A comparative review on symmetric and asymmetric DNA-based cryptography

Baraa Tareq Hammad[1], Ali Maki Sagheer[2], Ismail Taha Ahmed[3], Norziana Jamil[4]
[1,2,3]College of Computer Sciences and Information Technology, University of Anbar, Iraq
[4]College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia

Article Info

Article history:

Received Mar 14, 2020
Revised May 30, 2020
Accepted Jun 23, 2020

Keywords:

Asymmetric cryptography
DNA-based
GZIP
OTP
RSA
Symmetric cryptography

ABSTRACT

Current researchers have focused on DNA-based cryptography, in fact, DNA or deoxyribonucleic acid, has been applied in cryptography for performing computation as well as storing and transmitting information. In the present work, we made use of DNA in cryptographic, i.e. its storing capabilities (superior information density) and parallelism, in order to improve other classical cryptographic algorithms. Data encryption is made possible via DNA sequences. In this paper, two cases utilizing different DNA properties were studied by combining the DNA codes with those conventional cryptography algorithms. The first case concerned on symmetric cryptography that involved DNA coding with OTP (one time pad) algorithms. Asymmetric cryptography was considered in the second case by incorporating the DNA codes in RSA algorithm. The efficiencies of DNA coding in OTP, RSA, and other algorithms were given. As observed, the computational time of RSA algorithm combined with DNA coding was longer. In order to alleviate this problem, data redundancy was reduced by activating the GZIP compressed algorithm. The present experimental results showed that DNA symmetric cryptography worked quite well in both time and size analyses. Nevertheless, it was less efficient than the compressed DNA asymmetric cryptography.

Corresponding Author:

Baraa Tareq Hammad,
College of Computer Sciences and Information Technology,
University of Anbar,
Anbar, Iraq.
Email: baraa.tareq@uoanbar.edu.iq

1. INTRODUCTION

Cryptography involves encoding a message (encrypted format) prior to transmission so that the data is unreadable for security reasons. Numerous security algorithms have been proposed as security in data storage is a major concern nowadays. There are two types of cryptography: symmetric and asymmetric. Traditional cryptography can be traced back to Caesar cipher proposed ~2000 years ago. One of the recent cryptography methods is DNA cryptography which was reported twenty years ago [1].

DNA cryptography is a relatively new cryptographic method that is inspired from DNA computing by using DNA as information carrier [2]. In fact, DNA can be used for performing computation and storing/transmitting information [3] thanks to its vast parallelism and extraordinary information density. Due to these reasons, it has been used in encryption [4], authentication [5], and signature [6]. In general, the main security depends on the limitation of biotechnology, and not on the computing power [7]. The main limitation of DNA cryptography is the lack of effective protected theory and simple achievable method. Therefore, the current research trend in DNA cryptography is to explore the peculiarity of DNA molecule and reaction so that more useful theories can be established. Typically, a gram of DNA consists of 1021

DNA bases, which is equivalent to 108 TB of data [8]. Gehani *et al.* [9] introduced the first algorithm of DNA-based cryptography.

Raj and Sharmila [10] reviewed some DNA cryptographic approaches and highlighted their merits and demerits. Thilagavathy and Murugan [11] highlighted the security concern in cloud computing, and proposed a DNA and JPEG Zigzag coding with an encryption scheme. They have reported some technological implications and contemporary research issues as well. Furthermore, they have proposed an improved identity-based cryptographic approach. Kannadasan *et al.* [8] conducted a survey on the performances of some recent molecular DNA big data technologies. Chauhan and Jain [12] highlighted the pros and cons of some DNA cryptography methods. Bhateja and Mittal [13] provided a holistic view on the current trend of DNA steganography by studying their minute aspects related to information security. Kaur and Malhotra [14] argued that DNA cryptography could ensure data security. The application of DNA cryptography in RLE data compression has been reported as well. Cherian *et al.* [15] provided an overview of several approaches in DNA cryptography. According to them, all digital data can be encrypted by using extended ASCII. Abood and Guirguis [16] provides a survey of DNA computing by focusing on its application.

