generated byte, so, these step produce two encrypted bytes with binary form. Thus finally each encrypted byte is converted to the form according to the file's type that was encrypted. While the steps of key generator algorithm shown in Fig. 2.

Firstly, two initial keys are input they are a set of symbols, named first key (k_1) and second one (k_2). Then, the symbols of each key are transferred to the numerical matrix according to the ASSCII code table, k_1 transferred to horizontal matrix M_1, k_1 transferred to vertical matrix M_2. Now applying Eq. 1 and 2 on each element of M_1 and M_2, respectively. The result of Eq. 1 is matrix A and of Eq. 2 is matrix B:

$$A(p) = M_1(p)\text{-}p \quad (1)$$

$$B(p) = M_2(p)\text{-}2p \quad (2)$$

where, p is the element's position in the 1D matrix, p = 1, 2, ..., n. Then, reverse the matrix A and multiply it by matrix B to get 2D matrix C which is converted to 1D and finally is converted to binary form it represents the final generated key that will be used in the encryption process.

The generated key will also be used in the decryption process. About the generated key, in encrypt or decrypt each byte one byte is used from the key, so, that in working with the next byte of data, the next byte from key will be used and so on.

The idea of decryption is firstly convert the encrypted data to the binary form, then do mutation operation on each byte of two consecutive of encrypted bytes and do recombination between them. Then, each resulted byte of them will be input with the generated key to the XOR gate to get the original data.

In the crossover operation (recombination) of GA three kinds were used they are single point, two points and multipoint. One type was used in each time according to the result of modulation of summation of sequence of the two consecutive bytes ($byte_i$ and $byte_{i+1}$) by three. The type of crossover was chosen as follow:

- If 2i+1 mod 3 equal 0 then use single point type
- If 2i+1 mod 3 equal 1 then use two point type
- If 2i+1 mod 3 equal 2 then use multipoint type

These rules were used in both encryption and decryption process to know which kind of crossover was used. Figure 3 shows an example of the types of crossover that were used in this research. In the mutation operation, the components of each resulted offspring will be flipped by converting the bit of 0-1 and vice versa.

RESULTS AND DISCUSSION

The implementation of the proposed encryption system is as follows. Firstly, convert the data from its clear form to the binary form according to the type of data file whereas any type of digital data such as image for any type, text, audio, etc., then, the key that will be used in encryption process is generated based on entering two initial keys of symbols. The proposed algorithm of key generator achieves randomness, diffusion and confusion.

The generated key was used in encryption and decryption processes where in encryption it was entered to XOR gate with a byte of binary data, after get two encrypted bytes, the crossover operation is applied on them, the type of recombination was chosen according to the modulation of sequences of those two bytes by three. After that, the mutation operation was applied. Table 1 shows samples of experimental result of proposed encryption schema.

For example, if the message "ARMY" will be encrypted and for example if the entered two initial keys of symbols are (Hi) and (Dr), the steps of encryption process is as follow. The decimal values of the two initial keys are (72, 105) and (68, 114), then after applying Eq. 1 on first key, then reversing it and Eq. 2 on second key, the two keys become (104, 71) in horizontal vector and (66, 110) in vertical vector. Now multiplying these vectors to get a vector (6864, 11440, 4686, 7810), since, there are only 128 entries in ASSCII table, the modulation result by 128 is dependent, so, the new vector is (80, 48, 78, 2) which its binary form is (01010000, 00110000, 01001110, 00000010) it is a generated key that will be used in encryption and decryption processes. The binary form of the entered data (ARMY) is (01000001, 01010010, 01001101, 01011001), now for each two consecutive bytes applying the XOR operation between a byte from the generated key and a byte from the original data, so for the first two bytes, the results of XOR for the first and second bytes are (00010001) and (01100010), then doing the crossover between these resulted two bytes (according to the result of modulation by three of summation of sequences of the two consecutive bytes as cleared previously, single point type was used because now the working is on first and second resulted bytes) whereas the two resulted bytes of the crossover are (00010010) and

