I. J. Mathematical Sciences and Computing, **2022, 4, 30-40**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2022.04.03

A 4-D HyperChaotic DNA Encryption/Decryption Algorithm for Securing Students Data System

Ghada Yousef
Faculty of Science, Al-Azhar University,Cairo, Egypt
E-mail: ghadaelwan.el20@azhar.edu.eg

Gaber A. Elsharawy
Faculty of Science, Al-Azhar University,Cairo, Egypt
E-mail: gaberelsharawy274.el@azhar.edu.eg

Amany A. Naim
Faculty of Science, Al-Azhar University,Cairo, Egypt
E-mail: amany.naim@azher.edu.eg

Heba F. Eid
Faculty of Science, Al-Azhar University,Cairo, Egypt
E-mail: heba.fathy@azhar.edu.eg, eid.heba@gmail.com

Received: 11 January 2022; Accepted: 23 March 2022; Published: 08 October 2022

Abstract: Data security has become a significant issue nowadays with the increase of information capacity and its transmission rate. The most common and widely used techniques in the data security fields is cryptography. Cryptography is the process of concealing and transmitting data in an appropriate format, so that only authorized people can access and process it. The main goal of the cryptographic process is protecting data from being hijacked and altered. This paper proposes an algorithm for encrypting data through the use of Deoxyribo Nucleic Acid (DNA) sequence and four-dimensional hyper chaotic system. Whereby, the hyper chaotic system is applied to generate a binary sequence which is later passed to a permutation function for the key generation of the first level encryption. The proposed encryption algorithm includes several intermediate steps, which are binary-coded form and the generation of arbitrary keys. Experimental results were analyzed by calculating encryption time, key generation time, histogram and correlation coefficient entropy. Furthermore, the proposed text encryption algorithm is implemented on two different students' datasets to improve the security of educational systems. Finally, experimental and comparative studies have shown that, the proposed encryption algorithm reported a uniform encrypted text distribution and correlation coefficient values nearer to '0', which are close to the theoretical optimal value.

Index Terms: Text Encryption, DNA Computing, Hyperchaotic System, Students' Record

1. Introduction

Organizations have become over dependent on information systems in the age of high technology and various types of information and data stored on a variety of media have become the most precious resource of organizations. As a result, one of the most significant aspects of network development is the hunt for intelligent information security solutions [1,2]. In the new generation of continuous intelligence development, network security monitoring and information network technology must be capable of combining and applying intelligent advantages to improve network security monitoring and self-organized network computing, and then provide more comprehensive services when involved in information [3, 4].

Cryptography is described as the study of encoding and decoding data using logical and mathematical procedures in order to protect data [5,6,7]. This technique has advanced quickly in terms of securing computing technology applications such as educational, medical, financial, and transportation services. The encryption key is an essential element in encrypting and decrypting the message [8]. In symmetric algorithm, the sender and recipient share the same

encryption and decryption key during data transfer. In asymmetric algorithm, key is called public key cryptography and it involves public and private keys for both encryption and decryption process. The transmitter encrypts plain text using a public key and the receiver decrypts this cipher text using its private key [9].

Due to its sensitivity to the initial conditions and deterministic pseudorandom behavior, chaos-based cyphers can be employed to implement robust and secure cryptosystems [10]. In consequence of the unique properties of the DNA molecule, such as its high information density and parallelism, DNA coding is used in cryptography to improve the efficiency and security of the encryption techniques [11, 12].

Motivated by the chaos and DNA computing advantages, in this paper, a secure robust text encryption model is proposed. The proposed cryptography Framework aims to enhance the confidentiality of students' information by protection of the student's records transformation. The proposed text cryptographic model encrypt uses a chaotic neural network for first-order encryption and DNA cryptography for second-order encryption. For which, the hyper-chaotic systems form the chaotic sequence that is used as the key to encrypt the plain text and produce the cipher text.

The reminder of this paper is organized as follows: Section 2 presents the existing work related to encryption algorithms. Section 3 presents DNA computing cryptography. In section 4, a brief description of the hyper chaotic system is presented. While section 5 elaborate the proposed text encryption hyper chaotic -DNA model. In section 6, the simulation and security analysis of the proposed encryption model discussed. In section 7 presents the Implementation of the proposed encryption model on two different students' dataset. Finally, in section 8 the main findings of this work are discussed.

2. Related Work

X. Li et al., [13] proposed A novel generation key scheme based on DNA using key expansion matrix. They increased computation by using a random key generation approach. Author of this algorithm utilized DNA sequences, block cyphers, data signatures, identity authentication, and randomized databases.

Roy et al., [14] proposed an improved symmetric key cryptography using a powerful encryption based on DNA. Author emphasized the use of DNA computational logic for data encryption, storage, and transmission. This study discussed the novel cipher-text method and key generation method. The author limited his discussion to DNA computing and cryptography.