The purpose of this paper is to study the efficiency of DNA cryptography using the DNA coding with the conventional cryptography algorithms. A compressed DNA-RSA was studies to speed up the conventional RSA algorithm and remove the redundancy. Replace the conventional cryptography by using (DNA cryptography) to give more strength, by combining the Power of bio-cryptography with computational cryptography to increase the data security. In section 2 include DNA Structure. Section 3 overview on DNA symmetric and asymmetric cryptography. The performance analysis was given in section 4. Section 5 explained a theoretical analysis of some types of attacks on DNA Cryptography. Section 6 concludes the current work.

2. DNA STRUCTURE

Nowadays, biological cryptography algorithms become more and more popular, and they are applied to many kinds of applications. One of the most of these techniques is DNA. DNA is the basic tools of storage in every living cell. The DNA main function is to absorb and transfer the data for millions of years. The information in DNA is passed from one generation to the next. The DNA guides the cell to making new proteins that determine the biological traits for every human being and copy this information and keep it for billions of years. Thus, it could be around 10 trillion DNA molecules in small size [17]. The structure of DNA is composed of two twisted strands of four bases that represent the genetic code, adenine (A), cytosine (C), thymine (T), and guanine (G). (A) bonds with the complementary (T), (G) bonds with the complementary (C), and vice versa. Thus, one strand and the corresponding complementary strand constitute DNA. For example, one strand is ACTGAA, so the other is should be TGACTT as shown in Figure 1 [18, 19]. In Table1 we can see that for each DNA bases there is an equivalent DNA coding, for Example the DNA bases A can be logically represented it by “00”, the same things about the other three DNA bases T “01”, C “10”, and G by”11”.

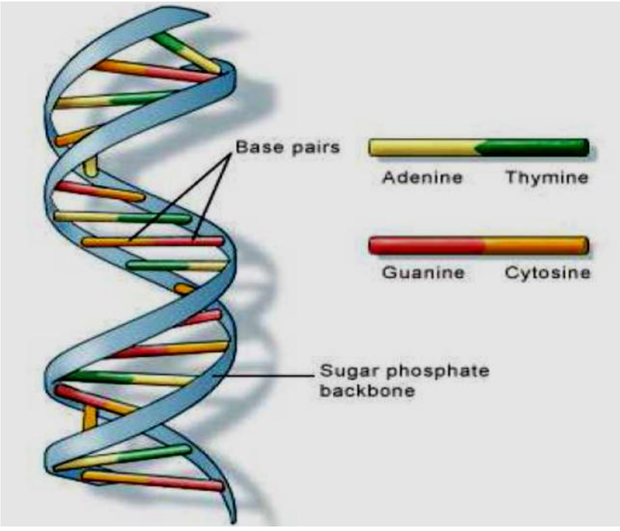

Figure 1. The Structure of part of A DNA double helix [19]

Table1. DNA coding

DNA sequence	Binary
A	00
T	01
C	10
G	11

3. DNA SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY: OVERVIEW

The use of DNA computing in cryptography was initialized by Adleman in 1994 where he uses DNA computing instead of traditional cryptography in solving a directed Hamiltonian path problem [12]. Ashish *et al.* [5] 1999 use the DNA computing concept on DNA Steganography. There are many researches in the DNA cryptography fields, Table 2 includes a brief Description for some researches in DNA cryptography, and also discuss some of the techniques that been used in these researches, we can see from Table 2 that the research has been divided into two type's symmetric and asymmetric cryptography as summarized below:

