Grenze International Journal of Engineering and Technology, June Issue

Survey on DNA Encryption Techniques

Sowmya D[1] and Dr. Manjula G R[2]
[1]Assistant Professor, Department of CS&E, JNNCE, Shivamogga
[2]Professor, Department of CS&E, JNNCE, Shivamogga
Email: sowmyad84@jnnce.ac.in, grmanjula@jnnce.ac.in

***Abstract*— The area of DNA cryptography is an interdisciplinary field that has emerged recently, focusing on the possible applications of DNA (deoxyribonucleic acid) molecules for secure encryption and data storage. It uses DNA sequences to create methods for encoding, encrypting, and decoding data by fusing concepts from cryptography and molecular biology. This paper presents various works proposed in DNA encoding.**

***Index Terms*— Chaotic, tent map, renyi map, hyperchaotic, trellis algorithm, hyper-chaotic Lorenz, Chebyshev chaotic key.**

I. INTRODUCTION

Transfer of confidential data across the internet requires protection from the intruder. Converting this data into a form that is difficult to understand is a technique used to safeguard data. This process is termed as encryption. Encrypted data is transmitted over the network to the receiver. Receiver has to again convert encrypted data into an understandable format, the Decryption process. Adelman introduced DNA computing in cryptography. It uses the chemical nature of DNA series with classical cryptography to secures the data to be transmitted. DNA abbreviated as deoxyribonucleic acid which is the storehouse of all the genetic details of living organisms. DNA has a huge storage capacity, massive computing capability, and parallelism. Here the alphabet characters are changed to bases as, Adenine, Cytosine, Guanine, and Thymine. Each base is represented by using binary characters as A-00, C-01, G-10 and T-11. Fig. 1 shows composition of DNA.

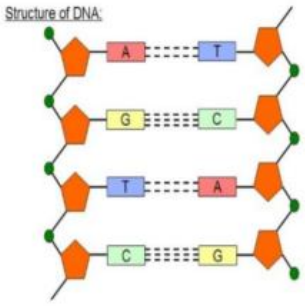

Figure 1: Structure of DNA

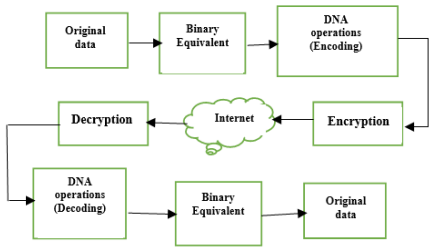

Figure 2: Block diagram of DNA encoding and decoding method

Fig. 2 shows the general procedure followed for the encoding and decoding of private data. The original data is transformed into binary then the DNA encoding operations are applied. This scrambled data is finally encrypted. This encoded data is transmitted to the receiver. On the recipient side, this data is decrypted, and DNA decoding

Grenze ID: 01.GIJET.10.2.241

operations are applied. The resultant is binary data that can be later converted into its original format. There are 2 types of cryptography—namely private, and public key cryptography. In private key encryption same keys are used for the encoding and decoding. Eg: DES, AES, Blowfish, etc,. Public key cryptosystem uses distinct keys for encoding and decoding. The foremost is a private key which is hidden from the world whereas the next one is a public key made public. Both the keys are alike but are mathematically related to each other. Eg: RSA, Elliptic key cryptography, SHA-2 etc., Among the possible uses for DNA cryptography are, safe Data Storage due to its high storage density and long-term stability. DNA-based encryption may be used to create secure communication channels. DNA sequences may provide random or pseudorandom information for the purpose of creating cryptographic keys. It is used in steganography to conceal hidden signals within DNA sequences

A. DNA Cryptography Methodologies

Different methods to encode the data are[15],

- *One-time Pad(OTP):* OTP follows generation of an arbitrary keys for encryption/decryption. A unique key is generated which is used only once.
- *Bio-molecular structure*: A three-dimensional arrangement of molecules which are the prerequisite for life processes is called as Bio-molecular structure. These are originally present in living organisms and play crucial roles in various biological functions. This structure is used in message encryption/decryption in data transmission.
- *Polymerase chain reaction (PCR):* It is a potent technique of molecular biology. It amplifies selected segment of DNA.
- *DNA chip technology*: Also known as DNA microarray technology or gene chips, is a powerful tool used in genomics and molecular biology to simultaneously analyze thousands of genes' expression levels.
- *DNA fragmentation*: Fragmentation is nothing but splitting of DNA strings into pieces which may be helpful in course of time.

