VG4 Cipher: Digital Image Encryption Standard

Akhil Kaushik[1]
Ph.D Scholar, CSE Department
Amity University, Gurugram
India

Dr. Vikas Thada[2]
Associate Professor, CSE Department
Amity University, Gurugram
India

***Abstract*—When it comes to providing security to information systems, encryption emerges as an indispensable tool, as it has been used extensively in the past few decades for securing stationary data as well as data in motion. With the rapid data transmission techniques and multimedia options available for data representation, the field of information security has become very significant. The state-of-art cryptographic technique is DNA encryption, which uses biological principles for safeguarding data. The use of Bio-inspired ciphers is becoming the de-facto safety standard, especially for digital images as they are a key source of extracting crucial information. Hence, image encoding becomes of ultimate importance when there is a need to send them via an insecure communication channel. The purpose of this research paper is to present a DNA- inspired cryptosystem that can be employed in the domain of image encryption that provides superior security with enhanced efficiency. The experimental outcomes prove that this novel cryptographic algorithm not only provides better security but also at a reasonable pace.**

Keywords*—*DNA cryptography; cipher; information security; encryption; decryption

I. Introduction

With the epoch of information explosion, information has become the most crucial asset of any individual, corporate, or government. This vital data may contain the personal record of any person, trade secrets of any business organization, or official documents of any government and hence needs to be kept in a secure place. Besides the physical security needs, there is also a need for safety while this significant data during transmission over the vulnerable interaction channel. Cryptography is the remedial solution for such a situation which keeps the information correct and intact between sender and recipient by making the data in a mangled form. Cryptography depends on two things: encryption algorithm and encoding key. The key may be a shared secret key or may form a public-private key pair depending upon the nature of the encryption algorithm. Without the right encryption steps and correct key, the unveiling of secret data can be a herculean task for the adversaries. Thus, cryptography provides impenetrable data which will be meaningless for the eavesdropper [1]. The data is growing immensely as ‘big data’ and it can now be represented in various forms like text, image, sound, animation, video, etc. This extended volume and multimedia forms of data require modern crypto solutions that can provide information security from malevolent adversaries and uncover the actual information only to the intended recipient. There are a plethora of options available to provide robust security and not all options are suited for all sorts of media. Some ciphers work best on textual data but may perform poorly on video data, although some security algorithms may perform brilliantly on all sorts of media. Every media form has its peculiar attributes that cause the deviation in the encryption process and outcomes [2].

The most prevalent form of media besides textual data is digital images as they are used widely for information storage and broadcast due to their enhanced data-carrying capacity. The images may contain classified data such as military maps, government documents, healthcare images. The security mechanisms for images can be done in two ways: steganography and cryptography. Image Steganography can be defined as the myriad ways of concealing confidential information in the images, while Image Cryptography alters the image’s data to a garbled form making it irrelevant rather than hiding it. Earlier, both of these techniques were used individually, but nowadays they can be combined to provide an even stronger sanctuary solution. Image cryptography is primarily done in two ways: frequency-domain techniques and spatial-domain approaches. The frequency-domain techniques rely on the Fourier transformations, while the spatial-domain approaches simply involve the manipulation of pixels’ data in such a way that the real information contained in the pixels of images get altered on the sender’s side and gets reverted into the original shape and form on the receiver’s side [3]. Apart from the pixel level, encoding can also be done at the bit level, adding more perplexity to the existing encryption systems. There can be innumerable methods of image encryption and the method under consideration in this study makes use of DNA computing.

DNA computing made its way into the modern world when Leonard Adleman experimented with biological data and discovered that biological methods can give productive outcomes while solving baffling computational problems in 1994. Later this phenomenon received greater appreciation and researchers invested their time and money to apply these newly fangled principles into the newer and unexplored domains. DNA cryptography is inspired by the natural process of translation and encoding genetic information in DNA sequences. DNA is the abbreviated form of Deoxyribonucleic Acid that encodes genomic information using enormous sequences of four nucleotide bases $\sum = \{A, C, G, T\}$. These chemical bases are Adenine (A), Cytosine (C), Guanine (G), and Thymine (T) can be connected into a variety of combinations to pass the genetic information from parents to their children. This information is present in the form of genes which are enormously long DNA distinguishable sequences using complementary pairs of bases and called genes [4], as shown in Fig. 1. There can be multiple ways in which DNA can be utilized in the cryptographic sphere like hiding classified information in long DNA sequences, generating one-time pads, DNA intensification using Polymerase Chain Reaction (PCR) for using in data encryption, and many more.

