The Chaotic Dynamics of DNA: A Survey on DNA Cryptography

Akhil Kaushik
Computer Engineering Department
TIT&S Bhiwani
Haryana, India

Satvika
Computer Engineering Department
TIT&S Bhiwani
Haryana, India

ABSTRACT

The advent of digital technology has irrevocably transformed societies, economies, and individual lives. Concomitantly, it has introduced novel challenges, most notably in the realm of information security. DNA cryptography, inspired by the intricate structure of deoxyribonucleic acid, has emerged as a promising field for secure data transmission and storage. This paper explores the fundamental principles of DNA cryptography, including DNA encoding, associated basic and advanced operations, and key generation. Another revolutionary change occurred when chaos theory with its study of complex, unpredictable systems, found an intriguing application in the field of cryptography. By leveraging the inherent randomness and complexity of DNA sequences, along with the chaotic properties of mathematical functions, researchers have developed innovative cryptographic techniques. This review paper delves into the synergistic integration of chaotic functions and DNA cryptography, examining their potential to enhance security and efficiency.

Keywords

Chaotic Functions, Chaos Theory, DNA Cryptography, Decryption, Encryption, Information Security.

1. INTRODUCTION

In the ever-evolving landscape of information security, the requirements of enhanced safeguarding measures has paved the way for novel and improved cryptosystems. With the exponential growth rate of data and superior sophisticated means of cyberattacks, myriad cryptographic and steganographic techniques are available for handling refuge of vital data like sensitive code, digital images of importance like military maps, identity cards, etc. However, it is vital to understand that the concept of safeguarding information predates the digital era. Ancient civilizations employed various techniques to protect sensitive knowledge, such as encryption, physical security measures, and restricted access. For instance, the Egyptians used hieroglyphics, a complex writing system, to conceal information from the uninitiated. Similarly, the Roman Empire implemented sophisticated cryptographic methods to protect military communications [1]. A renowned Scytale cipher used by the Roman Army is depicted in figure 1 below.

The mid-20th century marked a significant turning point with the emergence of computers and digital networks. As technology advanced, so did the potential for information breaches. Early cyberattacks, such as hacking and virus dissemination, highlighted the vulnerability of digital systems. The 1990s witnessed a surge in cybercrime, with malicious actors targeting individuals, organizations, and governments. This trend increased exponentially in the later period when the attackers and hackers launched more financial and personal attacks like malware, man-in-the-middle attack, denial-of-service attack, SQL injection, ransomware, phishing, identity theft, digital arrest and even cyber bullying [2].

Fig 1. Scytale Cipher used by Ancient Greeks & Spartans [3]

To counter these growing threats, information security professionals developed a multifaceted approach to protect digital assets. This approach, commonly referred to as the CIA triad, encompasses three core principles: Confidentiality means ensuring that sensitive information is accessible only to authorized individuals. Integrity is protecting information from unauthorized modification or destruction. Availability is guaranteeing that information and systems are accessible whenever needed [4]. To achieve these objectives, a range of security measures have been implemented, including Cryptography, Steganography, Access Control mechanisms, Firewalls & Intrusion Detection Systems (IDS), etc. Out of these, steganography and cryptography are the most popular options. On the one hand, where the steganography deals with hiding the crucial information, the cryptography employs mathematical algorithms to encrypt data, rendering it unintelligible to unauthorized parties, which will be discussed in detail in the next sub-section.

1.1. Cryptography

Cryptography is formally defined as the art and science of protecting the crucial communication and information. It has been a cornerstone of human civilization even before the dark ages of Europe. At its core, cryptographic process is bifurcated into two process: encryption and decryption; where the former method converts the human-readable message (plaintext) into a labyrinthine form (ciphertext) and the latter is the vice-versa of former. Broadly, there are three eras namely: ancient, classical and modern cryptography. The ancient crypto was based on mostly symbols that was used primarily for religious purposes. The classical cryptography chiefly encompasses two major techniques: substitution (altering the characters by new ones) and transposition (changing the position of characters). The modern cryptography is the period when mechanical machines especially computers were employed in the usage of forming ciphertexts from plaintext and vice-versa. Here, the crypto process became so labyrinthine that it was impossible to do with pen and paper [5].

For instance, Cyclometer was a Polish cryptology device was a device used to break the encryption codes of Enigma machine [6].

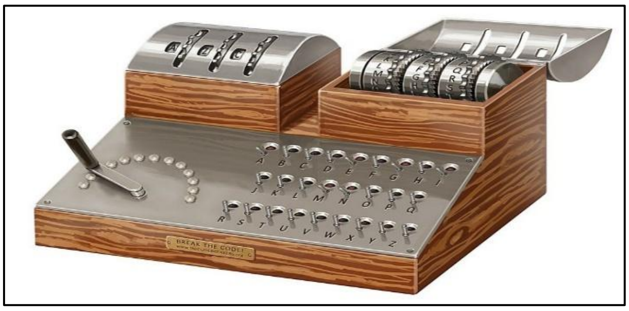

Fig 2. Polish Cyclometer Device [6]

1.2 Chaos Systems

Chaos theory, a branch of mathematics and physics, explores the behavior of dynamical systems that exhibit sensitive dependence on initial conditions. This phenomenon, often referred to as the "butterfly effect", implies that small changes in initial conditions can lead to significant variations in long-term outcomes. While chaos theory may seem counterintuitive, it has profound implications for various scientific disciplines, including cryptography. The core concept underlying chaos theory is the idea of deterministic chaos. A deterministic system is one whose future behavior is entirely determined by its present state and the laws governing its evolution. However, chaotic systems, despite being deterministic, exhibit seemingly random and unpredictable behavior. This apparent randomness stems from the exponential divergence of trajectories, which makes it difficult to predict long-term behavior [7].

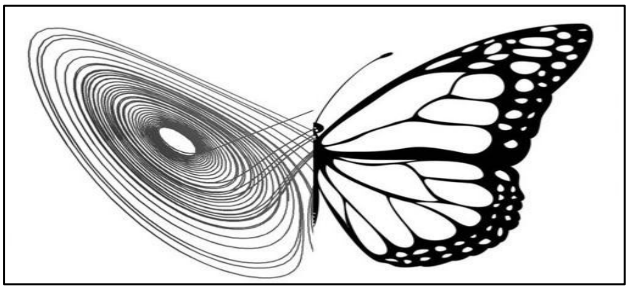

Fig 3. Butterfly Effect in Chaos Theory [8]

The functions based on chaos theory are known as chaotic functions and exhibit an unpredictable yet deterministic pattern—when iterated repeatedly. The key point here is that these functions are non-linear and irregular in nature, which make it extremely handy in cryptology. For instance, logistic map, a simple nonlinear recurrence relation that demonstrates how complex behavior can emerge from simple rules. The logistic map is given by:

$$x_{n+1} = rx_n(1 - x_n) \qquad (1)$$

Here, $\boldsymbol{x_n}$ is a value between 0 and 1 representing the state of the system at iteration $\boldsymbol{n}$ and $\boldsymbol{r}$ is a parameter controlling the system's behavior. For diverse values of $\boldsymbol{r}$, the chaotic function displays varied behaviour [8].

