Journal of Techniques, ISSN: 2708-8383, Vol. 5, No. 3, 2023, Pages 116-128
DOI: https://doi.org/10.51173/jt.v5i3.1134

JOURNAL OF TECHNIQUES

Journal homepage*: http://journal.mtu.edu.iq*

REVIEW ARTICLE - ENGINEERING

Medical Image Encryption and Decryption Based on DNA: A Survey

Saja Theab Ahmed[1*], Dalal Abdulmohsin Hammood[1], Raad Farhood Chisab[2], Nurulisma Binti Hj. Ismail[3]

[1] Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq

[2] Technical Institute / Kut, Middle Technical University, Baghdad, Iraq

[3] Faculty of Electronic Engineering & Technology (FKTEN), Universiti Malaysia Perlis (UniMAP) 02600 Arau, Perlis, Malaysia

[*] Corresponding author E-mail: bbc0070@mtu.edu.iq

Article Info.

Article history:

Received
20 December 2022

Accepted
12 April 2023

Publishing
30 September 2023

Abstract

In the medical field, advanced techniques such as e-health, intelligent health, and telemedicine apps are being deployed. These approaches use open-source networks to send digital medical images. Patients' private and sensitive diagnosis is contained in the digital medical image. Then sent the digital medical images are used for diagnosis by the remote center. For this reason, protecting patient privacy and the integrity of medical images is of paramount importance. DNA Digital coding is the most popular form of cryptographic technology, and it is frequently employed to strengthen information security, and the most prevalent constraints of DNA cryptographic schemes feature a high degree of temporal and algor. If DNA is employed appropriately, it can be used to achieve a number of security technologies, including encryption, steganography, signature, and authentication through the use of DNA molecules as information carriers. In this paper, a survey on the digital medical image was done. This survey contains the methods of encryption, and decryption of the image which is based on DNA with all the related methods and makes the comparison between the previous papers and explain which is the best to use.

Publisher: Middle Technical University

Keywords: DNA Cryptography; Digital Medical Image; Encryption; Decryption.

1. Introduction

"Cryptography" is the study and analysis of encrypted data or the processing of confidential information, by applying logical and mathematical information security concepts. It is a form of information technology that is used in banking, and health care systems, transport and communication, and various other IoT applications. The importance of cryptography has increased along with security considerations. Symmetric encryption claims to offer a cost-effective information protection approach without compromising security nonetheless, sharing the secret key between encrypting and decrypting processes is essential. Compared to symmetric encryption, the problem of sharing encryption keys is circumvented by using asymmetric encryption, meanwhile, the self-contained method is slower and requires more computational [1]. Substitution, transposition, the hill cipher, the Play fair cipher, Vigener, and other ciphers are examples of symmetric keys [2]. The term "asymmetric key" describes a system in which two different keys, one private and one public, are used for encryption and decryption [3,4]. Each system is designed with its own strengths in cryptography. The main purpose of cryptographic encryption is to protect private information from being tampered with [5]. To provide secure communication, the data must be encoded in such a way that if a hacker manages to steal an encrypted file, they will still be unable to read the contents of the file because they lack the key to decrypt the message. Cryptanalysis is the process of deciphering encrypted or hidden data without knowing how it has been converted from plain data to cipher data. Encryption is the process by which unencrypted data is transformed into encrypted data, while decryption refers to the reverse process, where encrypted data is converted back into plain text. Confidentiality, integrity, non-repudiation, and information authentication are the four main goals of cryptography. Cryptosystems are the information security controls and regulations that achieve some or all of the goals [5]. The block diagrams for symmetric and asymmetric keys in cryptography are shown below in Fig. 1 and 2, respectively.

Color coding is one of the most common ways to show scaled values in visualizations, it is frequently utilized in a wide range of application settings, it is a method for converting data sets to colors; it works like this: f: D→C, where D stands for numbers and C for color scale [6,5]. In order to create a digital image, an analog one is. Therefore, it represents a finite-sample analog image. Pixels are the fundamental units or cells which comprise an image. A two-dimensional array or series of pixels in two dimensions is what makes up a digital image. As a result, a collection of pixels which are organized in a meaningful pattern can represent an image. Binary images, grayscale images, and color images make up a representation of a digital image. A binary image is sometimes known as a 1-bit image since each pixel in it is represented by only one binary number. The pixels only have a limited set of values available to them [7]. The practice of applying algorithms to digital images is known as "digital image processing"[8]. Today, several vital sectors rely on the free flow of image data, including e-commerce, the armed

Nomenclature & Symbols

DNA	Deoxyribose Nucleic Acid	AI	Artificial Intelligence
NPCR	Number of Pixels Change Rate	DL	Deep Learning
UACI	Unified Averaged Changing Intensity	ML	Machine Learning
PSNR	Peak Signal -to-Noise Ratio		

forces, medical, education, aerospace, and many more [9]. The fundamental functions of encryption can be broken down into two categories. securing data storage and sending private data through networks, respectively [10]. Because of the features and importance of digital images, as well as to avoid attacks from unauthorized people/companies/systems, etc., many various preventive approaches and techniques have been created to ensure that data transmitted via networks is secure and enduring, as well as to store data in secret [11]. The aim of this paper is to provide a high-level overview of DNA as an image encryption approach and its relevant aspects.

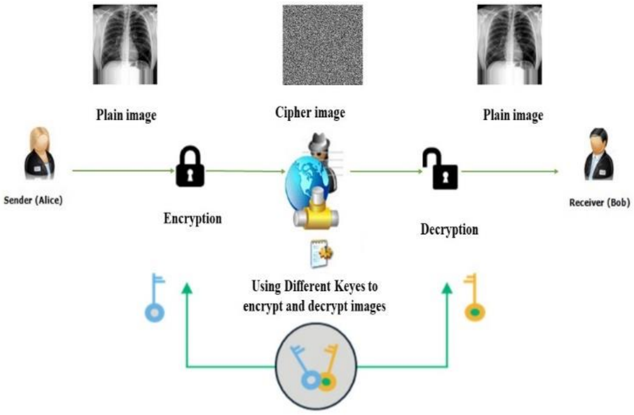

Fig. 1. Asymmetric key cryptography

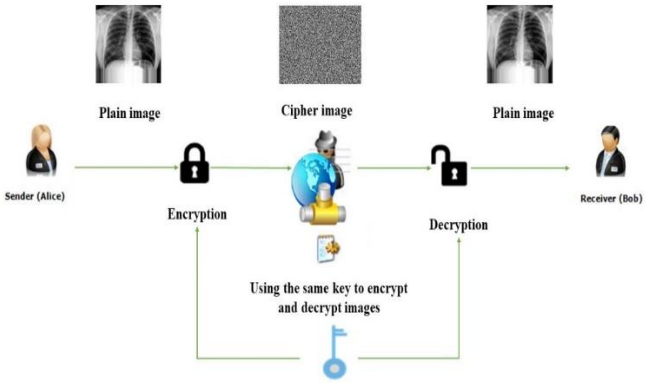

Fig. 2. Symmetric key cryptography

2. Image Encryption Techniques

Currently, data security has become a critical issue due to increase a need for digital transmission and large losses owing to improper access. Encryption is used to solve these problems and safeguard information while restricting access only to authorized parties. The traditional methods of encrypting data are only successful when applied to textual information, and the methods that are used to encrypt video streams and photos both have some flaws, several different methods of image encryption [12]. In Fig. 3 see a Taxonomy of Image Cryptographic Techniques. DNA research has received considerable interest from the scientific community in recent years. The primary focus of this review paper is on DNA cryptography, which covers everything from the algorithms that are currently in use to the numerous parameters that are necessary to evaluate the performance of the suggested algorithm, such as the following: correlation, entropy, Peak Signal-to-Noise Ratio, (PSNR), Unified Averaged changing Intensity (UACI) and finally the Number of Pixels Change Rate (NPCR).

