DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

D-GIFT: Cryptography Algorithm Development Using Dynamic DNA and A Chaos Map

Ghada k. Emad[1], Soukaena Hassan Hashem[2]

[1,2]Computer Sciences Department, University of Technology, Baghdad, Iraq

[1]cs.19.20@grad.uotechnology.edu.iq, [2]soukaena.h.hashem@uotechnology.edu.iq

Abstract*— Recently, the growth of data transmission through various networks has the necessity for an elevated level of security. Encryption is one of the essential technologies for protecting and ensuring the integrity of IoT devices. Secure communication among constrained devices is critical during data transmission from the client to the server devices. Lightweight cipher algorithms are defined as a secure solution for devices with limited computational functions and memory. On the other hand, most lightweight algorithms suffer from a trade-off between complexity and speed to produce a robust cipher algorithm. This paper evaluates the effectiveness of an image encryption technique that uses a Lightweight GIFT algorithm and logistic map equation-based dynamic DNA coding to create a secure, lightweight cipher algorithm for IoT devices. When we employed dynamic DNA coding by the binary bit method, we observed that the developed approach is more secure and has a high level of randomness due to the results. Additionally, the correlation between nearby pixels is approximately zero; there is no association between the two images. Therefore, the developed approach achieves a higher encryption efficiency when compared to the original algorithm.*

Index Terms— *lightweight image encryption, DNA image encryption, chaotic map, dynamic DNA.*

I. INTRODUCTION

Cryptographic algorithms are used to ensure the security of sensitive data. The use of such algorithms enables the sender to send valuable information securely over the internet. These days, the Internet of Things (IoT) technology is being used to deploy many constrained devices. Cryptography is critical in this context for securing the valuable information exchanged between clients and servers by IoT devices. Devices on the Internet of Things, such as memory and processors, are designed to operate continuously with limited resources. Additionally, conventional cryptography algorithms are computationally intensive and thus unsuitable for IoT devices. The primary reason for this is that conventional cryptography is extremely complex and involves a variety of mathematical operations that require an efficient processor and sufficient memory[1]. As a result, lightweight cipher algorithms are introduced to address these concerns, making them more appropriate for IoE devices. The GIFT algorithm is one of the most compact algorithms available and is widely used in constrained devices[2]. The GIFT algorithm is implemented in a 64/128 -bit block cipher with a 128-bit key size, making it suitable for both hardware and software applications within the IoT system[3]. Additionally, recent research has demonstrated that the GIFT algorithm is efficient for constrained devices, as it operates via a substitution-permutation network (SPN)[3]. The algorithm's structure is straightforward and requires little computational effort. Nonetheless, the GIFT cipher's complexity should be increased to make it more resistant to cipher attacks based on the state of the art[2]. DNA cryptography is a relatively new development that has been applied to a variety of cryptosystems domains recently[4].The DNA structure is made up of genetic information sequences referred to as genes, which are used to conceal data in cryptosystems[5]. Cryptosystems, on the other hand, can be broadly classified into three types: asymmetric keys, symmetric keys, and hash functions[6]. The

Received 06/April/2022; Accepted 22/June/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