Zhong et al. proposed an Index based DNA encryption algorithm. They turned a message into DNA sequences using a secure communication method while encrypting it using a block cypher and an index of string. The message is first transformed to ASCII code, then to binary code, and finally to a DNA sequence. Index number is written after a DNA sequence search in the key sequence [15].

K. S. Sajisha, S. Mathew, proposed a security system to protect a confidential text by presenting multilayer of security. The confidential text is cyphered by using DNA format, the next level is applying the AES algorithm. Eventually, another DNA format was used to hide the original encrypted DNA. The presented three levels of protection to secure a confidential text [16]. It is better to enhance the protection way by using the feature of hide data inside a specific media.

M. Sabry, M. Hashem, developed and executed technique by using DNA and the AES algorithm [17]. They designed an algorithm of DNA instead of bits. To providing the ability of implementing the DNA format by creating an evolved system based on DNA algorithm. The proposed algorithm carries the same security features. The method used is strong, but it needs to be strengthened by adding the level of concealment into a particular media.

More researchers are relying on Chaos to encrypt data and use different nonlinear low dimension chaos generators, such as in Pinchers Map, Logistic Map and Sine-Circle Map were used, which were commonly referred in the literature used to realise application [18, 19].

3. DNA Computing Cryptography

DNA computing is a bio-inspired approach proposed by L. Adleman [20] in 1994. It provides a promising cryptography research technique. For which, DNA is employed to store and convert information. The DNA sequence contains four types of bases; Adenine, Thymine, Cytosine, and Guanine, as shown in Figure 1 [21]. In short, the approach changes each letter of the alphabet into a complex combination of the four bases that make up DNA (A,T,C and G). Where, the genetic code of information is encoded in DNA. DNA computing cryptograpghy masks information by converting the message to ASCII code (decimal format) and then to binary format. Then, the binary sequence is partitioned into two-digit groups. Finally, these groups are converted to DNA code with A representing 00 , T representing 11, G representing 01 , and C representing 10 as shown in the Table 1 [22,23].

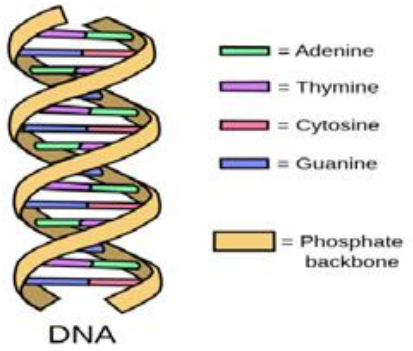


Fig. 1. The structure of DNA

Table 1. Coding Based on DNA Nucleotids

DNA component	Binary coded form
Adenine (A)	00
Cytosine (C)	01
Guanine (G)	10
Thymine (T)	11

4. Hyper Chaotic System

The hyper chaotic system contains two or more of positive Lyapunov exponents in chaotic systems. The chaotic sequences of the chaotic system are based on parameters and initial conditions. Predict their dynamic behavior and attractive chaos is very complex and impossible. The hyper-chaotic system of excessive chaos on a low level of chaos offers a specific advantage [24]. In cryptography utilized of hyper-chaotic systems lead to desirable cryptography characteristics such as high randomness, more security and efficiency [25]. The proposed encryption method utilized the chaotic sequence generated from different hyper-chaotic systems to encrypt message text, Chen's hyper chaotic system and Four-dimensional hyper chaotic system.

4.1. Chens Hyper Chaotic system

Chen's hyper chaotic system has two positive Lyapunov exponents and four chaotic sequences with high randomness. The text file is more chaotic if there are more positive Lyapunov exponents [26]. Chen's hyper chaotic sequences are described as follow [27].

$$\begin{cases} \dot{x} = a(y - x); \\ \dot{y} = -xz + dx + cy - q; \\ \dot{z} = xy - bz; \\ \dot{q} = x + k; \end{cases} \tag{1}$$

where, $a = 36, b = 3, c = 28, d = 16$ and $\{-0.7 <= k <= 0.7\}$. The above equations are solved by using Runge-kutta method to obtain four Lyapunov exponent $[\lambda 1 = 1.552, \lambda 2 = 0.023, \lambda 3 = 0, \lambda 4 = -12.573]$.

4.2. Four Dimention Hyper Chaotic System

The 4-D hyper chaotic system formula is described as follow [28].

$$\begin{cases} \dot{x} = a(y - x) + yz; \\ \dot{y} = cx - y - xz + w; \\ \dot{z} = xy - bz; \\ \dot{q} = dy - xz; \end{cases} \tag{2}$$

Where, a,b,c and d are the system parameters and are set as $a = 35, b = 8/3, c = 55$, and $d = 13$, which makes the system in the chaotic state.

5. The Proposed 4-D HyperChaotic DNA Encryption Algorithm

The proposed encryption algorithm hybrid the 4D hyper-chaotic random sequence and DNA computation for text encryption. The Structure of the proposed method is shown in Fig.2.