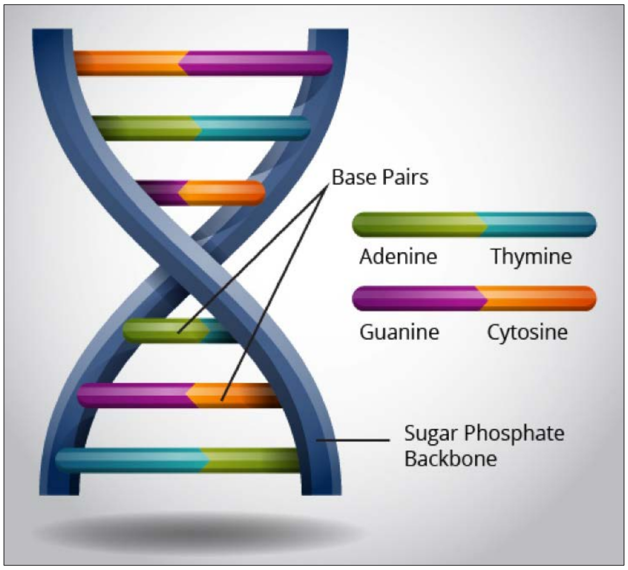

Fig. 1. DNA Structure [4].

The rest of the paper is organized as follows: Section II discusses the background and related work to the research. Section III highlights the system model and adversary model of the proposed research. Section IV details the stepwise proposed methodology for the presented work. Section V presents the simulation outcomes and examines the performance of the proposed cipher. Finally, Section VI entails the conclusion and the direction of future work.

II. Related Work

As the name suggests, DNA cryptography is the amalgamation of biological methods and encryption. As discussed above, DNA computing was introduced in 1994 to solve intricate problems by Leonard Adleman and the concept grew stronger with time. In 1999, Cleland et. al. demonstrated the usage of DNA in steganography by hiding the renowned WWII phrase “June 6 attack; Normandy” in DNA strings [5]. Then, A. Gehani et al. demonstrated the myriad ways to encode data using DNA principles like OTP-based ciphers, Chip-based DNA microarray technology, and DNA steganography also. However, with the period of nearly 20 years, DNA cryptography has achieved new heights and plentiful novel DNA encoding algorithms have been developed, which have been listed below:

One exemplary work was proposed by Suri & Vijay (2017) which mixes a fast chaotic multi-image encryption algorithm with the AES encoding standard for a speedy encoding of multiple images. The concept is unique as it uses Cramer’s rule for decryption of digital images at the receiver’s end [6]. The use of biological methods in image encoding was also suggested by Enayatifar et al. (2017) that first brings the two-dimensional image into a single dimension and later applies permutation and diffusion parallelly for faster encryption. Both operations employ DNA sequences and results show quicker and securer output [7].

Niyat et. al. (2017) recommended the usage of non-uniform Cellular Automata (CA) for image cryptography. This non-uniform CA and hyperchaotic function create a stronger key image that generates a colossal number of random keys. Further usage of chaotic maps to add confusion and later using diffusion principles to create perplex cryptosystem [8]. The encoding of medical images is also a common practice and various studies have been conducted for the same. One such study is done by Akkasaligar & Biradar (2016) which blends DNA with chaotic theory to encode the odd and even pixels of medical images individually. This system is symmetric in nature that maintains integrity and efficiency along with security [9]. Ochani et al. (2017) also worked on the medical images using both steganography and cryptography. The chief technique here is to apply encryption on data and then hiding the patient’s vital encoded data in the cover medical image [10].

Another research done by Wang et. al. (2018) displayed that random numbers can also be used in the image encryption process. The authors have worked on both permutation and diffusion levels to increase the information security, besides including SHA-3 hashing with Chaotic systems to provide ultimate refuse against any unauthorized attacks [11]. Xiuli et. al. (2018) showed the embedding of DNA techniques in encryption. Initially, the image’s color is permuted and concerted into DNA codes. Consequently, DNA is used to produce random numbers that will be used to alter the pre-obtained DNA codes for further diffusion [12]. A similar approach was suggested by Rehman et. al. (2018) for encoding the colored images by combining SHA1 encoding, DNA complementary rules, and chaotic functions. The output obtained exhibited lesser noise and comparatively lower data loss [13].

Two-dimensional Logistic-Sine-Coupling map (2D-LSCM) can also be considered for encryption of colored images. It uses the typical confusion-diffusion structure i.e. transposing the pixels within the image first and then apply diffusion to further modify the pixels. This approach by Hua et. al. (2018) demonstrated better ergodicity than the traditional chaotic systems [14]. Another notable research was carried out by Li et al. (2018) for the encoding of multiple images simultaneously. First of all, Lifting Wavelet Transform (LWT) method is used to produce sparse images and then these scrambled images are XORed to further induce complexity. Finally, the images are compressed to form ghost images that can be traced only through bucket detector arrays [15].