symmetric-key algorithm was proposed in this work, which utilized a single secret key for both encryption and decryption[7]. The proposed D: GIFT algorithm is a block cipher that splits the received data into blocks and processes them sequentially. Block cipher algorithms are characterized by their low computational complexity and are widely used in lightweight cryptosystems[8]. Thus, the proposed work's primary objective is to develop a lightweight and efficient cipher algorithm for securing valuable data from constrained devices during data exchange over communication channels. Using DNA cryptography, this study enhanced the GIFT cipher algorithm[4]. The study in [9] proposed a hybrid DNA-encoded ECC (Elliptic curve cryptography) scheme which extends multi-level security. The DNA sequence was chosen, and utilizing a sorting algorithm, a unique set of nucleotide sets was assigned. In [10] employed two layers of encryption where DNA encoded ECC was used to minimize processing time and memory footprint to make IoT devices more suitable. In [11] proposed a new lightweight encryption's algorithm based on the DNA sequence to be adequate for IoT device's resources. In the proposed algorithm, it utilized the DNA's random nature to generate a strong secret key, which is hard to be broken by attackers. Khan and Masood[12] presented a chaos-based encryption technique for color images that involves multiple discrete dynamical maps. To carry out diffusion and confusion, the scheme makes use of several 1D and 2D maps. Farah et al.[13] used chaos theory, fractional Fourier transform, and DNA operations to propose an optical image encryption scheme. A DNA matrix was obtained upon the transformation of the plain image by generating random phase masks utilizing the Lorenz map. Then, fractional Fourier transform was implemented thrice on the matrix. Kang and Guo[14] presented a spatiotemporal chaotic system and DNA encoding-based color image encryption technique. Firstly, three DNA matrices are obtained from the plain image based on DNA coding rules. Then, a mixed linear non-linear coupled map lattice (MLNCML) system is used to generate a scrambling matrix that is used to perform permutation on the combined DNA matrix.

II. DYNAMIC DNA CODING AND CHAOTIC MAPPING

A. Coding of the DNA Alphabet

Nucleic acid bases A, C, G, and T make up the four nucleic acid bases that construct the DNA sequences [15]. A and T are complementary, whereas G and C are not [16]. Researchers utilize the binary numbers 00, 01, 10, and 11 to represent these four bases. It is possible to determine that the binary coding system has 24 distinct forms of coding, although 00 and 11 are complements and 01 and 10 are complementary. Consequently, eight of the twenty-four coding rules selected in *Fig. 1* fulfill the fundamental complementary requirement. It's possible, for example, that the four-bit DNA bases constituting a single pixel value may be made up of eight-bit binary integers, as in the range [0, 255] [17]. There are eight rules that may be used to encode and decode DNA sequences, such as R1 rule in Table I, where a pixel value of 175 corresponds to "10101111," and the DNA sequence created by this rule is "GGTT." It is nearly impossible to separate the DNA coding rule from existing picture encryption methods based on this rule or its modification[18].

TABLE I. RULES OF DNA

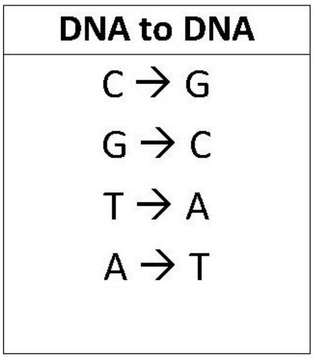
	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

Received 06/April/2022; Accepted 22/June/2022

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

B. Rules of DNA complement

There are two methods for encrypting images using the complement of DNA sequences: (1) single base direct complement and (2) using the principle of a single base and double base complementary pairing in biotechnology to perform the complement operation. *Fig. 1* shows a single base direct complement[19]:



DNA to DNA
C → G
G → C
T → A
A → T

FIG. 1. COMPLEMENT OF DNA [19].

Here, the function of the complement (.) is denoted. A T complement is found in the first base, whereas a G complement may be found in the second. Completing 00 and 01's binary complements are both fulfilled if both complements are 11 and vice versa [20]. The structure of a double helix is used to establish the complement rule, which pairs nucleosides. Consider Table II for more information.

TABLE II. COMPLEMENT OPERATIONS

Rules	Complement operation			
R1	AT	TC	CG	GA
R2	AT	TG	GC	CA
R3	AC	CG	GT	TA
R4	AC	CT	TG	GA
R5	AG	GC	CT	TA
R6	AG	GT	TC	CA

C. Gift Proposed enhancement of GIFT algorithm

Images are encoded using dynamic DNA coding, which creates the DNA sequence for each pixel or a binary bit for the complete picture according to various criteria (recall *Fig. 1*) [21]. Encryption security is strengthened by employing logistic maps to choose encoding rules for distinct encoding objects at random, making decoding more challenging. An 8-bit binary pixel may be encoded into one base utilizing multiple rules controlled by the chaotic sequence utilized in this paper's Dynamic Coding according to Binary Bit (Bit-by-Bit) dynamic coding technique. There are now many dynamic coding schemes in use, as shown in *Fig. 2*.