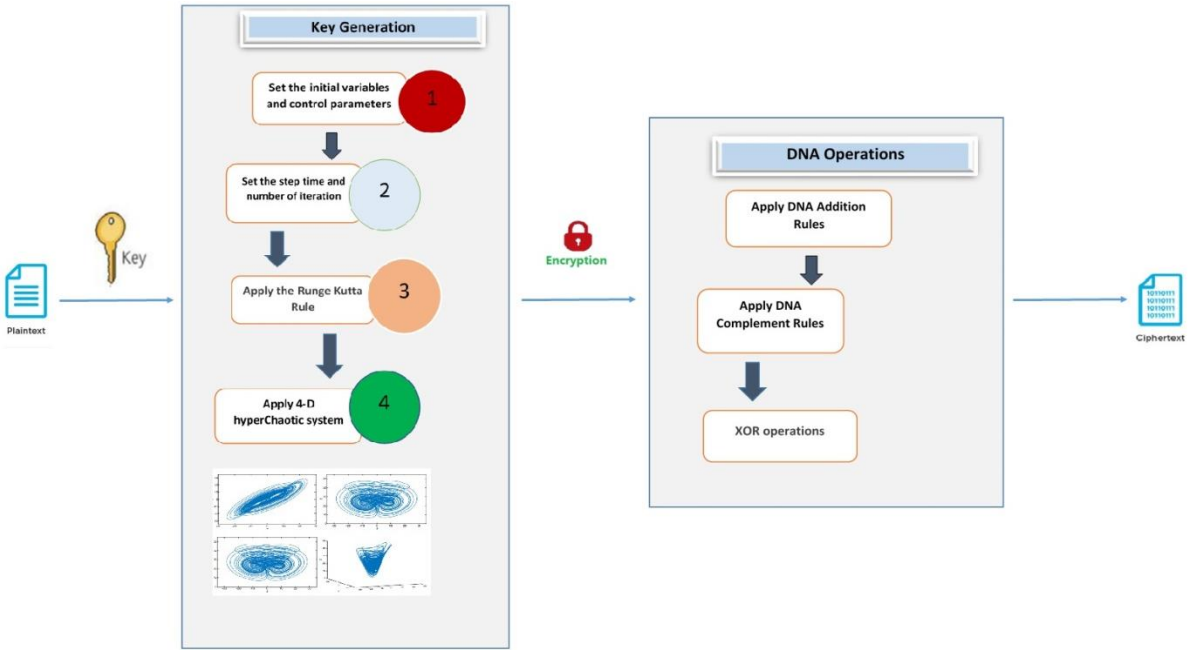


Fig.2 The 4D hyper-chaotic DNA text Encryption Framework.

The dynamics of the proposed encryption algorithm consists of three phases as follows:

- **Phase I:** Arbitrary keys generation, in this phase, a random key is generated by using hyper chaotic systenm which is used for next level of encryption.
- **Phase II:** Encryption, in this p, the sourse data is encrypted by implementing binary coding and complementary rules.
- **Phase III:** Decryption, it takes place which is reverse process of encryption.

5.1 Key generation

The 4-D hyperChaotic systems iterate with the values of initial conditions and control parameters to generate the chaotic sequence which utilized asa key to encrypt the plain tex and produce the cipher text.

The key generation procedure is described in the following steps:

Step 1: Set the initial condition and control parameter.
Step 2: Set the step time and number of iteration.
Step 3: For N times of iteration, Calculate the 4-D hyperChaotic system values (x1, x2, x3 and x4) using the runge kutta rule which is described as the follow:

$$
\begin{aligned}
K1 &= \alpha * \big(x2(1,j) - x1(1,j)\big) + \lambda 1 * x4(1,j) \\
K2 &= \alpha * \begin{pmatrix} \left(x2(1,j) + \frac{h}{2} * K1\right) \\ -\left(x1(1,j) + \frac{h}{2} * K1\right) \end{pmatrix} + \lambda 1 * \left(x4(1,j) + \frac{h}{2k1}\right) \\
K3 &= \alpha * \begin{pmatrix} \left(x2(1,j) + \frac{h}{2} * K2\right) \\ -\left(x1(1,j) + \frac{h}{2} * K2\right) \end{pmatrix} + \lambda 1 * \left(x4(1,j) + \frac{h}{2k2}\right) \\
K4 &= \alpha * \begin{pmatrix} \left(x2(1,j) + \frac{h}{2} * K3\right) - \\ \left(x1(1,j) + \frac{h}{2} * K3\right) \end{pmatrix} + \lambda 1 * \left(x4(1,j) + \frac{h}{2k3}\right)
\end{aligned}
\tag{3}
$$

Step 4: Obtain the random sequence key k.

