International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 1, February 2021, pp. 434~441
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i1.pp434-441

Features of genetic algorithm for plain text encryption

Riyadh Bassil Abduljabbar, Oday Kamil Hamid, Nazar Jabbar Alhyani
Department of Computer Techniques Engineering, Dijlah University College, Iraq

Article Info

Article history:

Received Apr 24, 2020
Revised Jun 15, 2020
Accepted Aug 5, 2020

Keywords:

Crossover
Genetic algorithm
Mutation
Plain text
Text encryption

ABSTRACT

The data communication has been growing in present day. Therefore, the data encryption became very essential in secured data transmission and storage and protecting data contents from intruder and unauthorized persons. In this paper, a fast technique for text encryption depending on genetic algorithm is presented. The encryption approach is achieved by the genetic operators Crossover and mutation. The encryption proposal technique based on dividing the plain text characters into pairs, and applying the crossover operation between them, followed by the mutation operation to get the encrypted text. The experimental results show that the proposal provides an important improvement in encryption rate with comparatively high-speed processing.

Corresponding Author:

Riyadh Bassil Abduljabbar,
Department of Computer Engineering Techniques,
Dijlah University College,
Baghdad, Iraq.
Email: riyadh.bassil@duc.edu.iq

1. INTRODUCTION

Cryptography field has been attracted a lot of concern especially in network security. Internet popularity and its usage increases due and to the exponential increase in the security needs for the transactions ine-commerce field [1]. In addition to risks which involved regarding the communication of raw data via the Internet. High and importance gain could be provided by data integrity, non-repudiation, confidentiality, and authenticity which become more important component in the security of information [2, 3]. The best solution for keeping safe data transfer is the use of cryptography as a technique for encrypting and decrypting messages soany body can not interpret it, only the message sender and the receiver can. Consequently, data encryption has become an inevitable and integral part of any application in e-commerce [4-6]. Therefore, it is very important to encrypt data using a robust and fast encryption algorithm in order to make sure of secret transmission and data delivery to protect it from any intruder. In general, the concept of encryption techniques is converting the plain text to cipher text before storage or transmission [7-10]. The Genetic algorithm properties (mutation, crossover and selection) have been exploited by many researchers for data encryption optimizing and searching problems through generating typical solutions [11, 12]. This paper introduces new method for data encryption based on the Genetic algorithm operators (Crossover and mutation) with a varying crossover and mutation points of indexs between character pairs.

The outline of this paper is ordered: Section 1 focoused on the work review. The suggested technique is described in section 2. The experimental results and encryption analysis are highlight in section 3. Finally, conclusion is showed in section 4. In Cryptography, many researches have been done to enhance the genetic algorithm. Jhingran and Vikas [13] presented Studies on cryptography techniques using

genetic algorithm. In which, cryptography system is proposed by utilized thegenetic algorithm and public key. In 2014, Sindhuja and Pramela [14, 15] introduced a symmetric key for message encryption and decryption. The length of secret key is concerned with number point of both crossover and mutation processing.

Srikanth and Noha proposed mutation and crossover operations of genetic algorithm with pseudorandom function for data encryption [16]. To increase the robustness of the secret key, Nazeer and Ghulamo, suggests genetic algorithm with random number generator to introduce a secret key. The raw data is diffused by crossover and mutation. Finally, the diffused data and key are undergoing to logical operations [17]. In 2019, Alsadig and Mandour [18] have proposed a text encryption using genetic algorithm. The secret key is generated by exploit the crossover and mutation. Then, the permutation factor generated randomly. Subsequently, the secret key and the permutation factor are applied to the plain text.

Shafiul and Sabir also proposed genetic algorithm combined with fitness function for text encryption, in which the crossover and mutation operations are combined with a random function generator for best key generation [19]. Afigha and Sofia [20] suggested security improvement to randomness of security key unexpected based on crossover and mutation features of genetic algorithm. The results show that the generated secret key is most randomness and unpredictable by the intruder.

In order to protect and secured data in cloud computing, Amitha and T.R suggested algorithm called DSLA, in which a private key is used to investigate the user reliability [21]. The IOT (Internet of Thing) is a device useful for communicate and exchange information between computerize schemes. Rubesh and kirybanand presented a proposal to increase the security level between IOT and clients by integrate the public key, asymmetric and symmetric cryptography system [22].