3. Encryption Based on The Sequence Of DNA

The emergence of artificial intelligence (AI) has altered the modern healthcare system, smart communication networks, and (IoT)-based technologies [13]. In the e-healthcare system, Artificial intelligence and Big Data analysis are increasingly being used for remotely consultation, surveillance, and diagnosis [14]. "Deep medicine," is the application of AI in healthcare which includes Deep learning, often known as (DL), and machine learning (ML) applied to automatic image categorization, analysis, and segmentation based on a variety of approaches [15,16]. Customized medication is another application of AI models, medication discovery, and the coordination of treatment plans. Intelligent medical devices improved healthcare service quality while simultaneously reducing transmission time [17]. As a result of advancements in technology, digital images are increasingly being put to use in a wide variety of applications, including diagnostic imaging, environment monitoring, and private conferencing [18]. In some cases, the content of these images may be private and/or sensitive [19]. These images are exposed to dangers like modification and unauthorized access when transmitted over public networks [18]. The disclosure of private data may give rise to concerns about medical information military readiness, national security, and discretion. Additionally, individuals must ensure their privacy when exchanging images over a public network [18]. Consequently, images need to be protected against various security attacks [20]. It has been learned through published works that these images can be encrypted using standard procedures [18]. Telediagnosis and telesurgery are only two examples of how the convergence of IT and healthcare has increased the prevalence of digital medical images. DNA is used as a data carrier. The term "DNA cryptography" refers to a relatively recent technique that combines the protection of sensitive information with biological data[19]. DNA computing has been used in recent researches to meet the demand for sufficient and reliable data confidentiality [21]. DNA is an abbreviation for Deoxyribose Nucleic Acid, Adleman first introduced DNA computing in 1994, solving the Hamilton path problems, He also claims that DNA computing can solve a variety of other challenging issues, such as non-computable (NP, NP-COMPLETE, and SAT) problems. Adleman also claims that DNA is extremely parallel and has an exceptional information density[22,23]. DNA was used as a carrier for information, and modern biological technology was used as a method for its execution[18]. All living creatures are represented in the molecule DNA[18]. DNA is responsible for the transmission of the genetic information that is essential for the growth, development, and proper functioning of all lifeforms, from the tiniest viruses to the most complex people[18]. Instead of using electronic chips, DNA computing uses molecular biology, technology, and biochemistry[21].The DNA molecule stores genetic information in the form of code. DNA is made up of two long strands that are twisted on each other, These two strands are linked together by units known as nucleotides, giving DNA the structure of a helix ladder[24].which is made up of four chemical components[25]. In DNA computing, the four nitrogen bases (Adenine, Guanine, Cytosine, and Thymine) are used to represent data in the same way that the human genetic code uses them[26]. These two strands are joined together by nucleotide pairs. This connection is not formed randomly. Double hydrogen bonds always exist between A and T, while triple hydrogen bonds always exist between C and G[24]. Fig. 4 explains the DNA structure [27].

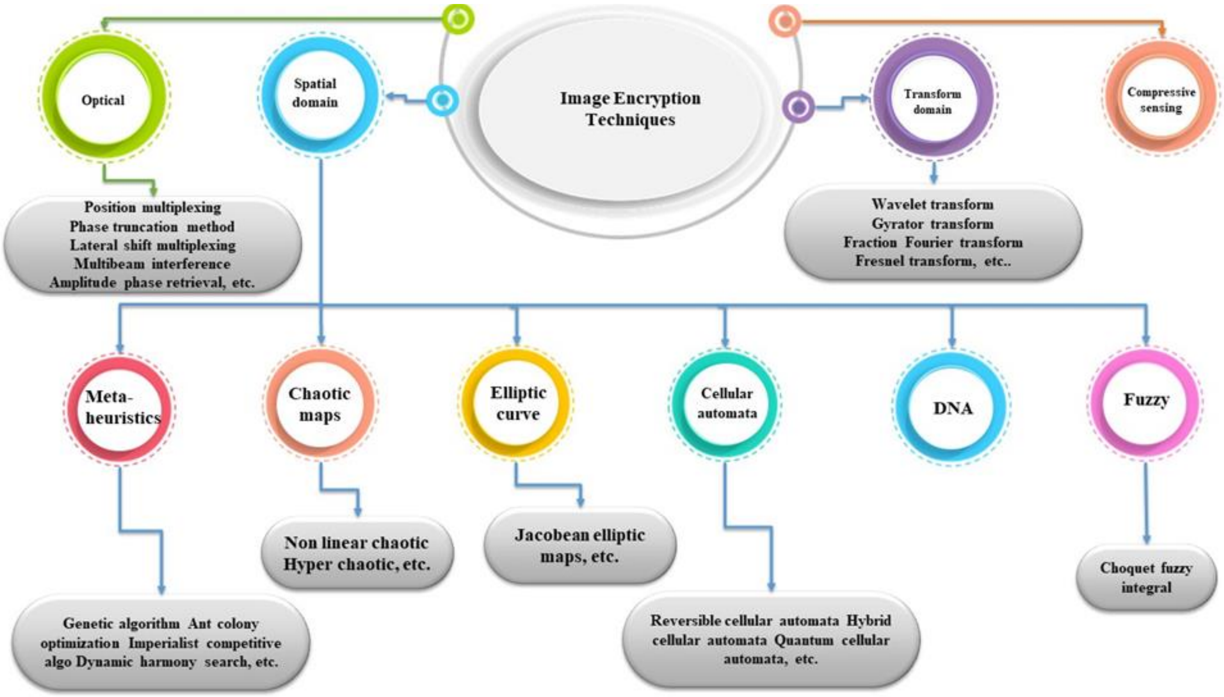
Image Encryption Techniques
Optical
Spatial domain
Transform domain
Compressive sensing
Position multiplexing
Phase truncation method
Lateral shift multiplexing
Multibeam interference
Amplitude phase retrieval, etc.
Wavelet transform
Gyrator transform
Fraction Fourier transform
Fresnel transform, etc..
Meta-heuristics
Chaotic maps
Elliptic curve
Cellular automata
DNA
Fuzzy
Non linear chaotic
Hyper chaotic, etc.
Jacobean elliptic maps, etc.
Choquet fuzzy integral
Genetic algorithm Ant colony optimization Imperialist competitive algo Dynamic harmony search, etc.
Reversible cellular automata Hybrid cellular automata Quantum cellular automata, etc.

Fig. 3. Classification of image encryption techniques

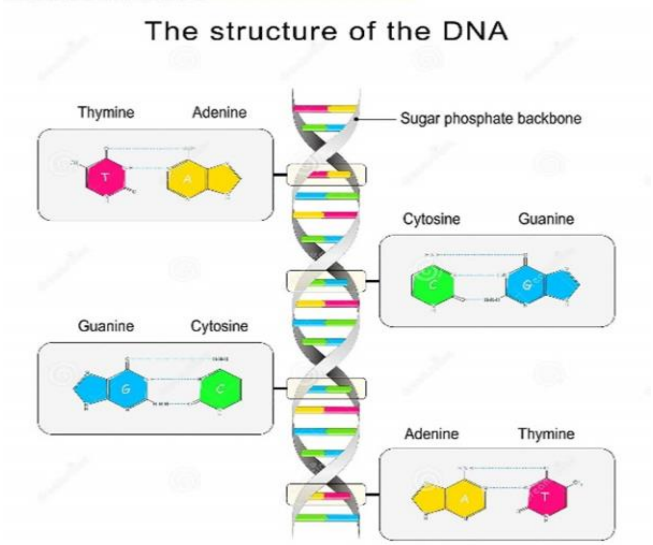

Fig. 4. DNA Structure[27]

It won't get into more details about the biological information of DNA but instead, we commit to the essential required information for DNA encryption. Exactly just as DNA transmits information from one generation to the next generation, DNA coding is used to transfer and hide information, and as such, it is used in the security of information storage and encryption. Table 1 shows the formula for converting binary code to DNA nucleotides and its complement. By mapping the binary forms to the four DNA nucleotides we deduce that we have four factorial combinations that is 24 types of coding rules. Also, keep in mind that A and T, as well as C and G, are complementary pairs.