The application of chaos theory in cryptography leverages the inherent unpredictability and sensitivity to initial conditions of chaotic systems. By exploiting these properties, cryptographic algorithms can generate strong encryption keys, secure communication protocols, and robust digital signatures. By carefully selecting appropriate chaotic maps and initial conditions, it is possible to generate cryptographic keys that are statistically indistinguishable from true random numbers. Moreover, chaos theory can be employed to develop robust digital signature schemes. Digital signatures are used to verify the authenticity and integrity of digital documents. Chaotic systems can be used to generate unique digital signatures that are difficult to forge. By selecting appropriate chaotic maps and initial conditions, it is possible to create digital signatures that are resistant to various attacks, including forgery and replay attacks [9].

However, it is important to note that the application of chaos theory in cryptography is not without its challenges. One of the primary challenges is the selection of appropriate chaotic maps and initial conditions. A poorly chosen chaotic system can lead to weak cryptographic algorithms that are vulnerable to attacks. Additionally, the implementation of chaotic systems in hardware and software can be complex and computationally intensive. In conclusion, chaos theory offers a powerful tool for enhancing the security of cryptographic systems. By leveraging the inherent unpredictability and sensitivity to initial conditions of chaotic systems, it is possible to develop robust and secure cryptographic algorithms.

1.3 Bio-Molecular Computation

Biomolecular computation is an emerging field that leverages the principles of molecular biology to perform computational tasks. By harnessing the power of DNA, RNA, and proteins, scientists are exploring innovative approaches to solving complex problems. At the heart of biomolecular computation lies the concept of using DNA molecules as information storage and processing units. DNA, with its four nucleotide base pairs (A, T, C, G), can encode vast amounts of information. By carefully designing sequences of DNA strands, researchers can represent and manipulate data. For instance, DNA hybridization which involves complementary base pairing of DNA strands and by controlling the conditions of hybridization, scientists can create complex molecular structures that represent specific computational states [10].

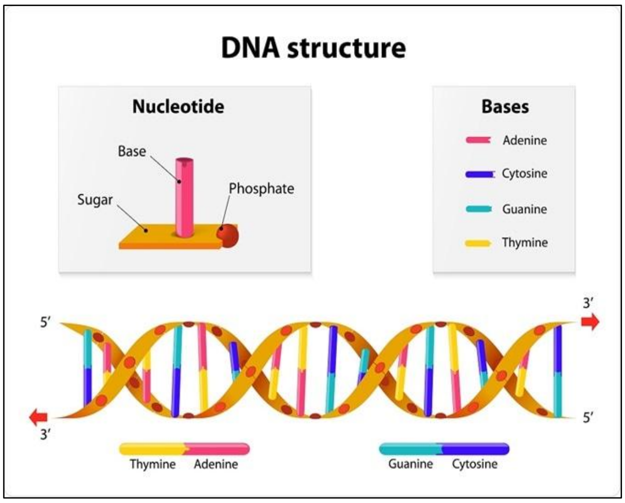

Fig 4. DNA Structure in detail [10]

Biomolecular computation has the potential to revolutionize various fields, including drug discovery, medical diagnostics, materials science and information security. Despite its immense potential, biomolecular computation faces several challenges. One of them is scalability, i.e. scaling up the DNA strands to handle large-scale problems. Another challenge is the need for wet laboratories for complex bio-chemical processes; however, the evolution of digital DNA has provided an alternative solution.

As technology advances and the understanding of molecular biology deepens, biomolecular computation is poised to become a powerful tool for addressing complex challenges. By harnessing the power of nature, new frontiers in computing can be unlocked and pave the way for a future filled with innovation.

2. DNA CRYPTOGRAPHY

Although, cryptology has been in the life of man since the ancient times but with the advent of computing and embryonic challenges, DNA cryptography has emerged as a main savior.

2.1 DNA One-Time Pads

DNA one-time pads offer a promising avenue for exploring novel cryptographic techniques, leveraging the immense information density of DNA molecules. By encoding plaintext messages and a random key sequence into complementary DNA strands, perfect secrecy can be achieved. During encryption, the plaintext and key are combined using a one-time pad scheme, where each bit of the plaintext is XORed with a corresponding bit of the key. The resulting ciphertext is then encoded into a DNA sequence, where each nucleotide represents two bits of information [11]. However, practical challenges remain in implementing DNA one-time pads. Accurate synthesis and sequencing of long DNA strands are essential for reliable encryption and decryption. Additionally, errors during the hybridization process can lead to decryption errors. To address these challenges, researchers are exploring error-correcting codes and advanced DNA synthesis techniques. Despite these limitations, DNA one-time pads offer a compelling vision for future cryptographic systems. With continued advancements in biotechnology and nanotechnology, it is possible that DNA-based cryptography will become a viable and secure method for protecting sensitive information.

2.2 DNA Substitution

DNA substitution, a fundamental type of mutation, occurs when one nucleotide base is replaced by another. This seemingly simple alteration can have profound consequences, ranging from silent mutations with no phenotypic effect to severe genetic disorders. Silent mutations often result from changes in the third position of a codon, which frequently codes for the same amino acid. However, missense mutations, where a codon is altered to encode a different amino acid, can lead to significant changes in protein structure and function. These changes may impact protein stability, enzymatic activity, or interactions with other molecules. Nonsense mutations, on the other hand, introduce a premature stop codon, resulting in truncated proteins that may be nonfunctional or unstable. Additionally, insertions and deletions, which involve the addition or removal of nucleotides, can shift the reading frame and disrupt the entire protein sequence. These types of mutations often have severe consequences, as they can lead to the production of nonfunctional or harmful proteins [12].