B. Types of possible Attacks

Security-providing algorithms should be vulnerable to attacks. Different types are:

- *Brute force attack*: An attempt to use all the available keys to disrupt the system.
- *Plain text attack*: Alternate name is Meet in the Middle attack. Here an attacker attempts to find an intermediate value used to encode input text.
- *Side-channel attacks*: Here the physical implementation information is borrowed from a security algorithm.
- *Cipher text attack:* The attacker analyses the encrypted text to extract plain text from it.[1]

II. LITERATURE SURVEY

Here the literature review on various encryption algorithms are included.

In Ref. [2] a methodology presented is called as "Blum Blum Shub (BBS) generator" applied on block cipher. To enhance security the message to be shared is undergoing several DNA operations. This approach follows multiple levels of data processing. The first level includes two stages, key production and encoding of private data using DNA arithmetic operations. In the second level, Gen Bank is used to choose a DNA reference, based on the key's specification, size, and location of the blocks that are selected. Various procedures are followed on these chosen blocks to attain higher security to the block of DNA against various attacks. At the final level, the 2-bit value is chosen on the basis of the Knight tour movement as in the Hadamard matrix. Double-level security is expected from this method. The suggested scheme's security analysis and robustness have been provided and debated. It has been shown that there is very little chance for guessing attackers to recover the original plaintext, indicating very good security.

Ref. [3] proposed a methodology where a randomly generated key is generated at the sender each time which makes it robust against various attacks. Here the given text file, image or audio file can be converted into ASCII form and later into Unicode. This Unicode is transformed into hexadecimal then into binary and finally into DNA digital code. The DNA digital code is substituted with the amplified data using the standard table. The receiver must decrypt the data to decode the original message. This approach provides 2 stage security, high reliability, and robust against different types of attacks. It is challenging to defeat the suggested strategy using standard cryptanalysis methods. Better time, computational complexity, and enhanced dependability are all provided by this method.

The symmetric key cryptography method presented in Ref. [4] where a 1D discrete chaos and DNA encoding methods are used for image encryption. Chaotic maps encode secret images as DNA sequences, resulting in a

cipher image. According to this, two DNA-encoded images that the current approach handles are i) one that is created from the provided plain image and ii) one that is derived from the key image. Renyi map as in (1) is utilized to create the key image, and the Tent map as in (2) is used to design the DNA encoder. Initial parameters are necessary for any chaotic map to obtain the random sequences. Although they should be inside the domain, the starting parameters might be chosen at random. The starting parameters in this approach are generated using the plain image. The plain image is subjected to the SHA-256 procedure for this purpose.

$$\left.\begin{aligned} F(x_n, a, b) &= \tan(x_n)(1 + x_n) \times b + (1 - x_n)x_n \times a \\ x_{(n+1)} &= \text{fraction}(F(x_n, a, b)) \times \alpha \end{aligned}\right\} \quad (1)$$

where a, b ∈ [0, 10] and α ∈ (0, 12345].

$$x_{(n+1)} = r \min\{xn, 1 - xn\} \quad (2)$$

where x_0 is the initial value, $x_i \in [0, 1]$ and $r \in [0, 2]$.

It's possible that the first segment of the sequence produced by the chaotic map is not entirely random. So the first thousands of items in the sequence are disregarded; the remaining portion is then regarded as the sequence that the map generated and will be utilized in the experiment. It is anticipated in this design that once a sequence is utilized for a certain purpose, the corresponding portion will be used for future requirements and the removed portion will be kept in the series.

