Journal of Soft Computing and Computer Applications

Manuscript 1013

Survey: A Study on Image Encryption Using DNA in Bioinformatics

Rana M. Zaki

Zaed S. Mahdi

Matheel E. Abdulmunim

Follow this and additional works at: https://jscca.uotechnology.edu.iq/jscca

 Part of the Computer Engineering Commons, and the Computer Sciences Commons

The journal in which this article appears is hosted on Digital Commons, an Elsevier platform.

JOURNAL OF SOFT COMPUTING AND COMPUTER APPLICATIONS 2024;1:1013

Scan the QR to view the full-text article on the journal website

REVIEW

Survey: A Study on Image Encryption Using DNA in Bioinformatics

Rana M. Zaki [a,*], **Zaed S. Mahdi** [b,1], **Matheel E. Abdulmunim** [a,1]

[a] Department of Computer Science, University of Technology – Iraq, Al-Sina'a St., Al-Wehda District, 10066 Baghdad, Iraq
[b] Information Technology Center, University of Technology – Iraq, Al-Sina'a St., Al-Wehda District, 10066 Baghdad, Iraq

ABSTRACT

One area of study between computer science and biology is bioinformatics, which deals with methods for collecting, processing, storing, and evaluating biological data. Sequences of RiboNucleic Acid (RNA), DeoxyriboNucleic Acid (DNA), and proteins make up biological data, which has a wide range of uses in domains such as feature extraction, data segmentation, data security, and more. In cryptography, DNA sequences are used as data carriers, enhancing the unique properties of biomolecules. This approach involves using DNA sequences to enhance the security of confidential data that must be transmitted over networks or stored securely. Several DNA-based security techniques have been developed, each with its own strengths and weaknesses. The bioinformatics offers innovative solutions for data security, especially in the realm of cryptography. By employing DNA sequences as data carriers, bioinformatics techniques can significantly enhance the protection of confidential data. The goal of This survey aims to summarize the existing literature on DNA-based security techniques. It highlights various methods that use DNA sequences to protect confidential data, either during transmission or in storage and identifies the strengths and weaknesses of these methods, providing a comprehensive overview for researchers to assist in planning and designing secure techniques based on bioinformatics methods. By understanding the existing approaches and their limitations, researchers can develop more efficient and robust security techniques that leverage the power of DNA sequences and bioinformatics. This survey serves as a valuable resource for researchers seeking to explore and develop secure methods based on the intersection of bioinformatics and cryptography.

Keywords: Image encryption, Bioinformatics, DNA, Chaotic map

1. Introduction

For many businesses, data security has become a fundamental necessity. Through networks like the internet, several entities can communicate with one another. As a result,

Received 20 April 2024; accepted 22 December 2024.
Available online 31 December 2024

* Corresponding author.
E-mail addresses: rana.m.zaki@uotechnology.edu.iq (R. M. Zaki), zaed.s.mahdi@uotechnology.edu.iq (Z. S. Mahdi), 110104@uotechnology.edu.iq (M. E. Abdulmunim).

https://doi.org/10.70403/3008-1084.1013
3008-1084/© 2024 University of Technology's Press. This is an open-access article under the CC-BY 4.0 license (https://creativecommons.org/licenses/by/4.0/).

a secure connection must be provided. One way to prevent unwanted access to data is encryption. This encryption procedure provides security. Over years, data protection's main issue was security, Bioinformatics implementation in the procedure of improving data protection watch to raise the security level of such system [1], whereas cryptography is the science that deals with hiding or transforming sensitive and private data into an unintelligible form. The person who possesses or owns the secret key will use the cryptography method to alter the data body. To meet an item's secrecy attribute, a number of well-known encryption/decryption methods have been proposed, including Rivest Shamir Adelman (RSA), Advanced Encryption Standard (AES), and Data Encryption Standard (DES) [2]. These are frequently categorized as either symmetric or asymmetric approaches. While the latter uses different keys, the former uses the same keys for both encryption and decryption. Although traditional encryption methods are effective, they were created for text data without taking into account the special qualities of image data. A combination of DNA approaches and other cryptographic methods has been employed recently by a number of researchers [3–5]. The Shannon rule, which states that a system of encryption must satisfy the confusion and diffusion properties, is the foundation of this combination technique. Since DNA can also be used as a transporter for information and computation to enable subatomic procedures, the discovery of its computational potential may have introduced a new area of cryptography that depends on DNA [6]. DNA is a popular topic in current study and has been used for numerous computational applications. The capacity of DNA to store almost 108 terabytes of data in one gram is an amazing property [7–9]. But DNA needs to be protected using security measures because it's a data storage device. Many biological characteristics of DNA can be exploited to improve the security of steganography and cryptography methods [10]. Researchers have proposed numerous data hiding approaches in the field of data security by utilizing DNA techniques, which take advantage of the biological properties of DNA sequences to obtain stronger security and higher protection. Additionally, some academics use a variety of fields, such as frequency, geometric domain, and DNA, to improve the security of picture and software watermarking [11–14]. The field of DNA computing research was established due to the increased interest in DNA and its novel prospect [15]. Below is a summary of the contributions of this paper.

1. Survey of the literature on security methods-based DNA sequencing: This offers a thorough overview of recent studies on data that uses DNA sequencing to increase security, whether it be during storage or transmission.
2. Strengths and weaknesses analysis: The study analyzes several DNA-based data security techniques, pointing out their advantages and disadvantages to help researchers comprehend how these strategies differ from one another.
3. The role of bioinformatics in security and guidance for future research: The research highlights the application of DNA sequencing as data carriers in bioinformatics to enhance data security. By providing a comprehensive analysis of the difficulties and limitations of existing methods, helps researchers plan and create more effective and reliable security measures.

The rest of this paper is organized as follows: explains molecular biology in Section two and it contains, bioinformatics component, followed by a description of image encryption in Section three, also a current perspectives of image encryption are given in Section four. Section five contains the comparative study results of all studies, comparing them and analyzing their advantages. Lastly, the final section discusses the findings of the DNA-build encryption of picture algorithms.

