Iraqi Journal of Intelligent Computing and Informatics (IJICI)
Vol. 1, 2, December 2022, pp. 56~65
ISSN: 2791-2868, DOI: 10.52940/ijici.v1i2.10

A Review of DNA-Based Color Image Encryption Algorithms

Ghofran K. Shraida[1], Hameed A. Younis[1]
[1]Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received August 10, 2022
Revised August 25, 2022
Accepted September 8, 2022

Keywords:

Chaos theory
Color image encryption
Cryptography
Deoxyribonucleic Acid (DNA)
Security

ABSTRACT

Several encryption techniques based on DNA encoding have been presented in recent years for color image encryption. Image encryption is one of the most significant fields of study that has piqued the worldwide attention of scholars, and it is relevant in transferring important images via communication channels, that are insecure. In this paper, a review of color image encryption algorithms based on DNA coding is conducted from 2015 to 2021. The comparison findings on 12 included experiments in relation to correlation coefficient, key space, information entropy, NPCR, and UACI revealed that the encryption methods improved significantly. In conclusion, the DNA-based image encryption approaches offer a superior trade-off between security and computational complexity, and have been highlighted as an essential component in the construction of a trustworthy and authenticated cryptosystem.

Corresponding Author:

Ghofran Khaled Shraida
Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq
Email: itpg.ghofran.shraida@uobasrah.edu.iq

1. INTRODUCTION (10 PT)

Currently, technology and Internet contacts across various human societies are unavoidable [1], and the tendency toward participating in these types of network links is expanding drastically over time. Daily Internet traffic consists mostly of the transfer of data spanning from basic text and images to high-sensitivity data. While two or more parties are exchanging data, it must comply with fundamental security services, such as, confidentiality, integrity, and availability, which are mostly met by upgrading current cryptographic methods [2]–[5]. When establishing a connection between organizations or people via server endpoints and clients, security attributes must be provided [6]. Numerous well-known encryption/decryption techniques, such as, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest Shamir Adelman (RSA) [7]–[10], and others, have been suggested to satisfy an item's secrecy property. These are often classified as symmetric or asymmetric techniques [11], [12], the former uses identical keys for encrypting and decrypting operations, whereas the latter employs various keys [2]. Traditional encryptions are good, but it have been developed for text data without considering the unique characteristics of image data [13]. Compared to the encryption of traditional alphanumeric data files, the encryption of image data has encountered several new challenges due to their unique characteristics, such as, the size of the image content is often substantially larger than that of the text data [14], [15]. As a result, the encryption approach that encrypts the image demands a very large amount of computation [16]. This means that the above techniques are not inefficient only but, also, less secure [17].

Recently, several researchers have used the benefits of parallel processing on GPUs like OpenGL, OpenCL, and CUDA to enhance but not cure the computational cost and time inadequacies of traditional encryption techniques [18]. As proposed new economical, quick, and highly efficient RGB image encryption methods are required primarily, for example, in medical situations where safe image transmission is a necessity, particularly for telemedicine experts [19]. Many experiments have lately been undertaken to fulfill these requirements, using a hybrid of Deoxyribonucleic Acid (DNA) techniques and other cryptographic methods. This combination strategy is based on Shannon's rule, which states that an encryption scheme must meet the confusion and diffusion qualities [20].

DNA nucleotide bases, including adenine (A), cytosine (C), guanine (G), and thymine (T), are employed as information carriers in DNA computing [21]; it offer significant benefits in dealing with power consumption of information, parallel, and huge storage capacity [22]. To address practical difficulties, DNA computing mostly employs biological experiments. However, investigating DNA computing is challenging because to the limits of biochemical reaction circumstances, such as, expensive experimental equipment, environmental requirements, trouble extracting DNA sequences, and issues regulating the concentration, temperature, and PH of the reactant. In DNA computing, researchers disregard the complicated experimental linkages of DNA, simply utilize DNA coding to carry image information, and build an acceptable and effective encryption scheme by combining DNA coding with various approaches. This concept opens up new avenues of investigation in image encryption research. DNA-based image encryption techniques have emerged as a hotspot field for image encryption and security research [23].

Researchers typically increase the performance of cryptography algorithms by modifying DNA encoding methods and procedures [24]. Without comprehensive comparison or analysis of the techniques or operations, the current researches merely apply a DNA encoding method, a DNA encoding process (addition, subtraction, complement, XOR, etc.), or a combination of various coding operations to accomplish image coding. In other words, the purpose of choosing a certain DNA encoding method (static or dynamic), the DNA encoding process, or a mix of various encoding processes to accomplish image encoding are not obvious in any current study. As a result, this research includes assessments of existing DNA-based image encryption techniques comprehensively and compared all these researches.