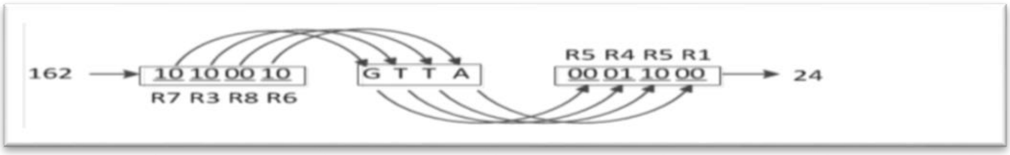


FIG. 2. BINARY BIT METHOD [21].

Received 06/April/2022; Accepted 22/June/2022

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

D. Logistic chaotic system

A logistic map is a superior chaotic map in many ways. In this work, an experimental simulation is carried out using a logistic map, which is characterized as follows[22]

$$u(1-x_n) \qquad (1)$$

Where μ 2 [0, 4], *xn*2 (0, 1), *n* = 0, 1, 2, ….

III. DEEPER INTOGIFT BLOCK CIPHER

The GIFT block cipher employs the Substitution Permutation Network (SPN) method of symmetric key cryptography. There are two types of GIFT: GIFT-64/128 (64-bit block and 128-bit key) and GIFT-128/128 (64-bit block and 128-bit key) (128-bit block and 128-bit key) [3]. Each round in the GIFT block cipher consists of four operations: Sbox, Permutation, Add RoundKey, and Constant XOR. *Fig. 3* illustrates the N NGIFT block cipher's encryption operation[23].

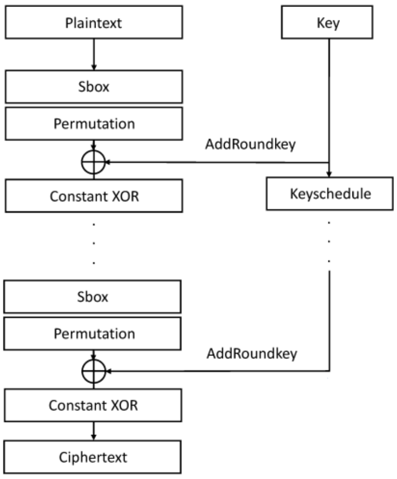
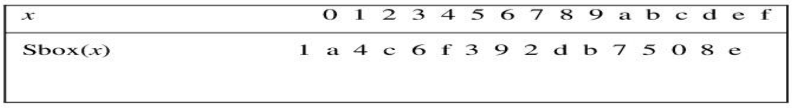


FIG. 3. GIFT DIAGRAM[3].

A. Sbox of GIFT Block Cipher

The n-bit block (n = 64, 128) is split into 4 bits and becomes the input value of the 4-bit Sbox, *Fig. 4* illustrate that [24].



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Sbox(x)	1	a	4	c	6	f	3	9	2	d	b	7	5	0	8	e

FIG. 4. S-BOX OF GIFT[3].

B. Permutation of GIFT block cipher

GIFT-64/128 replaces the P64(i)-the bit of block B with the i-th bit of block B in the permutation. Table IV contains information about the permutation of GIFT-64/128[3]. The detailed Table on permutation of GIFT-128/128 is omitted from this paper. Table III has the GIFT-128/128 permutation table[25].