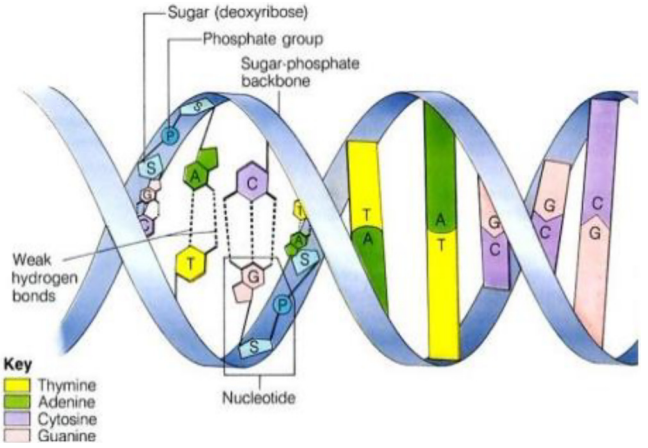

Fig. 1. Helical structure of DNA [20].

2. Molecular biology

A field of study known as bioinformatics serves as a bridge between computer science and biology. Scholars and the internet have proposed a number of definitions. Compared to others, some are more generic. As stated by Luscombe et al. [16].

"Bioinformatics is the branch of technology that deals with the distribution, retrieval, manipulation, and storage of data pertaining to biological macromolecules, including DNA, RNA, and proteins, using computers" [16]. The considerable processing power required to handle genomic data because of its complex mathematics and large repeat rates is interesting [17, 18]. Bioinformatics is concerned with unlocking the mysteries of living cells. By looking at and evaluating the building blocks and molecular sequence [16].

Bioinformatics includes biological sequences (deoxyribonucleic acid, Ribonucleic acid, ribonucleic acid and proteins) among its constituents. In the study of molecular biology, DNA is thought to be the location where genetic information and traits are stored [14–19]. All of the behavioral and physical characteristics of living things are determined by their genetic makeup since it regulates the functions of every known living thing's organs [13]. The long strand-like structure of DNA is known as the double helix, and the building blocks of each helix are known as nucleotides, as illustrated in Fig. 1. There are two types of DNA nucleotides. either a Pyrimidine base, which comprises T and C, or a Purine base, which includes A and G bases. When nucleotides interact, they usually form hydrogen bonds between A and T or between C and G [20, 21]. As seen in Fig. 2, bioinformatics is used in many computer science fields, such as sequence analysis, genome mapping, data integration, biological graphics, and data management. These components are each their own subject [22, 23] in this paper explain the DNA encoding and rules as shown:

2.1. Coding DNA

In a binary system, 0 and 1 are typically complimentary. Consequently, it is possible to encode the integers 00, 11, 01, and 10 into the four bases [24]. According to combinatorics, there are 24 possible DNA encoding methods. As seen in Table 1, only eight coding combinations are permitted due to the complementary nature of the four.

In image encryption, the gray value of a pixel can be defined as its corresponding binary representation [26]. It is then possible to easily transform this binary representation into a

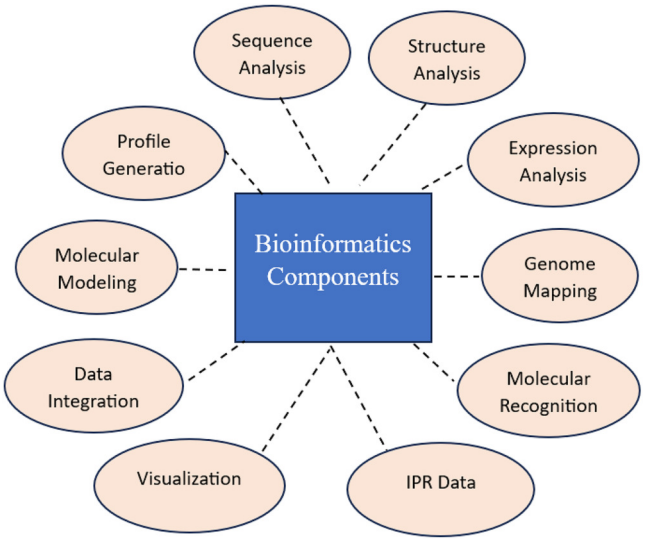

Fig. 2. Components of bioinformatic [13].

Table 1. Coding DNA rules [25].

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

DNA representation. However, a DNA representation can be easily transformed into a pixel in an image. For instance, a pixel value of 196 represents the binary code 11000100. It can be encoded into the DNA representation GCAC using DNA encoding Rule 5. The pixel value that results from applying Rule 7 to DNA decoding to this sequence is 55 [27]. This coding rule is almost inseparable from or distorts current DNA-based image encryption methods.

2.2. Rules of DNA's complement

DNA sequence complement-based image encryption can be done in two ways, which are: (Eq. (1)) the complement operation that makes use of the idea of single and double base complementary coupling, and (Eq. (2)) the single base straight complement technique. [28]. The definition of a single base straight complement is as follows:

$$\begin{aligned} T &= Complement(A) \\ A &= Complement(T) \\ C &= Complement(G) \\ G &= Complement(C) \end{aligned} \tag{1}$$

where the function of the complement is indicated by *Complement* (.). The complements of bases A and C are T and G, respectively. When 00 is the complement A nucleoside

Table 2. The complementary operation [30].

rules	Operations			
rules (1)	(AT)	(TG)	(GC)	(CA)
rules (2)	(AT)	(TC)	(CG)	(GA)
rules (3)	(AC)	(CT)	(TG)	(GA)
rules (4)	(AC)	(CG)	(GT)	(TA)
rules (5)	(AG)	(GT)	(TC)	(CA)
rules (6)	(AG)	(GC)	(CT)	(TA)

Table 3. XOR and addition operations in DNA sequence [33].

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

is connected utilizing the structure with two helices. It is used to determine the rule of complement [29]. Every nucleoside x_i satisfies (Eq. (2)), assuming that D is the complementary transformation:

$$\begin{aligned} X_i \neq D(X_i) \neq D(D(X_i)) \neq D(D(D(X_i))) \\ X_i = D(D(D(D(X_i)))) \end{aligned} \tag{2}$$

x_i and D(x_i) are base pairs if they are complementary; these base pairs need to satisfy the single-shot mapping condition. Table 2 lists the base pairings that satisfy single-shot mappings based on (Eq. (2)).

2.3. Algebraic XOR, DNA Addition, and Subtraction

Moreover, the image was encrypted using a number of procedures on the DNA representation. DNA sequences can be added, subtracted, and XORed in the same manner as binary integers, and the rules that are applied to carry out these operations have an impact on the outcomes. In encryption and decryption, the addition and subtraction processes are mutually exclusive. Furthermore, XOR's reverse remains an XOR operation [31, 32].