Using DNA in image encryption is also verified by Sun (2018). Primarily, five-dimensional hyperchaotic systems are calculated to generate the chaotic sequences. Then, DNA is combined in several ways like DNA XOR operation, DNA complementary rules, DNA encoding, etc. to enhance the algorithm’s robustness. Besides these superior methods involved, the transposition is also done at two levels: pixel level and binary level [16]. A similar yet different approach was recommended by Zhang et al. (2018) that computed encoding key in two ways i.e. DNA sequencing and logistic chaos mapping. Later, these keys are applied to the plain image using DNA complementary rules to obtain the final ciphered image [17].

Liu et al. (2019) extended the image encryption using DNA to the next level by using 4-D memristive hyper-chaos to generate the chaotic matrices. Then, dynamic DNA is applied on the plain image to produce three matrices, and hence the combination of confusion, diffusion, and encryption creates vigorous cipher [18]. Zhang & Wang (2019) also demonstrated that using a three-dimensional DNA matrix to encode the digital images. First of all, numerous images are combined into a single image and then scramble using chaotic principles. Later on, multiple images are again taken away from the bigger image before applying diffusion using DNA codes and SHA-256 [19].

III. System and Adversary Model

A. System Model

Fig. 2 shows the system model considered in this paper, in which there are three major components: Sender's end, Receiver's end, and Genetic Database. The sender's end consists of the user and the machine to generate and encode the message that needs to be sent over to the other end. The message has to be sent over the insecure public communication channel; hence the encoding must be done to keep it intact and away from prying eyes. The receiver's end is quite similar to the sender's end that encompasses the intended recipient and his/ her machine that not only accepts the transmitted message but also decodes it to obtain the original plaintext. However, the process of decryption is somewhat different from encryption depending upon whether it is symmetric or asymmetric cryptography. The third significant component of the model is the Genetic database, which is responsible to create, maintain and securely send the encryption key to the users. There are ample genetic databases that already contain the extremely long DNA sequences stored in the electronic form. The electronic form of DNA strings makes it easier enough for the administrators to store, maintain and give access to the authenticated users. It also eases the user to access, manipulate and regenerate the biological sequences by combining them in several ways. However, genetic databases also play a vivacious role in sharing the secret key that is used by sender and receiver. As the secret key used in the model is deduced from a specific DNA sequence, hence only its sequence number in the genome database or its URL can be shared with the intended addressee via a safe and trusted channel rather than sending the entire genetic sequence over untrusted communication channels.

B. Adversary Model

In the system model, the real communique takes place on the public insecure channel; hence there is a stout possibility of attacks to compromise the security. This is due to an imperious factor - an adversary who could try to catch the encoded message and try to either read or manipulate it. An adversary is defined as a computer wizard with malicious intent whose goal is to interrupt or halt the proper functioning of the cryptosystem. In this paper, the following threats are considered:

- Shared Secret Key Security Threat: As the communication under consideration is fairly dependent on the shared secret key that is generated using the DNA sequences stored in the genetic databases, hence if the key gets in the wrong hands, the whole system is compromised. Thus, the channel required to send this key must be trusted and secure enough to tackle this threat. Also, the property of backward secrecy should be followed while the generation of session key i.e. knowing one session key should not let the adversary extract other session keys.

- Privacy Threat: The message contents need to be kept private although the adversary may feel the message's presence but not its contents. If the adversary can read the message, he may replay the message multiple times or he may be able to modify the message contents or masquerade himself as an authenticated communicating party to gain undue advantage.

- Physical Security Threat: The physical security of all the crypto-system components must be of utmost priority as the attacker may try to physically damage or steal the devices or access the system's memory where session keys and messages are stored. Hence, the user credentials' information should be kept integrated and away from the hands of attackers.