The rest of this paper is organized as follows: the theoretical foundation of this study is provided in the second Section. In the third Section, we showed existing DNA-based color image encryption techniques. While, the four Section contained results of all studies, compare, analyze their merits. Finally, the conclusions of DNA-based image encryption algorithms are discussed in the last Section.

2. THEORITICAL FOUNDATIONS

2.1. DNA encoding

A, T, G, and C are the four DNA bases. G and C, as well as, A and T, are complimentary. Normally, in a binary system, the numbers 0 and 1 are complementary. As a result, the numbers 00, 11, 01, and 10 may be encoded into the four bases [25]. There are 24 potential DNA encoding techniques, according to combinatorics. According to the complimentary nature of the four, only eight coding combinations are acceptable, as shown in Table 1.

The gray value of an image pixel may be described in image encryption as its equivalent binary representation [26]. This binary representation may then be readily converted into a DNA representation. On the other hand, a DNA representation can be simply converted into an image pixel. A pixel value of 196, for example, corresponds to the binary representation 11000100. Using DNA encoding Rule 5, it may be encoded into the DNA representation GCAC. When DNA decoding, Rule 7 is applied to this sequence, the resulting pixel value is 55 [27]. Existing DNA-based image encryption techniques are nearly inextricably linked to or deformed by this coding rule.

Table 1. DNA encoding rules [28].

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

2.2. DNA complement rules

There are two ways for DNA sequence complement-based image encryption [29]: (1) method of single base straight complement and (2) method that performs the complement operation using the notion of single, as well as, double base complementary coupling. The following is the definition of a single base straight complement:

$$\begin{cases} T = Complement\ (A) \\ A = Complement\ (T) \\ C = Complement\ (G) \\ G = Complement\ (C) \end{cases}, \quad (1)$$

where $Complement\ (.)$ denotes the complement's function. T is the complement of base A, while G is the complement of base C. When the complement of 00 is 11 and the complement of 01 is 10, the corresponding binary complement is satisfied, and vice versa [30].

A double helix structure is used to determine the complement rule; a nucleoside is coupled using the double helix structure [31]. Assuming D is the complementary transformation; each nucleoside x_i fulfills the following equation [32]:

$$\begin{cases} x_i \neq D(x_i) \neq D(D(x_i)) \neq D(D(D(x_i))) \\ x_i = D(D(D(D(x_i)))) \end{cases}, \quad (2)$$

if x_i and D(x_i) are complimentary, x_i and D(x_i) are base pairs; these base pairs must meet the single-shot mapping requirement. Table 2 lists the base pairings that satisfy single-shot mappings based on the aforementioned equation.

Table 2. Base complementary principle complement operation [33].

Rules	Complement operations			
Rule 1	(AT)	(TG)	(GC)	(CA)
Rule 2	(AT)	(TC)	(CG)	(GA)
Rule 3	(AC)	(CT)	(TG)	(GA)
Rule 4	(AC)	(CG)	(GT)	(TA)
Rule 5	(AG)	(GT)	(TC)	(CA)
Rule 6	(AG)	(GC)	(CT)	(TA)

2.3. DNA addition, subtraction, and XOR algebra operations

Furthermore, several operations on the DNA representation were used to encrypt the image [34]. As with binary numbers, the DNA sequences can be addition, subtraction, and XOR operations in the same way, and the results are influenced by the rules that are used to perform these operations. The addition and subtraction procedures in encryption and decryption are reciprocal. In addition, the opposite of XOR stays an XOR operation [35]. As a result, we only mention addition and XOR operations in Table 3, which is based on Rule 1's addition and XOR operations in Table 1.

Table 3. DNA sequence of addition and XOR operations [36].

ADD	A	C	G	T	XOR	A	C	G	T
A	A	C	G	T	A	A	C	G	T
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	T	A	C
T	T	A	C	G	T	T	G	C	A

3. COLOR IMAGE ENCRYPTION BASED ON DNA

None of the twelve hybrid studies is entirely based on DNA, but they are applied and linked with other computational models, such as, chaotic systems, hyper-chaotic systems, secure hash functions, couple map lattice (CML), genetic algorithm, and neural network. A brief summary of these strategies is provided below.

In 2015 [37], (X. Wu et al.) introduced a novel encryption technique based on DNA sequence operations and several upgraded one-dimensional (1D) chaotic systems. To begin, the key streams were constructed utilizing the secret keys and the plain-image from three upgraded 1D chaotic systems. Using the DNA encoding principles, randomly transform the key streams and plain-image into DNA matrices. Then, on the scrambled DNA matrices, the DNA complementary and XOR operations were done. Next, the scrambled DNA matrices were divided into equal blocks and randomly mixed these blocks. Finally, the DNA XOR and addition operations applied to the DNA matrices and key streams obtained in the previous stage, and then used the DNA decoding procedures to generate the cipher-image from the encrypted DNA matrices.