Ref. [5] introduced a methodology where Genetic Algorithm in conjunction with the Needleman-Wunsch (NW) algorithm is used along with the method for implementing encryption and decryption based on DNA computing using biological operations such as transcription, translation, DNA sequencing. DNA cryptography with deep learning method is followed to encode and decode the given information. The primary text(P) is encoded into DNA nucleotide(P') and transcript text T, representing the mRNA is produced as a result of complementing the current encoded text P'. The tRNA's complementary strand carries the amino acids. 64-bit mRNA, tRNA, and amino acid are blocked into a group of 8 bits and transformed to decimal. Sequence of permuation and bitwise XOR as per Vernam cipher gives M whose hexadecimal equivalent is ciphertext.

A security system is proposed in Ref. [6] for cloud data using a methodology termed as "binary version of DNA cryptography(BDNA)". A randomly shuffled encoding table is referred to encode given text. The outcome is a 7-bit sequence of binary numbers. After dividing this sequence into 2 halves, left and right shifts are applied on each block respectively. Later interchange these halves and divide them into 6-bit blocks. Add padding bits if necessary. By using one more encoding table, generate the final cipher text. Results say that this method is productive in terms of space, time, and throughput. Secure against chosen plaintext attack.

In Ref. [7], an approach is proposed for using a DNA-based key to authenticate the users of the cloud/network applications. The entire system is summarised as three stages namely, generation of key, arbitrary key creation, and encryption/decryption. Here the given plaintext is converted into ASCII equivalent whose binary equivalent is encoded into DNA sequence as A-00, T-01, G-10, and C-11. The resultant DNA code pattern is converted into a random key(P_k) using a table. The outcome of this stage is an encrypted password or secret key. The exact reverse order procedure is followed to decode the encrypted key. Comparitively this method spares a small amount of time.

Ref. [8] presented a methodology as per which DNA is used as the carrier of information instead of images, audio, or video. As per this technique, the digital data is transformed into 0's and 1's and DNA bases are formed from this. This data is split into groups and then compressed using certain rules. After this resultant data is encoded with the usage of Feistel network. The decoding procedure follows the reversal of the encoding procedure to obtain original data. This approach has an efficient outcome capacity. It can stand strong for brute force attacks, keyspace, and entropy. But the private key approach is not secure and it requires new techniques to speed up the time taken for processing and synthesis. Improvement in the robustness is required.

Ref. [9] put forth a methodology lying on the foundation of trellis algorithm. An arbitrary key is produced by the recipients during communication. Here security is provided at two levels. Initial security is ensured by an arbitrary key agreed between the recipients. At the second level trellis algorithm is utilized for encoding the data in combination with DNA sequences. Binary conversion, key generation in random, and encryption are the three main tasks to be considered. Given data is transformed to ASCII equivalent and the outcome is grouped into 7-bit binary. An arbitrarily selected nucleotide of DNA series acts as a random key. As a part of the final stage, encode the data using the trellis algorithm and it results in the trellis encoded data. A trellis-encoded results and the DNA series are XORed. Finally, encoded data is obtained for safe communication between the transmitter and receiver.

Data is decoded and sent to its primary format at the recipient side. This approach is suitable to resist brute force and timing attacks.

In Ref. [10], a symmetric picture encryption technique is created using a novel plaintext-related mechanism based on the peculiarity of plaintext DNA coding (PPDC). Four chaotic sequences are generated by the use of a hyper-chaotic Lorenz system as in (3). First, the original picture is encoded to acquire the image DNA coding and PPDC by utilizing one chaotic sequence to govern the DNA rules. Next, another chaotic sequence is encoded into a DNA sequence, which is employed in the DNA XOR operation. The final two chaotic sequences are processed using the PPDC to produce two key streams that are utilized in the permutation step. The cipher picture is obtained by running the DNA XOR operation and the conventional permutation operation. The encryption system has higher plaintext sensitivity and security due to the usage of the PPDC, which links the key streams utilized in the permutation stage to the secret keys and plaintext picture. The security analysis and simulation experiment findings show that the suggested encryption system has good security and efficiency and can successfully fend off a variety of common assaults, including statistical, differential, and exhaustive attacks.

$$\left.\begin{aligned} x^{\cdot} &= a(y - x) + w \\ y^{\cdot} &= cx - y - xz \\ z^{\cdot} &= xy - bz \\ w^{\cdot} &= -yz + rw \end{aligned}\right\} \qquad (3)$$

where parameters a = 10, b = 8/3, c = 28, $-1.52 \leq r \leq -0.06$, and the hyper-chaotic Lorenz system is chaotic.