In 2020, Nedal.and Ashraf, introduced a combine chaotic map with RSA algorithm to improve security level of RSA key. The results show that the security level of new approach is enhanced compared with RAS public key standalone and reduced the computational processing time [23]. The main security of WSN established on key distribution between nodes. Jyothi and Nagarai defines a new method for key distribution within WSN based on ECC. The proposal reshuffling the ECC public key by utilized Arnold map. The result show that the suggestion can be applied on poor recourse communication system [24]. Several ciphers have been developed to text encryption. Oday and nazar in 2019, described cipher algorithm for text encryption. The encryption implements Pascal matrix and inverse Pascal matrix preformed for decryption processing [25].

2. RESEARCH METHOD

The proposed algorithm is divided into two main processes, the encryption process and the decryption process each onedepends on genetic operators to implement the encryption and decryptionwith the aid of character pairs technique.

2.1. Encryption process

As shown in Figure 1, encryption process can be characterized starting from reading the plain text message, converting the text characters into binary form after taking its equivalent Unicodevalues. The first generation is produced when crossover operation is implemented between the binary pairs (crossover index (1) is used for the first pair (1) for the second pair (3) for the third pair till (8) for the eighth pair and the cross over is restarted to (1) for the nineth pair and so on. Mutation point is applied to the resulted generation (mutation index (1) is used for the first pair (1) for the second pair (3) for the third pair till (8) for the eighth pair and the cross over is restarted to (1) for the nineth pair and so on. Ciphered text is produced after getting the equivalent characters according to ASCII table. The methodology of the encryption process is illustrated in Figure 1.

2.2. Decryption process

The decryption method is shown in Figure 2, and described as follows, at the receiver part the receiver will receive the encrypted text that consists of two parts the first part is (Parent1) and the second part is (Parent2). Both (Parent1) and (Parent2) characters are converted to its equivalentuincodevaluesand then to their equivalent binary form of byte length. Mutation operation is implemented on (Parent1) and (Parent2)(mutation index (1) is used for the first pair (1) for the second pair (3) for the third pair till (8) for the eighth pair and the cross over is restarted to (1) for the nineth pair and so onthe result is (Child1 & Child2). Crossover operation is donebetweenthe (Child1) and (Child2)(crossover index (1) is used for the first pair (1) for the second pair (3) for the third pair till (8) for the eighth pair and the cross over is restarted to (1) for the nineth pair and so onto get theoriginalplain text. The methodology of the decryption process is illustrated in Figure 2.