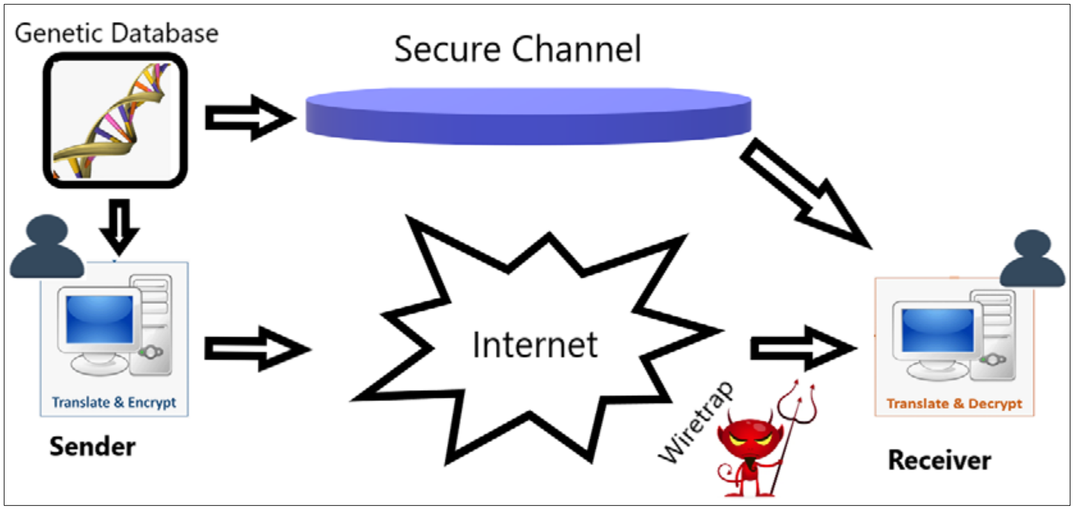

Fig. 2. System Model.

IV. Proposed System

This section proposes the novel encoding system – VG4 cipher which is based on the existing VG1 cryptographic algorithm. VG1 cipher is a DNA Indexing cryptosystem that is a homophonic substitution cipher for textual data [20]. Several modifications have been done on the VG1 cipher for making it more efficient and secure to apply to digital images.

Image encryption is quite a tedious process with the inclusion of two steps: confusion and diffusion. Confusion refers to the permutation or transpositions of image components (blocks or pixels) so that the correlation among the pixels and the obvious redundancy gets altered. Another vital point is that the confusion step must be reversible to obtain the original image [21].

The second major operation is Diffusion which is stated as the process of altering the value of image components especially the value of pixels to make the encoding robust against differential and noise attacks. The diffusion procedure is done at two levels: block-level and pixel level. The encryption process in detail is described as follows:

- Step 1: The input is a color image of M & N dimensions, where M and N represent the width and height of the image.
- Step 2: The confusion step is done here at block level i.e. grouping of multiple pixels. The block size should be kept an even number and multiple of 8 for ease of operation. Here, the image is divided into 64 blocks and these 64 blocks are shuffled randomly.
- Step 3: There are two encoding keys used in the VG4 cipher. The first key is the 'Primary Key' which is deduced from the plethora of DNA sequences available from the genomic databases like GenBank, NCBI, DDBJ, EMBL-Bank, etc. Out of these ample DNA sequences, one peculiar DNA sequence is selected. In this particular DNA sequence, the position of every possible 4-DNA character combination is recorded in a separate dictionary. This dictionary contains position values of a specific DNA byte order (Ex: AATG) in the selected DNA sequence. This dictionary will form a homophonic substitution encryption cipher that works at the pixel level diffusion. An example of such a dictionary is demonstrated in Table I. The subsequent key is the 'Secondary Session Key' which is calculated prelude to applying diffusion at the block level. A set of session keys is produced (one for each block) by picking three random symbols from a set of pre-defined characters, S = {A-Z, a-z, 0-9, #, @, !, $, %, ^, &, *, etc.} The secondary session key for each block thus consists of three characters, which are then changed to their binary equivalent.
- Step 4: Prelude to apply diffusion at the block level, a set of session keys is produced (one for each block) by picking three random symbols from a set of pre-defined characters, S = {A-Z, a-z, 0-9, #, @, !, $, %, ^, &, *, etc.} The secondary session key for each block thus consists of three characters, which are then changed to their binary equivalent. For every block, its combined RGB value is extracted and changed into the binary form so that the corresponding secondary session key can be applied to it. This process is repeated for every block in the image.
- Step 5: After applying diffusion at the block level, the next step is to apply the same at the pixel level. A pixel's RGB color code in decimal form is acquired using the NumPy library of Python. Using the VG1 encryption process, this decimal value is converted to the binary representation depending on the occurrence and frequency of the decimal values.
- Step 6: The binary data obtained from the previous step is then retransformed using shift-right or shift-left and then coded according to DNA rules (00-c, 01-a, 10-t, 11-g). This DNA encoding output converts all the binary data to DNA form.
- Step 7: The DNA homophonic substitution cipher is then applied on the output of step 6 and hence the 4-letter DNA codes are transformed into decimal numbers (index values in the given DNA sequence). Consequently, decimal values are changed into binary form and finally converted into a ciphered image. The whole encryption procedure is displayed in Fig. 3.