In 2016 [38], (X. Wang et al.) presented a color image encryption method that makes use of DNA sequence operations and a chaotic system. Three components for the color plain image were used to produce a matrix, and the pixels matrix formed by CML (coupled map lattice) was then confused. During the permutation phase, DNA encoding and decoding rules were added. The DNA matrix's rows and columns were permuted to obtain the color cipher image.

In 2017 [39], (J. Wang et al.) developed a unique encryption technique based on DNA sequence operations and cellular neural network (CNN). To begin, the original color image was divided into three matrices (R, G, B), which were then turned into DNA matrices. Then, the chaotic sequences generated by CNN

were used to scramble the three matrices of DNA sequence. Finally, the three DNA matrices were added together using specific rules and complement with complimentary rules, the cipher-image was created using the DNA decoding rules.

In 2018 [40], (A. ur Rehman et al.) presented a color image encryption technique that uses the hash function SHA-256 to change the chaotic system's starting circumstances and control settings. Three-color image channels were sorted using the chaotic sequence created by the Piecewise Linear Chaotic Map (PWLCM). The array was then individually permuted using Lorenz's chaotic system. Every channel was chaotically encoded into DNA bases. The exclusive-OR procedure was repeated with numerous DNA complementary rules. This cycle of operation repetition continued to create cipher image.

In 2019 [41], (N. Iqbal et al.) suggested a unique RGB image cipher utilizing DNA computing. The color image was divided into three parts: red, green, and blue. The grayscale images were then concatenated to form a single grayscale image. This single grayscale image was split into many blocks. The 15-puzzle problem was used to suggest a block level permutation (BLP) on this grayscale image. To further randomize the image pixels, pixel level permutation was used. This scrambled image was then encoded and decoded with DNA bases to produce an encrypted image.

In 2019 [42], (G. Ye and K.-W. Wong) suggested color image encryption based on dynamic DNA and 4-D memristive hyper-chaos. First, the 4-D memristive hyper-chaos was used to construct chaotic matrices. Second, three components of the plain image were dynamically encoded to produce three DNA matrices. The encoded DNA matrices were then subjected to dynamic confusion and diffusion. Finally, the encrypted image was produced by decoding DNA and assembling components.

In 2020 [43], (K. C. Jithin and S. Sankar) presented an image encryption system based on DNA encoding and chaotic maps. To improve security, the Arnold map was applied individually on each of the three channels of the color image. The chaos in image encryption has increased the security of image data transmission.

In 2020 [44], (S. Zhou et al.) introduced a dynamic DNA image encryption based on the Secure Hash Algorithm-512 (SHA-512), with the structure of two rounds of permutation-diffusion, by utilizing two chaotic systems, conditional shifting, dynamic DNA coding, and DNA sequencing operations.

In 2020 [45], (N. Iqbal et al.) suggested a novel strategy for color image encryption based on DNA strands level scrambling (DNASLS) and a chaotic system. The streams were generated via an intertwining logistic map (ILM). These streams were utilized to DNA-encode the image and key image, an XOR operation was performed on the DNA-encoded image and key image, and then decoded the DNA-encoded pixels into decimal form to get.

In 2021 [46], (X. Chai et al.) suggested a DNA-based RGB image encryption and an upgraded genetic algorithm, as well as, a matrix semi-tensor product (STP). Preprocessing, DNA encoding, crossover, mutation, and DNA decoding were the five phases of the encryption process. The DNA encoding rules were formed dynamically by chaotic sequences, and the DNA decoding rules were constructed based on the encoding rules.

In 2021 [47], (S. Patel et al.) suggested a DNA-based RGB image encryption and a customized neural network (NN). The NN model was made up of one input layer, three hidden layers, and one output layer, with chaotic maps serving as the neuron transfer function in each layer. For cryptography purposes, the generator generates four chaotic sequences. Color image encryption uses these sequences. Pixel permutation, DNA encoding, and pixel diffusion were three important processes in the encryption method.

In 2021 [48], (Q. Zhang and J. Han) developed a revolutionary color image encryption technique based on dynamic DNA coding, six-dimensional (6D) hyperchaotic, and image hashing. The RGB color image's three-color channels were combined into a 2D matrix, and the pixels were replaced using the enhanced 2D chaotic map. The encrypted image was generated by using a 6D hyperchaotic system to create random sequences for DNA dynamic encoding and arithmetic operation on color image.