Table 2. Previous symmetric and asymmetric researches description

Author name	Year	Description	Type
F´abio *et al.* [13]	2007	They use RSA and Diffie-Hellman with DNA computing. They also used DCT (discrete cosine transform) coefficients to transfer messages in steganography. They claim that this proposed provide an extra security for a specific application where more security is required.	*Asymmetric*
Alberto *et al.* [14]	2009	In this proposal authenticate was identify, they used a combine between a DNA and fuzzy logic. Those results were compared with previous work, show some achievements. This proposed show a better results in accessing time by comparison between the protein template and a database template.	*Symmetric*
Ranbir *et al.* [16]	2010	This approach is a combine between DNA and elliptic curve discrete logarithm problem (ECDLP) used for authentication. This paper discussed the previous DNA and ECDLP. They also show the problems that could face the researchers when using DNA in information security.	*Asymmetric*
Tatiana Hodorogea *et al.* [20]	2011	In this paper the authors choose technique near to the human DNA sequence. By using the same gene from different genes. ProbCons tool and a pair-hidden Markov model have been used to provide the users with the private/public keys.	*Asymmetric*
Zhang Yunpeng *et al.* [21]	2011	This research includes an index-based symmetric DNA encryption algorithm. By using the block-cipher and index of string, the algorithm has a specific step for encoding the plaintext. Each character will be encrypted into its ASCII codes. After that it should be converted into the DNA coding (according to DNA index). To generate the keys the authors used the chaos key generator based on the logistic mapping.	*Symmetric*
Olga Tornea, Monica E. Borda [22]	2013	This research includes a study of DNA cryptography. They also propose an algorithm that's a combine between DNA and OTP. This paper took the benefits from the randomness and non-repeating that DNA medium provide.	*Symmetric*
Anchal Jain [23]	2013	By using DNA computing the researchers propose a technique that provides key length for encrypt images. The large key 72-bit addition with DNA complementary provides the encryption text with extra security level.	*Asymmetric*
Shipra Jain [24]	2014	The researchers proposed a way for providing security by using DNA computing in producing a key. They claimed that this technique can be used in any application or any type of data. The strength of security in this technique depends on the complexity of keys.	*Symmetric*
Sreeja C.S [25]	2014	The researchers present DNA symmetric algorithm by using the central dogma of molecular biology and pseudo DNA cryptography. In this algorithm they use splicing and padding rules to add extra security level.	*Symmetric*
Mona Sabry *et al.* [26]	2015	The researchers proposed an algorithm by combine the DNA sequence instead of the bits and the advanced encryption standard (AES). They took the benefits from the biological environment and the DNA computing.	*Asymmetric*
Raj et.al. [27]	2016	They proposed a symmetric algorithm by using DNA cryptography. They present a secured symmetric key generation process which generates initial cipher and this initial cipher is then converted into final cipher using random key generated DNA sequences.	Symmetric
Alaa Kadhim F. [28]	2016	The authors proposed a new s-box by using the properties of DNA sequence, XOR and some mathematical operations. They claimed that by changing only one bit could provide secure S-box, with 255 differences of key. Also, the S-box inverse could be generated by using same strings that are used in generating the S-box.	*Asymmetric*
Bismi Beegom S. *et al.* [29]	2017	They present method that use round key selection. They provide three levels of security in first level they use the round key selection and message encryption, in the second level they use asymmetric key encryption with 16×16 matrix manipulation, while in the last level they use the shift operation.	*Asymmetric*
Md. Rafiul Biswas *et al.* [30]	2017	In this research a combination of DNA encoding and asymmetric cryptosystem was used. To produce the key the plaintext was split into chunks with fixed sized, then encrypts by using asymmetric cryptosystem after that by using DNA encoding concatenated these chunks to produce the ciphertext.	*Asymmetric*
Ahgue *et al.* [31]	2018	This research proposed an algorithm that combine between chaotic and DNA sequences, its symmetric cryptography. The parameters of the algorithms could be customized by the user according to the requirements.	*Symmetric*

Table 2. Previous symmetric and asymmetric researches description (c*ontinue*)