2.3 DNA Synthesis

DNA synthesis, a cornerstone of molecular biology, involves the construction of DNA molecules, either naturally or artificially. This process is essential for cellular replication, genetic engineering, and various biotechnological applications. In nature, DNA synthesis occurs through a complex enzymatic process, where DNA polymerase catalyzes the addition of nucleotides to a growing DNA strand, guided by base pairing rules. However, synthetic DNA synthesis, pioneered by Khorana in the 1960s, has revolutionized molecular biology. Modern DNA synthesis techniques, such as solid-phase synthesis, enable the rapid and efficient assembly of custom DNA sequences. This technology has enabled the creation of synthetic genes, the production of recombinant proteins, and the development of gene therapies. While significant advancements have been made, challenges remain, including the synthesis of long, error-free DNA sequences and the cost-effective production of large quantities of DNA [13].

2.4 DNA Ligation & Hybridization

DNA ligation and hybridization are fundamental processes in molecular biology, enabling the manipulation and analysis of DNA molecules. DNA ligation involves the joining of two DNA fragments through the formation of phosphodiester bonds, catalyzed by the enzyme DNA ligase. This process is essential for various applications, such as cloning, DNA sequencing, and gene synthesis. DNA hybridization, on the other hand, is the process of forming double-stranded DNA by pairing complementary single-stranded DNA molecules. This process is driven by hydrogen bonding between complementary base pairs (A-T and C-G). Hybridization is widely used in techniques like Southern blotting, Northern blotting, and polymerase chain reaction (PCR). By understanding and manipulating these processes, researchers can explore the intricacies of DNA structure and function, develop new diagnostic tools, and engineer novel genetic constructs [14].

2.5 Polymerase Chain Reaction (PCR)

Polymerase Chain Reaction (PCR) is a revolutionary technique that enables the amplification of specific DNA sequences, revolutionizing molecular biology. This technique involves a cyclical process of denaturation, annealing, and extension.

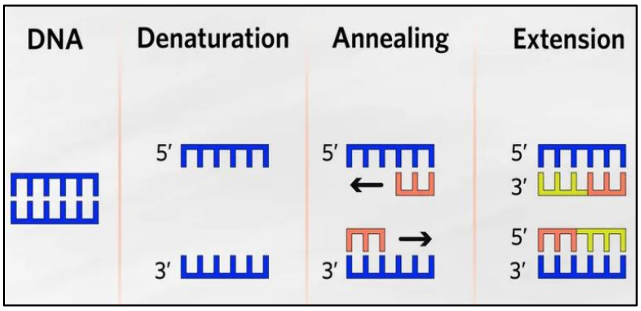

Fig 5. Explanation of PCR Process [16]

Initially, the DNA template is denatured into single strands by heating. Subsequently, short, synthetic DNA primers anneal to complementary sequences on the template strands. A DNA polymerase enzyme then extends the primers, synthesizing new DNA strands. This cycle is repeated multiple times, exponentially amplifying the target DNA sequence. The advent of thermostable DNA polymerases, such as Taq polymerase, has made PCR a highly efficient and versatile technique. PCR has numerous applications in various fields, including molecular diagnostics, forensic science, genetic engineering, and basic research [15]. The figure 6 above represents the PCR process.

2.6 Gel Electrophoresis

Gel electrophoresis is a foundational technique in molecular biology that separates biomolecules based on their size and charge. In this method, a sample containing DNA, RNA, or proteins is loaded into a gel matrix, typically composed of agarose or polyacrylamide. An electric field is applied across the gel, causing the charged molecules to migrate through the porous matrix. Smaller molecules, with less resistance, move faster through the gel than larger molecules. This differential migration results in the separation of molecules based on their size. The gel matrix acts as a molecular sieve, allowing smaller molecules to pass through more easily.

By staining the gel with appropriate dyes, such as ethidium bromide for nucleic acids or Coomassie Blue for proteins, the separated bands can be visualized. The pattern of bands provides valuable information about the size, quantity, and purity of the biomolecules. Gel electrophoresis is widely used in various applications, including DNA fragment analysis, protein separation, and nucleic acid sequencing. By understanding the principles of gel electrophoresis, researchers can gain insight into the structure, function, and interactions of biological molecules [17].

2.7 DNA Encoding

It is the most fundamental enciphering of data using DNA nucleotide bases (A, C, T & G). According to the Watson-Crick base pairing rules: C & G are complementary and A & T are complementary too. To apply DNA encoding there are eight possible rules which are listed in table 1 below.

Table 1. DNA Encoding Rules

Rules	**Watson-Crick Complementary Rules**							
	I	***II***	***III***	***IV***	***V***	***VI***	***VII***	***VIII***
00	A	A	C	G	C	G	T	T
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C
11	T	T	G	C	G	C	A	A

Apart from the DNA Encoding, there are three major operation that can be applied among DNA nucleotide bases: Addition, Subtraction & XOR, which are listed in table 2, 3 & 4 respectively.

Table 2. DNA Addition Operation

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

Table 3. DNA Subtraction Operation

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

Table 4. DNA XOR Operation ()

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

3. LITERATURE REVIEW

In this survey process, the initial steps were collection of research articles, followed by scanning of title and abstract and finally, full-text reading. In this way, total 47 articles were collected from myriad online databases like IEEE Xplore, ACM, Springer, Google Scholar, etc. and then 25 research papers were selected on the basis of innovative ideas presented in the articles. These research papers are taken from a span of 10 years i.e. from year 2015 to 2024 and are discussed one by one in detail.

In an inventive research article by Basu et. al. (2019), authors have proposed bio-inspired cryptosystem that provides a competent solution for encrypting and decrypting large amounts of data, offering sufficient security while saving memory and reducing the number of cryptographic operations. The proposed bio-inspired cryptosystem using Bidirectional Associative Memory Neural Networks (BAMNN) for key generation and DNA-based encryption and decryption algorithms is a secure and efficient cryptosystem that achieves good randomization and exhibits the properties of confusion and diffusion. The DNA cryptography simulates the processes of genetic encoding, transcription, and translation from the Central Dogma of Molecular Biology (CDMB). The proposed algorithm exhibit strong avalanche effect as 93.59% change is experienced in ciphertext by 1-bit change in plaintext and 96.15% change by change in 2-bits of plaintext. The proposed cryptosystem is resilient to brute-force, ciphertext-only, known plaintext, and differential cryptanalysis attacks also [18].

