VG3 Cipher for Secure Image Transmission

A Kaushik¹, V Thada² and J Singh³
¹ PhD Scholar, Amity University, Gurugram, India
² Associate Professor, Amity University, Gurugram, India
³ Associate Professor, GJUS&T, Hisar, India
E-mail: akhilkaushik05@gmail.com

Abstract. The rampant growth of Internet and communication has revolutionized the way people communicate and it has led to rapid enhancement in modern information warfare. The world around us requires the information security more than ever before due to copious reasons primarily being the importance of financial and personal data which can be utilized by the malicious hackers to gain undue advantage. Out of innumerable methodologies available for data safeguarding, cryptography has always been an indispensable tool. However, the changing ways of cyber-attacks demand an upgraded cryptographic version that can handle potential attacks on media of myriad data types. This paper proposes one such encrypting technique which is based on biological methods and used principally for the encoding of digital images based on amalgamation of DNA encryption and Rubik’s cube.

Keywords: DNA computing, DNA sequences, Genetic databases, One-Time Pad (OTP), Rubik’s Cube.

1. Introduction
The end of 20th century brought a major technical revolution namely Internet in the life of mundane man and the whole life of modern man took a whirlwind. Nowadays, even general elections of many countries are done on the internet and even if they are not conducted electronically, the internet based social media sites play a herculean role in influencing voter’s mind. This has happened in major democratic countries like India and USA, where social networking sites especially Twitter and Facebook are the new battlegrounds for political parties [1]. Due to the internet, modern person is living a virtual life where a smartphone is his lifeline. Now, as more and more applications are dominating life more than ever, the need of information security is vital than ever before. The data has become big data now and data is present in every form of media possible like text, image, video, audio, animation, etc. Due to this varied media presence, a more robust way of safeguarding is needed for present day information. This has made the traditional cryptographic methods belittle for current big data and myriad media forms and there is a need of a novel encryption method. The ultra-modern cryptosystems like the Elliptical Curve Cryptography (ECC) and Quantum Cryptography brought innovative ideas to attain perfect clandestineness, but the latest addition is the DNA encryption. The DNA cryptography is the savior that provides a perfect secrecy solution in this imperfect world with insecure data transmission.

DNA computing arrived on the computing stage when Leonard Adleman did some biological experiments for solving the Hamilton Path problem. This paved the way for elated research in this area and Ashish Gehani et. al. suggested that the newest branch of computing can be equally effective when applied to the information protection domain [2]. Nevertheless, it is imperative to understand that the DNA encryption mingles the biological methods with encryption to solve the most challenging problems [3]. Some novel approaches for DNA encryption have arrived on horizon since 1999 and these new-fangled solutions can prove fruitful for all sorts of media exclusively for the digital images.
The immense parallelism and information density features of biological molecules can be used extensively for authentication, digital signature, symmetric and asymmetric encoding, etc. Innumerable genetic methods like Polymerase Chain Reaction (PCR), DNA chips, DNA tiles, etc. can be employed for all crypto solutions. One such example of using DNA PCR for replication is demonstrated in the Figure 1 below.

![DNA Replication Process](image)

**Figure 1.** DNA Replication Process [4].

The output of DNA encryption can also be hidden using DNA steganography where data can be hidden inside immensely long DNA nucleotide sequences, which act as brilliant hidden layer. The crux of the matter is that the contemporary cryptography offers innumerable ways to provide information security. The rest of the paper is formatted in the following manner. The section II gives some background on Rubik’s cube and its role in encryption. The section III throws some light on the literature review related to the work presented in this paper. The section IV details how the proposed methodology works. The subsequent section V does the discussion and showcase the results obtained. Finally, the last section VI concludes the work and suggests the direction of future work.

### 2. Rubik’s Cube

Rubik’s Cube is an excellent and amazing product developed by Professor Erno Rubik of Hungary in 1974 that could be twisted at various angles while remaining intact. This cube basically has small cubes which can be colored in different colors and the most important thing is that it could be dismantled and congregated with ease [5]. There is total 6 colored faces, each with 9 visible pieces and the cube center is not movable. Overall, there are total 26 pieces - 12 edges, 8 corners and 6 centers. Initially all the same colored nine pieces are one side. After shuffling the cube, the chief play is to bring back the cube to the initial state. Professor Rubik himself took 1 month to solve the cube for the first time.
Figure 2. Rubik’s Cube Structure [6].