5.2 Encryption Algorithm

For the encryption algorithm, the sender consider a file with the input of .txt extension. The encrypted data is obtained through multiple sub-steps and then transfer to the receiver.

The encryption procedure is described in the following steps:

Step 1: Import the plain text file .
Step 2: Generate the 4-D hyperChaotic random key k, as discussed above.
Step 3: Convert the input text to an ASCII value that corresponds to it.
Step 4: Convert the ASCII code to binary code, with each character represented by 8 bits.
Step 5: Represent this binary data as DNA coded data, as seen in Table 1.
Step 6: Choose randomly a DNA encoding rule, Table 2 .
Step 7: Apply encoding rule for the DNA sequence then addition rule, as show Table 3.
Step 8: Apply complementary rule for DNA sequence.
Step 9: Create a DNA sequence with a two-nucleotide group.
Step 10: The binary values of the related couple of nucleotide are transformed in decimal values using Table 4.
Step 11: The encrypted data is retrieved.

Table 2. DNA Encoding Rule

Rule	**A**	**T**	**G**	**C**
Rule1	00	11	10	01
Rule2	00	11	01	10
Rule3	11	00	10	01
Rule4	11	00	01	10
Rule5	10	01	00	11
Rule6	01	10	00	11
Rule7	10	01	11	00
Rule8	01	10	11	00

Table 3. DNA Addition Rule

+	**A**	**T**	**G**	**C**
A	C	A	G	T
C	A	C	T	G
T	G	T	C	A
G	T	G	A	C

Table 4. DNA Pair Binary Value

DNA	***Binary Bits***	***DNA***	***Binary Bits***
AA	0000	GA	1000
AC	0001	GC	1001
AG	0010	GG	1010
AT	0011	GT	1011
CA	0100	TA	1100
CC	0101	TC	1101
CG	0110	TG	1110
CT	0111	TT	1111

6. Experimental Results and Security Analysis

The prototype of the proposed algorithm is developed under the environment on intel (R) Core™ i7-8550U 1.8GHz 64-bit processor with 8G Bytes of RAM running on windows 10 operating system. Matlab R2019b was used to implement the proposed 4-D hyperChaotic encryption algorithm with the goal of determining its efficiency and capabilities.

6.1. Experimental Setup

The proposed 4-D hyperChaotic DNA encryption algorithm is applied on different text file with different size. For which, the initial parameters of the proposed encryption algorithm are set as following: x1(0), x2(0), x3(0), x4(0) = 0.12, 0.23, 0.34, 0.45. The encryption algorithm GUI is given in Fig. 3.

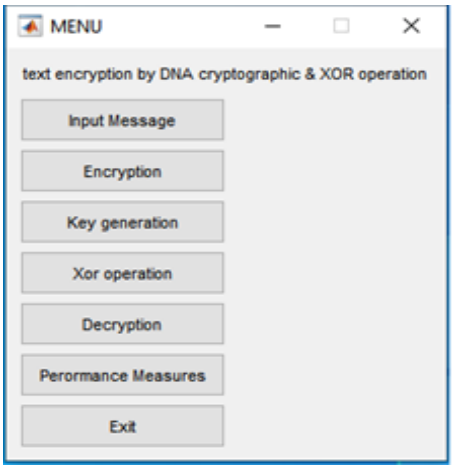


Fig. 3. GUI of the proposed 4-D hyperChaotic DNA text encryption algorithm.

6.2. Experimental Results

Different security performance analysis of the plaintext and the encrypted version obtained by the proposed algorithm is performed such as encryption time, key generation time, histogram and information entropy.

6.2.1. Encryption Time and Key Generation Time Analysis

In this section, the performance of the proposed 4-D hyperChaotic encryption algorithms in term of encryption time and key generation time is analyzed. . Table 5 and 6 show the encryption time of Chens hyperChaotic, 4-D hyperChaotic, AES-ECC- SHA256 [29] and chaos based encryption algorithm [30] on different file sizes.

Table 5. Text Encryption Time on Different File Sizes

File Size (KB)	AES-ECC-SHA256 (ms)	Chens hyperChaotic (ms)	4-D hyperChaotic (ms)
20	838	283	289
25	911	343	350
50	941	666	680
75	1145	1033	1014
100	1704	1306	1260
150	1815	1543	1532

Table 6. Text Encryption Time on Different File Sizes

File Size (KB)	Chaos based encryption (ms)	Chens hyperChaotic (ms)	4-D hyperChaotic (ms)
3136	1016	96	84
3600	1201	88	95
4096	1506	89	22
4624	1569	64	63
5184	1770	77	72

It is clear from Table 5 and 6 that encryption time of AES-ECC- SHA256 algorithm is more than all other algorithms. The Chens hyperChaotic encryption time is less than all other algorithms for small file size, while the 4-D hyperChaotic encryption time is less for bigger file size.