Received 06/April/2022; Accepted 22/June/2022

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

TABLE III. GIFT PERMUTATION

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	3	19	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

C. Add Round key of GIFT block CIPHER[26]

In the GIFT-64/128 block cipher, k0 and k1 (32-bit total) are selected from the key (K = k7, …, k0). K0 and k1 are used as U and V of the round key as follows, RK = UjjV = u15…u0jjv15…v0 (U = k1,V = k0). The round key is exclusive-ored with block B, where U is XORed to b4i+1 and V is XORed to b4i.

$$b_{4i+1} \leftarrow b_{4i+1} \oplus u_i, b_{4i} \leftarrow b_{4i} \oplus v_i, i=0,\dots,15 \qquad (2)$$

In the GIFT-128/128 block cipher, k0, k1, k4, and k5 (64-bit in a total) are selected from the essential K. k0, k1, k4, and k5 are used as U and V of the round key as follows, RK = UjjV = u31…u0jjv31...v0 (U = k5jjk4,V = k1jjk0). The round key is XORed to block B, where U is XORed to b4i+2 and V is XORed to b4i+1.

b4i+2 _b4i+2 _ ui, b4i+1 _b4i+1 _ vi, i = 0, ..., 31 (3)

D. Constant XOR of GIFT block CIPHER[27]

Round constants C given in Table IV are used in GIFT-64/128 and GIFT-128/128 block ciphers. Single bit and round constants (C = c5c4c3c2c1c0) are XORed to block B as in Equation (4).

$$b_{n-1} \leftarrow b_{n-1} \oplus 1,$$

$$b_{23} \leftarrow b_{23} \oplus c_5, b_{19} \leftarrow b_{19} \oplus c_4, b_{15} \leftarrow b_{15} \oplus c_3,$$
$$b_{11} \leftarrow b_{11} \oplus c_2, b_7 \leftarrow b_7 \oplus c_1, b_3 \leftarrow b_3 \oplus c_0. \qquad (4)$$

TABLE IV. CONSTANT C ROUND

Rounds	Constants
1 to 16	01 03 07 0F 1F 3E 3D 3B 37 2F 1E 3C 39 33 27 0E
17 to 32	ID 3A 35 2B 16 2C 18 30 21 02 05 0B 17 2E 1C 38
33 to 48	31 23 06 0D 18 36 18 2D 1A 34 29 12 24 08 11 22 04

E. Key schedule of GIFT block CIPHER[17]

In GIFT-64/128 and GIFT-128/128 block ciphers, the Key schedule updates key (K = k7, ..., k0) and extracts the round key from the updated key K. The Key schedule is shown in Equation (5). The notation (oi) denotes a right rotation operation (i-bit) [20].

$$k_7||k_6||...||k_1||k_0 \leftarrow k_1 \gg 2||k_0 \gg 12||...||k_3||k_2, \dots (5)$$

Received 06/April/2022; Accepted 22/June/2022

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

IV. PROPOSED D- GIFTTO ENCRYPTE IMAGE BASED ON DYNAMIC DNA AND LOGISTICMAP

In this part, see *Fig. 5* the development of the D- GIFT algorithm work more secure and efficient, will be discussed in depth. In the beginning, the picture will be acquired from an IOT device, fed into the algorithm to be evaluated, and converted to be processed through the S-box and permutation before becoming processed. Prior to the constant XOR level, we have dynamic DNA, which is expressed by a binary bit layer. The ideas of encoding and decoding relate to chaotic sequences E=5,1,7, 2,...8 and D=4,4,2,1, respectively. It can be observed in the graphic that dynamic DNA has been encoded and decoded with the gift method base on dynamic DNA utilizing binary bits (9). This means that the first-pixel value (162) of the picture captured by the IoT device corresponds to the binary encoding value "01010000." The bit of Each binary values encoded using the R3, R2, R8, and R1 registers, while all binary value bits are decoded using the R7, R2, R6, and R8 registers. The outcome is a pixel value of 24.