Since DNA cryptography first emerged, an increasing number of academics have dedicated their time and energy to creating safe and secure methods for information transfer between reliable parties. A new method for encoding coloured images utilizing DNA and hyperchaotic systems has been proposed by Cui et al. (2020). In order to create the enciphered image, first coloured images are stacked and DNA encoded, then hyper-chaotic and DNA operations are performed. Here, confusion operation is done using hyper-chaotic sequences and DNA addition operation is employed for diffusion operation. The experimental findings demonstrate uniform distribution in the histogram and resilience to numerous attacks [19].

Another outstanding study by Pourasad, Ranjbarzadeh & Mardani (2021) demonstrate the combination of wavelet decomposition and chaos theory on greyscale images. The image is first captured as a matrix of m * n, where m and n are the image's height and width, and then it is diffused using logistic maps' chaotic sequences. The wavelet decomposition is then used at different stages to create a strong encoded image that is challenging for adversaries to decipher. The proposed cipher is tested on four diverse images and four major attacks- Rotation, Histogram Equalization, Gaussian Noise and Media Filtration; and it was established that the algorithm is robust enough to tackle all chief attacks [20].

Samiullah et al. (2020) used DNA sequencing in conjunction with three chaotic functions- PWLCM, Lorenz and 4D Lorenz-type to offer the highest level of protection for digital images up to 512*512 pixels. In contrast to the state-of-the-art encryption standards, robustness against major sounds and improved protection are ensured here by the use of numerous chaotic functions, SHA-256, and DNA functions at both the confusion and diffusion processes. The purported cipher is tested against all major attacks like known/chosen plaintext attacks, mean absolute error, irregular deviation, entropy, maximum deviation, etc. As the size of the input image increases, the algorithm's complexity grows logarithmically [21].

A non-linear 16*16 DNA Playfair matrix and chaotic systems were used in the innovative picture encoding suggested by Ibrahim et al. (2022). Each of the 16 rounds of this method, which is based on the feistel structure, has a unique key derived from logistic maps. In this case, the RGB image is divided into three distinct Red, Green, and Blue colour channels. It is more robust and effective than the majority of its competitors because it uses a larger key space. Also the suggested algorithm has extremely low value for correlation and optimal values for UACI & NPCR. Finally, to check the randomness provided by cipher, NIST is also applied and results show better efficacy [22].

DNA maneuvers and chaotic sequences have also been studied by Shakir, Mehdi, and Hattab (2022); the former is utilized for diffusion, while the latter is used for confusion operations. Here, the authors propose a novel 4-D chaotic system that is highly nonlinear and dynamic in nature as shown in figure 6 below. Additionally, it reshapes the coloured image into various vectors and separates it into channels of three primary colours. The final ciphered picture is created by recombining the three distinct images after all the appropriate procedures have been applied. The highlight of this work is the larger key space i.e. 2^{627} keys, which makes it almost immune to brute-force, statistical and differential attacks [23].

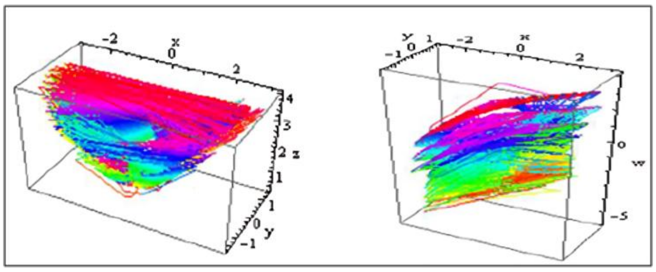

Fig 6. Chaotic attractors' 3-D views [23]

Li et al. (2016) defined how DNA & chaotic functions based one-time pads can do a fantastic job when it comes too cryptology. The secret keys are generated using the intricate hyper-chaotic Lorenz system. After being transformed into binary vectors, the three colour image channels are XORed using DNA strands. Here, the Hyper-Lorenz system creates six chaotic sequences that carry out the scrambling. In this case, the encryption and decryption processes are completely opposite. This approach is highly resistant to differential assaults since it generates keys using hamming distance and one-time pads [24].

By utilizing Choquet Fuzzy Integral (CFI) and DNA approaches to improvise substitution-boxes (S-boxes), Mohamed, Korany, and El-Khamy (2021) proposed a novel encryption algorithm-DNAFZ S-boxes. After applying M-sequence to scramble the input image, it is divided into four sub-images, which are subsequently diffused using Chen's hyper-chaotic map's DNA-encoded chaotic sequence. This proposed system's numerical efficacy in terms of correlation, entropy, homogeneity, etc., is a powerful defense against numerous attacks. The experimental results exhibit superiority when compared to established standards- LSS chaotic map, Arnold transforms, Dynamic Henon map, etc. [25].

Using a 2-D Sine logistic modulation map (SLMM) with modified primary values is recommended by Naskar et al. (2021). The 64-bit external key and 32-bit hash value are used to create the chaotic function's initial parameters. At the 64-byte block level, the confusion is used first in row-wise operations and subsequently in column-wise operations. A key feature of this algorithm is that all the chaotic values created from chaotic maps are highly sensitive to the plaintext and key. Multiple images of varied sizes and shapes are taken as input in the cryptosystem to check the uniformity of the system. The p-values (NIST test) of all ciphered images certify the merit of the proposed algorithm [26].

An additional study by Singh & Singh (2023) proposed a hyper chaotic Lorenz function-based DNA-based image encryption method that is both secure and effective. The SHA-512 hash function's primary key is used to first jumble the image, and then the Lorenz function is used to transpose the rows and columns. Later, the DNA processes perform the diffusion operation [27].

The research by Khan et. al. (2020) introduces a novel image encryption scheme that integrates DNA-based operations with chaotic maps and visual cryptography. The proposed method enhances security by incorporating plaintext dependence, where the encryption process is dynamically influenced by the image content itself, thereby increasing resilience against known-plaintext attacks. Furthermore, the scheme offers selective encryption capabilities, enabling users to encrypt and decrypt specific regions of interest within the image. This flexibility is achieved through the integration of visual cryptography techniques, allowing for fine-grained control over access to sensitive information. The authors demonstrate the efficacy of their approach through rigorous analysis and experimental evaluation, highlighting its potential for secure image transmission and storage in various applications, including medical imaging, military data protection, and secure personal image sharing [28].

The brainy authors Almasoud et. al. (2024) presented a novel image encryption scheme (CIEAIBO-DNAC) that integrated chaotic systems, DNA-based encoding, and an improved Bonobo Optimizer for enhanced security. Furthermore, the employment of an improved Bonobo Optimizer allows for dynamic optimization of the chaotic parameters and DNA operations, leading to adaptive and robust encryption performance. The proposed scheme demonstrates promising potential for secure image transmission and storage in various domains, including medical imaging and critical data protection, by significantly increasing key space, enhancing sensitivity to initial conditions, and improving fight against a wide range of attacks [29].