Author name	Year	Description	Type
Zhang, Zhou, and Niu [32]	2018	They proposed an image encryption by using DNA cryptography and the Feistel network. Initially to produce the hash digest they use the SHA-3 algorithm, while to produce the Hill cipher matrix they use the chaos-generated sequence. Then in the Feistel network the DNA sequence has been used.	*Symmetric*
Patnala [33]	2019	The researchers present a DNA-based cryptography algorithm using DNA Codons. They use a random lookup table contains the DNA codons and their corresponding equivalent alphabet values as substitution method.	*Symmetric*
Siddaramappa and Ramesh [17]	2019	They propose an algorithm that uses DNA sequences for encryption and decryption. The key of 64, 128, 192, 256 bits length can be produce by using genes.	*Symmetric*
Basu *et al.* [34]	2019	The researchers design a new system by using the central dogma of molecular biology (CDMB) by simulating the Genetic Coding and the other operation of DNA sequence. The plaintext is chunks into 16-bits blocks. Then to produce the ciphertext the blocks merge in the form of protein bases.	*Asymmetric*

4. PERFORMANCE ANALYSIS

This paper combined between the use of symmetric and asymmetric cryptography, the purpose from this combination is to see the effect of DNA coding on the cryptography algorithm. One of the most important points that must be taken into account is the size of files and the time required to accomplish the encryption and decryption process. Actually, it’s hard to say that this comparison is faire because each algorithm has its own criteria. The principle goal in the design of any algorithm must be security, performance, and implementation cost. The performance test method determines the amount of time and size required to perform cryptographic operations. There is no a standard tool or specific technique for evaluating or testing algorithm design, because each algorithm is different from the other in designing structure and internal operations in addition to mathematical bases. The comparison carries out among three algorithms combined between DNA coding and the traditional algorithms: DNA-OTP, DNA-RSA, and compressed DNA-RSA. This test also includes executing all the necessary algorithms, symmetric algorithm (OTP), and asymmetric algorithm (RSA). Table 3 shows the difference in size between the plaintext and ciphertext for each algorithm.

Table 3. Plain text size vs. cipher text size

Algorithms	Test file	Size of plaintext in bytes	Size of ciphertext in bytes
DNA-OTP	500 char	1070	4352
	1000 char	1685	6912
	2000 char	3070	12288
	3000 char	4834	19456
	4000 char	6056	24320
OTP	500 char	1070	1280
	1000 char	1685	1792
	2000 char	3070	3072
	3000 char	4834	4864
	4000 char	6056	6144
DNA-RSA	500 char	1070	113028
	1000 char	1685	177868
	2000 char	3070	324324
	3000 char	4834	510320
	4000 char	6056	651376
RSA	500 char	1070	32694
	1000 char	1685	39836
	2000 char	3070	54793
	3000 char	4834	86284
	4000 char	6056	103945
Compressed DNA-RSA	500 char	1070	40164
	1000 char	1685	57872
	2000 char	3070	91948
	3000 char	4834	110828
	4000 char	6056	106632

Based on the results and the files obtained in Table 3, Figure 2 indicates that the size of the cipher text is increased in every test case. It also shows that a large file can also be encrypted using this procedure. From Figure 2, it can be seen that the DNA-RSA encrypts the text into a huge size while the other algorithms take a normal size in spite of that the texts are converted into DNA coding before interring into the encrypt algorithm. The size of decryption cipher text in DNA-OTP are four time more than the plaintext because the plain text is converted into DNA coding which is depends on four bases (A, T, C, G), while the compressed DNA-RSA take a normal size near to the conventional RSA algorithm. Table 4 shows the difference in time (in milli-second) between the encryption and decryption for each algorithm to make a good analysis between them.