Table 1. DNA nucleotides, their complements, and their binary values

DNA Nucleotides	Decimal Value	Binary Value	Complement
A	0	00	T
T	1	01	A
C	2	10	G
G	3	11	C

For this reason, the only rules that satisfy the complementary rule of Watson's Crick rules are only eight. This was found by Watson's Crick and named Watson's Crick complement rule[28]. Finally, as can be seen in Table 2, there are only eight rules that govern DNA coding. It is important to remember that the same rule that was applied during encryption must be applied during decryption.

Table 2. The Rules for DNA Coding

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

3.1. DNA operations

DNA molecules may undergo a wide variety of biological operations that will aid in the solution of mathematical and computational problems[29]. Fig. 5 explains the DNA Operations [30]. Here are just a few of the many mathematical and logical manipulations that can be applied to DNA:

3.1.1. Arithmetical operations

DNA nucleotides are amenable to the elementary arithmetic operations of addition and subtraction[31]. The following section will go into additional detail regarding these topics.

- Addition: DNA nucleotide addition works in the same way as any other binary addition. The result of adding the binary digits 10 and 11 is 01, for instance. Let's pretend for a moment that the digits 00, 01, 10, and 11 correspond to the DNA bases A, T, C, and G. For this reason, it's possible to discover that the sum of C and G is T. Table 3 shows the DNA addition.
- Subtraction: DNA nucleotide subtraction works the same way as any other binary subtraction. For instance, if 01 is subtracted from 11, we get 10. Imagine that the four DNA bases (A, T, C, and G) are represented by the binary digits 00, 01, 10, and 11. Then, by taking T away from G, we get C. Table 4 shows the DNA subtraction.

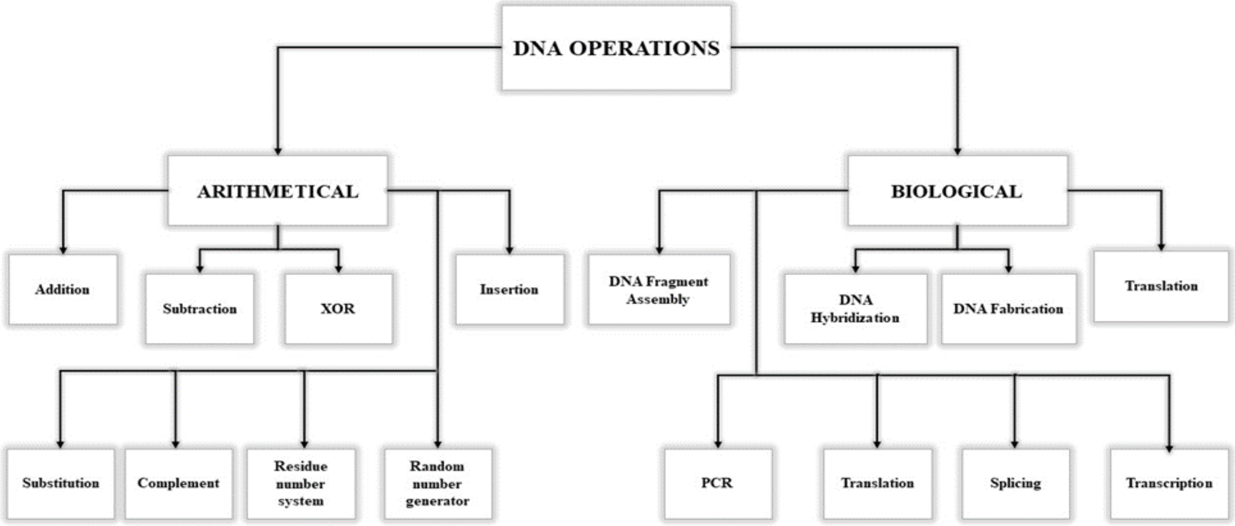

Fig. 5. DNA Operations[30]

3.1.2. Logical operations

The logical operations NOT, OR, AND, XOR, NOR, NAND, and XNOR can be applied to Nucleotides.

- The NOT Operation: it is used to switch the order of bases in a DNA strand. Inversion, also known as negation, is one of the simplest logic operations that can be performed on DNA. OR Operation: If at least one of the provided inputs is true, the result of an OR operation is true. Any single-stranded sequence can be terminated by DNA, but if a double-stranded sequence is found, the result will be false.
- OR Operation: If at least one of the provided inputs is true, the result of an OR operation is true. Any single-stranded sequence can be terminated by DNA; however, the result will be erroneous if a double-stranded sequence is discovered.
- AND Operation: If both inputs are true, the AND operation would form a true result. Whenever there is a sequence of single-stranded molecules in the mix, DNA will always terminate it. Additionally, the result will be true or false depending on whether or not a double-stranded sequence was found.
- XOR Operation: The XOR operation yields true t only if at least one of the sequence's inputs is true. The binary equation for XOR is true if and only if the input values are diametrically opposed to one another. Since the XOR logical operation can be performed with any given base sequence, it provides the simplest solution. An example of this is the formation of a double-stranded sequence from two

"complementary" input sequences. Once the inputs are no longer at odds with one another, the sequences will no longer bind to one another, and DNA will be able to terminate both input sequences. Table 5 shows the DNA XOR.

- XNOR Operation: By applying NOT to the output of the XOR operation, we get the XNOR operation, which checks to see if its two inputs are the same before returning a result. It follows that if there is a double stranded sequence, the outcome of this operation is true, but if there isn't one, it is false, just like the other logical operations.
- NAND Operation: To produce a true output if the inputs (two or more inputs) are false, the NAND operation is used. The base sequence for this operation is the sequence that represents the actual value rather than the false value, making it identical to the OR operation as shown above. Before a double stranded sequence may occur, one of the inputs must be false. If the DNA detects a double-stranded sequence, the combination is correct; if not, it is incorrect.
- NOR Operation: The NOR operation returns true if and only if both inputs are false. The NOT operation is used to accomplish this operation on the OR logical operation's output.

The DNA computation technique can be divided into three stages[29]:

- Information encoding in the DNA sequence.
- Computation (molecular operation).
- Solution extraction.

Table 3. DNA add-on operation

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

Table 4. Subtraction of DNA

-	C	T	A	G
C	C	G	A	T
T	T	C	G	A
A	A	T	C	G
G	G	T	T	C

Table 5. DNA XOR

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

3.2. DNA cryptographic techniques

Fundamental methods for DNA encryption include digital coding of DNA and PCR amplification. numerous researchers have made use of these techniques, while other encryption algorithms are also used for encryption activities.

- The Digital Coding of DNA
- PCR-B: Polymerase Chain Reaction (PCR)
- DNA-based random one-time pads (OTPs)
- DNA Chip Based
- DNA Steganography
- DNA Fragmentation

The DNA encryption fundamental techniques are briefly described in the section below.