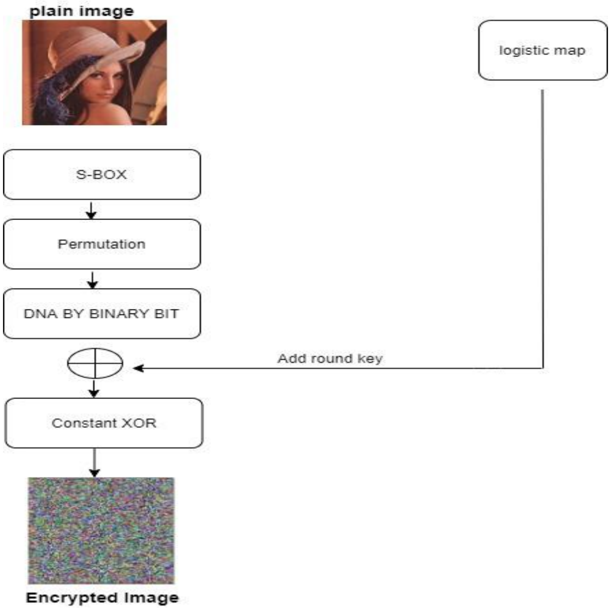


Fig. 5. Proposed D- Gift Based on dynamic DNA and logistic map diagram.

Algorithm 1: Encryption Algorithm

Input	image key bin 32bit
Output	Encryption image

```
1: for each block do size 16bit
2:     Convert to hex for 4bit
3:     Change a bit from the key by using a Logistic map
4:     for each round do
4-1:       Sub Cells
4-2:       permute the bits
4-3:       permute DNA with a Logistic map
4-4:       Add Round Key
4-5:       Add constant
4-6:       key update
5:     end for
6: end for
```

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

Algorithm 2: Decryption Algorithm

Input	input key bin
Output	Encryption image

```
Step1: compute and store the round keys
        For each R in rang(round)
           For each I in rang(32)
                Round key state[R][I] = key[i]
Step2: key update
        For each i in rang(32)
           Temp key[i] = key[(i+8)%32]
        For each I in rang (24)
            key[i] = Temp key[i]
Step3: For each R in rang(round-1,0)
            Add Round Key
           key to key bits
           add round key
           add constant
           permute DNA with Logistic map
           Sub Cells
        End for
```

V. EXPERIMENTAL RESULTS OF STATISTICAL AND SECURITY ANALYSIS

An Intel(R) Core(TM) i7-10750H CPU processor running at 2.60GHz with 16 GB of RAM and the Microsoft Windows 11 operating system comprise the experimental environment. Python 3.9 includes support for encryption and decryption algorithms. The results of encryption/decryption are shown in *Fig. 6.* The plain photos and the decoded photographs are identical. In conclusion, D- GIFT implementation is more sophisticated than GIFT. As a result, D-GIFT has superior encryption, a higher level of scrambling, and also can resist exhaustive attack.

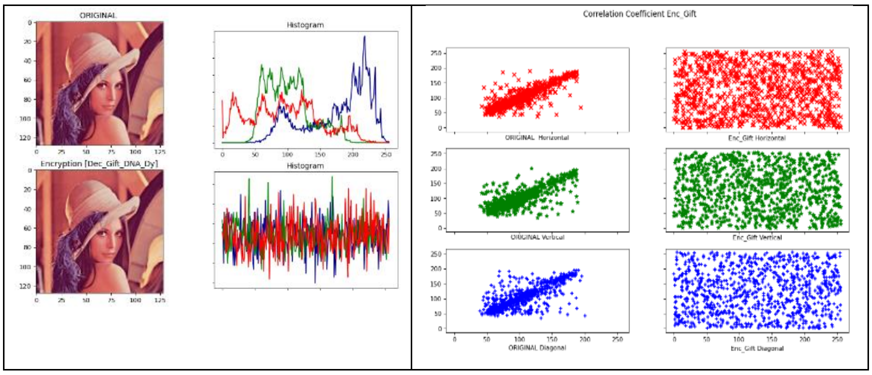


FIG. 6. THE RESULTS OF ENCRYPTION AND DECRYPTION.