4. COMPARATIVE ANALYSIS OF THE SCHEMES

Throughout all of these algorithms experiments, for verifying the encryption approach in relation to the current security analysis criteria, Lena was used. The plain image of Lena has a size of M ×N, with M and N being respectively the width and height of the image. Each pixel's value is made up of R, G, and B (red, green, and blue, respectively) color components. Thus, depending on the color planes, the color image can be translated into three gray images, with the size of the matrix for each color (R, G, or B) being M × N. As it is illustrated in Fig. 1 , the color Lena image (Fig. 1 (a)) with a size of 256 × 256 is the color original image with red, green, and blue components shown in Fig. 1 (b) − (d), respectively. The value of each gray pixel ranges from 0 to 255. The most prevalent security measures were those designed to withstand statistical, exhaustive search, and differential attacks, as well as, to quantify image uncertainty [49]. Key space, correlation coefficients, NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), and information entropy will be used to meet these requirements.

(a) (b) (c) (d)

Figure 1. Lena image including (a) Color plain image, (b) Red component, (c) Green component, and (d) Blue component.

Table 4. A comparison of 12 research' resistance to brute-force attacks.

Studies	Key length	Precision
Ref.[37]	2^{299}	10^{-15}
Ref.[38]	2^{220}	10^{-16}
Ref.[39]	2^{186}	10^{-14}
Ref.[40]	$2^{79.72}$	10^{-12}
Ref.[41]	2^{356}	10^{-15}
Ref.[42]	2^{373}	10^{-14}
Ref.[43]	$(2\times10^{15})^3\times10^2\times(256)^{(65,536\times3)}$	10^{-15}
Ref.[44]	2^{326}	10^{-14}
Ref.[45]	2^{348}	10^{-15}
Ref.[46]	2^{280}	10^{-14}
Ref.[47]	2^{128}	--
Ref.[48]	2^{536}	--

To withstand an exhaustive key search assault (brute force attack), the key length must be more than 2^{100} [50]–[52]. For this reason, the key spaces for several DNA-based color image encryption algorithms are being analyzed. Table 4 summarizes the supported key length values and precision for the target investigations. Researches' proposed key spaces meet the key length (above 2^{100}) criterion for practical usage.

To eliminate statistical attacks on a suggested encryption method, correlation coefficients analysis should be as close to zero as possible [53]–[56]. This is accomplished by calculating the correlations of numerous (for example, 5000, 10000, etc.) random neighboring pixel pairings between the original image and ciphered image to get lower values of correlation coefficients for ciphered image in comparison to the original image. The following equations are used to calculate the correlation coefficients [53]:

$$\bar{x} = \frac{1}{M\times N}\sum_{i=1}^{M\times N} x_i \tag{3}$$

$$\sigma_x = \frac{1}{N}\sum_{i=1}^{n}(x_i - \bar{x})^2 \tag{4}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \tag{5}$$

$$corr_{xy} = \frac{cov(x,y)}{\sqrt{\sigma_x}\sqrt{\sigma_y}}. \tag{6}$$

Except four studies, all give values of correlation coefficients for Red, Green, and Blue components in three directions: diagonal, vertical, and horizontal, Table 5 summarizes the values of the three components and the average of these components evaluated to the plain and ciphered images to compare the findings. The average findings of 12 experiments reveal that the correlation coefficient of ciphered images is close to zero.

NPCR and UACI are the other two security criteria for analysing methods in terms of differential attacks [57], [58]. These are numerical measurements, in which the NPCR depicts the percentage of pixel changes in the ciphered image compared to the plain image when a single pixel of the plain image is modified [59]. In other words, the higher the NPCR number, the more resistant the encryption method is to plaintext

attack [60], [61]. The latter (UACI) represents the average of the discrepancies between the original and ciphered images [62]. The greater the value, the more resistant the encryption methods are to differential attack. The Equations (7) and (8) can be used to compute their value [63], [64]:

$$NPCR = \frac{\sum_{i,j} D(i.j)}{M \times N} \times 100\% \quad (7)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%, \quad (8)$$

where $C_1(i,j)$, and $C_2(i,j)$ represent two encrypted images with only one pixel value change from the corresponding plain images, $D(i.j)$= 0 when it is the same value in C_1, and C_2, while, it is 1 when it is different. M and N denotes the image's height and width, respectively.

Table 5. Comparison of correlation coefficient values on ciphered images using three components (R, G, and B values, as well as, their averages) and three directions (H, V, and D).