3.2.1. The digital coding of DNA

It's a way of associating numerical values of 0 and 1 with DNA's four individual bases (A, C, T, and G) [31]. This technique makes it simple to encrypt plain text messages. There are 24 such patterns that can exist, but only 8 distinct combinations that correspond to the complementing criteria are taken into consideration. The next example will make this clear. Let's say someone wishes to use DNA encoding to communicate the number 46. To begin, we'll turn 46 into binary. By converting the binary digits 4 and 6 to the four-bit forms 0100 and 0110, respectively. The binary representations of 4 and 6 are then combined. The outcome will be the binary number 01000110. Two successive binary digits are taken starting from the leftmost bit and translated to corresponding DNA nucleotide bases according to the plan shown in Table 1. Finally, the number "46" will be encoded as "TATG" in this manner. Once the channel is established, the encrypted message "CTTG" will be delivered to the intended recipient. After that, the receiver decodes it to obtain the original message.

3.2.2. PCR-B: polymerase chain reaction (PCR)

PCR is a DNA amplification and quantification technique [32]. Here, two primers have DNA sequences written into them. Primers are tiny DNA units. The two primer combinations can be used as the master key for the PCR amplification process. For the purpose of encoding the original data into a new sequence, the original information can be safely positioned between the two primers. If the PCR primers are not known, it is highly challenging to amplify the resulting message. Primer accuracy is crucial in this process because different length primers will provide different results. Operations for biological PCR are Denaturation, Primer Annealing and Primer Extension.

4. Literature Review

Because communication through open networks is becoming increasingly common, it is critical to transmit data in a secure and disguised manner using various methods [10]. Due to the rapid growth of Internet technology, multimedia communication techniques have emerged as dominating modes of communication [33]. When compared to text files, images can carry more and intuitive information, allowing individuals to access useful information more conveniently. Image to image encryption introduced in [34] to enhance key space, the suggested algorithm segments the color picture into the primary, secondary, and tertiary RGB channels, image hashing is used in the suggested approach Standard 512x512 color photos of Lena, peppers, a baboon, an airplane, and a sailboat are subjected to image permutation and diffusion processing. The resulting images are robust enough to withstand a brute-force attack.

The author in [35] applied two image styles, greyscale and RGB images with different sizes on the proposed S-box bent with DNA approach to maintain security, where the proposed S-Box is the proposed S-Box being a scalar function which substitutes a byte with the byte that corresponds to it. A positive number up to 255 of GF (28) is the non-linearity of the proposed one to overcome the hiatus. The study in [36] tries to connect the keystream to the simple image by introducing SHA-256 algorithm to the system of cryptography. Plain image is sent through SHA-256, which generates a value K of the 256-bit hash function that is progressively grouped into 32 different sections and each block consist of 8 bits equivalent to a decimal value between 0 and 255. Regardless of the two crucial phases, confusion and diffusion of the traditional methods of encryption, [37] utilizes DNA by producing both short and long strands of DNA at once. In order to facilitate DNA strand exchange, short DNA strands are typically used, while lengthy DNA strands are necessary for the process of DNA strand diffusion. The initial values are derived from the unprocessed image. Where each pixel of the plain image is replaced by a DNA strand, which is then reshaped into two groups. The study encrypts five types of images all of L equals 100 is the size of the ITDCCML system. The article in [38] tries to overcome the problems caused by DNA methods by providing a robust encryption algorithm that is reliant on both DNA and hyperchaotic ciphering approaches. The suggested approach makes use of a hyperchaotic system that hyperscale’s between the 1D Logistic and 3D Hénon maps to produce a key space that is larger than each one produced alone. According to test results on the medical and classical images, the proposed approach has excellent statistical features, a very sensitive encryption key, and a large key space (up to 1084 bits) that makes it resistant to exhaustion-based attacks. For color images [39] employs Intertwining Logistic Map (ILM). The algorithm composed of two steps; In the first step, the ILM-developed 3D chaotic sequence is used to randomly shuffle the pixels of the original image. In this stage, the pixels that were shuffled in the first step is diffused the following phase using the DNA XOR function.

In [40], Using DNA complementarity rules for an exclusive-or operation and interpretation are proposed. Changes to the 2-Dimensional Logistic map's utilizing the SHA-256 hashing technique, initial conditions are constructed. During the initial stage of the diffusion process, the rows of the three different colored channels are shuffled around using a random selection of DC-Boxes, and the same procedure is subsequently performed on the columns. Each color channel is separately permuted in the second diffusion phase using a chaotic sequence. Also [41], present an algorithm for securing medical images by using the masking technique before encryption. Despite being keyless, the technique increases the unpredictability of the original image. The suggested technique makes advantage of generalized for the confusion: Arnold's Cat Map. While, a developed unique diffusion technique that operates at both the pixel and DNA-plane levels. An image encryption method is proposed in [42] that takes advantage of adaptable DNA code bases, as well as an original multi-chaotic map design to address the limitations. In this study a recent development in chaotic mapping method in one dimension (HGL) is employed in conjunction with adaptive DNA coding initially, the input medical image is subjected to a SHA-256 hashing operation in order to obtain the chaotic series and the beginning chaotic map (HGL) value. At this point, the picture is crossed over, and adaptive DNA coding is applied to both the chaotic map and the image in order to create two DNA matrices. To create a new DNA strand, the two DNA strand are Xored using the Xor technique. Image encryption is achieved in [43]. It used dynamic row and column chain operation, DNA dynamic coding, and producing a novel DNA matrix. First, A pixel's binary bit is used to dynamically encode the original image, and the DNA sequence matrix is scrambled in the process. Second, matrices of the DNA sequence are constantly subdivided into DNA chains of various lengths. Next, the row deletion and column transposition operations of the DNA dynamic chain are executed, resulting in a twofold shuffle of the DNA chain matrix. In order to secure medical images a hybrid deoxyribonucleic acid (DNA) masking model, the SHA-2 the secure Hash Algorithm, in addition to an innovative hybrid chaotic map is proposed in [44]. The study is distinguished by the originality of using S-Box to improve the algorithm performance. The keys of the cryptosystem were produced from the plain image hash values. While, the plain image and the secret hash keys are utilized in order to create the one-time keys using SHA-2. The hybrid chaotic map is used to produce random sequences. The plain image is shuffled using these sequences and the DNA XOR algorithm is used in the confusion step to jumble the simple image's pixel values.

Another encryption technique is proposed in [45] which is, Encryption through DNA and the Theory of Finite Automata. Based on the characteristics of the receiver, private key is generated by the sender. with a 256-bit DNA base that is used to encrypt data. The suggested system consists of three entities which are: (KPG) the technique for generating key pairs, this entity gives the sender and receiver the public and private keys during the registration. The next entity is sender who keeps both private and public data and last is the third entity which is the receiver requests for the sender to access any necessary data are sent by this entity. The study [46] provide a formula for the DNA coding and the hyperchaotic behavior. to have sophisticated and pseudo-random characteristics. Using nonlinear analysis methods, the entirety of the dynamic processes involved in a financial system that is hyperchaotic are investigated in order to properly choose the sequence key. In order to maximize the effectiveness of the dispersion and confusion caused by digital images, a set made up of DNA coding, the financial sector's pseudo-random number generator, used in every stage of the encryption process, and the placements of each image pixel are all used. Another study based on DNA, row by row and column by column, closed loop double scrambling algorithm based on a system that is chaotic [47]. The Knuth-Durstenfeld shuffle algorithm is combined with the Hilbert curve in the scrambling step to provide a new pixel reconstruction approach that addresses the problem of close storage of the Hilbert curve. A one-dimensional vector's pixel matrix can be reconstructed using this method thanks to the Hilbert curve. Dynamic updates to the encryption system are implemented in a closed loop, with the first line of ciphertext being modified after the final one is generated. The final step involves using SHA-256 to determine the chaotic system's starting value and provide the secret key. Two main parts include in [48], In the first section, the plain image is encrypted and compressed with the help of the PCS and the Arnold map. The image that the first portion of the process has encrypted is permutated and diffused by the second component using DNA sequence. Additionally,[49] propose an algorithm to secure medical images that is based on the integer wavelet transform (IWT) combined with DNA and chaos. Two phases are comprising phase one consisting of two stages of shuffling, and phase two consisting of two stages of diffusion. Analysis of the suggested algorithm is performed using 512×512 medical test images. Block-wise confusion is used in the first step of shuffling, which is based on the key sequences produced by chaotic maps. To divide the scrambled image into four sub bands, it is translated to IWT coefficients. The second stage involves row and column reordering. Rule 1 encoded diffusion in a DNA unit; DNA processes referred to as XOR and XNOR are carried out and also deciphered. MIE (multiple-image encryption) is proposed in [50] Addressing the problems of weak security, insufficient encryption tools, and inefficient encryption. This algorithm uses the plain image hash value from SHA-256 along cooperatively generating keys based on shared external parameters. Using SHA-256, the algorithm generates a 256-bit hash value called Hk, which is then divided into blocks of 8 bits each. Table 6 contains the state-of-the-art for image encryption techniques.