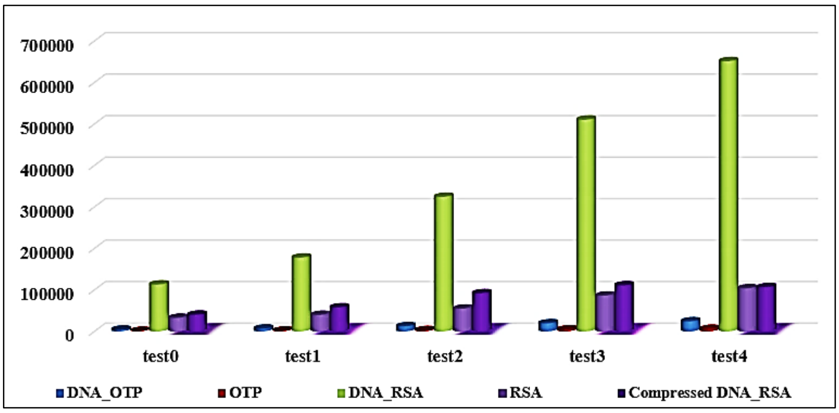

Figure 2. Plain text size vs. cipher text size

Table 4. The time comparison among algorithms

Algorithms	Test file	Encryption time in milli-second	Decryption time in milli-second
DNA-OTP	500 char	1.3	1.42
	1000 char	2.00	2.30
	2000 char	2.76	2.85
	3000 char	3.12	3.45
	4000 char	4.23	4.55
OTP	500 char	0.4	0.2
	1000 char	0.2	0.3
	2000 char	0.38	0.3
	3000 char	0.4	0,29
	4000 char	0.5	0,28
DNA-RSA	500 char	28.77	33.22
	1000 char	72	69
	2000 char	188	249
	3000 char	325	334
	4000 char	461	415
RSA	500 char	4.86	6.74
	1000 char	7.23	8.11
	2000 char	11.67	12.48
	3000 char	16.9	16.77
	4000 char	20.13	21.46
Compressed DNA-RSA	500 char	5.94	8.30
	1000 char	10.47	16.17
	2000 char	14.78	20.21
	3000 char	23.96	28.61
	4000 char	28.17	40.57

In Figure 3 it could be seen that the compressed DNA-RSA achieved the goal that has been illustrated, when uses the compression made the result better. The value of encryption and decryption are near to the symmetric cryptography (DNA-OTP). In spite of using public key in this algorithm which make it require more computational time. From Table 4 and by using online T.TEST calculator, the P-value of (DNA-OTP & DNA-RSA) encryption is (0.057) and decryption is (0.042) so it could be said that these values are Alternative hypothesis. The P-value of (DNA-OTP & compressed DNA-RSA) encryption is (0.027) and decryption is (0.022) so it's also considered as alternative hypothesis. The same expatiated result can be seen for (DNA-RSA & compressed DNA-RSA) the P-value encryption is (0.068) and decryption is (0.055). To compare the time required and to complete the encryption/decryption operations compared the execution time of the DNA algorithms with the time required by the traditional algorithms using a random text of 360 characters, in string format which was applied to all tests. As shown in Table 5, a fair comparison could not be reached because the download algorithms were executed on different computer with different properties.

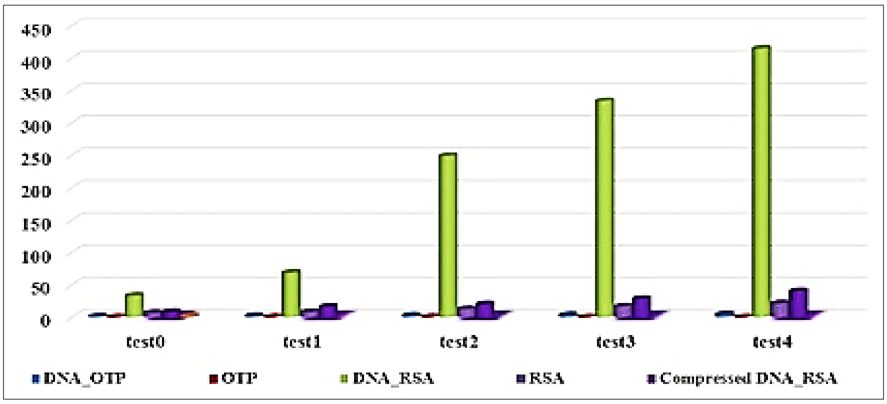

Figure 3. Plain text time vs. cipher text time

Table 5. Comparison between DNA algorithms and conventional algorithms

Algorithms	Encryption time in milli-second	Decryption time in milli-second
DNA-OTP	1.95	1.98
OTP	0.12	0.07
DNA-RSA	11.78	16.92
RSA	5.34	6.7
Compressed DNA-RSA	4.3	6.3
AES	2.8	2.9
DES	3.4	0.75