In Ref. [11] usage of a 3D chaos logistic map strengthens the encryption technique. Three symmetric keys are utilized: the prime key, the Chebyshev chaotic key, and the 32-bit ASCII key. To create beginning conditions, the algorithm initially uses a 3D non-linear logistic chaotic map with three-column symmetric keys. Then, to provide randomness to the pixels, these criteria are applied to the row and permutations of the image. The key image is produced using the third chaotic sequence that the 3D map produces. DNA encoding is used to diffuse these random pixels, and an XOR logical operation is then applied between the key picture and the input image encoded with DNA. The suggested algorithm's analysis parameters, such as NPCR, UACI, entropy, histogram, chi-square test, and correlation, are computed and compared with several currently used encryption techniques.

Utilizing the Huffman coding technique, a novel and effective symmetric DNA encryption scheme was created in Ref. [12]. The primary key, or a DNA strand of choice, must initially be shared by both parties. Three parameters (Start Pos, Nbr Bases, and a round NR1 number) comprise the secondary key. The primary key uses the Huffman coding method to code short sequences of four bases starting at the Start Pos location and continuing until a binary sequence with the same image length (L_M) is obtained. The binary plain-image M and the sequence S, both of which have the same length, are subjected to an XOR operation in the second phase. Consequently, a binary sequence representing the encrypted image C1 is obtained. The received message will be diffused to fortify the encryption and to do so, the permutation box is employed. Each block of 16 bits that make up the encrypted sequence C1 will be an entry in the permutation box. The permutation function works based on 16 bits, which include 8 even locations (2, 4, 6, 8, 10, 12, 14, 16) and 8 odd positions (1, 3, 5, 7, 9, 11, 13, 15). The odd positions will be taken in decreasing order after the even spots are taken in increasing order. Eventually, the encrypted image's binary sequence C is discovered.

Ref. [13] introduced a hyperchaotic system planted on symmetric encryption. The encryption algorithm includes five main stages. The conservative hyperchaotic system is iterated to generate four chaotic sequences, {x, y, z, w}, each with a length of L (L is the total number of pixels in the image to be encrypted). The four chaotic sequences are then connected to form a chaotic sequence X with a length of 4L. Lastly, the chaotic real number sequence X is transformed into an integer sequence IntX. These initial values (x0, y0, z0, w0) and the system parameters (a, b, c) are input in stage (1). In step (2), the DNA coding picture is created by encoding the original image using coding rule r1. Index scrambling is used in step (3) to alter the DNA characters' locations for every row in the DNA coding picture. In step four, dynamic DNA operations are carried out using the DNA coding picture and chaos sequence, and pixel diffusion is accomplished by applying the principles of DNA addition, subtraction, and xor. DNA dynamic decoding is used in step (5) to produce the cipher image. The starting values of the conservative hyperchaotic system (x0, y0, z0, and w0) are part of the cryptosystem's secret key set. The images of the plaintext are represented by P_{MXN}, the DNA coding image by PCMX4N, the DNA coding sequence after row permutation by $P1_{1\times4MN}$, the DNA coding sequence after diffusion by $P2_{1\times4MN}$, and the final ciphertext image by $C_{M\times N}$. All P_{MXN} and C_{MXN} are M × N matrices.

The "dynamic sequence table" and "dynamic DNA encoding" are two dynamic mechanisms-based DNA cryptography techniques that are proposed in Ref. [14]. To create a dynamic sequence table, 256 ASCII characters are first randomly assigned to each DNA base sequence. DNA base sequence locations are rearranged iteratively according to a mathematical series in order to achieve dynamism. Similarly, to create dynamic DNA encoding, the

number of DNA bases needed to combine the ciphertext of each of the two chunks is determined dynamically by utilizing the NCBI bank genome sequence in conjunction with a mathematical series. This encryption process involves converting the plaintext into DNA bases, assigning them to ASCII characters using a dynamic sequence table, splitting the data into a limited number of chunks, encrypting each chunk using an asymmetric cryptosystem, and finally combining the chunked ciphertext via dynamic DNA encoding. Thus, it is evident that using dynamic mechanisms in conjunction with an asymmetric cryptosystem raises the data's level of secrecy.