Table 6. illustrates the state-of-the-art in color-coding algorithms for image-to-image encryption

Ref. No.	Objective	Approaches used	Database information	Attack considered
[34]	To enhance the key space of the color image encryption algorithm, improve its responsiveness to the content of plain images, strengthen its resistance to the many different types of attacks that are already known, and conduct tamper location analysis	DNA encoding that is both hyperchaotic and dynamic on a six-dimensional (6D) scale	Peppers, Lena, the Baboon, the Plane, and the Sailboat	Capping attack Noise attack
[35]	confirms its suitability for use in contemporary cryptosystems used for multimedia data transfer.	Substitution Box Using DNA Coding	Baboon 256*256 Lenna 256*256 Digital Electronics 600*450 Monaliza 900*1285 Egyptian civilization 259*149 Racoon face 1024*768 Peppers 255*255	interpolation assaults, algebraic assaults, the avalanche phenomenon, nonlinearity, and the period
[36]	Existing DNA encryption techniques use a limited number of processes, numerous examples of these can be broken into using selected-plaintext assaults.	Sequence-based DNA operations and the ensuing chaotic system	Lena, Peppers, Baboon, house, Barbra, Airplane and Sailboat	attacks using differential data, attacks using plaintext data, attacks using noise data, and attacks using occlusion data
[37]	compared to cross-coupled map lattice and tent-dynamic cross-coupled map lattice, it is suggested that the latter has the greater ergodicity, larger chaotic range, and higher information entropies; thus, it is more appropriate for use in a chaos-based picture encryption technique.	DNA strand exchange and diffusion	Lena, Baboon, house, Airplane and boat	Different attacks
[38]	to address the issues with the DNA method	Encrypting photos with DNA and a Hyperchaotic key	-	both a differential attack and a Chosen/Known plaintext attack are being used.
[39]	in order to supply a dependable technique for image encryption which offers a completely integrable approach and can fend off numerous attacks.	DNA,1D & 2D Chaotic maps	USC-SIPI	Known plaintext attack, Statistical attacks, Differential attacks
[40]	to create a quick technique for image encryption and decryption	DNA encoding, Pair coupled Chaotic map	Lena (256×256) Color image	Statistical attack, Differential attack, Exhaustive attack
[41]	to give an accurate disease diagnosis, treatment recommendations, and treatment follow-ups	DNA-level bit diffusion	X-Ray CT Scans MRI Imaging Ultrasound	brute force and statistical attacks
[42]	to overcome the limits by the use of adaptable molecular bases in DNA and the design of a new kind of multi-chaotic map	adaptive DNA and modern multi chaotic map	A Lena, MRI, CT scan, X-ray, ultrasound, and an ECG were all performed.	brute force attack, differential attacks
[43]	To show a superior security performance	DNA chain of dynamic length,	A child's brain Vertebrae cervicale's	Noise attack, occlusion attack, and

			MRI Brain Knee-joint Chest reinforcement Abdominal reinforcement Chest X-ray Pelvic	all common cryptographic attacks
[44]	To make the cryptosystem more robust	DNA masking hybrid model, SHA-2 secure hash algorithm, and novel hybrid chaotic map	Medical images	Statistical and exhaustive attacks
[45]	In order to guarantee the safety of the data transmission from sender to recipient	Encryption through DNA and the Theory of Finite Automata	-	Numerous attacks exist, including brute force, known plaintext, differential cryptanalysis, cipher text only, man in the middle, and phishing.
[46]	In order to improve upon the unfortunate one-dimensionality of a map and its odd image storage format, a small secret key space has been included.	Complexity and pseudo-randomness characterize hyperchaotic behavior and genetic coding.	The Airport, Lena, Peppers, Aerial, Barbara, and Circuit	brute force attacks
[47]	To improve information transmission effectiveness while maintaining high security.	a closed loop with double scrambling of DNA rows and columns, based on a chaotic system	Baboon, Barbara, Boat, Couple, Chemical plant, Clock, Elaine, Fingerprint, Gold Hill, Peppers, Plane, Resolution chat, MEAN	Statistical attack, Differential attack
[48]	in order to limit the amount of information that is delivered and to improve the efficiency of computing	Combining chaos, DNA sequence, and parallel compressive sensing (PCS) .	Lena	differential attack
[49]	To safeguard digital medical images	Combining (DNA) and chaos with an Integer Wavelet Transform	Medical image	attacks based on statistics as well as differentials
[50]	To address the issues of insufficient encryption capacity, insufficient encryption efficiency, and insufficient encryption capacity	technique for multiple-image encryption (MIE), built on the three-dimensional scrambling concept and dynamic DNA coding	Lena, Peppers, Watch, Fishing boat	Statistical, Brute-Force, and Selected-Plaintext Attacks

The algorithms' strength and effectiveness are validated using measures including NPCR, UACI, KA, HA, MAE, EI, ET, NA, KS key sensitivity, and PSNR. Table 7 provides a clear comparison of previous studies upon those metrics.

Table 7. Compares the results of previous studies

	Evaluation metric used							
Ref.no.	**NPCR and UACI**	**PSNR**	**Key space**	**Complexity (Time or speed)**	**Entropy**	**CC**	**Histogram**	**MSE**
[34]	Yes	Yes	$10^{161} \approx 2^{536}$	Time	Yes	-	Yes	-
[35]	Yes	Yes	-	Speed	Yes	-	Yes	Yes
[36]	Yes	-	10^{60}	-	Yes	Yes	Yes	-
[37]	Yes	-	2^{4788}	Time	Yes	-	Yes	-
[38]	Yes	Yes	10^{84}	-	Yes	Yes	Yes	Yes
[39]	Yes	Yes	10^{96}	Time	Yes	Yes	Yes	-
[40]	-	-	10^{450}	-	Yes	Yes	Yes	-
[41]	Yes	-	-	Time	Yes	Yes	Yes	-
[42]	Yes	Yes	$2^{128} \times 10^{105} \approx 3.4028 \times 10^{143}$	-	Yes	Yes	Yes	Yes
[43]	Yes	Yes	$(10^{14})^7 = 10^{112} \approx 2^{372}$	-	Yes	Yes	Yes	-
[44]	Yes	-	2^{199}	-	Yes	Yes	Yes	-
[45]	-	-	-	Time	-	-	-	-
[46]	Yes	Yes	5.898×10^{72}	Speed	Yes	Yes	Yes	Yes
[47]	Yes	Yes	2^{445}	Time	Yes	Yes	Yes	Yes
[48]	Yes	Yes	2^{372}	-	Yes	Yes	Yes	-
[49]	Yes	Yes	2^{128}	-	Yes	Yes	Yes	Yes
[50]	Yes	Yes	$1.1579 \times 10^{189} \approx 2^{628}$	Time	Yes	Yes	Yes	Yes

5. Results and Discussion

In addition to its role in encryption, DNA technology is also employed in the storage and protection of sensitive information. Although DNA technology is still in the theoretical stage, it has offered new methods of encryption that include numerous possibilities. This is especially true with regard to the encryption of medical images; Nonetheless, this technique has only been utilized to solve problems that are specific to a restricted level. Mathematical encryption of DNA technology, which has the great ability to enhance the length of an encrypted message, makes it possible to thwart a powerful attack. In Tables 8 and 9, it provides a comparison of the outcomes of the various algorithms that were utilized in the earlier research that were discussed before. It is important to keep in mind that a higher PSNR value means the encoded image is more similar to the original message's image. While the MSE values refer to the difference in the actual values of each pixel between the encoded image and the original image. Fig. 6 contains a graphical graph of the PSNR values.