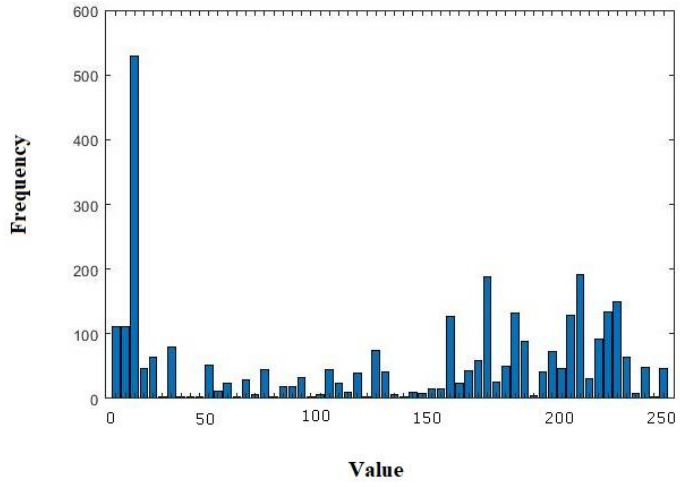
The time required the key generation function to generate keys is known as the key generation time. For which, the bit length of a key determines how long it takes to generate a key. Table 7 shows the key generation time of Chens hyperChaotic and 4-D hyperChaotic encryption algorithms for different key length.

Table 7. Key generation Time

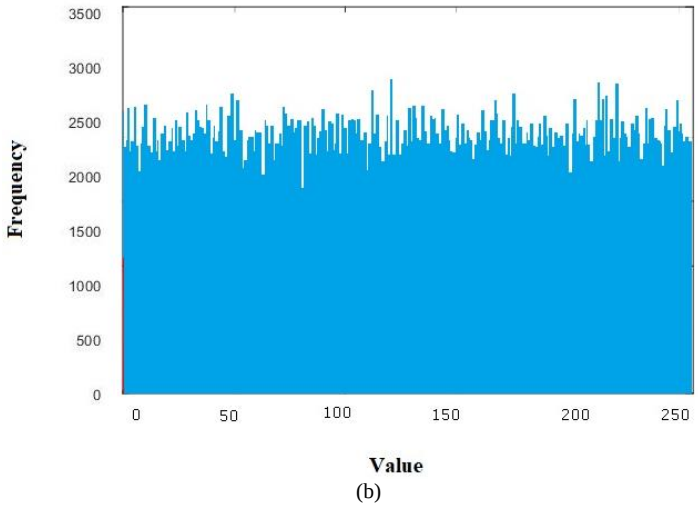
Key length (bit)	Key generation time (ms)	
	Chens hyper chaotic	4-D hyper chaotic system
56	0.636	0.5881
128	0.6919	0.6049
1024	0. 7555	0. 7068

6.2.2. Histogram Analysis

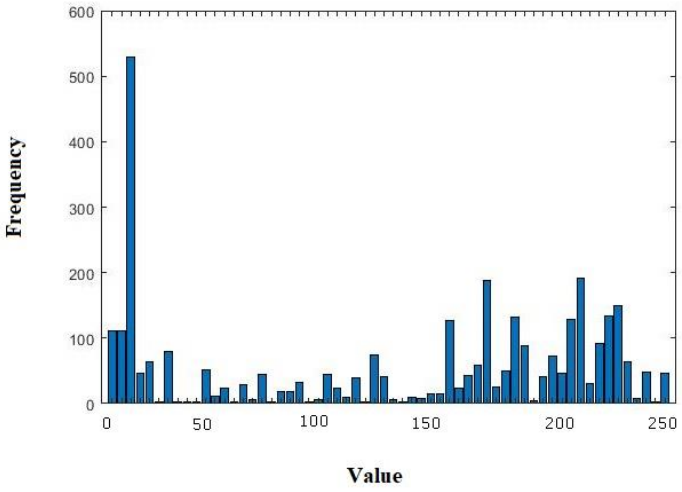
The statistical analysis of the proposed encryption algorithms can be evaluated by histogram analysis. The histogram illustrates information about the plain text, the secret key, or both. Figure 4 illustrates the histogram of the plain and cipher text. From figure 4, it can be seen that, the cipher text histogram is uniform and stale. This uniform encrypted image distribution will not provide any meaningful information to an attacker; therefor, the proposed HC RK45-DNA resists statistical attacks effectively. To conclude that, the proposed hyperChaotic algorithm is powerful against frequency attacks in addition to histogram attacks.