Ref. [15] put forth a secure communication approach in a Wireless sensor network. This methodology uses chronological order to translate input plain text into its numerical equivalent. then encrypts using RSA, a public key cryptosystem. Next, translates the binary equivalent of the prime cipher to its Base-4 equivalent. Then converts the binary data to a nucleotide of DNA. Later creates a fake sequence that complies with the nucleotide bases produced during the PCR procedure. A series of data encrypted as DNA nucleotide is the result of the encryption process. The other strand of the DNA is created by using the encrypted DNA sequence as one strand. By matching each nucleotide base with its complementary counterpart, a fake sequence is created. As a result, base A generates fake base T, and vice versa. The bogus base that is constructed for base C is G. Every DNA nucleotide of the encrypted message is suffixed with a complimentary base to form the structure of the DNA strand. Data compression is an encoding technique that significantly lowers the number of bits needed to transmit data. The data has been compressed using two stages:

1. Using DNA base binary scheme
2. Using the Huffman encoding technique.

De-hybridization and decompression are used at the receiving node to retrieve the original cipher, which is then decrypted to recover the original data. Security is achieved here in several stages.

Ref. [16] presents the invention of an asymmetric image encryption technique based on hyperchaotic system and DNA coding. To address these issues, three stages are investigated as follows, in contrast to existing picture encryption techniques, such as sharing of the same private keys between the sender and recipient and set rules with straightforward operation. In order to mitigate any potential risks associated with key transmission and management, the RSA (Rivest-Shamir-Adleman) algorithm and the plain image are used to generate the initial values of the hyperchaotic system. This involves computing the sum of odd rows, even rows, odd columns, and even columns in order to extract the plain message from the plain image and feed it into the RSA algorithm. After that, a mathematical map is created to convert each of them into the hyperchaotic system's initial values. Second, the image is confused using pixel-level permutation in accordance with the chaotic sequences that are produced. Lastly, dynamical DNA encryption is intended to disperse the permuted image in order to address the issue of fixed rules with straightforward operations in existing DNA-based image encryption techniques. DNA coding, DNA operation, and DNA decoding are all steps in the DNA encryption process. Specifically, DNA rules are not fixed rules with straightforward operations, but rather are selected dynamically based on chaotic patterns. Numerical simulations and theoretical research demonstrate the security and dependability of the suggested approach for picture encryption.

Asymmetric encryption on Arabic plaintex is proposed in Ref. [17]. The Arabic Plian Text material is divided alphabetically into groups of sixteen characters. There will be a Dynamic DNA Sequence Table created. By substituting the next letter for each one in relation to the matching DNA base sequence, each block is transformed into a DNA sequence. The DNA B1 and B2 sequences will be transformed into binary bit format in this stage by substituting: A=00, T=01, C=10, and G=11. Create the Fibonacci series using E1 as the initial series number, then utilize it to generate the RK_1 round key. RK1 should be divided into several 64-bit parts, C_1, C_2, C_3,..., and C_L. The number L in this case denotes the quantity of pieces contained in the RK_1 key. Assign $B1=B1 \oplus C_j$. Repeat this for each j=2, 3,..., L. The preceding step is repeated, and each time an XOR operation is carried out on B2 and sections C1, C2, C3,... CL. The stages from 5 to 9 will be repeated for the remaining round keys RKi, i = 2, 3,... 14. Both B1 and B2 will be transformed into a DNA sequence. After selecting Decryption Starting Key CT is shared with the reciever. Because dynamic data, data dependencies, dynamic round keys, and encoding tables are used, hackers cannot extract the input plaintext from the receiving text, or ciphertext.