Table 8. Comparison of PSNR values between previous studies

		PSNR		
Ref. No.	**Image details**	**PSNR value**	**Size of image**	**Other observations**
[34]	Lena1/64	28.0397	64×64	-
	Lena 1/16	22.7408	128×128	-
	Lena 1/4	17.0754	256×256	-
	Lena 1/2	14.3698	256×512	-
[35]	Baboon	9.709454474	256×256	-
	Lena	9.25467847	256×256	-
	Digital Electronics	6.189448384	600×450	-
	Monalisa	7.244519301	900×1285	-
	Egyptian civilization	8.16000813	259×194	-
	Racon face	8.74592675	1024×768	-
	Peppers	8.923619682	255×255	-
[36]	-	-	-	-
[37]	-	-	-	-
[38]	CT Brain.JPEG	−41.0078	(256×256)	-
	MRI Skull.JPEG	−42.1540	(490×276)	-
	RGB Pepper.JPEG	−41.5460	(256×256×3)	-
	Grey Lena.JPEG	−39.5765	(256×256)	-
[39]	-	-	-	-
[40]	Lena	20.73	-	-
	Baboon	17.70	-	-
	Average	14.72	-	-
[41]	-	-	-	-
[42]	Lena	8.56	-	-
	MRI	7.35	-	-
	CT	7.09	-	-
	X-ray	6.82	-	-
	Ultrasound	75.49	-	-
	ECG	7.18	-	-
[43]	0.002	33.8870	-	Density of salt & pepper noise
	0.005	29.6681	-	Density of salt & pepper noise
	0.05	19.7353	-	Density of salt & pepper noise
	0.1	16.6353	-	Density of salt & pepper noise
	0.25	12.4552	-	Density of salt & pepper noise
	0.5	9.1951	-	Density of salt & pepper noise
[44]	-	-	-	-
[45]	-	-	-	-
[46]	0.005	31.4477	-	Density of salt & pepper noise
	0.050	21.7103	-	Density of salt & pepper noise
	0.100	18.7514	-	Density of salt & pepper noise
[47]	Peppers	9.3422	-	-
	Baboon	9.4860	-	-
	Plane	7.3983	-	-
[48]	Lena	24.39		
[49]	30.71			
	30.02	-	-	
	Osirix-1	4.8456	-	-

	Osirix-2	4.8587	-	-
	Osirix-3	4.8562	-	-
	Osirix-4	4.8557	-	-
	Osirix-5	4.8413	-	-
	Thorax-1	4.8719	-	-
	Thorax-2	4.8979	-	-
	Thorax-3	4.8539	-	-
	Thorax-4	4.8640	-	-
[50]	Thorax-5	4.8839	-	-

Table 9. comparison of MSE values between previous studies

		MSE		
Ref. No.	**Image details**	**MSE value**	**Size of image**	**Other observations**
[34]	Lena1/64	102.1201	64×64	-
	Lena 1/16	345.9399	128×128	-
	Lena 1/4	1275.090	256×256	-
	Lena 1/2	2377.410	256×512	-
[35]	Baboon	6952.402603	256×256	-
	Lena	7719.914917	256×256	-
	Digital Electronics	15636.35502	600×450	-
	Monalisa	12263.8952	900×1285	-
	Egyptian civilization	9932.9797	259×194	-
	Racon face	8679.359673	1024×768	-
	Peppers	8331.407802	255×255	-
[36]	-	-	-	-
[37]	-	-	-	-
[38]	CT Brain.JPEG	1.2612e+04	(256×256)	-
	MRI Skull.JPEG	1.6421e+04	(490×276)	-
	RGB Pepper.JPEG	1.4276e+04	(256×256×3)	-
	Grey Lena.JPEG	9.0709e+03	(256×256)	-
[39]	-		-	-
[40]	Lena	550.55	-	-
	Baboon	1097.90	-	-
	Average	2190.94	-	-
[41]	-		-	-
[42]	Lena	9131.17	-	-
	MRI	12077.12	-	-
	CT	12819.64	-	-
	X-ray	13623.49	-	-
	Ultrasound	11670.33	-	-
	ECG	12558.48	-	-
[43]	0.002		-	Density of salt & pepper noise
	0.005		-	Density of salt & pepper noise
	0.05		-	Density of salt & pepper noise
	0.1		-	Density of salt & pepper noise
	0.25		-	Density of salt & pepper noise
	0.5		-	Density of salt & pepper noise
[44]	-		-	-
[45]	-		-	-
[46]	0.005		-	Density of salt & pepper noise
	0.050		-	Density of salt & pepper noise
	0.100		-	Density of salt & pepper noise
[47]	Peppers	7815.1	-	-
	Baboon	7319.4	-	-
	Plane	10076.2	-	-
[48]	Lena		-	-
[49]	Osirix-1	1.4073e+09	-	-
	Osirix-2	1.4031e+09	-	-
	Osirix-3	1.4039e+09	-	-

	Osirix-4	1.4040e+09	-	-
	Osirix-5	1.4087e+09	-	-
	Thorax-1	1.3988e+09	-	-
	Thorax-2	1.3905e+09	-	-
	Thorax-3	1.4046e+09	-	-
	Thorax-4	1.4014e+09	-	-
	Thorax-5	1.3949e+09	-	-
	Average	1.3949e+09	-	-
[50]	Proposed	8522	-	-