Table 5 shows the DNA algorithms along with the traditional algorithms, DNA with RSA takes the processing time of 11.78 milli-seconds whereas DNA with compress RSA takes only 4.3 milli-seconds. In spite of that the compressed DNA-RSA algorithm is a public key cryptography and other algorithm is symmetric algorithm. As shown in Table 5, the DNA cipher requires a longer execution time for encryption and decryption, comparatively to the other ciphers. It's expectable because of the nature of conversion in DNA coding. The traditional cryptography process array of bytes while in the DNA cryptography is about strings. The extra conversions efforts make this encryption\decryption require more time.

5. ATTACK ON DNA BASED-CRYPTOGRAPHY

A good security algorithm should be venerable against most kinds of attacks. The purpose from these algorithms is to reduce the probability of a successful attack and to protect the valuable data. So below there is an analysis for some types of attack on DNA -based cryptography from theoretical view [35]. A brute force attack systematically attempts every possible key used in a known plaintext/ciphertext attack. In DNA the four base genes lack linguistic properties or redundancy as in human language. If the attacker tries to attacks the communication by using this attack, it would be a very expensive computational problem. For more security a big key size is very important, to make the primitives more venerable to it [36].

Side channel attacks depends on the additional information taken from the physical implementation of a security algorithm, like the hardware used to encrypt/decrypt data, the CPU cycles used, performance calculation, and voltage. DNA cryptography take the benefits from the combinatorial properties of DNA computation to be more venerable to this type of attacks [37]. Another kind of attacks is meet-in-the-middle attacks, this kind of attacks used with multiple keys algorithms. It is a known plaintext attack; the attacker should have access to both the plaintext and ciphertext. This attack attempts to find a middle value that be used by both plaintext and ciphertext. So, we can say that in DNA cryptography it's hard to find these values because there is no relation between the plaintext (regular text) and the ciphertext (DNA coding).

Linear cryptanalysis and Differential cryptanalysis also same as the meet-in-the-middle attacks is a known plaintext attack. These attacks require a statistical analysis on large amounts of ciphertext. It can take the benefits from DNA computing, with a very high parallelism and a big amount of storage [3]. The DNA cryptography could be used to pre-process the plaintext. So by combine between the biological and traditional cryptography could be provide an extra security levels [37].

6. CONCLUSION

In this paper, we have reviewed some of the existing DNA based-cryptography with two cases symmetric and asymmetric cryptography. First, a combination of DNA coding with OTP (one time pad) algorithms, second, the DNA codes in RSA algorithm was studied. The efficiencies of DNA coding in OTP, RSA and other algorithms were given. From result it could be Saied that the computational time of RSA algorithm combined with DNA coding was longer. In order to solve this issue, data redundancy was reduced by activating the GZIP compressed algorithm. The present experimental results showed that DNA symmetric cryptography worked quite well in both time and size analyses. Nevertheless, it was less efficient than the compressed DNA asymmetric cryptography.

REFERENCES

[1] P. Rakheja, "Integrating DNA computing in International data encryption algorithm (IDEA)," *Int. J. Comput. Appl.*, vol. 26, no. 3, pp. 1-6, 2011.

[2] D. Prabhu and M. Adimoolam, "Bi-serial DNA encryption algorithm (BDEA)," *arXiv Prepr. arXiv1101.2577 Computer Science:Cryptography and Security*, 2011.

[3] S. Sadeg, M. Gougache, N. Mansouri, and H. Drias, "An encryption algorithm inspired from DNA," in *2010 International Conference on Machine and Web Intelligence (ICMWI)*, pp. 344-349, 2010.

[4] S. K. Muttoo, D. Aggarwal, and B. Ahuja, "A secure image encryption algorithm based on hill cipher system," *Bulletin of Electrical Engineering and Informatics*, vol. 1, no. 1, pp. 51-60, 2011.

[5] E. R. Arboleda, J. L. Balaba, and J. C. L. Espineli, "Chaotic rivest-shamir-adlerman algorithm with data encryption standard scheduling," *Bulletin of Electronics Engineering and Informatics*, vol. 6, no. 3, pp. 219-227, 2017.