The rotations in Rubik’s Cube are very interesting and they act according to their position in the cube. The corner pieces remain at the corner, no matter the movement and hence there are 8! possible combinations. Another consideration is that 7 out of 8 corners can have 3 probable rotations, hence the total number of likely arrangements becomes 8! * 37. The edge pieces are 12 and the number of combinations for an edge is 12! /2. However, a key point here is that the central piece of each cube is not movable, hence 0 blends [6]. Overall, it is stated that a total of 43 quintillion blends (8! × 37 × (12!/2) × 211 = 43252003274489856000) can be grasped using a single Rubik’s cube [7]. This wide variety of permutations and combinations can be utilized to pursue a miscellany of solutions in all sorts of problems.

3. Background Work
Although Rubik’s Cube was invented as a broods’ toy and it gained huge popularity among children and teenagers. Later on, the concept was extended to cryptography, where myriad approaches were employed to either encode or conceal the secret message using this cube. One such work encrypts data by using a cube and customized number of rotations called critical data, which is transmitted to the other end using SHA1 cipher. The discussed algorithm is symmetrical which has pre-defined five ways to input plaintext. To speed up the process, the block cipher technique was used along with the transposition mechanism. Due to block encryption, the ciphertext obtained was different for each block, and obtaining one does not give way security of the other blocks. This research work was published by ElayaRaja and Sivakumar, DCE Chennai in 2010 [8].

Another brilliant work by Loukhaoukha, Chouinard, and Berdai in 2011 highlights a similar cryptosystem that trundles the plain image randomly at the first step in the Rubik’s cube fashion. Then two secret keys are selected to apply encoding on the rows and columns of the image. After the initial cryptography application, steganography is employed using the Least Significant Bit (LSB) or spatial and frequency expanses to add perplexity [9].

The additional aesthetic contribution was done by Rawat, Mishra, and Upadhay in 2016 that works on binary data using spatial steganography. Initially, all the faces of the cube are initialized either using 0 or 1, then the characters are imposed on them and finally, the cube is rotated in one of the 18 possible alternations. After the whole encryption process is completed, the text file is embedded in a steganographic image. The observed results show superior security than the existing standards [10].

Helmy, El-Rabaie, Eldokany & El-Samie suggested that 3-D image encryption can prove fruitful for digital images. The initial enciphering step is the use of RC6 cipher for encoding numerous images in parallel. Later on, Rubik’s Cube-based permutation is applied to add confusion before applying the Orthogonal Frequency Division Multiplexing (OFDM) system and transmitting wirelessly to the other end. The final outputs of the cryptosystem reveal better yield in the image quality [11].
A general viewpoint on the advantages of using Rubik’s Cube in the field of the mechanism was discussed in detail by Zeng et. al. in 2018 [12]. The authors have given profound details about the history and evolution of the Rubik’s cube. The paper also describes the myriad ways how this super cube can be used in the cipher world especially image encryption. One such mapping of Rubik’s cube and an image is shown in Fig. 3 below. The cube has a total of 6 faces and each face has 3 rows and 3 columns, hence 6*3*3 equals 54, which can be also be represented in a 3-dimensional matrix called ‘cubelet’.

Another vital research article by Dharavathu & Mosa (2020) emphasizes the usage of designing a novel encryption system based on Rubik’s Cube for sending data over the insecure AWGN channel condition. For the same, a DCT-based crypto-Orthogonal Frequency Division Multiplexing system (crypto-OFDM system) is deliberated using the MATLAB stimulating environment. For analysis of better quality of images, Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER) is used. Other statistical measures like correlation coefficient, histogram, entropy, Number of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity (UACI), etc. are also employed to assess the forte of newly developed cipher [13].

4. Proposed Work
The proposed encryption algorithm in this work is based on the concept of Rubik’s Cube that works primarily on digital images. The encryption procedure is alienated into two parts: the first one does the shuffling in the image and the second one applies the secret keys on the pixel data of the image. The first work i.e., shuffling is based on the principle of Rubik’s Cube-based rotation. For that, first of all, a block of pixels (a group of 54 pixels) should be mapped on the Rubik’s cube and then rotated. This mapping is done as demonstrated in Fig. 3 above. 18 basic rotations are possible, and they are listed in table 1 below:

| S. No. | Rotation Style             |
|-------|-----------------------------|
| 1     | Row1 towards RHS            |
| 2     | Row1 towards LHS            |
| 3     | Row3 towards RHS            |
| 4     | Row3 towards LHS            |
| 5     | Both Row1 and Row3 towards RHS |
To obtain the random secret keys, the DNA sequences are accessed via publicly available biological databases like FASTA and GenBank. It is done because the keys needed for enciphering must be random and non-repetitive, and genomic databases can be a good source of producing a vast number of keys that are truly random in nature. One such working example is given by Zhang, Liu & Sun, (2017) where random binary sequences are generated using genetic databases and these sequences help solve the generation and distribution of extremely long and robust keys that can be used in One-Time Pad (OTP) ciphers [14]. Once more than one random sequence is produced, they can be combined in several ways like shifting, multiplexing, and concatenating to yield a new crop of random sequences. The major shortcomings here are the transmission and storage of these sequences. The biological code has four bases: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). The length of DNA sequences in biological databases varies in length which is measured in base pairs (bp). One such example of chromosomal sequences in base-pair length are shown in Figure 4.