Since Addition and XOR operations for base 1 in Table 1 serve as the foundation for Table 3, addition and XOR operations are exclusively discuss there.

3. Image encryption

The combination of cryptographic systems and chaos theory is known as chaos-based cryptography. In simple terms, chaos is a state of disorder or unpredictable behavior. One area of mathematics is called chaos theory. It focused on the unexpected behavior of dynamical (nonlinear) systems that are highly sensitive to initial conditions. The main concepts of every cryptosystem, confusion and diffusion, are related to all these properties of a chaotic system. Because chaotic systems are very sensitive to their initial conditions, even small changes in their input values such as initial conditions or control parameters have a large effect on the outputs of chaotic systems, which is why they produce unexpected values. For example, two chaotic systems that are exactly the same but have slightly different initial conditions will have completely different outcomes. Sensitivity to initial

conditions is a fundamental feature of the outputs of chaotic systems. These properties of the outputs of chaotic systems have inspired many researchers to use chaotic systems to improve the security of many cryptographic systems [34–37].

The use of biometric information in image encryption provides many benefits including high security, high resistance to classical attacks and large storage potential. However, disadvantages such as computational complexity and high costs must be taken into account. The combined application of chaos theory can enhance the capabilities of these techniques, providing more complex and secure solutions in the field of image encryption [38–41].

4. Current perspectives of image encryption

Various image encryption-based DNA techniques are discussed next. The main objective is to specify the general objective of using image encryption based on DNA is to make a reliable and effective contribution towards the image security as will be explained next.

In 2012, Xiaoling and Guodong [42], suggested a method that converts a pseudo-random sequence into a biologic sequence by using a four-dimensional hyper-chaos system to produce it. To dilute the blocks of the image, a DNA sequence was used. A permutation is performed in a circular fashion on the DNA state of the plain image. The encryption performance of the technique shows promising results in the simulation because of the product of permutation plus diffusion.

In 2015, R. Guesmi et al. [43] proposes a new image encryption technique based on a DNA masking hybrid model, the Secure Hash Algorithm (SHA-2), and the Lorenz system. DNA sequences and operations, along with the chaotic Lorenz system, were employed to enhance the cryptosystem.

In 2015, Eman and Mahmoud [44] published an article outlining a DNA sequence-based cryptography method and a two-dimensional chaotic system. Two random DNA sequences, S1 and S2, are generated via the 2D chaotic map. To encrypt the message, encrypt the original message (plain) with the first (S1) DNA sequence. The sender employs the second (S2) DNA sequence to embed (hide) the ciphered message in a third (S3) sequence picked up from a list of real sequences at random. Hamming code was used next to verify that the original message M is not tampered with during transmission on decryption. The proposed strategy compared to earlier methods presented a more secure technique.

In 2015, Abolfazl, Reza, and Majid [45] stated that permutation and diffusion are two aspects of their suggested encryption technique. To encrypt the RGB image, the image was broken into red, green, and blue color bands, and then generate three chaotic sequences using chaotic maps. The red, green, and blue color bands, as well as the chaotic sequences, are then transformed into DNA code, yielding a DNA sequences matrix. Second, the RGB image's DNA matrices are permutated using Chen's hyper chaos system. Third, XOR the DNA sequence matrices using the DNA sequence XOR operation. Then, using decoding, obtain three gray images. To get encrypted RGB images, combine the R, G, and B components.

In 2016, K. Santoso et al. [46] produced an article outlining a sector-based DNA steganography system that stores binary data on non-coding DNA sequence segments. Maintaining the original biological information contained in the DNA while attaining high levels of error control, data capacity, and security is the aim of sector-based embedding. A sector is composed of three different types of bases: parity bases, reference bases, and segmented message bases. Mutation errors can be identified and handled by the parity bases in each sector. Sector length governs data security and capacity.

In 2016, Xinyuan and Changming [47] present an innovative and efficient image encryption technique based on Chaos and DNA encoding rules in this study. To produce all

of the parameters that the presented algorithm requires, the Piecewise Linear Chaotic Map (PWLCM) and logistic map are used, with the utility is DNA barcoding technology. The proposed algorithm consists of the following elements: start with PWLCM to generate a master image. Secondly, use DNA rules to encode the plain picture and the key image by rows. The logistic map will choose which rules to use for each row. Next, execute DNA operations using the encoded key image given the encoded plain image row. to perform DNA operations.

In 2017, Matheel and Zena [20], created a novel technique for image encryption that uses a Nonlinear-Feedback Shift Register (NLFSR) as a random generator system and a proposed DNA computing with multi-operation based on Feistel structure to increase complexity during an attack.

In 2018, Xuncai, Zheng, and Ying [13], published a paper that encrypt the image by proposed a strategy suggested utilizes the "permutation–diffusion–scrambling" structure. The hash value of the plain picture that the hyperchaotic system would employ was determined using SHA-3. It is then utilized to produce hill cipher coefficients, which are employed to alter the image's pixelation. Second, the Feistel system uses the DNA sequence as one of its functions, and the database of DNA sequences served as a key to access this system. Image pixels are diffused using this Feistel. Ultimately, additional diffusion is introduced by the use of ciphertext feedback and the three rounds of "chaotic scrambling-DNA encoding-Feistel transformation-DNA decoding" ciphertext confusion-diffusion making the encrypted image pixel randomness high and strong against attacks and ensuring a secure encrypted ciphertext.

In 2018, Jiahui and Xiaofeng [48] proposed a two-dimensional H'enon-Sine Map (2D-HSM). In comparison to many chaotic systems at that time, the new created map has pseudo-randomness and high ergodicity, and its variables have a large chaotic range. Then, because a DNA approach applied to image-encryption can considerably increase the effectiveness of data diffusion and permutation, DNA encoding is established, along with a DNA XOR operation rule. Additionally, a new image encryption technique is offered to safeguard the image while transmission over the internet. It uses 2D-HSM to permute image pixel data that has been diffused by DNA.

In 2018, A. Rehman et al. [49] proposed a method for encrypting color images that modifies the chaotic system's initial conditions and control parameters using the SHA-256 hash algorithm. The chaotic sequence produced by the PWLCM was used to sort the channels of three-color images. Next, Lorenz's chaotic system was used to permute each element of the array separately. Each channel was encoded into DNA nucleotides in a haphazard manner. Several DNA complementary rules were used to repeat the exclusive-OR process. The cipher image was created by repeating this cycle of operations.