[6] C. Meshram, "The beta cryptosystem," *Bulletin of Electronics Engineering and Informatics*, vol. 4, no. 2, pp. 155-159, 2015.

[7] M. Misbahuddin, "An efficient solution for remote user authentication using DNA crypto and steganography," in *Proceedings of the International Conference on Security and Management (SAM)*, pp. 54-60, 2018.

[8] R. Kannadasan, M. S. Saleembasha, and I. Arnold Emerson, "Survey on molecular cryptographic network DNA (MCND) using BIG DATA," *Procedia Comput. Sci.*, vol. 50, pp. 3-9, 2015.

[9] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in *Aspects of Molecular Computing*, Springer, pp. 167-188, 2003.

[10] B. B. Raj and V. C. Sharmila, "An survey on DNA based cryptography," in *2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)*, pp. 1-3, 2018.

[11] R. Thilagavathy and A. Murugan, "Cloud computing: A survey on security issues and DNA, ID-base cryptography," *Indian J. Sci. Technol.*, vol. 9, no. 28, pp. 1-6, 2016.

[12] J. Chauhan and A. Jain, "Survey on encryption algorithm based on chaos theory and DNA cryptography," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 8, pp. 7801-7803, 2014.

[13] A. Bhateja and K. Mittal, "DNA steganography: Literature survey on its viability as a novel cryptosystem," *J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 8-14, 2015.

[14] S. Kaur and S. Malhotra, "A review on image encryption using DNA based cryptography techniques," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 4, no. 3, 2016.

[15] A. Cherian, S. R. Raj, and A. Abraham, "A survey on different DNA cryptographic methods," *Int. J. Sci. Res.*, vol. 2, no. 4, pp. 167-169, 2013.

[16] O. G. Abood and S. K. Guirguis, "DNA computing and its application to information and data security field: A survey," *DNA*, vol. 3, no. 1, pp. 1-5, 2019.

[17] V. Siddaramappa and K. B. Ramesh, "DNA-based XOR operation (DNAX) for data security using DNA as a storage medium," in *Integrated Intelligent Computing, Communication and Security*, Springer, pp. 343-351, 2019.

[18] H. Mousa, K. Moustafa, W. Abdel-Wahed, and M. M. Hadhoud, "Data hiding based on contrast mapping using DNA medium.," *Int. Arab J. Inf. Technol.*, vol. 8, no. 2, pp. 147-154, 2011.

[19] K. Hameed, "DNA computation based approach for enhanced computing power," *Int. J. Emerg. Sci.*, vol. 1, no. 1, pp. 23-30, 2011.

[20] T. Hodorogea, I. S. Otto, and S. Janetta, "Deriving DNA cryptographic keys based on evolutionary models," in *2011 12th International Carpathian Control Conference (ICCC)*, pp. 144-147, 2011.

[21] Z. Yunpeng, Z. Yu, W. Zhong, and R. O. Sinnott, "Index-based symmetric DNA encryption algorithm," in *2011 4th International Congress on Image and Signal Processing*, vol. 5, pp. 2290-2294, 2011.

[22] O. Tornea and M. E. Borda, "Security and complexity of a DNA-based cipher," in *2013 11th RoEduNet International Conference*, pp. 1-5, 2013.

[23] A. Jain and N. Rajpal, "Adaptive key length based encryption algorithm using DNA approach," in *2013 International Conference on Machine Intelligence and Research Advancement*, pp. 140-144, 2013.

[24] S. Jain and V. Bhatnagar, "Bit based symmetric encryption method using DNA sequence," in *2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence)*, pp. 495-498, 2014.

[25] C. S. Sreeja, M. Misbahuddin, and M. H. NP, "DNA for information security: A survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology," in *International Conference on Computing and Communication Technologies*, pp. 1-6, 2014.

[26] M. Sabry, M. Hashem, T. Nazmy, and M. E. Khalifa, “Design of DNA-based advanced encryption standard (AES),” in *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, pp. 390-397, 2015.