Ref. [18] includes an asymmetric encryption approach where blocks of some fixed size are formed by using text data. A dynamic DNA sequence table is generated using which given text data is transformed into a sequence of DNA. This block is then changed to binary format. This block is XORed with the generated round key. Set the start decryption key(SDK) and convert it to a series of 0's and 1's and later to DNA sequence. Sandwich these blocks together with SDK which results in ciphertext. A reverse procedure is followed to gain the plaintext from the encrypted text. This method has a strong avalanche property. Since this approach uses a dynamic table for encoding, it is tedious job for an attacker to extract plain text. The avalanche property of the suggested encryption algorithm is excellent.

By combining the hyper-chaotic system (HCS), deoxyribonucleic acid (DNA) level operation, Arnold transform (ART), and phase-truncated fractional Fourier transform (ptFrFT), a novel asymmetric image encryption technique is devised in Ref. [19]. The primary values and control variables are produced from SHA-256 hash algorithm. An important technique followed here is to scramble the primary image using ART and then encoded using ptFrFT using the keys generated from HCS. Now it looks like a noise. Ciphertext is generated by using DNA diffusion and scrambling. This system is can afford different attacks.
Ref. [20], suggested a novel method for encrypting images that is based on four distinct algorithms. This approach combines symmetric and asymmetric encryption techniques with scrambling to produce a meaningless or disorganized image that improves security by strengthening its resistance to attack. This method's primary goal is to secure an image through the use of several encryption algorithms. Four encryption algorithms—two symmetric key and one asymmetric key—are employed here. Using this technique, a picture is split into four blocks, denoted B1, B2, B3, and B4. For B1 and B2, asymmetric key algorithms like RSA and DNA are used. DES and Chebyshev, two symmetric key algorithms, for B3, B4. Arnold Cat Map is used to muddle the original image, and natural DNA sequence K1 is used to obtain a frequency value. Next, a fresh picture and three DNA templates are produced by XORing the other DNA sequence, K2. After K2 is rotated by 900, the second DNA sequence produces the DNA template K3. After that, K3 can be further rotated by 900 to create the DNA template K4. In this approach, the grey value consists of four bases. When binary stream coding DNA sequences, DNA Digital Coding Technology replaces A, G, C, and T with 00, 01, 10 and 11. This results in the representation of two binary digits in a single base. With DNA Digital Coding Technology, two binary digits are represented in one base, with A, G, C, and T being substituted by 00, 01, 10 and 11. The range of gray values for any pixel in the binary stream coding of the DNA sequences is 0-255, or 00000000-11111111. The outcomes of the DNA Algorithm for two distinct pictures.
Ref. [21], an approach is proposed to secure the outcome of the IoT devices that are sent to the outside world. The suggested DNA-based technique is a block cipher that modifies the Source Image's bytes by transposing and substituting them. The SImage needs to be divided into N segments, each of which is 1 byte in size (B1, B2,..., Bn), before the substation phase is applied. After that, perform an XOR operation on the DNA segments of Sk (k1,k2,...,kn) and the I byte (B1, B2...Bn) of SImage segments. New bytes (A1, A2,..., An) are formed by the XOR operation, and this process is repeated N times. The final result of the entire process will be new AI bytes. In the transposition process, some of the resulting AI bytes are switched. The Sk bytes produced from the DNA sequence and the set of rules indicated in Table 1 provide the basis of the bits swapping procedure that is carried out on A (A1, A2,...., An). In Figure 2, A1 denotes one byte of the result substitution and AT1 byte represents the result of transposition operation. For instance, if the first two bits in A1 are 00 (DNA letter A) and the last two bits are 01 (DNA letter T), then don't swap them. Alternatively, if the third and fourth bits of A1 were 01 and 11, then swap these bits. Until the entire SImage is encrypted (EImage), this process is repeated.