In 2019, Alaa and Rasha [50] published a study that examines steganography using Least Significant Bit (LSB), DNA computing, and the creation of a hidden map to hide data. The secret data was encrypted using DNA computing, the LSBs were used to embed the encrypted data with the cover's LSBs, and the secret-map was used to as a locator of the hidden data. The transmitter and receiver must apply the same equation to build the secret-map, and the development of this map is dependent on the shared key.

In 2020, Xingyuan and Lin [51] Propose a two-stage image encryption algorithm. The first stage creates two encryption seque. TThe properties of these two sequences include the generation of pseudo-random numbers using highly chaotic Chain systems and the absence of repeated values. the image data is mixed twice using these sequences.

The second step of this method involves implementing the propagation by creating a DNA substitution base with coding bases and a highly chaotic system. This step involves

first encryption the image, then applying the rules that have been generated to replace the DNA codes, and finally decryption the DNA back into image.

In 2020, T. Wang, M.-h. J. O. Wang, and L [52] proposed a system for image encryption used for generating key 6-dimensional hyperchaotic related to the original image, second bit-level permutation is used to increase the security, finally, change pixels by DNA coding.

In 2020, S. Zhou, P. He, and N. J. E. Kasabov [53], proposed a dynamic DNA picture encryption technique that makes advantage of two chaotic systems: DNA sequencing operations, dynamic DNA coding, and conditional shifting. It is built on top of the SHA-512 and consists of two permutation-diffusion rounds.

In 2020 N. Iqbal et al. [54], proposed a novel method for encrypting color images using a chaotic system and DNA Strands Level Scrambling (DNASLS). Utilizing an Interconnecting Logistic Map (ILM), the streams were created. These streams were used to DNA-encode the picture and key image. The DNA-encoded pixels were then decoded into decimal form after an XOR operation was applied to the DNA-encoded and key images.

In 2021, Xiaoping and Yongming [55], suggested multiple picture encryption that reduces the lowering of dimensionality by using 3D model scrambling and zigzag transformation. Following the collection of several photos into a 3D model cube, the final encrypted image is obtained by dynamic DNA operation. The third phase involves dealing with DNA dynamic coding utilizing a chaotic system.

In 2021, Qiuyu and Jitian [56] proposed dynamic DNA coding and 6-dimensional hyperchaotic depend on image hashing. Firstly, pre-processing uses image hashing to generate hash sequence which is used as initial value and control of a chaotic system, next image (R, G, B) is split into three channels and gathered into the two-dimension matrix the pixels change according to the chaotic system, lastly 6-dimensions hyperchaotic is implement to produce random sequence for dynamic coding DNA and arithmetic operations for an image.

In 2021, S. Patel et al. [57], proposed a customized Neural Network (NN) and RGB picture encryption based on DNA. Chaotic maps were used as the neuron transfer function in each of the three hidden layers, one input layer, and one output layer that comprised the NN model. The generator creates four chaotic sequences for use in cryptography. These sequences are used in color image encryption. Three crucial steps in the encryption process were pixel diffusion, pixel permutation, and DNA encoding.

In 2022, K Qian et al. [58] suggest a brand-new image encryption method that uses memory. At the bidirectional bit level of standard DNA diffusion, the chaotic system combines transformation and periodic dynamics. Initially, a distinct Memorabilia Chaos map is employed to produce chaotic sequences. The plain text picture is then bit-by-bit moved in accordance with the hash value and chaotic sequences. The shifted array is then put back together at the bit level. DNA coding rules that encode data dynamically.

In 2023, S. Geng et al. [59] According to the proposed research, The augmented Hilbert curve of DNA coding serves as the basis for image coding technology. First, the high and low frequency components of the plain text image are extracted using three-level discrete wavelet transform (DWT).Second, to mix the low-frequency components and the high-frequency components, several Hilbert curve modes are used.. Then, using the inverse discrete wave transform (IDWT), the high and low frequency components are rebuilt independently.

In 2023, Jianfeng, Shuying, and Litao [60] proposed encryption algorithm according to new dynamical system, zigzag transform, and DNA is used. Based on the enhanced zigzag transform, the simple image is shuffled into blocks, and the DNA is encoded using the processed chaotic sequences. Combining several photos at once increases conversion efficiency.

In 2024, Heping and Yiting [61] image encrypted using Quantum Chaos Maps and DNA encoding is commonly used, so it has been proposed technique of attack to defeat QCMDC-IEA, which allows it to negate domain substitution and control by obtaining the equivalent change key through differential analysis. It does complete decryption with minimal complexity by taking use of the internal security signaling pathway in QCMDC-IEA, better exposing its security mechanism. Creative suggestions to strengthen the security of analogous cryptographic systems in order to increase performance. The impact approach is practical and safe to apply on QCMDC-IEA, according to the findings of both theoretical analysis and experimental testing. As a result, this paper's cryptography analysis can take into account certain enhancement analysis to examine a class of image reading algorithms to encode chaos and information.

In 2024, V. M. V. Moorthi, M. R. Krishna, G. A. Kumar, V. Thanikaiselvan, S. Subashanthini, and R. Amirtharajan [62] proposed independent on the receiver side key in this paper. To improve the security of the delivered image, this method makes use of techniques like DNA encoding, chaotic dynamics, and key hiding mechanisms. Experimental testing of the suggested approach has produced results that support its efficacy.

In 2024, Basim [63] suggested model uses the idea of reduction is based on the idea of clustering, which is to collect sets of primary key values, whose contents are reduced and interrupted at each level of the binary tree built for the genetic rules of the key sequence. The split-and-conquer strategy and the DNA binary tree assembly technique are two distinct procedures used in the model that greatly narrow the solution space and search for the first letters of Linear Feedback Shift Registers (LFSRs) and Nonlinear Feedback Shift Registers (NLFSRs).

5. Comparative study

During the proposed studies on DNA algorithm and its use in image encryption, a number of criteria were used within the presented studies. Comparison tables will be made between the studies to verify the encryption method with respect according to current security analysis standards using Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI), information, Correlation Coefficients (CC), and entropy as shown in Table 4, Table 5 and Table 6. Finally, Table 7 shows the pros and cons of the papers in a comparative study on image encryption using different methods using DNA.