Studies	Directions	Correlation coefficients of encrypted image			
		R	G	B	Averages
Ref.[37]	Horizontal Vertical Diagonal	-------	-------	-------	-0.0084 0.0004 -0.0015
Ref.[38]	Horizontal Vertical Diagonal	0.0090 -0.0013 -0.0025	-0.0027 -0.0051 -0.0103	-0.0155 -0.0078 0.0099	-------
Ref.[39]	Horizontal Vertical Diagonal	-------	-------	-------	-0.0219 0.0326 -0.0098
Ref.[40]	Horizontal Vertical Diagonal	-0.0073 0.0010 -0.0013	0.0011 -0.0020 0.0078	-0.0061 0.0058 -0.0003	-----
Ref.[41]	Horizontal Vertical Diagonal	0.0091 0.0124 0.0010	-0.0015 0.0023 0.0241	-0.0068 0.0006 -0.0116	0.0003 0.0051 0.0028
Ref.[42]	Horizontal Vertical Diagonal	0.0045 0.0009 -0.0036	-0.0005 -0.0018 -0.0033	0.0017 -0.0039 -0.0058	0.0011 -0.0013 -0.0019
Ref.[43]	Horizontal Vertical Diagonal	0.0021 0.0018 -0.0026	-0.0006 0.0004 0	-0.0050 0.0010 -0.0104	-0.0011 0.0010 -0.0043
Ref.[44]	Horizontal Vertical Diagonal	0.0140 0.0110 0.0350	0.0110 0.0200 0.0160	0.0090 0.0220 0.0210	------
Ref.[45]	Horizontal Vertical Diagonal	--------	-------	-------	0.0042 0.0087 -0.0031
Ref.[46]	Horizontal Vertical Diagonal	0.0094 -0.0011 0.0009	-0.0018 -0.0076 0.0006	0.0019 -0.0042 0.0022	-------
Ref.[47]	Horizontal Vertical Diagonal	-------	-------	-------	-0.0287 0.0071 0.0007
Ref.[48]	Horizontal Vertical Diagonal	-0.0002 -0.0023 -0.0021	-0.0002 -0.0043 0.0007	-0.0074 -0.0010 -0.0007	-------

As a results of the data presented in Table 6 for 12 research, it is possible to conclude that all the researches had values for NPCR greater than 99 % (around 100 %) and for UACI greater than 33 % when the values of the three components (R, G, and B) and the average of these components are included. These findings suggest that these techniques are robust to differential and plaintext assaults.

The information entropy is in charge of assessing image randomness [65]–[67]. That is, this parameter expresses the degree of uncertainty or image information gray-level distribution. The closer the number is to 8 [68]–[70], the better the gray level distribution and hence the more accurate the encryption procedure. The following equation can be used to calculate image information entropy [71]:

$$H(d) = \sum_{i=1}^{2^l - 1} p(d_i) log_2\left(\frac{1}{p(d_i)}\right), \quad (9)$$

where l is the number of digits in the image pixel gray value, and $p(d_i)$ signifies the likelihood of a pixel with value d_i occurring. The average value of information entropy for the three components (R, G, and B) of the image for 12 researches are presented in the last columns of Table 6, and they are approximately 8.

Table 6. The NPCR, UACI, and information entropy outcomes of the 12 researches.

Studies	NPCR (%)	UACI (%)	Information entropy (bit)
Ref.[37]	99.60	33.48	7.9897
Ref.[38]	99.61	33.43	7.9972
Ref.[39]	99.51	33.36	7.9910
Ref.[40]	99.60	33.42	7.9968
Ref.[41]	99.60	33.46	7.9971
Ref.[42]	99.61	30.41	7.9993
Ref.[43]	99.57	33.33	7.9992
Ref.[44]	99.60	33.47	7.9975
Ref.[45]	99.60	33.46	7.9974
Ref.[46]	99.63	33.40	7.9972
Ref.[47]	99.61	33.44	7.9914
Ref.[48]	99.60	33.45	7.9994

5. CONCLUSION

Many image encryption research articles employing DNA encoding have been published. The goal of this review study is not to recommend a suitable encryption approach, but to share insights about previously investigated DNA encoding and image encryption methods. The study discussed twelve strategies utilized by various authors in image encryption systems. According to the findings of the aforementioned publications, DNA encoding plays a vital role in providing a safe cryptosystem when compared to a traditional system. DNA's huge information store capacity, powerful parallel processing capacity, and ultralow energy consumption make it ideal for designing an effective, efficient, and safe cryptosystem. The DNA-based image encryption approaches offer a superior trade-off between security and computational complexity, and have been highlighted as an essential component in the construction of a trustworthy and authenticated cryptosystem.

REFERENCES

[1] S. Zhong *et al.*, *Security and Privacy for Next-Generation Wireless Networks*. Springer, 2019, doi:10.1007/978-3-030-01150-5.

[2] L. A. Shihab, "Technological Tools for Data Security in the Treatment of Data Reliability in Big Data Environments," *Int. Trans. J. Eng. Manag. Appl. Sci. Technol.*, vol. 11, no. 9, pp. 1–13, 2020, doi:10.14456/ITJEMAST.2020.175.