The research work by Gasimov & Mammadov (2021) proposes an image encryption scheme that integrates DNA-based encoding with chaotic maps, incorporating an expanded set of DNA pseudo-symbols to augment cryptographic strength. The algorithm leverages chaotic maps to introduce non-linearity and sensitivity to initial conditions, while DNA operations and the expanded symbol set further enhance the complexity and diffusion of information within the encrypted image. By effectively combining these techniques, the authors aim to achieve a robust and secure encryption scheme with a large key space and strong resistance to various cryptanalytic attacks, thereby providing a viable solution for secure image transmission and storage in sensitive applications [30].

This study by Pavlos et al. (2015) investigates the intricate characteristics of the Major Histocompatibility Complex (MHC) DNA sequence by employing advanced mathematical and statistical tools. The research delves into the complexities of this crucial genomic region, exploring its inherent order, non-extensivity, and potential chaotic behavior. By analyzing the DNA sequence, the authors aim to gain deeper insights into the underlying mechanisms driving the immune system's remarkable diversity and its intricate relationship with various diseases. The experimental results reveal that DNA has a low-dimensional deterministic non-linear chaotic behavior [31].

This brilliant study by Zhang & Wang (2019) presents a novel multiple-image encryption algorithm that synergistically integrates DNA encoding and chaotic systems. By capitalizing on the inherent properties of chaotic maps, such as ergodicity and sensitivity to initial conditions, the scheme effectively permutes and modifies pixel values, while DNA encoding introduces a layer of biological-inspired complexity. This combined approach aims to achieve a vigorous and secure encryption solution for multiple images by significantly expanding the key space, enhancing sensitivity to minor key variations, and minimizing statistical redundancies within the encrypted data, thereby providing a viable solution for secure multi-image transmission and storage in various applications [32].

The research by Han et. al. (2024) explores the complex dynamics of the (2+1)-dimensional Beta-fractional double-chain DNA system, focusing on the emergence of chaotic patterns and solitary wave solutions. Through a combination of analytical and numerical methods, the study investigates the influence of fractional derivatives on the system's behavior, revealing intricate patterns and solitary wave solutions. These findings contribute to a deeper understanding of the complex interplay between nonlinearity, fractional calculus, and spatial dimensions in the context of DNA dynamics, potentially offering novel insights into the mechanisms underlying DNA replication and repair processes [33].

De Dieu et. al. (2022) presented a novel chaotic system distinguished by the absence of linear terms, leading to intricate and potentially unpredictable dynamical behavior. The study comprehensively analyzes the system's dynamics, including equilibrium point analysis, stability investigations, bifurcation diagrams, and Lyapunov exponent calculations. Furthermore, the research explores the practical implications of this novel chaotic system, demonstrating its potential utility in the field of DNA-based image encryption. By leveraging the inherent randomness and sensitivity to initial conditions exhibited by this system, the authors proposed a novel image encryption scheme that capitalizes on the unique properties of this non-linear dynamical system [34].

Chai et. al. (2019) research introduces a novel color image cryptosystem that effectively integrates dynamic DNA encryption with chaotic systems. After decomposing the colored image into Red, Green and Blue components, a Simultaneous Intra-Inter-Component Permutation Mechanism Dependent On The Plaintext (SCPMDP) is created to reorder them. The study also suggests that using random numbers in diffusion process will introduce additional complexity to the encoding process. This step is again followed by a confusion step and then SHA 384 hash function is combined to form one-time pads to further strengthen the encryption algorithm [35].

This research by Dagadu, Li & Aboagye (2019) presents a novel medical image encryption algorithm that integrates two chaotic systems- Bernoulli shift map and Zizag map with DNA. The process is bifurcated into two steps: key generation using chaos theory and diffusion using DNA. The two key metrices generation is achieved using MD5 hash function on plain image and two defined chaotic functions which is followed by DNA XOR operation applied alternative to finally obtained the ciphered image. This hybrid approach aims to achieve robust and secure encryption for medical images by capitalizing on the inherent properties of chaotic systems and DNA-based operations, thereby providing a viable solution for safeguarding sensitive medical data during transmission and storage [36].

An excellent research by Tokarev (2024) provides a comprehensive exploration of the intricate and often counterintuitive dynamics observed within living organisms. The work delves into the emergence of chaotic behavior within biological systems, investigating phenomena such as neural oscillations, cardiac rhythms, and population fluctuations. By examining the complex interplay between numerous interacting components, the research highlights the significance of chaotic dynamics in shaping biological processes, offering valuable insights into the emergent properties of living systems and their potential implications for various fields, including medicine and ecology [37].

Eldin et. al. (2023) introduced a novel cryptographic hash function that leverages the combined strengths of improved chaotic maps and DNA-based operations. The suggested scheme integrates multiple modified chaotic maps, including the Tent map, Cubic Tent map, and Logistic map, to enhance the complexity and unpredictability of the hash function. Also, design doctrine of two vital hash schemes- SHA-256 and RIPEMD-160 are studied in this paper to create a new and robust hash algorithm. Out of fifty-five discrete 1-D chaotic maps, four optimal 1-D maps were selected namely- TSS, CLM, LSS and hybrid. The amalgamation of these selected chaotic maps and DNA enhances the complexity of the correlation between plaintext and hash digest i.e., maximizing the protection level, and minimizing its vulnerabilities [38].

El-Meligy et. al. (2022) research introduced an innovative dynamic mathematical model for hash functions, integrating DNA algorithms and chaotic maps. This innovative approach leverages the inherent unpredictability of 1-D discrete chaotic maps mixed with DNA features to improve the SHA-512 hash buffer function. The study includes five types of 1-D maps- improved logistic, CLM, TSS, LSS, & hybrid; and based on these four diverse structures can be formed to boost performance of SHA-512. The authors claim that this dynamic approach improves the security and robustness of the hash function, making it a promising candidate for secure data integrity and authentication applications [39].

The original research by Alawida et. al. (2021) presented a novel cryptographic hash function that integrates a chaotic sponge construction with DNA sequence operations. DNA sequence is used to outline state modification rules of a deterministic chaotic finite-state automata (DCFSA). The incorporation of DNA sequence operations and hash function reduces number of message blocks, further increasing its security against various cryptanalytic attacks. This innovative approach demonstrates the potential of combining chaotic systems and bio-inspired operations to design robust and secure cryptographic hash functions with enhanced collision resistance and pre-image resistance [40].