Table 4. A comparison of NPCR and UACI with references.

Ref.	NPCR	UACI
[42]	0.996	33.343
[43]	99.60	33.42
[51]	99.645	33.463
[52]	99.636	33.465
[53]	99.60	33.47
[54]	99.60	33.46
[55]	99.594	33.452
[56]	99.61	33.44
[57]	99.60	33.45
[58]	99.609	33.459
[59]	99.607	33.468
[60]	99.593	33.478

Table 5. A comparison of CC with references.

Ref.	Vertically	Horizontal	Diagonal
[42]	−0.07963	0.0166	0.0032
[43]	−0.07963	0.0166	0.0032
[45]	−0.0089	0.0021	0.0013
[47]	−0.0089	0.0021	0.0013
[13]	0.0039	−0.0314	0.0158
[48]	0.0032	0.0037	0.0032
[49]	0.0058	−0.0061	−0.0003
[51]	0.0058	−0.0061	−0.0003
[52]	0.0054	0.0085	0.0049
[53]	0.0110	0.0140	0.0350
[54]	0.0087	0.0042	−0.0031
[55]	0.0011	−0.0003	0.0013
[56]	0.0071	−0.0287	0.0007
[57]	0.0023	−0.0002	−0.0021
[58]	−0.0023	−0.0002	−0.0021
[59]	0.0021	0.0013	−0.0028
[60]	−0.0002	0.0003	−0.0008

Table 6. A comparison of information entropy with references.

Ref.	Lena
[42]	7.9895
[43]	7.9992
[45]	7.9978
[47]	7.9975
[13]	7.9972
[48]	7.9976
[49]	7.9968
[51]	7.9975
[52]	7.9975
[53]	7.9972
[54]	7.9975
[55]	7.9974
[56]	7.9998
[57]	7.9914
[58]	7.9994
[59]	7.9994
[60]	7.9987

5.1. Number of pixel change rate and unified average changing intensity evaluation

NPCR specifies the number of pixels whose values have changed in both images (original and encoded or decoded) by using Eq. (3) while UACI provides the mean variation in pixel intensity at the appropriate locations in each of the two pictures (pictures R and H). As a percentage of the maximum pixel density in the case of an 8-bit image and the maximum pixel density of 255 as in the Eq. (4). Table 4 display the NPCR and UACI analysis results for various encryption and decryption images [64].

$$\mathrm{NPCR}(\mathrm{R},\mathrm{H}) = \frac{\sum_{\mathrm{IJ}}^{\mathrm{M}*\mathrm{N}} \mathrm{D}(\mathrm{I},\mathrm{J})}{\mathrm{M}*\mathrm{N}} * 100\% \tag{3}$$

$$\mathrm{UACI} = \frac{\sum_{\mathrm{I,J}}^{\mathrm{M}*\mathrm{N}} |\mathrm{R}(\mathrm{I},\mathrm{J}) - \mathrm{H}(\mathrm{I},\mathrm{J})|}{\mathrm{M}*\mathrm{N}} * 100\% \tag{4}$$

where M and N represent the width and height of images, respectively.

Table 7. Comparing the pros and cons of image encryption in DNA.

Ref.	Pros.	Cons.
[42]	The four parameters r_i (i = 1, 2, 3, 4) that are dependent on the plain image, their technique can withstand known-plaintext and chosen-plaintext attacks. Even if the initial conditions are the same, these parameters yield different key streams for different plain images.	Every initial condition is extremely sensitive to the system.
[43]	The method has a large key space, high key sensitivity, and the capacity to resist statistical and exhaustive attacks, according to theoretical and actual results. It also improves ciphertext security.	Complex and time consuming.
[44]	Uses three DNA sequences in the proposed system to encrypt, embed the secret, and as an encryption key.	High rate of modification. It does not maintain the biological DNA's functionality.
[45]	The encryption technique consists of two stages, switching and propagation., large secret key-space and strong secret key sensitivity, which can effectively protect the security of the encrypted image	the use of chaos and encryption rules can provide a high level of security, but the extent of its resistance to attacks such as brute force and statistical analysis must be studied.
[46]	It does not change the information of organism's biological information, so it won't cause anomality, large storage capacity. The embedding of the data in the DNA does not enlarge its size. XOR and Pseudo Random Bit Generator are used to carry out the encryption process of the secret data. To correct errors Reed-Solomon (RS) code was used. Secret key is used. And the high probability of cracking.	Not easy to implement, high modification rate.
[47]	The results of the experiments and analyses show that the suggested method can withstand common attacks and has a strong sense of security.	The use of chaotic maps (PWLCM and DNA) encoding techniques can increase the computational complexity, leading to longer execution times.
[20]	Lowest time consumption, combined with DNA computing to improve two common block cipher criteria: confusion and diffusion in the Feistel mode.	The complexity of the system.
[13]	The large capacity to hide large plain letters and mask their frequencies, easy to implement by computers, and encrypt and decrypt using a reversible matrix. It can be used to encrypt images. The encryption matrix is the Hill-cipher key. The ciphertext cannot be recovered to plaintext if the inverse of the encryption matrix cannot be computed (irreversible). They use a hyper-chaotic sequence to generate an irreversible encryption matrix to reduce the correlation between matrices and increase the resistance of the ciphertext to attacks.	Statistical method is essential, but it insufficient to show that the algorithm has higher security.
[48]	In experimental simulations and comparisons, they proved proposed system security from four perspectives: exhaustive, statistical, differential, and noise attacks. The proposed approach has improved security, according to simulation findings and its outputs are more unpredictable.	Possesses more complicated trajectories.
[50]	New steganography method and hard to detect the hidden image.	Complicated, the shared secure lookup table between the sender and receiver.
[51]	Reduce the correlation that exists between neighboring pixels. They were able to withstand attacks, had a broad encryption key space, a high key sensitivity level, and excellent encryption results.	Complex system.

(*continued on next page*)

Table 7. Continued.