The proposed cryptographic algorithm is primarily based on symmetric encryption and henceforth the decryption procedure of the VG4 cipher is exactly opposite to the encoding process. The genomic sequences from which the primary key is crafted are shared through the reliable secure channel to the recipient. Similarly, the set of secondary session keys are also shared over to the other end. After the generation of encoding keys and receiving the ciphertext by the intended recipient, the next step is to convert the ciphertext into the DNA codes and then to binary form which is rotated into the reverse direction. Subsequently, the data is changed to decimal equivalent and then into pixel's RGB contents and the original image is conclusively recovered.

TABLE I. Example of Key Indexing

DNA Combination	Position Index in the DNA Sequence
GGTA	58, 80, 249, 619, 645, 671, 896, 1197, 1605, 2766, 2958, 2972
AGAG	130, 161, 242, 453, 1011, 1442, 1458, 1512, 1997, 2295, 2789
CAAG	27, 458, 611, 656, 924, 1059, 1332, 1518, 1521, 1539, 1584, 1647, 1695, 1698, 1734, 1767, 1779, 1885, 1933, 2166, 2225, 2365, 2401, 2625, 2700, 2754
AACT	271, 746, 1062, 1188, 1250, 1259, 1409, 1466, 1470, 1491, 1581, 1616, 1701, 1882, 1984, 2095, 2118, 2151, 2198, 2382, 2622, 2655, 2684
AAGG	10, 246, 366, 666, 1182, 1375, 1461, 1448, 1527, 1590, 1593, 1955, 2238, 2338, 2606, 2812, 2864
GGTG	521, 1754, 1877, 1992, 2442, 2531, 2618, 2675

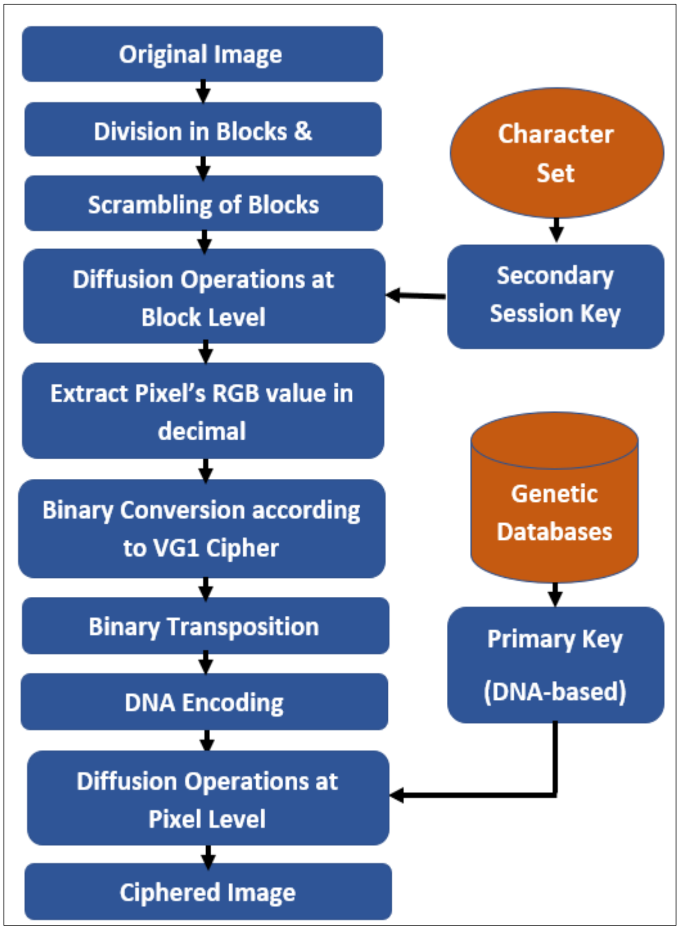

Fig. 3. Basic Block Diagram of VG4 Encryption Cipher.