In Table V explained the results have been obtained from implemented the D-GIFT algorithm. The results of the improved algorithm overcome the results of the original algorithm according to the execution time, correlation and entropy.

Received 06/April/2022; Accepted 22/June/2022

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

TABLE V. THE RESULTS OF D-GIFT

Images	Original Gift			Proposed D-GIFT		
	Time	Correlation	Entropy	Time	Correlation	Entropy
Im1	32.1292	-0.002945	7.7403	35.372	-0.0009	7.9960
Im2	34.1924	-0.000648	7.9966	36.086	-0.00006	7.9968
Im3	31.9310	0.004184	7.9932	35.961	0.00037	7.9964
Im4	35.5592	0.004410	7.1412	35.787	0.00181	7.9944

VI. CONCLUSIONS

We can see from the table's results that the Correlation and Entropy have improved (-0.002945 to -0.0009 and 7.7403 to 7.99960). The security of IoT systems is highly dependent on the lightweight cryptography of end nodes. However, implementing an efficient cipher method on restricted devices is challenging due to their resource constraints. For lightweight cryptosystems, a variety of cryptographic algorithms are acceptable. The primary argument for utilizing lightweight cryptographic algorithms is their ease of implementation and cheap cost. However, most lightweight algorithms make a trade-off between speed and complexity. DNA cryptography has been demonstrated to be an efficient technology for constructing lightweight communication systems. Thus, DNA cryptography is used in conjunction with an interesting cipher light algorithm. The primary objective of this paper was to create a lightweight cipher method called D-GIFT based on the GIFT algorithm and the dynamic DNA approach that has been enhanced in its present implementation.

REFERENCES

[1] J. R. Naif, G. H. Abdul-majeed, and A. P. D. A. K. Farhan, "Internet of Things Authentication Based on Chaos-Lightweight Bcrypt," *J. Baghdad Coll. Econ. Sci. Univ.*, vol. 2019, no. conference-8, 2019.

[2] D. Jamuna Rani and S. Emalda Roslin, "Optimized Implementation of Gift Cipher," *Wirel. Pers. Commun.*, vol. 119, no. 3, pp. 2185–2195, 2021.

[3] K. Jang, G. Song, H. Kim, H. Kwon, H. Kim, and H. Seo, "Efficient implementation of present and gift on quantum computers," *Appl. Sci.*, vol. 11, no. 11, p. 4776, 2021.

[4] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, "Lightweight cryptography system for IoT devices using DNA," *Comput. Electr. Eng.*, vol. 95, p. 107418, 2021.

[5] X. Xue, D. Zhou, and C. Zhou, "New insights into the existing image encryption algorithms based on DNA coding," *PLoS One*, vol. 15, no. 10, p. e0241184, 2020.

[6] M. S. Fadhil, A. K. Farhan, M. N. Fadhil, and N. M. G. Al-Saidi, "A New Lightweight AES Using a Combination of Chaotic Systems," in *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*, 2020, pp. 82–88.

[7] J. Ferdush, M. Begum, and M. S. Uddin, "Chaotic lightweight cryptosystem for image encryption," *Adv. Multimed.*, vol. 2021, 2021.

[8] A. Hamad and A. K. Farhan, "Image encryption algorithm based on substitution principle and shuffling scheme," *Eng. Technol. J.*, vol. 38, no. 3, pp. 98–103, 2020.

[9] H. D. Tiwari and J. H. Kim, "Novel method for DNA- based elliptic curve cryptography for IoT devices," *ETRI J.*, vol. 40, no. 3, pp. 396–409, 2018.