Ref.	Pros.	Cons.
[52]	The algorithm proposes hyper-clutter to show that the proposed algorithm is secure and reliable image encryption.	The increased computational complexity Using a 6D chaos system and bit-level DNA encoding may introduce significant requirements risks, which increases execution time and may affect performance in applications that require decryption.
[55]	Large encryption key space, high key sensitivity, novel encryption technique, and resilience to attacks.	Complex and time consuming.
[56]	Theoretical and practical results reveal that the technique increases encoding efficiency, improves security and strong robustness, and has a considerable key space and high key sensitivity, as well as the ability to withstand statistical and exhaustive form of attacks such as noise and cropping.	The complexity of the system leads to its inability to be implemented in devices with limited resources, such as smartphones or embedded devices, which limits the scope of use of the algorithm in practical applications.
[58]	It improves the cryptographic efficiency and ensures the security of the proposed cryptosystem again	It is sensitive to excessive complexity and may lead to unexpected vulnerability or fraying on complex systems.
[59]	good security performance. because this encryption algorithm provides against chosen brute-force attacks, plaintext attacks, differential attacks, statistical attacks, cropping attacks and noise attacks.	It increases computational complexity and consumes a lot of time.
[60]	Increase conversion efficiency by merging many photos at once, and fortify defense against different types of attacks. Based on visual analysis, the technique is thought to be secure and efficient for digital images.	Despite the security provided by the algorithm, if it is applied to a mobile phone, it needs further improvement.
[61]	The study identifies vulnerabilities inherent in the QCMDC-IEA method, which enhances security by structuring the encryption of document images for anarchy and personalization.	Although suggestions are made to improve security, the research does not provide concrete solutions or innovative applications to address the discovered flaws
[62]	Experience an algorithm with high entropy values (exceeding 7.995) and interaction agreement values of less than 1%) in the scientific, horizontal, and diagonal bases, indicating an algorithmic technology to achieve a robust and efficient reading experience.	Increased computational complexity
[63]	uses state-of-the-art methods that bring complexity and creativity to the realm of cryptanalysis, such as DNA binary tree clustering and hierarchical DNA clustering. Finding the starting values of LFSRs and NLFSRs may be simpler when the divide-and-conquer strategy and clustering are combined since they narrow down the solution space.	The C(2ˆn) complexity of the suggested method suggests that it demands significant computer resources, which may not be possible for all real-world applications.

5.2. Correlation coefficient

The CC is a statistical measure that describes the relationships between two variables. In most images with visible content, each pixel has a strong relationship with its neighbors in all, horizontal, vertical, and diagonal. The result of a good encryption model should be encrypted images without such correlations in the adjacent pixels. According to Eq. (5),

the CC of adjacent pixels is calculated [65, 66].

$$e(x) = {}^{1}/_{n}\Sigma_{i=1}^{n}xi \tag{5}$$

$$d(x) = {}^{1}/_{n}\Sigma_{i=1}^{n}(xi - e(x))^{2} \tag{6}$$

$$\text{Covariance}(x, y)\ {}^{1}/_{n}\Sigma_{i=1}^{n}(xi - e(x))(yi - e(y)) \tag{7}$$

$$CC_{xy} = \frac{\text{Covariance}(x, y)}{\sqrt{d(x) * d(y)}} \tag{8}$$

While are neighboring pixels of premier or encrypted images, e(x) represents mean value, d(x) represents deviation to the mean value, covariance (x, y) represents covariance between neighbor pixels and is the CC. The CC of pairs of neighboring pixels have been chosen randomly in horizontal, vertical, and diagonal locations to check for correlation between the encrypted and original images, and their coefficients of correlation are determined by calculating using Eq. (8). As shown Table 5.

5.3. Evaluation of entropy

The amount of randomness in the information contained is measured by the information entropy. The entropy of an image determines whether it is a random image with random pixel values. The term entropy refers to the amount of information that can be stored, as shown in the (Eq. (9)) [67].

$$E = -\Sigma_{g=0}^{n}P(g)\log_{2}(P(g)) \tag{9}$$

The g is present the probability of pixel value $P(g)$, and n the number of pixel values (0–256) for the gray level image 2^8. Since there is a correlation in the original plain image and pixel values are rarely random, the value of the entropy is usually less than 8. When all pixel values are distributed randomly, entropy reaches its maximal ideal value, which is 8. According to the findings, the encrypted images' the entropy is really near to the ideal value of 8

Table 7 included a comparative of several studies that deal with bioinformatics in different ways, showing the results of each, its strengths and weaknesses, and how to deal with them.

6. Conclusions

In this paper, a study to help researchers is presented to be aware of the limitations of cryptography The systems, therefore, inspire future progress in this field. As the demand for storage grows, there is a huge desire for new and changing ways for storing enormous volumes of data. DNA has recently been recognized as a useful data carrier with the added advantage of reliable data. Steganography and cryptography are using DNA's biomolecular computing capabilities and steganography. Bioinformatics have been used in many ways to make security higher, it can be concluded that DNA information has been used to increase the complexity of the systems. Some of the researchers employ DNA to increase the confusion while others focused on diffusion, a little group of them had employed both disciplines. Other researchers suffer from slowness in processing. Many good results have been obtained. Randomness was the goal of some research. In future, it can be increased the secrecy of the system using artificial intelligence techniques or it can be

used the irreducible polynomials to have an ideal algorithm for encryption to be resistant to different attacks.

Acknowledgment

The authors wish like to thank the Department of Computer Science, University of Technology—Iraq, for helping in the completion of this study.

Authors' contributions

The authors' contributions are as follows: Rana M. Zaki: conceptualization, methodology, analysis, and writing. Zaed S. Mahdi: draft manuscript preparation and writing. Matheel E. Abdulmunim and Abdullah Husin: review and editing.

Conflicts of interest

The authors declare that they do not have any conflicts of interest.

Data availability

No dataset has been used in this study.