TABLE I. SWAPPING RULES

DNA sequence letter	DNA sequence letter	Operations
A	T	Don’t Swap
C	G	Don’t Swap
T	T	Swap
T	G	Swap
G	G	Swap
A	T	Don’t Swap

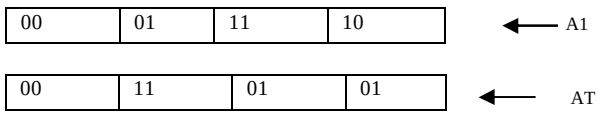

Figure 3. Transportation Example

Transposition is the first step in the decryption process, followed by substitution. Beginning with the final byte of the encrypted image (EImage), the decryption procedure works its way down to the encrypted picture's first byte. Since swapping rules in table 1 must be shared by the image's sender and recipient, the transposition phase restores the swapped bits to their original positions. Following the transposition phase, the substitution phase is initiated by applying an XOR operation to the final bytes of the DNA sequence and the final bytes of the EImage, where the sender of the EImage terminated the replacement operation. Up until the first byte of the EImage, the substitution is ongoing. When the substitution phase is over, the SImage, the original image, will be recovered.

III. SUMMARY

Table II summarises the analysis parameters used in various papers. 8 is the predicted entropy value. Ref.[3],[10]-[13],[16] and [20] have achieved 7.9. To ensure higher security, the security key space size should have a larger number. Ref.[10],[13]and [16] achieved the values as represented in the table II. The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) values ought to be higher than 99% and around 33%, respectively. Ref. [10]-[13], [16] and [20] achieved the nearest values. Ref [6],[10],[13], and [21] show faster encryption time. PSNR and MSE values obtained as per Ref. [20] are 7.96 and $1.04x10^{+4.}$

TABLE II. SUMMARY OF ANALYSIS PAREMATERS

Authors	Analysis Parameters							
	Entropy analysis	Throughput	Security Key Space	UACI	NPCR	Encryption time(sec)	PSNR	MSE
[3]	7.9	-	-	-	-	-	-	-
[5]	-	180.4kb/sec	-	-	-	-	-	-
[6]	-	-	-	-	-	0.149	-	-
[10]	7.9	-	2^{237}	33.28	99.60	0.744	-	-
[11]	7.9	-	-	31.55	99.69	-	-	-
[12]	7.9	-	-	33.60	99.60	-	-	-
[13]	7.9		2^{100}	33.35	99.60	1.077	-	-
[16]	7.9	-	2^{186}	33.45	99.61	-	-	-
[20]	7.9	-		33.1	98.6	-	7.96	1.04 e+4
[21]	-	-	-	-	-	0.125	8.27	-

REFERENCES

[1] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, 'A comparative review on symmetric and asymmetric DNA-based cryptography', Bulletin EEI, vol. 9, no. 6, pp. 2484–2491, Dec. 2020, doi: 10.11591/eei.v9i6.2470.

[2] D. A. Zebari, H. Haron, S. R. M. Zeebaree, and D. Q. Zeebaree, 'Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations', in 2018 International Conference on Advanced Science and Engineering (ICOASE), Duhok: IEEE, Oct. 2018, pp. 312–317. doi: 10.1109/ICOASE.2018.8548824.

[3] B. Akiwate and L. Parthiban, 'A Dynamic DNA for Key-based Cryptography', in 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), Belgaum, India: IEEE, Dec. 2018, pp. 223–227. doi: 10.1109/CTEMS.2018.8769267.

[4] M. Biswas, S. K. Das, and B. C. Dhara, 'An Image Encryption Method Using Chaos and DNA Encoding', in Computational Intelligence in Communications and Business Analytics, vol. 1406, Cham: Springer International Publishing, 2021, pp. 42–56. doi: 10.1007/978-3-030-75529-4_4.

[5] Kalsi, H. Kaur, and V. Chang, 'DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation', J Med Syst, vol. 42, no. 1, p. 17, Jan. 2018, doi: 10.1007/s10916-017-0-851-z.

[6] M. Sohal and S. Sharma, 'BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing', Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 1, pp. 1417–1425, Jan. 2022, doi: 10.1016/j.jksuci.2018.09.024.

[7] P. B. Narasingapuram, Dr. M. Ponnavaikko, and Provost, Bharath University, Chennai, India., "DNA Cryptography Based User Level Security for Cloud Computing and Applications," IJRTE, vol. 8, no. 5, pp. 3738–3745, Jan. 2020, doi: 10.35940/ijrte.B2845.018520.