V. Simulation Results and Performance Analysis

The proposed cryptographic algorithm can be implemented in any language that supports Unicode. It is implemented in Python Programming language using Google Colab IDE. It is also implemented on Jupyter Notebook on Intel Core i5 – 10th generation processor HP machine with 8GB RAM. Some crucial evaluation standards that focus on image encryption security are discussed and listed as follow:

A. Key Space Analysis

There is a total of nearly 420 billion DNA sequences available over genomic databases like EMBL-Bank, GenBank, NCBI, etc. Thus, first of all, the user needs to identify which genomic databases are exactly used for determining the primary key, otherwise, he will struggle for a lifetime to unearth it. Even if an attacker discovers DNA string is taken from NCBI, even then using the hit-&-trial method, he/she has to try 4163,000,000 combinations because there are 163 million nucleotide bases in NCBI and there are 4 bases -A, C, G, and T [22]. Thus, the probability of deciding accurate DNA sequence is $\frac{1}{163000000}$. Additional chaos will come into play if a longer biological series is chosen and out of this prolonged sequence only a fraction is extracted for spawning primary key. Hence, the huge keyspace for primary keys makes conventional attacks nearly impossible. Imperative consideration here is that the receiver only needs the correct DNA number for reproducing the primary key, hence the whole DNA sequence need not be shared over the internet, rather only series numbers can be communicated through secure telephone or any other system.

B. Correlation

The adjacent pixels in any image are correlated to each other and measuring this correlation is of extreme importance when it comes to image cryptography. The input image usually has a high correlation between pixels, while the correlation in the ciphered image is desired to be as low as possible [23]. As depicted in Fig. 4(a), a positive correlation exists between pixels before encryption. However, the results obtained after encoding exhibit that the ciphered images have nearly 0 value of correlation, as shown below in Fig. 4(b). It means that the proposed cipher is successful in weakening the bond between adjacent pixels and makes it harder for the attacker during cryptanalysis.

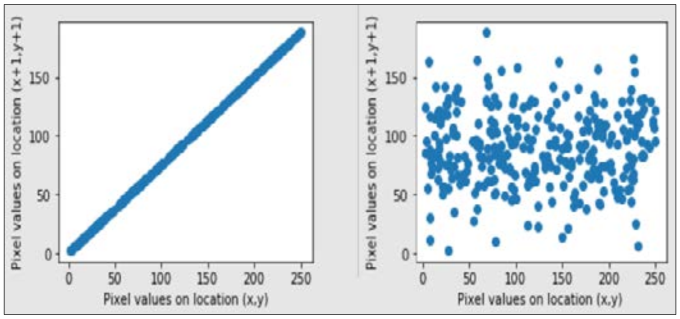

Fig. 4. Correlation between Adjacent Pixels in the Plain Image (a) and Ciphered Image (b) for a 512*512 Size Lena Image.

C. Histogram

The histogram analysis of the image cipher will demonstrate the pixel value distribution and it is desired to be uniform across the whole image. If the variance in histogram decreases in the enciphered image as compared to the plain image, then the cryptosystem is assumed to be fruitful [23]. As clearly observed from Fig. 5, the histogram of the plain image shows non-uniform dissemination, while the encoded image histogram has a uniform distribution pattern.

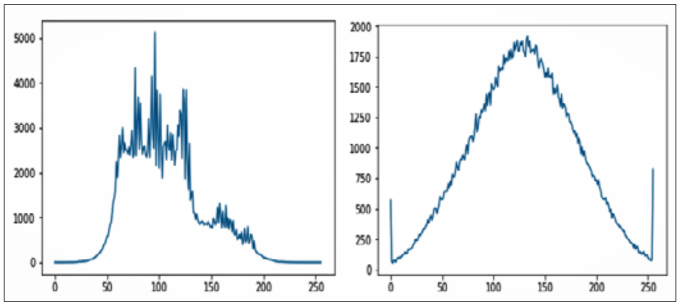

Fig. 5. Histogram of Plain Image (a) and Ciphered Image (b) for a 512*512 size Lena Image.

D. Analysis for Differential Attacks

Differential attacks are based on the idea of tracing the relationship between the original image and image obtained after encryption. Thus, the attacker tries to encode an image to obtain the ciphered image and then make some alterations in the plain image to observe the subsequent changes in the newly attained encoded image. To measure these changes, there are two quantitative measures: The Number of Pixel Changing Rate(NPCR) and the Unified Average Changing Intensity(UACI). The NPCR for an image of dimension (W * H) is calculated by the following equation [24]:

$$\text{NPCR} = \frac{\sum i,j\ D(i,j)}{W*H} * 100 \quad (1)$$

Where W is Width, H is Height, the value of i is between 1 and W, and the value of j lies within 1 and H. D(i, j) represents the difference between both images. The value of D(i, j) is 0 if the plain and encoded counterparts are the same, otherwise, the value equals 1. The lower bound of NPCR is 0% and the upper bound for NPCR is 100%. The NPCR calculated for VG4 cipher is estimated approximately at 97.65%, which means it is proximate to 100%, hence providing determined robustness.