References

1. G. Singh and Supriya "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33–38, April 2013, doi: 10.5120/11507-7224.
2. M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13-14, pp. 95–113, Nov. 2014, doi: 10.1016/j.cosrev.2014.09.001.
3. G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba, "Comparative study for various DNA based steganography techniques with the essential conclusions about the future research," in *Proc. IEEE 2016 11th Int. Conf. on Computer Engineering & Systems (ICCES)*, Cairo, Egypt, pp. 220–225, doi: 10.1109/ICCES.2016.7822003.
4. H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *The European Physical Journal Plus*, vol. 133, no. 1, Jan. 2018, Art. no. 6, doi: 10.1140/epjp/i2018-11834-2.
5. Z. S. Mahdi, R. M. Zaki, and L. Alzubaidi, "Advanced hybrid techniques for cyberattack detection and defense in IoT networks," *Security and Privacy*, pp. 1–19, Oct. 2024, doi: 10.1002/spy2.471.
6. A. K. Jabbar, A. T. Hashim, and Q. F. Al-Doori, "Secured medical image hashing based on frequency domain with chaotic map," *Engineering and Technology Journal*, vol. 39, no. 5, pp. 711–722, May 2021, doi: 10.30684/etj.v39i5A.1786.
7. A. S. Hamad and A. K. Farhan, "Image encryption algorithm based on substitution principle and shuffling scheme," *Engineering and Technology Journal*, vol. 38, no. 3, pp. 98–103, Dec. 2020, doi: 10.30684/etj.v38i3B.433.
8. M. T. Parvez and S. Alsuhibany "Segmentation-validation based handwritten Arabic CAPTCHA generation," *Computer & Security*, vol. 95, Aug. 2020, Art. no. p. 101829, doi: 10.1016/j.cose.2020.101829.
9. B. Anam, K. Sakib, A. Hossain, and K. Dahal, "Review on the advancements of DNA cryptography," 2010, *arXiv:1010.0186v1*.
10. S. Hamad, A. Elhadad, and A. Khalifa, "DNA watermarking using Codon Postfix technique," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1605–1610, Sep. 2018, Art. no. 8047268, doi: 10.1109/TCBB.2017.2754496.
11. S. H. Mnkash and M. E. Abdulmunem, "A review of software watermarking," *Iraqi Journal of Science*, vol. 61, no. 10, pp. 2740–2750, Oct. 2020, doi: 10.24996/ijs.2020.61.10.30.

12. R. M. Hassan and M. E. Abdulmuim, "Using Rubik's cube in fragile audio watermark encryption," *Diyala Journal for Pure Sciences*, vol. 15, no. 3, pp. 103–124, July 2019, doi: 10.24237/djps.15.03.490B.
13. X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic DNA encoding," *IEEE Photonics Journal*, vol. 10, no. 4, Aug. 2018, Art. no. 3901014, doi: 10.1109/JPHOT.2018.2859257.
14. K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *Journal of Electronic Imaging*, vol. 26, no. 1, Feb. 2017, Art. no. 013021, doi: 10.1117/1.JEI.26.1.013021.
15. R. A. Hussain, M. E. Abdulmunem, and A. M. J. Abdul-Hossen, "Propose Image Encryption Watermarking Algorithm Based on Frequency and Geometric Transform," in *Proc. IEEE 2019 2nd Scientific Conf. of Computer Sciences (SCCS)*, Baghdad, Iraq, pp. 143–147, doi: 10.1109/SCCS.2019.8852591.
16. N. A. Shaik, K. R. Hakeem, B. Banaganapalli, and R. Elango, *Essentials of Bioinformatics*, *Volume I*. Springer Cham, 2019.
17. H. B. AbdulWahab and T. M. Abed, "Anti-phishing based on visual cryptography and 4D hyperchaotic system," *Iraqi Journal of Information Technology*, vol. 9, no. 1, pp. 1–27, 2018.
18. C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018, doi: 10.1109/ACCESS.2018.2883690.
19. S. I. Batool and H. M. Waseem, "A novel image encryption scheme based on Arnold scrambling and Lucas series," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27611–27637, Oct. 2019, doi: 10.1007/s11042-019-07881-x.
20. Z. M. Saadi and E. Matheel, "*Image Encryption Using DNA Addition*," M.Sc. thesis, Baghdad, Iraq: Department of Computer Science, University of Technology - Iraq, 2017.
21. R. Premkumar and S. Anand, "Secured and compound 3-D chaos image encryption using hybrid mutation and crossover operator," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 9577–9593, April 2019, doi: 10.1007/s11042-018-6534-z.
22. A. T. Sadiq and H. S. Abdullah, "HDNA: Heuristic DNA computing algorithm,"*Eng. & Tech. Journal*, vol. 27, no. 6, pp. 1063–1073, 2009, doi: 10.30684/etj.27.6.4.
23. Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Optics and Lasers in Engineering*, vol. 134, Nov. 2020, Art. no. 106202, doi: 10.1016/j.optlaseng.2020.106202.
24. H. M. Al-Mashhadi and I. Q. Abduljaleel, "Color image encryption using chaotic maps, triangular scrambling, with DNA sequences," in *Proc. IEEE 2017 Int. Conf. on Current Research in Computer Science and Information Technology (ICCIT)*, Sulaymaniyah, Iraq, pp. 93–98, doi: 10.1109/CRCSIT.2017.7965540.
25. K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, Feb. 2020, Art. no. 115670, doi: 0.1016/j.image.2019.115670.
26. V. Rathore and A. K. Pal, "An image encryption scheme in bit plane content using Henon map based generated edge map," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 22275–22300, Mar. 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 Journal*, vol. 10, no. 3, pp. 1429–1434, Aug. 2021, doi: 10.18421/TEM103-54.
28. 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, Nov. 2021, Art. no. e0260014, doi: 10.1371/journal.pone.0260014.
29. X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Optics and Lasers in Engineering*, vol. 137, Feb. 2021, Art. no. 106393, doi: 10.1016/j.optlaseng.2020.106393.
30. S. Namasudra, R. Chakraborty, A. Majumder, and N. R. Moparthi, "Securing multimedia by using DNA-based encryption in the cloud computing environment," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 16, no. 3s, Dec. 2020, Art. no. 99, doi: 10.1145/33926.
31. M. Dua, A. Wesanekar, V. Gupta, M. Bhola, and S. Dua, "Differential evolution optimization of intertwining logistic map-DNA based image encryption technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 9, pp. 3771–3786, Nov. 2019, doi: 10.1007/s12652-019-01580-z.
32. H. Wu, H. Zhu, and G. Ye, "Public key image encryption algorithm based on pixel information and random number insertion," *Physica Scripta*, vol. 96, no. 10, Oct. 2021, Art. no. 105202, doi: 10.1088/1402-4896/ac0bcf.
33. X. Zhang and R. Ye, "A novel RGB image encryption algorithm based on DNA sequences and chaos," *Multimedia Tools and Applications*, vol. 80, no. 6, pp. 8809–8833, Nov. 2021, doi: 10.1007/s11042-020-09465-6.
34. A. T. Hashim and Z. M. Radeef, "Multiple image secret sharing based on linear system," *Indian Journal of Science and Technology*, vol. 10, no. 33, pp. 1–17, 2017, doi: 10.17485/ijst/2017/v10i33/113085.