(a)



(b)



(c)

Fig. 4. Histograms of (a) plain, (b) encrypted and (c) decrypted text file

6.2.3. Correlation Coefficient Analysis

To verify the proposed encryption algorithm security quality, the correlation coefficient is assessed. The correlation coefficient measures the linear dependency between two ASCII values whose value is between [-1, 1]. For which, the plain text and the cipher text is totally different if the correlation coefficient is nearer to zero [31]. The formula of the correlation coefficient is given by:

$$\lambda_{xy} = \frac{COV(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \tag{4}$$

$$\mathrm{D(x)} = \frac{1}{N}\sum_{i=1}^{N} (x_i - \bar{x})^2 \tag{5}$$

$$\mathrm{D(y)} = \frac{1}{N}\sum_{i=1}^{N} (y_i - \bar{y})^2 \tag{6}$$

$$\mathrm{Cov(x,y)} = \sum_{i=1}^{N} (x_i - \bar{x})\,(y_i - \bar{y}) \tag{7}$$

Where, N is the number of the characters, xi and yi are the ASCII character values of the plain and the encrypted files, x and y are the mean values. The correlation coefficient values for the Chens hyperChaotic, 4-D hyperChaotic, and chaos based encryption algorithm are listed in table 8. From Table 8, it is clear that the correlation coefficient of the encrypted file is nearer to '0' when compared to original plaintext. Furthermore, the correlation coefficient of 4-D hyperChaotic algorithm is less when compared to Chens hyperChaotic. Hence, the proposed Text encryption algorithm is robust against statistical attacks.

Table 8. The Correlation Coefficient of Different File Sizes

File Size (KB)	Encryption Algorithm	Horizontal correlation
2136	Plain text	0.1557
	Chens hyperChaotic	-0.0044
	4-D hyperChaotic	-0.00261
4624	Plain text	0.0682
	Chens hyperChaotic	0.0092
	4-D hyperChaotic	0.0038

7. The Proposed HyperChaotic DNA Encryption Implementation on Students' Data

In this section, the efficiency of the proposed hyperchaotic DNA encryption is implemented and evaluated by two different student's dataset. The first student dataset is a questionnaire of 'Assessment and Evaluation in Education', that includes 30 questions, conducted to 101 students [32]. The questions are divided into three different categories: Family (6 questions), Personal (10 questions) and Educational Preferences (14 questions).

While, the second dataset considers data collected during the 2005-2006 school year from two public schools in Portugal [33]. The dataset was built from two sources: school reports and questionnaires, conducted to 788 students.

Moreover, the data was integrated into two datasets related to the Portuguese language with 649 records and Mathematics with 395 records.

Table 9 shows the encryption and decryption time of Chens hyperChaotic and 4-D hyperChaotic algorithm on the students datasets. While, Figure 5 illustrates the histogram of the plain and cipher dataset text.

Table 9. Students' Dataset Analysis

Dataset	Encryption Algorithm	Encryption Time (s)	Decryption Time (s)
Dataset 1	Chens hyperChaotic	5.10	5.24
	4-D hyperChaotic	4.13	4.95
Dataset 2	Chens hyperChaotic	7.53	7.84
	4-D hyperChaotic	6.89	7.04

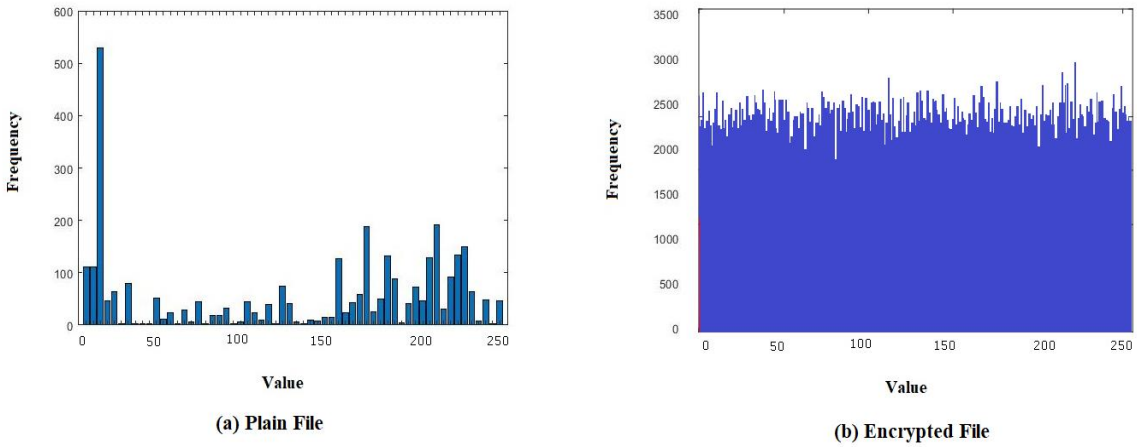


Fig. 5. Histograms of the plain and encrypted student's records file

8. Discussion

In this study, a 4D hyperchaotic framework combined with DNA to be utilized in the text encryption systems is presented. The 4D hyperchaotic DNA system has nonlinear terms, for which the maximum Lyapunov exponent is 1.552. The chaotic region's trajectories separate faster the larger the Lyapunov exponent is. Therefore, the system's dynamic behaviour is preferable to a one-dimensional chaotic system. Additionally, the conceptual foundation of the proposed framework is the DNA biological operation in conjunction with XOR computational and logical operations, which enables the 4D hyperchaotic system's uncertainty and randomness to expand. As a result, the proposed 4D hyperchaotic DNA text encryption system efficiently satisfies the secure performance against resistant statistical attacks and differential attacks, as demonstrated by the experimental experiments.