[3] A. Broumandnia, "Image encryption algorithm based on the finite fields in chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, p. 102553, 2020, doi:10.1016/j.jisa.2020.102553.

[4] S. R. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," *Microprocess. Microsyst.*, vol. 77, p. 103134, 2020, doi:10.1016/j.micpro.2020.103134.

[5] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey," in *IOP conference series: materials science and engineering*, 2019, vol. 518, no. 5, p. 52003, doi:10.1088/1757-899X/518/5/052003.

[6] M. K. Hasan *et al.*, "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi:10.1109/ACCESS.2021.3061710.

[7] H. A. Younis, T. Y. Abdalla, and A. Y. Abdalla, "Fast Techniques For Partial Encryption of Wavelet-based Digital Images," *basrah J. Sci.*, vol. 25, no. 2A english, 2007, https://iraqjournals.com/article_54373_0.html.

[8] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, pp. 617–624, 2016, doi:10.1016/j.procs.2016.02.108.

[9] D. M. Alsaffar *et al.*, "Image encryption based on AES and RSA algorithms," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020, pp. 1–5, doi:10.1109/ICCAIS48893.2020.9096809.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978, doi:10.1145/359340.359342.

[11] K. U. Shahna and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Appl. Soft Comput.*, vol. 90, p. 106162, 2020, doi:10.1016/j.asoc.2020.106162.

[12] Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map," *Phys. Scr.*, vol. 95, no. 3, p. 35223, 2020, doi:10.1088/1402-4896/ab52bc.

[13] L. Chen, H. Yin, L. Yuan, J. A. T. Machado, R. Wu, and Z. Alam, "Double color image encryption based on fractional order discrete improved Henon map and Rubik's cube transform," *Signal Process. Image Commun.*, vol. 97, p. 116363, 2021, doi:10.1016/j.image.2021.116363.

[14] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163–185, 2019, doi:10.1016/j.sigpro.2019.06.010.

[15] L. You, E. Yang, and G. Wang, "A novel parallel image encryption algorithm based on hybrid chaotic maps with OpenCL implementation," *Soft Comput.*, vol. 24, no. 16, pp. 12413–12427, 2020, doi:10.1007/s00500-020-04683-4.

[16] O. A. Khashan and M. AlShaikh, "Edge-based lightweight selective encryption scheme for digital medical images," *Multimed. Tools Appl.*, vol. 79, no. 35, pp. 26369–26388, 2020, doi:10.1007/s11042-020-09264-z.

[17] L. Y. Zhang *et al.*, "On the security of a class of diffusion mechanisms for image encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1163–1175, 2017, doi:10.1109/TCYB.2017.2682561.

[18] P. Czarnul, J. Proficz, and K. Drypczewski, "Survey of methodologies, approaches, and challenges in parallel programming using high-performance computing systems," *Sci. Program.*, vol. 2020, 2020, doi:10.1155/2020/4176794.

[19] V. Pavithra and J. Chandrasekaran, "Developing security solutions for telemedicine applications: medical image encryption and watermarking," in *Research anthology on telemedicine efficacy, adoption, and impact on healthcare delivery*, IGI Global, 2021, pp. 612–631, doi:10.4018/978-1-7998-8052-3.ch032.

[20] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949, doi:10.1002/j.1538-7305.1949.tb00928.x.

[21] E. Şatir and O. Kendirli, "A symmetric DNA encryption process with a biotechnical hardware," *J. King Saud Univ.*, vol. 34, no. 3, p. 101838, 2022, doi:10.1016/j.jksus.2022.101838.

[22] J. Yin, J. Wang, R. Niu, S. Ren, D. Wang, and J. Chao, "DNA nanotechnology-based biocomputing," *Chem. Res. Chinese Univ.*, vol. 36, no. 2, pp. 219–226, 2020, doi:10.1007/s40242-020-9086-5.

[23] S.-L. Cheng, L.-J. Wang, G. Huang, and A.-Y. Du, "A privacy-preserving image retrieval scheme based secure kNN, DNA coding and deep hashing," *Multimed. Tools Appl.*, vol. 80, no. 15, pp. 22733–22755, 2021, doi:10.1007/s11042-019-07753-4.

[24] W. Ran, E. Wang, and Z. Tong, "A double scrambling-DNA row and column closed loop image encryption algorithm based on chaotic system," *PLoS One*, vol. 17, no. 7, p. e0267094, 2022, doi:10.1371/journal.pone.0267094.

[25] H. M. Al-Mashhadi and I. Q. Abduljaleel, "Color image encryption using chaotic maps, triangular scrambling, with DNA sequences," in *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, 2017, pp. 93–98, doi:10.1109/CRCSIT.2017.7965540.