35. R. Abdulrida, M. E. A-Monem, and A. M. Jaber, "Quantum image watermarking based on wavelet and geometric transformation," *Iraqi Journal of Science*, vol. 61, no. 1, pp. 153–163, 2020, doi: 10.24996/ijs.2020.61.1.16.
36. S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy (Basel)*, vol. 20, no. 9, Sep. 2018, Art. no. 716, doi: 10.3390/e20090716.
37. Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7111–7130, May 2018, doi: 10.1007/s00521-018-3541-y.
38. R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, May 2014, doi: 10.1016/j.optlaseng.2013.12.003.
39. C. Li, G. Luo, and C. Li, "An image encryption scheme based on the three-dimensional chaotic logistic map," *International Journal of Network Security*, vol. 21, no. 1, pp. 22–29, 2019, doi: 10.6633/IJNS.201901_21(1).04.
40. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006, doi: 10.1142/S0218127406015970.
41. N. M. Abbas and M. E. Abdulmunim, "mRNA approach image encryption using LUC algorithm," *Iraqi Journal of Science*, vol. 64, no. 5, pp. 2545–2560, May 2023, doi: 10.24996/ijs.2023.64.5.37.
42. X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and DNA sequence," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 57–70, Dec. 2012, doi: 10.1007/s11042-012-1331-6.
43. R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016, doi: 10.1007/s11071-015-2392-7.
44. E. I. Abd El-Latif and M. I. Moussa, "Chaotic Information-hiding algorithm based on DNA," *International Journal of Computer Applications*, vol. 122, no. 10, pp. 38–42, July 2015.
45. A. Y. Niyat, R. M. H. Hei, and M. V. Jahan, "Chaos-based image encryption using a hybrid cellular automata and a DNA sequence," in *Proc. IEEE 2015 Int. Congr. on Technology, Communication and Knowledge (ICTCK)*, Mashhad, Iran, pp. 247–252, doi: 10.1109/ICTCK.2015.7582678.
46. K. Santoso, S.-H. Lee, W.-J. Hwang, and K.-R. Kwon, "Sector-based DNA information hiding method," *Security and Communication Networks*, vol. 9, no. 17, pp. 4210–4226, Sep. 2016, doi: 10.1002/sec.1599.
47. X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, Feb. 2016, doi: 10.1007/s11042-016-3311-8.
48. J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018, doi: 10.1016/j.sigpro.2018.06.008.
49. A. U. 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*, vol. 159, pp. 348–367, April 2018, doi: 10.1016/j.ijleo.2018.01.064.
50. A. Kadhim and R. S. Ali, "Hidden encrypted text based on secrete map equation and bioinformatics techniques," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 1, pp. 34–47, Jan. 2019.
51. X. Wang and L. Liu, "Image encryption based on hash table scrambling and DNA substitution," *IEEE Access*, vol. 8, pp. 68533–68547, 2020, doi: 10.1109/ACCESS.2020.2986831.
52. T. Wang and M.-H. Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Optics & Laser Technology*, vol. 132, Dec. 2020, Art. no. 106355, doi: 10.1016/j.optlastec.2020.106355.
53. S. Zhou, P. He, and N. Kasabov, "A dynamic DNA color image encryption method based on SHA-512," *Entopy*, vol. 22, no. 10, Sep. 2020, Art. no. 1091, doi: 10.3390/e22101091.
54. 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.
55. X. Zhang and Y. Hu, "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding," *Optics & Laser Technology*, vol. 141, Sep. 2021, Art. no. 107073, doi: 10.1016/j.optlastec.2021.107073.
56. Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13841–13864, Jan. 2021, doi: 10.1007/s11042-020-10437-z.
57. 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 Computing and Applications*, vol. 33, no. 21, pp. 14533–14550, May 2021, doi: 10.1007/s00521-021-06096-2.

58. K. Qian, W. Feng, Z. Qin, J. Zhang, X. Luo, and Z. Zhu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Front. Phys.*, vol. 10, Aug. 2022, Art. no. 10:963795, doi: 10.3389/fphy.2022.963795.
59. S. Geng, J. Li, X. Zhang, and Y. Wang, "An image encryption algorithm based on improved Hilbert curve scrambling and dynamic DNA coding," *Entropy*, vol. 25, no. 8, Aug. 2023, Art. no. 1178, doi: 10.3390/e25081178.
60. J. Zhao, S. Wang, and L. Zhang, "Block image encryption algorithm based on novel chaos and DNA encoding," *Information*, vol. 14, no. 3, Feb. 2023, Art. no. 150, doi: 0.3390/info14030150.
61. H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Systems with Applications*, vol. 237, Mar. 2024, Art. no. 121514, doi: 10.1016/j.eswa.2023.121514.
62. V. M. V. Moorthi, M. R. Krishna, G. A. Kumar, V. Thanikaiselvan, S. Subashanthini, and R. Amirtharajan, "Key-independent image encryption using dna encoding and chaotic dynamics," in *Proc. IEEE 2024 10th Int. Conf. on Communication and Signal Processing (ICCSP)*, Melmaruvathur, India, pp. 964–969, doi: 10.1109/ICCSP60870.2024.10544118.
63. S. Yaseen, "Constructing hierarchical DNA clustering model (HDCM) to cryptanalyze feedback shift register-based stream cipher," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1–8, 2024.
64. P. Kiran and B. D. Parameshachari, "Logistic sine map (LSM) based partial image encryption," in *Proc. IEEE 2021 National Computing Colleges Conference (NCCC)*, Taif, Saudi Arabia, pp. 1–6, doi: 10.1109/NCCC49330.2021.9428854.
65. E. Ashraf, N. F. F. Areed, A. Takieldeen, and M. Abdelazeem, "Novel cryptographic algorithm for 4G/LTE-A," *International Journal of Computer Applications*, vol. 163, no. 1, pp. 5–9, April 2017.
66. G. Hanchinamani and L. Kulakarni, "Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform," *International Journal of Hybrid Information Technology*, vol. 7, no. 4, pp. 185–200, 2014, doi: 10.14257/ijhit.2014.7.4.16.
67. R. M. Zaki and H. A. Wahab, "A novel of substitution-box design using PLL algorithms in magic cube," *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 4, pp. 674–684, 2021, doi: 10.21533/pen.v9i4.2402.