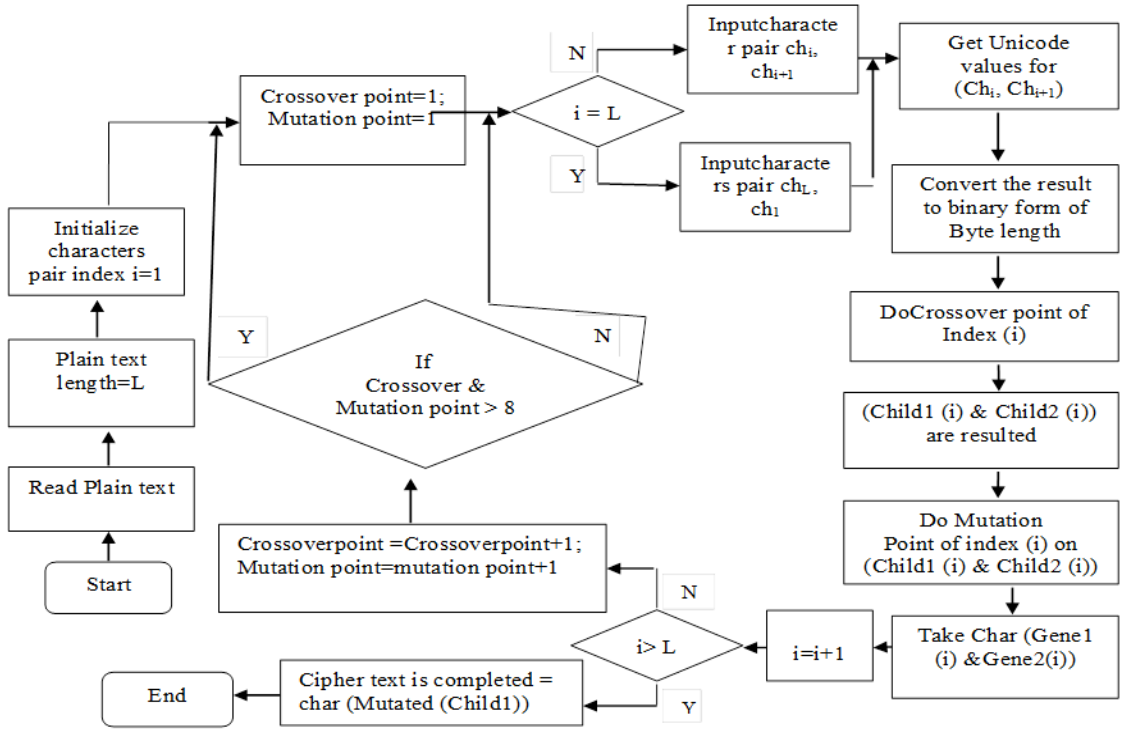

Figure 1. Flow chart of the encryption process

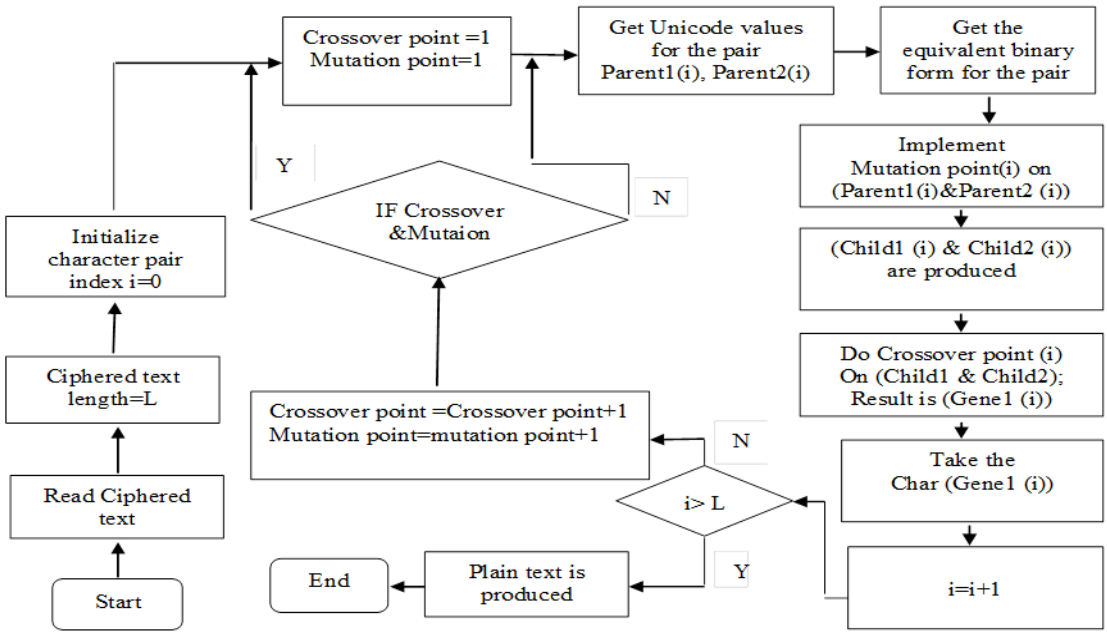

Figure 2. Flow chart of thedecryption process

3. RESULTS AND DISCUSSIONS

All the expermints have been preformed in MATLAB version 10 and achivied on Intel core i5 processor (2.4) GHz and RAM (8) GB.