Another factor UACI is computed as the following [24]:

$$\text{UACI} = \frac{1}{W*H}\left[\sum i,j \frac{|C1(i,j) - C2(i,j)|}{255}\right] * 100 \quad (2)$$

Where C1(i,j) and C2(i,j) are the encoded images of plain images with a one-pixel difference. The observed value of UACI is 39.42% which simply means that the proposed cryptographic algorithm is quite sensitive to the minor changes in the plain image and provides substantial security against the differential attacks.

E. Analysis for Noise

The communication channels always contain some kind of noise, which will affect the enciphered image. There can be numerous kinds of noise and quantitative measures to check the effects of these noise on the image quality. The first one in this series is the Mean Square Error (MSE) which is computed as [25]:

$$\text{MSE} = \frac{1}{W*H}\sum_{i=1}^{W}.\sum_{j=1}^{H}[I1(i,j) - I2(i,j)]^2 \quad (3)$$

Where W and H signify the Width and Height of the image respectively. I1(I,j) and I2(i,j) denote the plain image and encoded image correspondingly. MSE value for VG4 cipher is nearly equal to 0.00521.

Depending upon the MSE value, Peak Signal to Noise Ratio (PSNR) can also be computed which is defined as the ratio by which the decrypted image is affected by the noise. Mathematically, it can be defined as [25]:

$$\text{PSNR} = 10\ log\frac{(2^{n}-1)^2}{MSE} \quad (4)$$

The PSNR value is measured for various noises like Salt & Pepper Noise (SPN), Speckle Noise (SN), and Gaussian Noise (GN) in the units – decibels. The PSNR value for 512*512 'lena.jpg' for noise type SPN with parameters 0.001 is around 39.43. This result indicates detectible recovery from salt & pepper noise of up to 60%.

F. Timing Analysis

The performance analysis of any cryptographic algorithm depends upon security and speed. The encryption and decryption timings of the VG4 cipher are listed in the following Table II:

TABLE II. EXECUTION TIMINGS OF VG4 CIPHER

Image Size	Encryption Timings (Secs)	Decryption Timings (Secs)	Total Execution Timings (Secs)
512*512	40.3	37.6	77.9
700*400	53.2	44.7	97.9
1920*1080	210.6	199.5	410.1

The execution timings of VG4 cipher are compared with other state-of-art encoding algorithms in the following Table III:

TABLE III. COMPARISON OF EXECUTION TIMINGS OF VG4 CIPHER WITH EXISTING STANDARDS

Algorithm	Encryption (secs)	Decryption (secs)
Color image DNA encryption using NCA map-based CML and one-time keys [26]	1300.5	1300.7
Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme [15]	85.2	85.1
An AES-CHAOS-based hybrid approach to encrypt multiple images[6]	407.9	408.2
Multiple-image encryption using genetic algorithm [27]	149.7	144.5
Multiple-image encryption algorithm based on DNA encoding and chaotic system [19]	43	41.3
2D logistic-sine-coupling map for image encryption [14]	9.4	10.2
VG4 Cipher (Proposed)	40.3	37.6

VI. CONCLUSION

In the world of cybercrimes and online scams, a new defense is direly needed to guard the vital information, and for the same, the DNA cryptography approach reinforces the trust back into authenticated users. This paper presents a novel image encryption standard that uses biological principles in addition to traditional cryptography. First of all, the proposed algorithm uses two keys: primary key and secondary key. The primary key is deduced from a digital DNA sequence of long length and provides utmost security against brute-force attacks. The secondary key is also changed per session to enhance robustness. Both diffusion and confusion operations are applied to the image. Confusion or permutation of blocks are applied beforehand and then diffusion is applied at two levels. The secondary key works on a block of pixels and the primary key ensures encoding at the pixel level. The analysis for keyspace, histogram, correlation, etc. has been done and they determine the strength of enciphering algorithm. Also, the analysis for differential attacks and noise has been carried out and the desirable values of NPCR, UACI, PSNR, and MSE show better security and higher resistance against multiple attacks. The timing analysis done against the recent image encryption algorithms has been done and the results demonstrate the novel VG4 cipher is comparable to these modern standards both in encryption as well as decryption timings. Correspondingly, the execution (both encoding and decoding) timings are increasingly linearly with the increasing size of images, which proves the computational complexity is linear.

In the future, the work can be manifold like chaotic functions like the Chen system or 3D logistic map can be introduced for confusion or diffusion. Another imperative future work could be improving the efficiency of the proposed cipher both in terms of security as well as execution timings.