This study by Zefreh (2020) presents a novel image encryption scheme that integrates DNA computing, chaotic systems, and hash functions. Here, DNA is applied both at confusion and diffusion stages. In confusion step, a mapping function built on the logistic map is employed on the DNA image to randomly transform the arrangement of elements. Successively, the diffusion is achieved by DNA left-circular shift and DNA right-circular shift operations to diffuse the DNA key on image to further enhances the security and complexity of the encryption process. This hybrid approach demonstrates the potential of combining diverse cryptographic primitives to achieve a high level of security for image data, offering a promising solution for faster and secure image encryption [41].

This study by Patel, Bharath & Kumar (2020) introduced a novel symmetric-key image encryption algorithm that integrates 3-D chaotic systems with DNA encoding techniques. To initialize the 3-D maps, three symmetric keys are utilized- 32-bit ASCII key, Chebyshev chaotic key and prime key. The complex dynamics of 3-D maps (as depicted in figure 7 below) are then employed to do row-wise permutation, column-wise permutation and secret key image. This process is followed by the diffusion step which involves DNA XOR operation between key image and plain image. All the performance metrices exhibit that the given hybrid approach is better than the state-of-the-art methods [42].

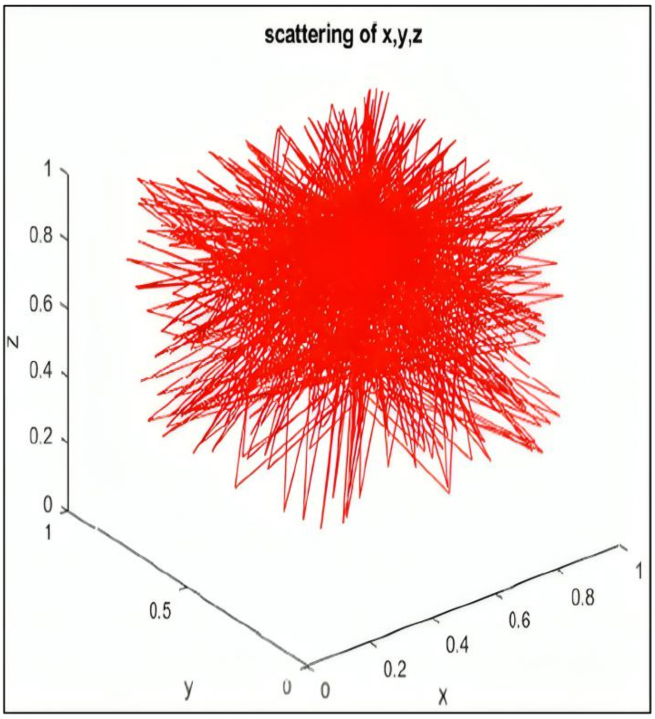

Fig 7. Chaotic Behavior of 3-D Logistic Map [42]

4. RESULTS AND DISCUSSION

As discussed in the previous section, this survey work covers only imperative research papers from the last decade. These papers were selected chiefly on the basis of their title and abstract before proceeding towards full-text reading. Other elements that were undertaken for paper selection are listed in the table 5 below.

Table 5. Data Extraction Elements

Data Item	Description
Title	Title of the Research Paper
Database	Name of online database from which research paper is downloaded
Year	Year of publication
Goal	Primary goal of the study
Publication Type	Book/ Journal/ Conference

Since the advent of DNA cryptology, multiple other security mechanisms have also been amalgamated with them to further strengthen the enciphering algorithms and one such technique is the use of chaotic functions with DNA operations. One of the key findings of the review is that researchers are more keen on using DNA operations for encryption of digital images. Both colored images and greyscale images have been popular in these encryption standards. Also, a majority of these papers not only add chaotic systems to add complexity, but also mix varied hash functions. Out of these SHA-256 and SHA-512 are the most utilized hash functions.

The following table 6 underlines the primary goal or highlights of the research paper under consideration in a chronological order.

Table 6. Highlights of Research Papers in Chronological Order

Primary Discussions	Author & Year
Complexity, Tsallis non-extensive statistics and Chaos in Major Histocompatibility Complex (MHC) DNA sequence	Pavlos et. al. (2015)
Colored Image Encoding using DNA OTPs + hyper-chaotic maps. Also, Lorenz system is used for creating secret keys	Li et. al. (2016)
DNA encoding + Central Dogma of Molecular Biology (Transcription + Translation) for text encryption	Basu et. al. (2019)
DNA + Chaotic functions + SHA-384 hash function for encoding of colored digital images	Chai et. al. (2019)
Encryption of colored medical images with DNA-XOR operation + 2 chaotic systems (zigzag map & Bernoulli shift map) + MD5 hash function	Dagadu, Li & Aboagye (2019)
Enciphering of Grayscale Images using DNA encoding + Chaotic Systems + SHA-256 hash function	Zhang & Wang (2019)
DNA sequence based Linear Feedback Shift Register + SHA-512 hash function + 3 chaotic systems (PWLCM, Lorenz and 4D Lorenz-type) for colored image encryption	Samiullah et. al. (2020)
DNA addition operation for diffusion & Hyper-chaotic sequences for confusion in colored images enciphering	Ciu et. al. (2020)
DNA + SHA-512 hash function + Chaotic maps for grayscale image encryption	Khan et. al. (2020)
Encoding of grayscale images using DNA encoding & 3-D chaotic maps, where 2 dimensions are used for confusion & 1 dimension is for key generation	Patel, Bharath & Kumar (2020)
Grayscale Image encryption using DNA operations (circular shift left & right) + Chaotic systems + Hash functions	Zefreh (2020)
Use of Deterministic Chaotic Finite State Automata (DCFSA) along with DNA to form sponge-based hash function for encoding textual data	Alawida (2021)
Wavelet transform and Chaotic systems employed with DNA operations in grayscale image encryption	Pourasad, Ranjbarzadeh & Mardani (2021)
Substitution-Boxes (S-Box) based on the Choquet Fuzzy Integral (CFI) and DNA techniques employed for digital image encoding	Mohamed, Korany & El-Khamy (2021)
DNA pseudo symbols from GenBank + Chaotic Maps for encoding of Images	Gasimov & Mammadov (2021)
DNA + 32-bit hash function + 2-D Sine Logistic Modulation Map (SLMM) for encryption of grayscale images	Naskar et. al. (2021)
DNA coding + 3-D chaotic systems for Image encoding that offers greater key space	Da Dieu et. al. (2022)
Text encryption using DNA sequences + 5 selected 1-D chaotic maps (improved logistic, CLM, TSS, LSS, & hybrid) + SHA-512 hash function	El-Meligy et. al. (2022)
Image encryption standard based on chaotic function + DNA Playfair Matrix + Feistel structure	Ibrahim et. al. (2022)
Colored Image Encoding using 4-D chaotic systems for confusion + DNA operations (XOR, Addition, Subtraction, Shift-Right & Shift-Left) for diffusion	Shakir, Mehdi & Hattab (2022)
DNA operations + 512 hash function + Lorenz Chaotic function-based image encryption	Singh & Singh (2023)