9. Conclusion

In order to improve the security of educational systems, encryption is the best method to conserve the student's confidentiality. This study aims to propose a robust and efficient text encryption model based on 4-D hyperchaotic -DNA. The proposed model chaotic sequences are produced by the runge Kutta method. Then, the sequence are incorporated to the 4-D hyperchaotic to generate the random key sequence. Moreover, DNA subtraction and addition operations were applied to increase the proposed model cipher efficiency. The proposed 4-D hyperchaotic -DNA text encryption model is implemented on two different students' datasets to improve the security of educational systems. The experimental results, including encryption and key generation time, histogram and correlation, reported a uniform encrypted text distribution and correlation coefficient values nearer to '0', which are close to the theoretical optimal value. Hence, the security analysis verify that the proposed 4-D hyperchaotic DNA encryption model provides good complexity and security and is robust against statistical and differential attacks. In future work, the proposed model will be improved by proposing and examining higher Hyperchaotic system dimensions.

References

[1] H. Yang, R. Zeng, G. Xu, and L. Zhang, "A network security situation assessment method based on adversarial deep learning," Applied Soft Computing 102, p. 107096, 2021.

[2] K. Roshan, A. Zafar "Deep Learning Approaches for Anomaly and Intrusion Detection in Computer Network: A Review," Cyber Security and Digital Forensics, pp. 551-563, 2022.