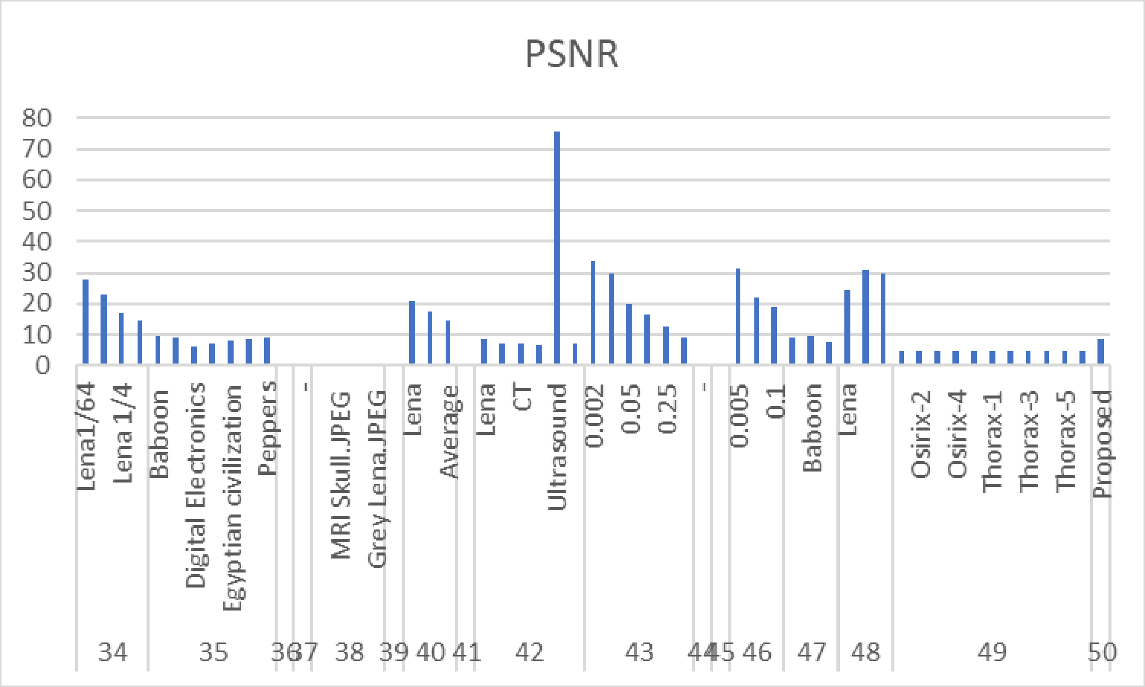

Fig. 6. PSNR values for each technique

6. Conclusion

In this review paper, we explored different DNA-based cryptosystems and other algorithms to secure sensitive data such as text and images such as medical images. The research into the various approaches has led us to the conclusion that the DNA cryptography methods that have been put out promise to be a better method to be used in secure networks. Based on the publications that were studied, it is obvious that genuine DNA implementation and comprehensive security analysis are required rather than computer simulations. Most of the techniques that were studied deals with both medical and classical images with a mutual complexity that is time. In [36][38][46] a DNA sequence operation with additional features and a hyperchaotic system were proposed and dialed with both classical and medical images. The suggested algorithm includes a lower computational more complicated than an algorithm based solely on DNA. While [35] proposed DNA with prementioned S-Box. Grayscale and RGB are the traditional image modalities that can be encrypted using this method. The S-box analysis is carried out utilizing a battery of standard procedures; using NL, SAC, and BIC as examples. These tests, which focus on the link among both plaintext and ciphertext modifications, are dynamic qualities. DNA and new multi chaotic map (HGL) were used to encrypt classical and medical images in [42] with a time complexity. For medical photos, which have extremely high storage requirements and a high level of pixel redundancy, the effectiveness, security, and efficacy of the encryption technology need to fulfill higher standards. In order to retrieve the keys, an algorithm combines the hamming distances and SHA-256 hashes were proposed in[43]. The suggested approach is applicable not only to encrypt medical images but also other types of images. As a result, scientists can use this paper to expand on the limitations of DNA cryptography. The main results of this paper can be summarized as: Using DNA as a form of encryption has led to the development of a significant number of highly effective encryption methods in the medical area. Here, after doing a comprehensive literature review on the topic of medical image encryption, we focus on a few of the challenges which are

- It should be our goal to maintain the accuracy of any encoded medical images; hence, in order to accomplish this, it is absolutely necessary to keep the quality of the medical images unaffected.
- The majority of existing encryption schemes only consider either one or two performance metrics, ignoring the need for a balanced approach to trade-offs between factors like security and complexity.
- Since the original data may only be accessed by the user encrypting it, standard encryption may severely compromise data availability.
- DNA's complicated structure, which ultimately determines security, also makes DNA computation over an image challenging.

Finally, after do this paper we can pointed the future works as: Finding a means to combine image compression with encryption to maximize bandwidth use is an intriguing area for future study.

Acknowledgment

The authors would like to acknowledge the cooperation and assistance they received from Electrical Engineering Technical College to complete this research.

References

[1] M. A. Iliyasu, O. A. Abisoye, S. A. Bashir, and J. A. Ojeniyi, “A review of DNA cryptograhic approaches,” Proc. 2020 IEEE 2nd Int. Conf. Cyberspace, CYBER Niger. 2020, pp. 66–72, 2021, doi: 10.1109/CYBERNIGERIA51635.2021.9428855.

[2] M. A. Naji et al., “Breaking A Playfair Cipher Using Single and Multipoints Crossover Based on Heuristic Algorithms,” 4th Int. Iraqi Conf. Eng. Technol. Their Appl. IICETA 2021, pp. 47–53, 2021, doi: 10.1109/IICETA51758.2021.9717757.

[3] N. S. Noor, D. A. Hammood, A. Al-Naji, and J. Chahl, “A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication,” Computers, vol. 11, no. 3, 2022, doi: 10.3390/computers11030039.

[4] S. Padhiar and K. H. Mori, “A Comparative Study on Symmetric and Asymmetric Key Encryption Techniques,” 2022, pp. 132–144. doi: 10.4018/978-1-7998-6988-7.ch008.

[5] C. Tominski, G. Fuchs, and H. Schumann, “Task-driven color coding,” Proc. Int. Conf. Inf. Vis., pp. 373–380, 2008, doi: 10.1109/IV.2008.24.

[6] N. S. Noor, D. A. Hammood, and A. Al-naji, “Applying TTIED-CMYK Algorithm in Wireless Sensor Networks Based on,” vol. 4, no. 3, pp. 1–7, 2022.

[7] L. Wang, T. Dong, and M. F. Ge, “Finite-time synchronization of memristor chaotic systems and its application in image encryption,” Appl. Math. Comput., vol. 347, pp. 293–305, 2019, doi: 10.1016/j.amc.2018.11.017.

[8] R. S. Jebur, C. S. Der, and D. A. Hammood, “A Review and Taxonomy of Image Denoising Techniques,” 6th Int. Conf. Interact. Digit. Media, ICIDM 2020, no. Icidm, 2020, doi: 10.1109/ICIDM51048.2020.9339674.

[9] G. Ye, C. Pan, X. Huang, and Q. Mei, “An efficient pixel-level chaotic image encryption algorithm,” Nonlinear Dyn., vol. 94, no. 1, pp. 745–756, 2018, doi: 10.1007/s11071-018-4391-y.

[10] C. TİKEN and R. SAMLI, “A Comprehensive Review About Image Encryption Methods,” Harran Üniversitesi Mühendislik Derg., vol. 8733, pp. 27–49, 2022, doi: 10.46578/humder.1066545.

[11] H. Kaur and A. Kakkar, “Comparison of different image formats using LSB Steganography,” 4th IEEE Int. Conf. Signal Process. Comput. Control. ISPCC 2017, vol. 2017-Janua, pp. 97–101, 2017, doi: 10.1109/ISPCC.2017.8269657.

[12] K. K. S. Pareek, Narendra K, Vinod Patidar, “A Symmetric Encryption Scheme for Colour BMP Images,” IJCA Spec. Issue “Network Secur. Cryptogr., no. January, pp. 42–46, 2011.

[13] F. Alshehri and G. Muhammad, “A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare,” IEEE Access, vol. 9, pp. 3660–3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[14] G. Muhammad, M. F. Alhamid, and X. Long, “Computing and processing on the edge: Smart pathology detection for connected healthcare,” IEEE Netw., vol. 33, no. 6, pp. 44–49, 2019, doi: 10.1109/MNET.001.1900045.

[15] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. M. Bhat, “A reversible and secure patient information hiding system for IoT driven e-health,” Int. J. Inf. Manage., vol. 45, no. March, pp. 262–275, 2019, doi: 10.1016/j.ijinfomgt.2018.09.008.

[16] G. Muhammad, M. S. Hossain, and N. Kumar, “EEG-Based Pathology Detection for Home Health Monitoring,” IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 603–610, 2021, doi: 10.1109/JSAC.2020.3020654.

[17] P. Sarosh, S. A. Parah, and G. M. Bhat, “An efficient image encryption scheme for healthcare applications,” Multimed. Tools Appl., vol. 81, no. 5, pp. 7253–7270, 2022, doi: 10.1007/s11042-021-11812-0.