DNA + 4 chaotic maps (improved logistic, TSS, CLM, LSS & hybrid) + combination of SHA-256 & RIPEMD-160 hash functions to strengthen the blockchain methodology	Eldin et. al. (2023)
Study of Chaos Patterns & Solitary Wave Solutions for (2+1) Beta-fractional double chain DNA	Han et. al. (2024)
Chaotic Image Encryption Algorithm with an Improved Bonobo Optimizer and DNA Coding	Almasoud et. al. (2024)
Importance of chaotic dynamics in shaping biological processes in living organisms	Tokarev (2024)

Another important finding of this study is that chaotic systems are mostly used in the scrambling or the confusion steps which is used for altering the positions of elements (either pixels or blocks of pixels). Another common use of chaotic functions is for generation of secret keys, which are used in the diffusion process along with DNA-based operations. The most frequent used DNA operations are XOR, addition and subtraction. Also, in some cases the circular-shift-right and circular-shift-left operations are also utilized to bring complexity in the cryptographic algorithm. Additionally, most of the cryptographic standards proposed by the elite academicians is requirement of larger key space which provides extra refuge and resilient to standard attacks like brute-force attack, known plaintext attack, etc. Almost all research papers highlighted that the produced histograms are uniform in nature indicating labyrinthine pattern recognition for attackers. The evaluation of Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) provides valuable information regarding the balance between the strength of encryption and the level of image distortion introduced. Lower Peak Signal-to-Noise Ratio (PSNR) values typically correspond to higher levels of encryption-induced distortion, a characteristic generally desirable for robust and secure encryption. Similarly, the entropy measures also reveal ideal randomness, which is the desired factor for enciphering.

5. CONCLUSION

This review paper delves into the synergistic relationship between DNA cryptography and chaotic systems, exploring their combined potential to enhance data security in the face of evolving threats. DNA cryptography leverages the unique properties of DNA molecules, such as massive storage capacity and inherent molecular operations, to encode and manipulate information at the molecular level. Chaotic systems, characterized by extreme sensitivity to initial conditions and complex, unpredictable behavior, offer a powerful tool for generating pseudo-random sequences and introducing non-linearity into cryptographic algorithms. The review examines various techniques that integrate these two paradigms, including DNA-based encryption schemes utilizing chaotic maps for key generation and data scrambling, as well as the application of chaotic dynamics to control and manipulate DNA operations for secure information processing. The paper also discusses the challenges and limitations associated with this interdisciplinary approach, such as the practical difficulties of implementing DNA-based computations and the potential vulnerabilities arising from the inherent stochasticity of biological systems. Finally, the review explores potential future directions for research in this field, including the development of novel DNA-based cryptographic primitives, the integration of chaotic functions principles, and the exploration of potential applications in emerging areas like DNA-based encryption and molecular communication.

6. DECLARATIONS

Conflict of interest - The authors declare that they have no conflict of interest.

7. REFERENCES

[1] Pal, S. K., & Mishra, S, "Revolutionary Change in Cryptography", *Invertis Journal of Renewable Energy*, 2019, *9*(2), 43-54.

[2] Sinha, P., kumar Rai, A., & Bhushan, B. 2019, July. Information Security threats and attacks with conceivable counteraction. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 1208-1213). IEEE.

[3] Mahender Kumar, "A Brief History of Cryptography: From Ancient Times to the Quantum Era", Publication Date: Jul 15, 2023, Accessed on: Nov 11, 2024, Available online at https://medium.com/@mahend72kr/a-brief-history-of-cryptography-from-ancient-times-to-the-quantum-era-f773b29a8039.

[4] Easttom, W. (2022). *Modern cryptography: applied mathematics for encryption and information security*. Springer Nature.

[5] Martin, K. (2020). *Cryptography: The key to digital security, how it works, and why it matters*. WW Norton & Company.

[6] Christensen, C. (2020). Review of The Enigma Bulletin edited by Zdzisław J. Kapera. *Cryptologia*, *44*(6), 569-572.

[7] Mohamed, K. S. (2020). *New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA*. Springer Nature.

[8] Aziz Alizadeh, "Attractors: the Platform for Creating New Futures in Chaotic Systems", Publication Date: Jul 21, 2022, Accessed on: Nov 25, 2024, Available online at https://extendednows.com/attractors-the-platform-for-creating-new-futures-in-chaotic-systems/

[9] Chen, G, "Chaos theory and applications: a new trend", *Chaos Theory and Applications*, 2021, *3*(1), 1-2.

[10] Figg, C. A., Winegar, P. H., Hayes, O. G., & Mirkin, C. A, Controlling the DNA hybridization chain reaction. *Journal of the American Chemical Society*, 2020, *142*(19), 8596-8601.

[11] Kaushik, A., Thada, V., & Singh, J. (2021). VG2—DNA-Based One-Time Pad Image Cipher. In *Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2020* (pp. 557-568). Springer Singapore.

[12] Betsy, C. J., & Siva, C. (2023). Mutations and Their Implications. In *Fisheries Biotechnology and Bioinformatics* (pp. 27-33). Singapore: Springer Nature Singapore.

[13] Weickert, P., & Stingele, J, "DNA–protein crosslinks and their resolution", *Annual Review of Biochemistry*, 2022, *91*(1), 157-181.

[14] Leung, H. Y., Yeung, M. H. Y., Leung, W. T., Wong, K. H., Tang, W. Y., Cho, W. C. S., ... & Wong, S. C. C, "The current and future applications of in situ hybridization technologies in anatomical pathology", *Expert Review of Molecular Diagnostics*, 2022, *22*(1), 5-18.