3.1. Encrypting an English text message

The proposal encryption structure as shown in Figure 3 and defined as follows:

At first the English plain text message to be encrypted using the proposed technique is read by using (text read) Matlab instruction. The plain textthatenterd to the program is "Very secret message" so the plain text message contains (19) characters. The encryption process for the plain text message is illustrated in the below steps:

1: Read the plain text message that is saved in a (.txt) file.
2: Calculate the length of the plain text (L=19)
3: Initialize character pair index (i=1)
4: Mutation point = 1; Crossoverpoint=1
5: If i=L then input (Ch_L& Ch_1) Else input (Ch_i & Ch_{i+1})
6: Gettheunicodefor each character.
7: Convert the unicodevaluesinto its equivalent binary form of (8-bit) length
8: Do single point Crossover operation of index (i) betweenthe pairs of indexs (i& i+1)
9: Mutate the result (Child1(i)) & (Child2(i)) using Mutation point index (i)
10: Get the (char) of the Mutation operation result
11: Ciphered character of index (i) is produced
12: Increment the variable (i) by one (i=i+1)
13: If (i>19) Then Ciphered text is completedElse (Crossover point= Crossoverpoint+1);
Mutation point = Mutation Point+1
14: If Crossover point& Mutation point> 8 Then (Crossoverpoint =1; Mutationpoint =1)
15: Check If i=19Then input the characters pair of indexes of (19&1) hence (Ch_{19}, Ch_1)
DoSteps (6-14) Else Do Steps (6-15)

The result is the encrypted text which is "dp}x3Q%ฺdvd%}G3ะfgR" is sent along with (Child2). The result which is "Wgv!`G#ิsg0huQ3ั ea" after running the Matlab program are illustrated in the Figure 3.

The plain text message	Very secretmessage
The Unicodevaluesofthe plain text characters	86 101 114 121 32 115 101 99 114 101 116 32 109 101 115 115 97 103 101
(Parent1) 8-bit binary equivalent for each Unicode value	01010110 01100101 01110010 01111001 00100000 01110011 01100101 01100011 01110010 01100101 01110100 00100000 01101101 01100101 01110011 01110011 01100001 01100111 01100101
Crossover operation result (Child1) between the pairs (i,i+1)	01100101 01110010 01111001 01110000 00100011 01110001 01100101 01110010 01100101 01110100 01100000 00101101 01101101 01100111 01110011 01100001 01100111 01100101 01110110
Crossover operation result (Child2) between the pairs (i,i+1)	01010110 01100101 01110010 00101001 01110000 01100111 01100011 01100011 01110010 01100101 00110100 01100000 01100101 01110001 01110011 01110011 01100001 01100111 01000101
Mutationoperationresult on (Child1)	01100100 01110000 01111101 01111000 00110011 01010001 00100101 11110010 01100100 01110110 01100100 00100101 01111101 01000111 00110011 11100001 01100110 01100111 01110010
Mutation operation result on (Child2)	01010111 01100111 01110110 00100001 01100000 01000111 00100011 11100011 01110011 01100111 00110000 01101000 01110101 01010001 00110011 11110011 01100000 01100101 01000001
Unicode equivalent values For (Child1)	100 112 125 120 51 81 37 242 100 118 100 37 125 71 51 225 102 103 114
The Ciphered text	dp}x3Q%ฺdvd%}G3ะfgr
Unicode equivalent values For (Child2)	87 103 118 33 96 71 35 227 115 103 48 104 117 81 51 243 96 101 65
Child2 text	Wgv!`G#ิsg0huQ3ั Ea

Figure 3. Program run results

3.2. Decrypting an English text message

The decryption steps and the results are summarized in Figure 4, and demonstrated as follows:

At the receiver end the receiver will receive the encrypted text“dp}x3Q%ۯdvd%}G3ڇfgr” which is considered as (Parent1) along with “Wgv!`G#ڑsg0huQ3ۯeA”which is considered as (Parent2) this encrypted text message is read by using (text read) Matlabinstruction. The encryption process for the plain text message is illustrated in the below steps:

1: Read theencryptedplain text message (.txt) file.
2: Calculate the plain text length (L=38), which is equal to ((Recived text length)/2) = (38/2) =19
4: Initialize character pair index (i=0)
5: Initialize the Crossoverpoint (Crossoverpoint=1)
3: Initialize Mutation point (Mutation point =1)
7: Input the characters pair (Parent1(i), Parent2(i))
8: Gettheunicodefor each character.
9: Convert the unicode values into its equivalent binary form of (8-bit) length
10: Do mutation operation of index (i) between (Parent1 (i) & Parent2(i)).
11: The Mutation operation result is (Child1(i) &Child2(i))
12: Do single point Crossover operation of index (i) between (Child1(i) &Child2(i))
13: Plain textcharacter of index (i) is produced
14: Increment the variable (i) by one (i=i+1)
15: If (i>19) Then Plain text is completed Else
(Crossover point= Crossoverpoint+1); Mutation point=Mutation point+1)
16: Crossover point= Crossoverpoint+1; Mutation point=Mutation point+1
17: If Crossover point& Mutation point> 8 Then (Crossoverpoint =1; Mutation point=1)
18: DoSteps (7-18)

Parent1	**dp}x3Q%ۯdvd%}G3ڇfgr**
Unicode equivalent values of(Parent1)	100 112 125 120 51 81 37 242 100 118 100 37 125 71 51 225 102 103 114
Parent2	**Wgv!`G#ڑsg0huQ3ۯeA**
Unicode equivalent values of (Parent2)	87 103 118 33 96 71 35 227 115 103 48 104 117 81 51 243 96 101 65
Binary equivalent values of(Parent1)	01100100 01110000 01111101 01111000 00110011 01010001 00100101 11110010 01100100 01110110 01100100 00100101 01111101 01000111 00110011 11100001 01100110 01100111 01110010
Binary equivalent values of (Parent2)	01010111 01100111 01110110 00100001 01100000 01000111 00100011 11100011 01110011 01100111 00110000 01101000 01110101 01010001 00110011 11110011 01100000 01100101 01000001
Child1: The mutation result on (Parent1)	01100101 01110010 01111001 01110000 00100011 01110001 01100101 01110010 01100101 01110100 01100000 00101101 01101101 01100111 01110011 01100001 01100111 01100101 01110110
Child2: The mutation result on (Parent2)	010101100110010101110010001010010111000001100111011000 011000110111001001100101001101000110000001100101011100 01110011011100110110000101100111010000101
Crossover operation result between (Gene1 & Gene2)	01010110 01100101 01110010 01111001 00100000 01110011 01100101 01100011 01110010 01100101 01110100 00100000 01101101 01100101 01110011 01110011 01100001 01100111 01100101
Unicode equivalent values ofthe crossover operation result	86 101 114 121 32 115 101 99 114 101 116 32 109 101 115 115 97 103 101
The decrypted text	**Very secret message**

Figure 4. Program run results

3.3. Execution time

Generally, the standard cipher AES, DES and RSA are more scure. On the other hand, have high computional cost to very large data files encryption [26]. In this approach, the compution time analysis has been performed for five different data file size as shown in Table 1. From Table 1 and Figure 5 it can be shown that the results of the proposal outperformed the RAS and DES in the execution time term. Undoubtedly, the computional cost proportional inverse with file size.

Table 1. Comparison between the proposed work and other traditional encryption algorithms

Data Encryption Standard	RSA Algorithm	Text Pair Genetic (Proposed Work)	Text Size (Kilobyte)
2.553 sec	5.6373 sec	1.636 sec	10 KB
6.865 sec	11.274 sec	5.980 sec	20 KB
11.652 sec	16.912 sec	9.175 sec	30 KB
15.175 sec	22.549 sec	13.361 sec	40 KB
19.719 sec	28.186 sec	16.557 sec	50 KB