[10] B. Al-Shargabi and M. A. F. Al-Husainy, "A New DNA Based Encryption Algorithm for Internet of Things," *Lect. Notes Data Eng. Commun. Technol.*, vol. 72, pp. 786–795, 2021, doi: 10.1007/978-3-030-70713-2_71.

[11] P. Barman and B. Saha, "DNA encoded elliptic curve cryptography system for IoT security," *Int. J. Comput. Intell. IoT*, vol. 2, no. 2, 2019.

[12] S. Mansoor, P. Sarosh, S. A. Parah, H. Ullah, and M. Hijji, "Adaptive Color Image Encryption Scheme Based on Multiple Distinct Chaotic Maps and DNA Computing," 2022.

Received 06/April/2022; Accepted 22/June/2022

DOI: https://doi.org/10.33103/uot.ijccce.23.1.15

[13] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, “A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation,” *Opt. Laser Technol.*, vol. 121, no. April 2019, p. 105777, 2020, doi: 10.1016/j.optlastec.2019.105777.

[14] K. Xuejing and G. Zihui, “A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system,” *Signal Process. Image Commun.*, vol. 80, no. June 2019, p. 115670, 2020, doi: 10.1016/j.image.2019.115670.

[15] V. Kolate and R. B. Joshi, “An Information Security Using DNA Cryptography along with AES Algorithm,” *Turkish J. Comput. Math. Educ.*, vol. 12, no. 1S, pp. 183–192, 2021.

[16] Q. Lu, L. Yu, and C. Zhu, “A New Conservative Hyperchaotic System-Based Image Symmetric Encryption Scheme with DNA Coding,” *Symmetry (Basel).*, vol. 13, no. 12, p. 2317, 2021.

[17] P. Pavithran, S. Mathew, S. Namasudra, and P. Lorenz, “A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine,” *Comput. Secur.*, vol. 104, p. 102160, 2021.

[18] M. Uddin, F. Jahan, M. K. Islam, and M. Rakib Hassan, “A novel DNA-based key scrambling technique for image encryption,” *Complex Intell. Syst.*, vol. 7, no. 6, pp. 3241–3258, 2021.

[19] S. Zhu and C. Zhu, “An Efficient Chosen-Plaintext Attack on an Image Fusion Encryption Algorithm Based on DNA Operation and Hyperchaos,” *Entropy*, vol. 23, no. 7, p. 804, 2021.

[20] M. Kaur, S. Singh, and M. Kaur, “Computational image encryption techniques: a comprehensive review,” *Math. Probl. Eng.*, vol. 2021, 2021.

[21] F. Masood *et al.*, “A new color image encryption technique using DNA computing and Chaos-based substitution box,” *Soft Comput.*, pp. 1–17, 2021.

[22] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, “Designing Substitution Box Based on the 1D Logistic Map Chaotic System,” in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1076, no. 1, p. 012041.

[23] M. J. Al-Muhammed and R. Abu Zitar, “Light and Secure Encryption Technique Based on Artificially Induced Chaos and Nature-Inspired Triggering Method,” *Symmetry (Basel).*, vol. 14, no. 2, p. 218, 2022.

[24] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, “A lightweight AES Algorithm Implementation for Secure IoT Environment,” *Iraqi J. Sci.*, vol. 62, no. 8, pp. 2759–2770, 2021.

[25] A. A. Abdallah and A. K. Farhan, “A New Image Encryption Algorithm Based on Multi Chaotic System,” *Iraqi J. Sci.*, pp. 324–337, 2022.

[26] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, “Drone secure communication protocol for future sensitive applications in military zone,” *Sensors*, vol. 21, no. 6, p. 2057, 2021.

[27] I. S. Tawfic, “Design and development of E-passport scheme using multi encryption biometric information,” *IRAQI J. Comput. Commun. Control Syst. Eng.*, vol. 19, no. 1, 2019.

Received 06/April/2022; Accepted 22/June/2022