[26] V. Rathore and A. K. Pal, "An image encryption scheme in bit plane content using Henon map based generated edge map," *Multimed. Tools Appl.*, vol. 80, no. 14, pp. 22275–22300, 2021, doi:10.1007/s11042-021-10719-0.

[27] S. M. Abdullah and I. Q. Abduljaleel, "Speech Encryption Technique using S - box based on Multi Chaotic Maps," *TEM J.*, vol. 10, no. 3, pp. 1429–1434, 2021, doi: 10.18421/TEM103-54, doi:10.18421/TEM103-54.

[28] 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, p. 115670, 2020, doi:10.1016/j.image.2019.115670.

[29] Z. Liang, Q. Qin, C. Zhou, N. Wang, Y. Xu, and W. Zhou, "Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation," *PLoS One*, vol. 16, no. 11, p. e0260014, 2021, doi:10.1371/journal.pone.0260014.

[30] P. Liu, T. Zhang, and X. Li, "A new color image encryption algorithm based on DNA and spatial chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 11, pp. 14823–14835, 2019, doi:10.1007/s11042-018-6758-y.

[31] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Opt. Lasers Eng.*, vol. 137, p. 106393, 2021, doi:10.1016/j.optlaseng.2020.106393.

[32] X. Ouyang, Y. Luo, J. Liu, L. Cao, and Y. Liu, "A color image encryption method based on memristive hyperchaotic system and DNA encryption," *Int. J. Mod. Phys. B*, vol. 34, no. 04, p. 2050014, 2020, doi:10.1142/S0217979220500149.

[33] S. Namasudra, R. Chakraborty, A. Majumder, and N. R. Moparthi, "Securing multimedia by using DNA-based encryption in the cloud computing environment," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 16, no. 3s, pp. 1–19, 2020, doi:10.1145/3392665.

[34] M. Dua, A. Wesanekar, V. Gupta, M. Bhola, and S. Dua, "Differential evolution optimization of intertwining logistic map-DNA based image encryption technique," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 9, pp. 3771–3786, 2020, doi:10.1007/s12652-019-01580-z.

[35] H. Wu, H. Zhu, and G. Ye, "Public key image encryption algorithm based on pixel information and random number insertion," *Phys. Scr.*, vol. 96, no. 10, p. 105202, 2021, doi:10.1088/1402-4896/ac0bcf.

[36] X. Zhang and R. Ye, "A novel RGB image encryption algorithm based on DNA sequences and chaos," *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8809–8833, 2021, doi:10.1007/s11042-020-09465-6.

[37] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, 2015, doi:10.1016/j.asoc.2015.08.008.

[38] X. Wang, H. Zhang, and X. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, 2016, doi:10.1016/j.biosystems.2016.03.011.

[39] J. Wang, F. Long, and W. Ou, "CNN-based color image encryption algorithm using DNA sequence operations," in *2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, 2017, pp. 730–736, doi:10.1109/SPAC.2017.8304370.

[40] A. ur Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik (Stuttg).*, vol. 159, pp. 348–367, 2018, doi:10.1016/j.ijleo.2018.01.064.

[41] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB image cipher using chaotic systems, 15-puzzle problem and DNA computing," *IEEE Access*, vol. 7, pp. 174051–174071, 2019, doi:10.1109/ACCESS.2019.2956389.

[42] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, 2012, doi:10.1007/s11071-012-0409-z.

[43] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *J. Inf. Secur. Appl.*, vol. 50, p. 102428, 2020, doi:10.1016/j.jisa.2019.102428.

[44] S. Zhou, P. He, and N. Kasabov, "A dynamic DNA color image encryption method based on SHA-512," *Entropy*, vol. 22, no. 10, p. 1091, 2020, doi:10.3390/e22101091.

[45] N. Iqbal, M. Hanif, S. Abbas, M. A. Khan, S. H. Almotiri, and M. A. Al Ghamdi, "DNA strands level scrambling based color image encryption scheme," *IEEE Access*, vol. 8, pp. 178167–178182, 2020, doi:10.1109/ACCESS.2020.3025241.

[46] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Processing*, vol. 183, p. 108041, 2021, doi:10.1016/j.sigpro.2021.108041.

[47] S. Patel, V. Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, "Colour image encryption based on customized neural network and DNA encoding," *Neural Comput. Appl.*, vol. 33, no. 21, pp. 14533–14550, 2021, doi:10.1007/s00521-021-06096-2.

[48] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 13841–13864, 2021, doi:10.1007/s11042-020-10437-z.

[49] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: an attack-resistant image encryption," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 11477–11489, 2020, doi:10.1007/s00521-019-04637-4.