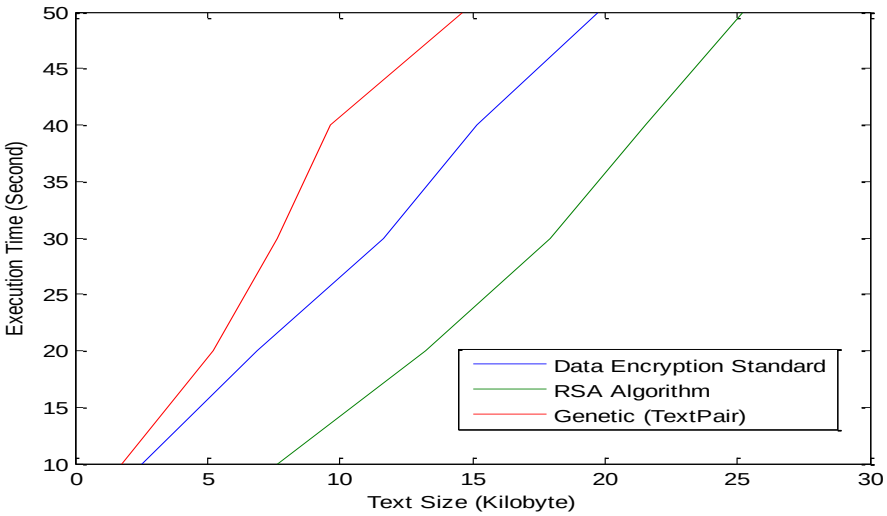

Figure 5. Encryption time of the approach, [RSA] and [DES] algorithms

3.4. Throughput

The calculation of Throughput is preformed by dividing the sum of the input files sizes to the time consumed by the encryption process as illustrated in (1). The comparison results between GA, DES and RSA is shown in Tables 2 and 3. As shown in previous tables, the GA achieved reasonable throughput compared with DES and RSA. Throughput (Kilobyte/Second) = SUM. (Input text file size)/SUM. (Encryption execution time)

Table 2. Comparison of encryption throughput of the proposed work [GA] and DES, RSA algorithms

Encryption Algorithm	File Size (KB)	Encryption Throughput (KB/Sec.)
Proposed work [GA]	225KB	4.0229
DES [6]	225KB	3.3011
RSA [6]	225KB	2.6608

Table 3. Comparison of encryption throughput of the proposed work [GA] and DES, RSA algorithms

Text File Size (Kilobyte)		
100KB	Algorithm	Throughput (Kilobyte/Second)
100KB	RSA	1.228 Seconds
100KB	Data Encryption Standard	1.963 Seconds

4. CONCLUSION

In this paper, encryption approach for ciphering Arabic text using genetic algorithm operators has been proposed. This approach is Simple and easy to implement in cryptographic system because it depends on two basic operations the crossover and mutation. In this proposal, Genetic operator algorithms, encryption and decryption processes are achieved in acceptable security level in both transmission and receiving end, due to the use of crossover and mutation operations in which binary and decimal conversions increase the strength of encryption approach. On other hand, the computational time of this approach is relatively high compared with other traditional cryptography schems like DES and RSA algorithms. Numerous expansions of the suggestion could be projected in the upcoming time like enhancing the security level of encryption by using chaotic logistic map. Secondly, implement it for multimedia encryption.

REFERENCES

[1] C. S. Cherian and Rasmi P. S., "Genetic Algorithm and Random number Generation for Symmetric Encryption," *International Journal of New Innovations in Engineering and Technology*, vol. 10, no. 2, pp. 1-5, 2019.

[2] A. Kumar and K. Chatterjee, "An efficient stream cipher using genetic algorithm," in *International Conference on Wireless Communications, Signal Processing and Networking*, pp. 2322-2326, 2016.

[3] Ragavan M. and K. Prabu, "Dynamic Key generation for Cryptographic Process using Genetic Algorithm," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 4, pp. 246-250, 2019.

[4] B. Maram, et al., "Intelligent security algorithm for UNICODE data privacy and security in IOT," *Service Oriented Computing and Applications*, pp. 1-13, 2018.

[5] P. A. N. Agbedemnab, et al., "A Novel Text Encryption and Decryption Scheme using the Genetic Algorithm and Residual Numbers," in K. Njenga (ed), *Proceedings of 4th International Conference on the Internet, Cyber Security and Information System*, vol. 12, pp. 20-31, 2019.

[6] H. M. Mousa, "Bat-Genetic Encryption Technique," *International Journal of Intelligent Systems and Applications*, vol 11, pp. 1-15, 2019.

[7] H. N. Hussain and W. N. Hussein, "Implementation of Symmetric Encryption Algorithms," *Computer Engineering and Intelligent Systems*, vol. 8, no. 4, pp. 13-18, 2017.

[8] K. K. Mandal, et al., "Applying Encryption Algorithm on Text Steganography Based on Number System," in *Computational Advancement in Communication Circuits and Systems*, pp. 255-266, 2020.