[18] M. Kaur, S. Singh, and M. Kaur, “Computational Image Encryption Techniques: A Comprehensive Review,” Math. Probl. Eng., vol. 2021, no. i, 2021, doi: 10.1155/2021/5012496.

[19] Y. Xie, J. Yu, S. Guo, Q. Ding, and E. Wang, “Image encryption scheme with compressed sensing based on new three-dimensional chaotic system,” Entropy, vol. 21, no. 9, 2019, doi: 10.3390/e21090819.

[20] M. Kaur and V. Kumar, “A Comprehensive Review on Image Encryption Techniques,” Arch. Comput. Methods Eng., vol. 27, no. 1, pp. 15–43, 2020, doi: 10.1007/s11831-018-9298-8.

[21] M. A. Alhija, N. Turab, A. Abuthawabeh, H. Abuowida, and J. Al Nabulsi, “Dna Cryptographic Approaches: State of Art, Opportunities, and Cutting Edge Perspectives,” J. Theor. Appl. Inf. Technol., vol. 100, no. 18, pp. 5346–5358, 2022.

[22] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” Opt. Lasers Eng., vol. 56, pp. 83–93, 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[23] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, “A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system,” J. Syst. Softw., vol. 85, no. 2, pp. 290–299, 2012, doi: 10.1016/j.jss.2011.08.017.

[24] O. H. Alhabeeb, F. Fauzi, and R. Sulaiman, “A Review of Modern DNA-based Steganography Approaches,” Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 10, pp. 184–196, 2021, doi: 10.14569/IJACSA.2021.0121021.

[25] G. Cui, C. Li, H. Li, and X. Li, “DNA computing and its application to information security field,” 5th Int. Conf. Nat. Comput. ICNC 2009, vol. 6, no. February, pp. 148–152, 2009, doi: 10.1109/ICNC.2009.27.

[26] A. Gehani, T. Labean, and J. Reif, “LNCS 2950 - DNA-based Cryptography,” pp. 167–188, 2004.

[27] “DNA Structure. Base Pairing and Nucleotide Stock Vector - Illustration of genome, medicine: 239446702.” https://www.dreamstime.com/dna-structure-base-pairing-nucleotide-cytosine-thymine-guanine-adenine-vector-illustration-image239446702 (accessed Oct. 29, 2022).

[28] C. R. Geyer, T. R. Battersby, and S. A. Benner, “Nucleobase Pairing in Expanded Watson-Crick-like Genetic Information Systems,” Structure, vol. 11, no. 12, pp. 1485–1498, 2003, doi: 10.1016/j.str.2003.11.008.

[29] A. Nath, “International Journal of Advance Research in Introduction to Malware and Malware Analysis : A brief overview,” no. November, 2016.

[30] S. Jain and V. Bhatnagar, “Analogy of various DNA based security algorithms using cryptography and steganography,” Proc. 2014 Int. Conf. Issues Challenges Intell. Comput. Tech. ICICT 2014, pp. 285–291, 2014, doi: 10.1109/ICICICT.2014.6781294.

[31] K. Gupta and S. Singh, “DNA Based Cryptographic Techniques: A Review,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 3, p. 2277, 2013, doi: 10.6633/IJNS.201811.

[32] B. B. Raj and V. Ceronmani Sharmila, “An survey on DNA based cryptography,” 2018 Int. Conf. Emerg. Trends Innov. Eng. Technol. Res. ICETIETR 2018, pp. 1–3, 2018, doi: 10.1109/ICETIETR.2018.8529075.

[33] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, “Image encryption process based on chaotic synchronization phenomena,” Signal Processing, vol. 93, no. 5, pp. 1328–1340, 2013, doi: 10.1016/j.sigpro.2012.11.008.

[34] Q. Zhang and J. Han, “A novel color image encryption algorithm based on image hashing , 6D hyperchaotic and DNA coding,” pp. 13841–13864, 2021.

[35] H. A. M. A. Basha, A. S. S. Mohra, T. O. M. Diab, and W. I. El Sobky, “Efficient Image Encryption Based on New Substitution Box Using DNA Coding and Bent Function,” IEEE Access, vol. 10, no. May, pp. 66409–66429, 2022, doi: 10.1109/ACCESS.2022.3183990.

[36] J. Yu, W. Xie, Z. Zhong, and H. Wang, “Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation,” Chaos, Solitons and Fractals, vol. 162, no. July, p. 112456, 2022, doi: 10.1016/j.chaos.2022.112456.

[37] C. Zou, X. Wang, C. Zhou, S. Xu, and C. Huang, “A novel image encryption algorithm based on DNA strand exchange and diffusion,” Appl. Math. Comput., vol. 430, 2022, doi: 10.1016/j.amc.2022.127291.

[38] S. A. Elsaid, E. R. Alotaibi, and S. Alsaleh, “A robust hybrid cryptosystem based on DNA and Hyperchaotic for images encryption,” Multimed. Tools Appl., 2022, doi: 10.1007/s11042-022-12641-5.

[39] S. Suri and R. Vijay, “A synchronous intertwining logistic map-DNA approach for color image encryption,” J. Ambient Intell. Humaniz. Comput., vol. 10, no. 6, pp. 2277–2290, 2019, doi: 10.1007/s12652-018-0825-0.

[40] A. ur Rehman and X. Liao, “A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2,” Multimed. Tools Appl., vol. 78, no. 2, pp. 2105–2133, 2019, doi: 10.1007/s11042-018-6346-1.

[41] “2021A medical image cryptosystem using bit-level difusion with DNA.pdf.”

[42] R. Ismail, A. Fattah, H. M. Saqr, and M. E. Nasr, “An efficient medical image encryption scheme for (WBAN) based on adaptive DNA and modern multi chaotic map,” Multimed. Tools Appl., 2022, doi: 10.1007/s11042-022-13343-8.

[43] X. Xue, H. Jin, D. Zhou, and C. Zhou, “Medical Image Protection Algorithm Based on Deoxyribonucleic Acid Chain of Dynamic Length,” Front. Genet., vol. 12, no. March, pp. 1–18, 2021, doi: 10.3389/fgene.2021.654663.

[44] R. Guesmi and M. A. B. Farah, “A new efficient medical image cipher based on hybrid chaotic map and DNA code,” Multimed. Tools Appl., vol. 80, no. 2, pp. 1925–1944, 2021, doi: 10.1007/s11042-020-09672-1.

[45] P. Pavithran, S. Mathew, S. Namasudra, and P. Lorenz, “A novel cryptosystem based on DNA cryptography and randomly generated mealy machine,” Comput. Secur., vol. 104, p. 102160, 2021, doi: 10.1016/j.cose.2020.102160.

[46] V. R. F. Signing, R. L. T. Mogue, J. Kengne, M. Kountchou, and Saïdou, “Dynamic phenomena of a financial hyperchaotic system and DNA sequences for image encryption,” Multimed. Tools Appl., vol. 80, no. 21–23, pp. 32689–32723, 2021, doi: 10.1007/s11042-021-11180-9.

[47] 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 July, pp. 1–30, 2022, doi: 10.1371/journal.pone.0267094.

[48] D. Wei and M. Jiang, “A fast image encryption algorithm based on parallel compressive sensing and DNA sequence,” Optik (Stuttg)., vol. 238, no. February, p. 166748, 2021, doi: 10.1016/j.ijleo.2021.166748.

[49] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, “An efficient medical image encryption using hybrid DNA computing and chaos in transform domain,” Med. Biol. Eng. Comput., vol. 59, no. 3, pp. 589–605, 2021, doi: 10.1007/s11517-021-02328-8.

[50] X. Zhang and Y. Hu, “Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding,” Opt. Laser Technol., vol. 141, no. January, p. 107073, 2021, doi: 10.1016/j.optlastec.2021.107073.