[3] P. Zorić, M. Musa, and TM. Kuljanić, “Use of Probabilistic Risk Assessment Methodology for Providers of Services in a Virtual Environment," Sustainable Management of Manufacturing Systems in Industry 4.0, pp. 129-142, 2022.
[4] X. Zhu, "Self-organized network management and computing of intelligent solutions to information security," Journal of Organizational and End User Computing (JOEUC) 33, no. 6, pp. 1-16, 2021.
[5] Rohit Verma, Jyoti Dhiman, "Implementation of Improved Cryptography Algorithm", International Journal of Information Technology and Computer Science(IJITCS), Vol.14, No.2, pp.45-53, 2022. DOI: 10.5815/ijitcs.2022.02.04
[6] Zuhi Subedar, Ashwini Araballi. "Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication ", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.6, No.4, pp.35-41, 2020. DOI: 10.5815/ijMSC.2020.04.04
[7] Shaymaa Fahmee Alqazzaz, Gaber A. Elsharawy, Heba F. Eid, "Robust 4-D Hyperchaotic DNA Framework for Medical Image Encryption", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.2, pp.67- 76, 2022. DOI: 10.5815/ijcnis.2022.02.06
[8] A. I. Mohammed, O. A. Abisoye, J. A. Ojeniyi, and A . B. Sulaimon. "A Review of DNA Cryptograhic Approaches," In 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), IEEE, pp. 66-72, 2021.
[9] B. M. Kumar, B. R. Sri, G. Katamaraju, P. Rani, N.Harinadh , and C. Saibabu,” File encryption and decryption using DNA technology.” In2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 382-385, 2020.
[10] S. G. Lian, A bloc cipher based on chaotic neural networks, Neuro computing 72 (4) (2009) 1296–1301.
[11] B. Wang, Q. Zhang, X. Wei, Tabu variable neighborhood search for designing dna barcodes, IEEE Trans. NanoBiosci 19 (2020) 127–131.
[12] X. Li, B. Wang, H. Lv, Q. Yin, Q. Zhang, X. Wei, Constraining dna sequences with a triplet-bases unpaired, IEEE Trans. NanoBiosci 19(2020) 299–307.
[13] X. Li, L. Zhang, and Y. Hu, “A novel generation key scheme based on DNA,” in 2008 International Conference on Computational Intelligence and Security, 2008, vol. 1, pp. 264–266.
[14] B. Roy, G. Rakshit, P. Singha, A. Majumder, and D. Datta, “An improved Symmetric key cryptography with DNA based strong cipher,” in 2011 International Conference on Devices and Communications (ICDeCom), 2011, pp. 1–5.
[15] Y. Zhang, B. Fu, and X. Zhang, “DNA cryptography based on DNA Fragment assembly,” in 2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012), 2012, vol. 1, pp. 179–182.
[16] K. S. Sajisha, and M. Sheena. "An encryption based on DNA cryptography and steganography," In 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA), vol. 2, pp. 162-167. IEEE, 2017.
[17] 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. IEEE, 2015.
[18] N. A. Al-Romema, A. S. Mashat, and I. AlBidewi. "New chaos-based image encryption scheme for RGB components of color image," Computer Science and Engineering 2, no. 5, pp. 77-85, 2012.
[19] J. Vahidi, M. Gorji, and I. Mazandaran. "The confusion-diffusion image encryption algorithm with dynamical compound chaos," Journal of Mathematics and Computer Science (JMCS), pp. 451-457, 2014.
[20] Adleman LM. “Molecular computation of solutions to combinatorial problems”. Science, JSTOR ,1994;266:1021–4
[21] S. S. Roy, S. A. Shahriyar, M. Asaf-Uddowla, K. M. Alam, and Y. Morimoto, "A Novel Encryption Model for Text Messages using Delayed Chaotic Neural Network and DNA Cryptography", International Conference of Computer and Information Technology (ICCIT), pp. 22 – 24, 2017.
[22] E. Vidhya, R. Rathipriya, “Two Level Text Data Encryption using DNA Cryptography, ” International Journal of Computational Intelligence and Informatics , Vol 8, No.3, December 2018.
[23] Y. Y. Ahmed, H. A. Haider, “TEXT ENCRYPTION AND DECRYPTION USING FIVE LEVELS DNA BASED ALGORITHM,” International Journal of Advanced Science and Technology, Volume 29, pp. 104-108, , January 2020.
[24] S. A. Mehdi, Z. L. Ali . "A New Six-Dimensional Hyper-Chaotic System." In 2019 International Engineering Conference (IEC), IEEE, pp.211-215, 2019.
[25] H. A. Qasim. "Text Encryption Method Using multi Hyperchaotic systems," Al-Qadisiyah Journal of Pure Science 26.3, pp. 1-8, 2021.
[26] K. R. Radhika and M. K. Nalini. "Biometric image encryption using DNA sequences and chaotic systems," In 2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT), pp.164-168, 2017.
[27] L. Zeng and R. R. Liu. "Cryptanalyzing a novel couple images encryption algorithm based on DNA subsequence operation and chaotic system," Optik 126, pp. 5022-5025, 2015.
[28] Y. Zhang, D. Xiao, W. Wen, and M. Li. "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process." Nonlinear Dynamics 76, no. 3, 2014, pp. 1645-1650.
[29] P. Patil, R. Bansode. "Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text Images," International Research Journal of Engineering and Technology (IRJET), pp. 3773-3778, 2020.
[30] S. J. Sheela, K. V. Suresh, D. Tandur. “Secured text communication using chaotic maps,” In2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), IEEE, pp.1-6, 2017.
[31] Babaei, M.. A novel text and image encryption method based on chaos theory and DNA computing. Natural computing, 12(1), 101-107, 2013.
[32] Yalmaz N., Sekeroglu B, “Student Performance Classification Using Artificial Intelligence Techniques”. In: 10th International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions - ICSCCW, 2020.
[33] P. Cortez and A. Silva. Using Data Mining to Predict Secondary School Student Performance. In A. Brito and J. Teixeira Eds., Proceedings of 5th FUture BUsiness TEChnology Conference (FUBUTEC 2008) pp. 5-12, Porto, Portugal, April, 2008,.

Authors' Profiles

Ghada Yousef is a administrator in Computer Science, Faculty of Science, Al-Azhar University, Cairo, Egypt

Gaber A Elsharawy, Professor of computer science at Faculty of science, Al Azhar university. Ph.D. in Computer and Systems Engineering, Faculty of Engineering, Al Azhar University. M.Sc.in computer system U.S. Air Force University, Air Force Institute of Technology (AFIT), Dayton, Ohio, USA. Author of many publications in the fields of Database management systems, artificial intelligent, modeling & simulation, and programming languages.

Amany A. Naim received the B.Sc. degree in science, in 2009, and the M.Sc. and Ph.D. degrees in computer science, in 2015 and 2019, respectively. She is currently a lecrature in computer science with the Mathematics Department, Faculty of Science, Al- Azhar University, Cairo, Egypt. She has published several research papers in the field of AI, machine learning, meta-heuristic optimization, and data mining and analysis.

Heba F. Eid is an Associate Professor at Faculty of Science, Al-Azhar University, Egypt. She received her Ph.D. degree in Network Intrusion Detection and M.S. degree in Distributed database systems, both from Faculty of Science, Al-Azhar University, Egypt. Her research interests include multi-disciplinary environment involving computational intelligence, pattern recognition, computer vision, bio-inspired computing and cyber security. Dr. Heba has served as a reviewer for various international journals and a program committee member of several international conferences

How to cite this paper: Ghada Yousef, Gaber A. Elsharawy, Amany A. Naim, Heba F. Eid, " A 4-D HyperChaotic DNA Encryption/Decryption Algorithm for Securing Students Data System", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.8, No.4, pp. 30-40, 2022. DOI: 10.5815/ijmsc.2022.04.03