[50] S. Patel and R. K. Muthu, "Image encryption decryption using chaotic logistic mapping and dna encoding," *arXiv Prepr. arXiv2003.06616*, 2020, doi:10.48550/arXiv.2003.06616.

[51] F.-P. An and J. Liu, "Image encryption algorithm based on adaptive wavelet chaos," *J. Sensors*, vol. 2019, 2019, doi:10.1155/2019/2768121.

[52] M. Kaur, S. Singh, M. Kaur, A. Singh, and D. Singh, "A systematic review of metaheuristic-based image encryption techniques," *Arch. Comput. Methods Eng.*, pp. 1–15, 2021, doi:10.1007/s11831-021-09656-w.

[53] Y. Sun, H. Zhang, X. Wang, and M. Wang, "Bit-level color image encryption algorithm based on coarse-grained logistic map and fractional chaos," *Multimed. Tools Appl.*, vol. 80, no. 8, pp. 12155–12173, 2021, doi:10.1007/s11042-020-10373-y.

[54] J. S. Khan, J. Ahmad, S. S. Ahmed, H. A. Siddiqa, S. F. Abbasi, and S. K. Kayhan, "DNA key based visual chaotic image encryption," *J. Intell. Fuzzy Syst.*, vol. 37, no. 2, pp. 2549–2561, 2019, doi:10.3233/JIFS-182778.

[55] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimens. Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, 2019, doi:10.1007/s11045-018-0589-x.

[56] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci. (Ny).*, vol. 515, pp. 191–217, 2020, doi:10.1016/j.ins.2019.10.070.

[57] H. M. Al-Mashhadi, "Quality Assessment for Image Encryption Techniques using Fuzzy Logic System," *Int. J. Comput. Appl.*, vol. 157, no. 5, 2017, doi:10.5120/ijca2017912706.

[58] X. Wang, S. Chen, and Y. Zhang, "A chaotic image encryption algorithm based on random dynamic mixing," *Opt. Laser Technol.*, vol. 138, p. 106837, 2021, doi:10.1016/j.optlastec.2020.106837.

[59] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *J. Supercomput.*, vol. 75, no. 10, pp. 6663–6682, 2019, doi:10.1007/s11227-019-02878-7.

[60] Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, "Image encryption algorithm with circle index table scrambling and partition diffusion," *Nonlinear Dyn.*, vol. 103, no. 2, pp. 2043–2061, 2021, doi:10.1007/s11071-021-06206-8.

[61] G. Shengtao, W. Tao, W. Shida, Z. Xuncai, and N. Ying, "A novel image encryption algorithm based on chaotic sequences and cross-diffusion of bits," *IEEE Photonics J.*, vol. 13, no. 1, pp. 1–15, 2020, doi:10.1109/JPHOT.2020.3044222.

[62] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020, doi:10.1109/ACCESS.2020.2965740.

[63] B. D. Parameshachari, "Logistic sine map (LSM) based partial image encryption," in *2021 National Computing Colleges Conference (NCCC)*, 2021, pp. 1–6, doi:10.1109/NCCC49330.2021.9428854.

[64] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps," *Math. Comput. Simul.*, vol. 178, pp. 646–666, 2020, doi:10.1016/j.matcom.2020.07.007.

[65] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Opt. Lasers Eng.*, vol. 128, p. 105995, 2020, doi:10.1016/j.optlaseng.2019.105995.

[66] X. Wang, W. Xue, and J. An, "Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household," *Chaos, Solitons & Fractals*, vol. 141, p. 110309, 2020, doi:10.1016/j.chaos.2020.110309.

[67] X. Zhang, L. Wang, G. Cui, and Y. Niu, "Entropy-based block scrambling image encryption using DES structure and chaotic systems," *Int. J. Opt.*, vol. 2019, 2019, doi:10.1155/2019/3594534.

[68] Z. Gan, X. Chai, J. Zhang, Y. Zhang, and Y. Chen, "An effective image compression–encryption scheme based on compressive sensing (CS) and game of life (GOL)," *Neural Comput. Appl.*, vol. 32, no. 17, pp. 14113–14141, 2020, doi:10.1007/s00521-020-04808-8.

[69] X. Jin, X. Duan, H. Jin, and Y. Ma, "A novel hybrid secure image encryption based on the shuffle algorithm and the hidden attractor chaos system," *Entropy*, vol. 22, no. 6, p. 640, 2020, doi:10.3390/e22060640.

[70] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-boxes," *Entropy*, vol. 21, no. 8, p. 790, 2019, doi:10.3390/e21080790.

[71] J. Xu, B. Zhao, and Z. Wu, "Research on Color Image Encryption Algorithm Based on Bit-Plane and Chen Chaotic System," *Entropy*, vol. 24, no. 2, p. 186, 2022, doi:10.3390/e24020186.