[15] Floriano, I., Silvinato, A., Bernardo, W. M., Reis, J. C., & Soledade, G. (2020). Accuracy of the Polymerase Chain Reaction (PCR) test in the diagnosis of acute respiratory syndrome due to coronavirus: a systematic review and meta-analysis. *Revista da Associação Médica Brasileira*, *66*, 880-888.

[16] Biswas T., "Optimizing PCR: Proven Tips and Troubleshooting Tricks", Publication Date: Feb 23, 2024, Accessed on: Nov 23, 2024, Available online at https://www.the-scientist.com/optimizing-pcr-proven-tips-and-troubleshooting-tricks-71660.

[17] Syaifudin, M. (2021, April). Gel electrophoresis: The applications and its improvement with nuclear technology. In *AIP Conference Proceedings* (Vol. 2331, No. 1). AIP Publishing.

[18] Basu, S., Karuppiah, M., Nasipuri, M., Halder, A. K., & Radhakrishnan, N, "Bio-inspired cryptosystem with DNA cryptography and neural networks", *Journal of Systems Architecture*, 2019, *94*, 24-31.

[19] Cui, J. X., Li, G. D., Wang, L. L., & Ma, C, "Colour image encryption algorithm based on hyperchaos and DNA sequences", *International Journal of Information and Communication Technology*, 2020, *16*(3), 230-244.

[20] Pourasad, Y., Ranjbarzadeh, R., & Mardani, A, "A new algorithm for digital image encryption based on chaos theory", *Entropy*, 2021, *23*(3), 341.

[21] Samiullah, M., Aslam, W., Nazir, H., Lali, M. I., Shahzad, B., Mufti, M. R., & Afzal, H, "An image encryption scheme based on DNA computing and multiple chaotic systems", *IEEE Access*, *8*, 2020, 25650-25663.

[22] Ibrahim, D., Ahmed, K., Abdallah, M., & Ali, A. A, "A new chaotic-based RGB image encryption technique using a nonlinear rotational 16× 16 DNA playfair matrix", *Cryptography*, 2022, *6*(2), 28.

[23] Shakir, H. R., Mehdi, S. A. A., & Hattab, A. A, "Chaotic-DNA system for efficient image encryption", *Bulletin of Electrical Engineering and Informatics*, 2022, *11*(5), 2645-2656.

[24] Li, X., Wang, L., Yan, Y., & Liu, P, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems", *Optik*, 2016, *127*(5), 2558-2565.

[25] Mohamed, A. G., Korany, N. O., & El-Khamy, S. E, "New DNA coded fuzzy based (DNAFZ) S-boxes: Application to robust image encryption using hyper chaotic maps", *Ieee Access*, *9*, 2021, 14284-14305.

[26] Naskar, P. K., Bhattacharyya, S., Mahatab, K. C., Dhal, K. G., & Chaudhuri, A, "An efficient block-level image encryption scheme based on multi-chaotic maps with DNA encoding", *Nonlinear Dynamics*, 2021, *105*(4), 3673-3698.

[27] Singh, A., & Singh, B, "An Efficient and Secure DNA based Image Encryption Technique", *International Journal on Recent and Innovation Trends in Computing and Communication*, 2023, 11 (8), 366-377.

[28] Khan, J. S., Boulila, W., Ahmad, J., Rubaiee, S., Rehman, A. U., Alroobaea, R., & Buchanan, W. J, "DNA and plaintext dependent chaotic visual selective image encryption", *IEEE Access*, *8*, 2020, 159732-159744.

[29] Almasoud, A. S., Alabduallah, B., Alqahtani, H., Aljameel, S. S., Alotaibi, S. S., & Mohamed, A, "Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security", *Heliyon*, *10*(3), 2024.

[30] Gasimov, V. A., & Mammadov, J. I. (2021, June). Image encryption algorithm using DNA pseudo-symbols and chaotic map. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-5). IEEE.

[31] Pavlos, G. P., Karakatsanis, L. P., Iliopoulos, A. C., Pavlos, E. G., Xenakis, M. N., Clark, P., ... & Monos, D. S. (2015). Measuring complexity, nonextensivity and chaos in the DNA sequence of the Major Histocompatibility Complex. *Physica A: Statistical Mechanics and its Applications*, *438*, 188-209..

[32] Zhang, X., & Wang, X, "Multiple-image encryption algorithm based on DNA encoding and chaotic system", *Multimedia Tools and Applications*, 2019, *78*(6), 7841-7869.

[33] Han, T., Zhang, K., Jiang, Y., & Rezazadeh, H, "Chaotic Pattern and Solitary Solutions for the (21)-Dimensional Beta-Fractional Double-Chain DNA System", *Fractal and Fractional*, 2024, *8*(7), 415.

[34] De Dieu, N. J., Ruben, F. S. V., Nestor, T., Zeric, N. T., & Jacques, K, "Dynamic analysis of a novel chaotic system with no linear terms and use for DNA-based image encryption", *Multimedia Tools and Applications*, 2022, *81*(8), 10907-10934.

[35] Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y, "A color image cryptosystem based on dynamic DNA encryption and chaos", *Signal Processing*, *155*, 2019, 44-62.

[36] Dagadu, J. C., Li, J. P., & Aboagye, E. O, "Medical image encryption based on hybrid chaotic DNA diffusion", *Wireless Personal Communications*, *108*, 2019, 591-612.

[37] Tokarev, M. CHAOTIC BIOLOGICAL SYSTEMS. *European Journal of Technical and Natural Sciences*, 10.

[38] Eldin, S. M. S., El-Latif, A. A. A., Chelloug, S. A., Ahmad, M., Eldeeb, A. H., Diab, T. O., ... & Zaky, H. N, "Design and analysis of new version of cryptographic hash function based on improved chaotic maps with induced DNA sequences", *IEEE Access*, *11*, 101694-101709, 2023.

[39] El-Meligy, N. E., Diab, T. O., Mohra, A. S., Hassan, A. Y., & El-Sobky, W. I, "A novel dynamic mathematical model applied in hash function based on DNA algorithm and chaotic maps", *Mathematics*, 2022, *10*(8), 1333.

[40] Alawida, M., Samsudin, A., Alajarmeh, N., Teh, J. S., & Ahmad, M, "A novel hash function based on a chaotic sponge and DNA sequence", *IEEE Access*, *9*, 2021, 17882-17897.

[41] Zefreh, E. Z, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions", *Multimedia Tools and Applications*, 2020, *79*(33), 24993-25022.

[42] Patel, S., Bharath, K. P., & Kumar, R, "Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique", *Multimedia Tools and Applications*, 2020, *79*(43), 31739-31757.