Table 1: Results of the experiments

Data	Encrypted data	Decrypted data
ARMY	m>d<	ARMY
Computer science	f?I/re!*+na 06jB	Computer science
Security	K8my#]r>	Security
Cryptographic system	Olp5?-Ip.?$sA&d<gjm*	Cryptographic system

(01100001). After applying the mutation operation on each resulted byte, to get the new 2 bytes (11101101) and (10011110) which their decimal values are (237) and (158). The results of XOR for the third and fourth bytes are (00000011) and (01011011), then crossover will be applied between these two bytes (using two points type because now the working is on third and fourth bytes) and the two resulted bytes from the crossover are (00011011) and (01000011). Then doing the mutation on them to get (11100100) and (10111100), their decimal values are (228) and (188).

From the above steps, the result of decimal values of encryption the characters of the message "ARMY" is (237, 158, 228, 188), now calculating the modular by 128 for each value that is >128, to get (109, 30, 100, 60). Due to the symbols of keyboard controlling and the symbols of controlling the information sending and saving, those symbols are in ASSCII table from entry 0-31. So, the solution of the state (if the final result of encryption the character in the decimal range (0.31) is by adding 32, so, the new result of encryption the second byte becomes 62. The corresponding characters of the decimal values (109, 62, 100, 60) are "m>d<".

CONCLUSION

The proposed encryption schema results the alphabetic (A, ..., Z and a, ..., z), numbers (0, ..., 9) and the other symbols like (*, ",/,+,?, $, etc.) that are in the ASSCII table, so that, this makes the encrypted result more variable and the same message can be encrypted to the different results by changing the entered two initial keys that produce the generated key which is used in encryption process.

ACKNOWLEDGEMENTS

Researchers thank and offer the Gratitude to the Information Technology College for its Support to the Postgraduates. Also, researchers present the thankfulness to them classmate for them encourage along the research.

REFERENCES

Afarin, R. and S. Mozaffari, 2013. Image encryption using genetic algorithm and binary patterns. Proceedings of the 2013 10th International ISC Conference on Information Security and Cryptology (ISCISC), August 29-30, 2013, IEEE, Yazd, Iran, ISBN:978-1-4799-1638-2, pp: 1-5.

Bhowmik, S. and S. Acharyya, 2011. Image cryptography: The genetic algorithm approach. Proceedings of the 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE) Vol. 2, June 10-12, 2011, IEEE, Shanghai, China, ISBN:978-1-4244-8727-1, pp: 223-227.

Dutta, S., T. Das, S. Jash, D. Patra and P. Paul, 2014. A cryptography algorithm using the operations of genetic algorithm and pseudo random sequence generating functions. Intl. J., 3: 325-330.

Enayatifar, R. and A.H. Abdullah, 2011. Image security via. genetic algorithm. Proceedings of the 2011 International Conference on Computer and Software Modeling IPCSIT Vol. 14, May 26, 2011, IACSIT Press, Singapore, pp: 198-203.

Gondro, C. and B.P. Kinghorn, 2007. A simple genetic algorithm for multiple sequence alignment. Genet. Mol. Res., 6: 964-982.

Hassan, A.K.S., A.F. Shalash and N.F. Saudy, 2014. Modifications on RSA cryptosystem using genetic optimization. Intl. J. Res. Rev. Appl. Sci., 19: 150-155.

Jhingran, R.,V. Thada and S. Dhaka, 2015. A study on cryptography using genetic algorithm. Int. J. Comput. Appl., 118: 10-14.

Matthews, R.A., 1993. The use of genetic algorithms in cryptanalysis. Cryptologia, 17: 187-201.

Singh, P., G. Gosawi and S. Dubey, 2014. Genetic algorithms: A technique for cryptography real time data transmission. Binary J. Data Mining Networking, 4: 37-40.

Stallings, W., 2011. Cryptography and Network Security: Principles and Practice. 5th Edn., Prentice Hall, Upper Saddle River, New Jersey, USA., ISBN: 9780137056323, Pages: 743.

Tragha, A., F. Omary and A. Mouloudi, 2006. ICIGA: Improved cryptography inspired by genetic algorithms. Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06) Vol. 1, November 9-11, 2006, IEEE, Cheju Island, South Korea, pp: 335-341.