[9] O. K. Hamid, "Arabic Text Encryption Using Artificial Neural Networks," *Engineering and Technology Journal*, vol. 34, no. 5, pp. 887-899, 2016.

[10] K. Alla, et al., "A Novel Encryption Using Genetic Algorithms and Quantum Computing with Roulette Wheel Algorithm for Secret Key Generation," in *ICT Analysis and Applications*, pp. 263-271, 2020.

[11] J. Rodriguez, et al., "Genetic Operators Applied to Symmetric Cryptography," *International Journal of Interactive Multimedia & Artificial Intelligence*, vol. 5, no. 7, pp. 39-49, 2019.

[12] M. Krajcovic, et al., "Parameter setting for a genetic algorithm layout planner as a toll of sustainable manufacturing," *Sustainability*, vol. 11, no. 7, 2019.

[13] R. Jhingran, et al., "A study on cryptography using genetic algorithm," *International Journal of Computer Applications*, vol. 118, no. 20, pp. 10-14, 2015.

[14] S. Mishra and S. Bali, "Public key cryptography using genetic algorithm," *International Journal of Recent Technology and Engineering*, vol. 2, no. 2, pp. 150-154, 2013.

[15] Sindhuja K. and Pramela D. S., "A symmetric key encryption technique using genetic algorithm," *International journal of computer science and information technologies*, vol. 5, no. 1, pp. 414-416, 2014.

[16] P. Srikanth, et al., "Encryption and Decryption Using Genetic Algorithm Operations and Pseudorandom Number," *IJCSN-International Journal of Computer Science and Network*, vol. 6, no. 3, pp. 455-459, 2017.

[17] M. I. Nazeer, et al., "Implication of Genetic Algorithm in Cryptography to Enhance Security," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 6, pp. 375-379, 2018.

[18] A. M. Abdallah and M. M. Ibrahim, "Text Encryption Using Genetic Algorithm," *IJCSN - International Journal of Computer Science and Network*, vol. 8, no. 1, pp. 36-39, 2019.

[19] Alam M. S., et al., "An improved fitness function for automated cryptanalysis using genetic algorithm," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 2, pp. 643-648, 2019.

[20] A. Z. Zakaria, "Enhancing the Randomness of Symmetric Key using Genetic Algorithm," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 8S, pp. 327-330, 2019.

[21] K. Anitha and T. G. Nair, "Data storage lock algorithm with cryptographic techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3843-3849, 2019.

[22] R. Bhandari and Kirubanand V. B., "Enhanced encryption technique for secure iot data transmission," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3732-3738, 2019.

[23] N. Tahat, et al., "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1430-1437, 2020.

[24] Jyothi R. and N. G. Cholli, "An efficient approach for secured communication in wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1641-1647, 2020.

[25] O. K. Riyadh, et al., "Fast and robust approach for data security in communication channel using pascal matrix," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 19, no. 1, pp. 248-256, 2020.

[26] N. Al-Hayani, et al., "Simultaneous video compression and encryption for real-time secure transmission," *2013 8th International Symposium on Image and Signal Processing and Analysis*, pp. 240-245, 2013.

BIOGRAPHIES OF AUTHORS

Riyadh Bassil Abduljabbar received his Bsc. Eng. and M.D. Eng. in Computer and Control Engineering from University of Baghdad Iraq in 2000 and 2003 respectivelt. Currently, he is a senior lecturer in the Faculty of Computer Engineering Techniques at Dijlah University College Iraq (DUC). His research interests include Data Security, Networking, Cluod Security, Computer Architecture.

Oday Kamil Hamid received his Bsc. in Electrical Engineering and M.D. Eng in Communication Engineering from University of Technology Iraq in 2000 and 2003 respectively. Currently, he is a senior lecturer in the Faculty of Computer Engineering Techniques at Dijlah University College Iraq (DUC). His research interest, communication, security, digital signal processing, speech recognition, neural network.

Nazar Jabbar Alhyani received his PhD of Science in Electronic Engineering from University of Buckingham - UK in 2015. Currently, he is a university staff at Dijlah University College Iraq (DUC). His research interests include secure transmission, video encryption and compression, cloud security and data encryption.