References

[1] M. E. Saleh, A. A. Aly, & F. A. Omara, Data security using cryptography and steganography techniques (2016).

[2] M. Jia, Y. Zhou, M. Shi, & B. Hariharan, A deep-learning-based fashion attributes detection model. arXiv preprint arXiv:1810.10148, (2018).

[3] Z. Hua, Y. Zhou, & H. Huang, Cosine-transform-based chaotic system for image encryption. Information Sciences, 480, (2019) 403-419.

[4] An online article “What is Chemical Structure of DNA” available at https://empoweryourknowledgeandhappytrivia.wordpress.com/2017/03/29/what-is-the-chemical-composition-of-dna/ (2017).

[5] A. Y. Niyat, & M. H. Moattar, Color image encryption based on hybrid chaotic system and DNA sequences. Multimedia Tools and Applications, 79(1), (2020) 1497-1518.

[6] S. Suri & R. Vijay, An AES-CHAOS-based hybrid approach to encrypt multiple images, Recent Developments in Intelligent Computing, Communication and Devices, Springer, Singapore (2017) 37-43.

[7] R. Enayatifara, A. H. Abdullah, I.F. Isnin, A. Altameem, & M. Leed, Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Eng 90, (2017) 146–154.

[8] A. Y. Niyat, M. H. Moattar, & M. N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90, (2017) 225–237.

[9] P. T. Akkasaligar, S. Biradar, Secure medical image encryption based on intensity level using chaos theory and DNA cryptography. International conference on computational intelligence and computing research, IEEE, Chennai, (2017).

[10] A. Ochani, D. Jadhav, R. Gulwani, DNA Image encryption using modified symmetric key (MSK). International conference on inventive computation technologies, IEEE, Coimbatore, (2017) 1–4.

[11] X. Wang, S. Wang, Y. Zhang, & C. Luo, A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems. Optics and Lasers in Engineering 103, (2018) 1–8.

[12] X. Chai, F. Xianglong, Z. Gan, Y. Lu & Y. Chen, A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, (2018).

[13] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, & H. Wang, A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. Optik 159, (2018) 348–367.

[14] Z. Hua, F. Jin, B. Xu & H. Huang, 2D logistic-sine-coupling map for image encryption,' Signal Process., 149, (2018) 148-161.

[15] X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, W. He, G. Dong, & H. Chen, Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme, Opt. Lasers Eng., 102, (2018) 106-111.

[16] S. Sun, A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling, IEEE Photon. J., 10(2), (2018) Art. no. 7201714.

[17] T. T. Zhang, S. J. Yan, C. Y. Gu, L. Ren, & K. X. Liao, Research on image encryption based on dna sequence and chaos theory, Proc. 2nd Int. Conf. Mach. Vis. Inf. Technol. (CMVIT), 1004, (2018), 149-154.

[18] Z. Liu, C. Wu, J. Wang, & Y. Hu, A color image encryption using dynamic DNA and 4-D memristive hyper-chaos, IEEE Access, 7, (2019) 78367-78378.

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

[20] A. Kaushik & V. Thada, VG1 Cipher – A DNA Indexing Cipher, International Journal of Innovative Technology and Exploring Engineering, 9(3), 2020 221-226.

[21] Z. Hua, B. Xu, F. Jin, & H. Huang, Image encryption using Josephus problem and filtering diffusion. IEEE Access, 7, (2019) 8660-8674.

[22] E. W. Sayers, R. Agarwala, E. E. Bolton, J. R. Brister, K. Canese, K. Clark, R. Connor, N. Fiorini, K. Funk, T. Hefferon & J. B. Holmes, Database resources of the national center for biotechnology information. Nucleic acids research, 47(Database issue), D23, (2019).

[23] C. Pak, & L. Huang, A new color image encryption using combination of the 1D chaotic map. Signal Processing, 138, (2017) 129-137.

[24] R. Anushiadevi, V. Venkatesh, & R. Amirtharajan, An image mathcrypt-a flawless security via flawed image. International Conference on Applications and Techniques in Information Security, Springer, Singapore, (2019) 16-31.

[25] S. Krivenko, M. Zriakhov, V. Lukin, & B. Vozel. MSE and PSNR prediction for ADCT coder applied to lossy image compression. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, (2018) 613-618.

[26] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, Color image DNA encryption using NCA map-based CML and one-time keys, Signal Process., 148, (2018), 272-287.

[27] S. Das, S. Mandal, & N. Ghoshal, Multiple-image encryption using genetic algorithm, Intelligent Computing and Applications, 343, (2015).