[27] B. B. Raj, J. F. Vijay, and T. Mahalakshmi, “Secure data transfer through DNA cryptography using symmetric algorithm,” *Int. J. Comput. Appl.*, vol. 133, no. 2, pp. 19-23, 2016.

[28] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, “Proposal new s-box depending on DNA computing and mathematical operations,” in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, pp. 1-6, 2016.

[29] S. B. Beegom and S. Jose, “An enhanced cryptographic model based on DNA approach,” in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 2, pp. 317-322, 2017.

[30] M. R. Biswas, K. M. R. Alam, A. Akber, and Y. Morimoto, “A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem,” in *2017 4th International Conference on Networking, Systems and Security (NSysS)*, pp. 1-8, 2017.

[31] A. O. Ahgue, S. Franz, J. D. De Nkapkop, P. Adelis, J. Y. Effa, and M. Borda, “A DNA-based chaos algorithm for an efficient image encryption application,” in *2018 International Symposium on Electronics and Telecommunications (ISETC)*, pp. 1-4, 2018.

[32] X. Zhang, Z. Zhou, and Y. Niu, “An image encryption method based on the feistel network and dynamic DNA encoding,” *IEEE Photonics J.*, vol. 10, no. 4, pp. 1-14, 2018.

[33] B. D. Patnala and R. K. Kumar, “A novel level-based DNA security algorithm using DNA codons,” in *Computational Intelligence and Big Data Analytics*, Springer, pp. 1-13, 2019.

[34] S. Basu, M. Karuppiah, M. Nasipuri, A. K. Halder, and N. Radhakrishnan, “Bio-inspired cryptosystem with DNA cryptography and neural networks,” *J. Syst. Archit.*, 2019.

[35] H. Tatiana, V. Mircea-Florin, B. Monica, and S. Cosmin, “A Java crypto implementation of DNAprovider featuring complexity in theory and practice,” in *ITI 2008-30th International Conference on Information Technology Interfaces*, pp. 607-612, 2008.

[36] S. R. Maniyath and M. Supriya, “An uncompressed image encryption algorithm based on DNA sequences,” *Comput. Sci. Inf. Technol.*, vol. 2, pp. 258-270, 2011.

[37] X. Lai, M. Lu, L. Qin, J. Han, and X. Fang, “Asymmetric encryption and signature method with DNA technology,” *Sci. China Inf. Sci.*, vol. 53, no. 3, pp. 506-514, 2010.

BIOGRAPHIES OF AUTHORS

Baraa Tareq Hammmad received her B.E. and M.Sc. degrees in Computer Science from College of Computer Science and Information Technology, University of Anbar, Anbar, in 2005 and 2012, respectively. She received her Ph.D. degrees in Computer Science from College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia, in 2018. Her research interests Include Information Security, IoT and Network Security.

Ali Makki Sagheer He got on B.Sc. of Information System in Computer Science Department at the University of Technology (2001)-Iraq, M.Sc. in Data Security from the University of Technology (2004)-Iraq and Ph.D. in Computer Science from the University of Technology (2007)-Iraq. He is interesting in Cryptology, Information Security, Cyber Security Number Theory, Multimedia Compression, Image Processing, Coding Systems and Artificial Intelligence. He obtained Professor scientific degree in Cryptography and Information Security since 18 Jul 2015.

Ismail Taha Ahmed received his B.E. and M.Sc. degrees in Computer Science from College of Computer Science and Information Technology, University of Anbar, Anbar, in 2005 and 2009, respectively. He received his Ph.D. degrees in Computer Science from College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia, in 2018. His research interests Include Image Quality Assessment, Deep Learning, and Computer Vision.

Norziana Jamil received her BSc (Information Technology), 2000, form Universiti Kebangsaan Malaysia, and she received her MSc (Information Security), 2005, from Royal Holloway University of London, UK, while she finish her PhD (Security in Computing), 2013, from UPM university, She is interested in cryptography, Authentication, SCADA system, wireless sensor network.