[8] E. Şatir and O. Kendirli, 'A symmetric DNA encryption process with a biotechnical hardware', Journal of King Saud University - Science, vol. 34, no. 3, p. 101838, Apr. 2022, doi: 10.1016/j.jksus.2022.101838.

[9] K. Rama Devi and E. Bhuvaneswari, 'An Enhancement in Data Security Using Trellis Algorithm with DNA Sequences in Symmetric DNA Cryptography', Wireless Pers Commun, vol. 129, no. 1, pp. 387–398, Mar. 2023, doi: 10.1007/s11277-022-10102-8.

[10] Y. Kang, L. Huang, Y. He, X. Xiong, S. Cai, and H. Zhang, 'On a Symmetric Image Encryption Algorithm Based on the Peculiarity of Plaintext DNA Coding', Symmetry, vol. 12, no. 9, p. 1393, Aug. 2020, doi: 10.3390/sym12091393.

[11] S. Patel, Bharath K P, and Rajesh Kumar M, 'Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique', Multimed Tools Appl, vol. 79, no. 43–44, pp. 31739–31757, Nov. 2020, doi: 10.1007/s11042-020-09551-9.

[12] M. Meftah, A. A. Pacha, and N. Hadj-Said, 'DNA encryption algorithm based on Huffman coding', Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 6, pp. 1831–1844, Aug. 2022, doi: 10.1080/09720529.2020.1818450.

[13] Q. Lu, L. Yu, and C. Zhu, 'A New Conservative Hyperchaotic System-Based Image Symmetric Encryption Scheme with DNA Coding', Symmetry, vol. 13, no. 12, p. 2317, Dec. 2021, doi: 10.3390/sym13122317.

[14] Md. R. Biswas, K. Md. R. Alam, S. Tamura, and Y. Morimoto, ‘A technique for DNA cryptography based on dynamic mechanisms’, Journal of Information Security and Applications, vol. 48, p. 102363, Oct. 2019, doi: 10.1016/j.jisa.2019.102363.
[15] M. Poriye and S. Upadhyaya, ‘A DNA Based Framework for Securing Information Using Asymmetric Encryption’, Wireless Pers Commun, vol. 129, no. 3, pp. 1717–1733, Apr. 2023, doi: 10.1007/s11277-023-10203-y.
[16] M. Liu, G. Ye, and Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China, ‘A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm’, MBE, vol. 18, no. 4, pp. 3887–3906, 2021, doi: 10.3934/mbe.2021194.
[17] M. Alruily, O. R. Shahin, H. Al-Mahdi, and A. I. Taloba, ‘Asymmetric DNA encryption and decryption technique for Arabic plaintext’, J Ambient Intell Human Comput, Apr. 2021, doi: 10.1007/s12652-021-03108-w.
[18] H. Al-Mahdi, M. Alruily, O. R.Shahin, and K. Alkhaldi, ‘Design and Analysis of DNA Encryption and Decryption Technique based on Asymmetric Cryptography System’, ijacsa, vol. 10, no. 2, 2019, doi: 10.14569/IJACSA.2019.0100264.
[19] Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, and Y. Zhao, ‘Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation’, Optics and Lasers in Engineering, vol. 143, p. 106626, Aug. 2021, doi: 10.1016/j.optlaseng.2021.106626.
[20] S. R. Maniyath and T. V., ‘A novel efficient multiple encryption algorithm for real time images’, IJECE, vol. 10, no. 2, p. 1327, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1327-1336.
[21] B. Al-Shargabi and M. A. F. Al-Husainy, ‘A New DNA Based Encryption Algorithm for Internet of Things’, in Innovative Systems for Intelligent Health Informatics, F. Saeed, F. Mohammed, and A. Al-Nahari, Eds., in Lecture Notes on Data Engineering and Communications Technologies, vol. 72. Cham: Springer International Publishing, 2021, pp. 786–795. doi: 10.1007/978-3-030-70713-2_71.