![Figure 4. DNA Sequence Lengths for a Cat [14].]
The encryption procedure can be described as follow:

i. The digital image is taken as input from the input file.
ii. A block of 54 pixels is read from the upper left side corner and mapped on the Rubik cube.
iii. These pixels are shuffled according to any one of the basic 18 rotations.
iv. A similar procedure is repeated for the remaining pixels of the image.
v. After the Rubik’s cube rotation, a random set of column keys ($C_k$) and row keys ($R_k$) are generated randomly from the DNA sequences.
vi. Then, pixels are read one by one column-wise and each pixel’s binary equivalent is XORed with a column key chosen from the set of $C_k$.
vii. Subsequently, the pixels are transformed row-wise by doing XOR between pixel’s binary values with a part of row key chosen from the set of $R_k$.
viii. The ciphered image is obtained and sent to the receiver.

![Diagram](image)

**Figure 5.** Encryption Procedure of VG3 Cipher.

The decryption method of the proposed cipher is exactly the opposite of the encryption course due to the symmetric nature of the algorithm. The various steps involved in the decryption are listed as follow:

i. The ciphered image is received through an insecure channel.
ii. The particular DNA sequence from the specific genetic database that was used to generate the random keys: $C_k$ and $R_k$ is communicated via an alternate channel.
iii. The row key $R_k$ is XORed with the binary values of all pixel’s row-wise.
iv. Consequently, the binary XOR operation is also applied to all pixel’s column-wise for reverse binary transformations.
v. The lower 54 pixels from the RHS corner are selected and rotated in reverse directions.
vi. Step v is repeated till all pixels in the image are rotated.
vii. The plain image is obtained, which is then processed by the receiver.
5. Results and Discussion

The encryption and decryption processes become quite straightforward once the DNA sequences are known and the random keys are obtained through it. However, it is vital to know that the unveiling of the DNA series will unravel the security triad and the whole message will be revealed to the eavesdropper. Sending the DNA series with the message over the insecure communication channel is not advised as it will increase the risk associated. Hence, this DNA sequence must be sent securely and privately to the other end. One such measure that can be employed for the same would be sending the exact genetic database name and sequence number in it over the telephone or any other secure means. Separating the ciphered message and DNA sequence will increase the cryptogram sanctuary.

The Rubik’s Cube-based cipher – VG3 cipher is realized on an HP Pavilion machine with Intel Core i5, 10th generation 1.19 GHz processor with 8 GB RAM. The proposed encryption algorithm is implemented in Python language using Google Colab (an online IDE provided by Google Inc.). An example of the image before and after encryption is shown below in Fig. 7.
As evident from the results obtained after the application of proposed cipher, the ciphered-image bears no resemblance to the plain-image and hence there is a thin chance of even imagining the plain-image by looking at the ciphered image. The VG3 cipher has been applied to multiple images with varying sizes and resolutions; however, the results still prove to be concrete against unauthorized attacks.

As rightly said, “a picture is worth a thousand words”, digital images can represent more than a thousand words, and that too in many ways. A lot of confidential data like defense maps, business trade secrets, etc. can be depicted easily through an image, and hence their security becomes the utmost priority of the security personals [15]. However, several factors like pixel correlations, spatial distribution, information redundancy, etc. come into play while doing cryptanalysis. The following analysis is done to check the newly proposed algorithm’s efficiency:

5.1. Security Analysis
The primary goal of any newly fangled cryptogram is to provide security against unauthorized attacks like brute-force attack, plaintext attack, ciphertext only attack, dictionary attack, etc. The chief point of consideration is that the main robustness lies in the secret key used in communication. The encryption key used in this planned work comprises of Row-key (Rk) and Column-key (Ck) which further contains multiple vectors to be used. This key acts as a One-Time Pad (OTP) which simply means that for the next round, a different key will be produced and used. Some vital properties that come with OTP are single usage only, known only to two communicating parties, truly random in nature, and complete discrete [16]. The usage of OTP-based enciphering keys makes the cryptosystem nearly impeccably secure.

The use of genetic material to harvest a wide variety of random keys makes the process even more computationally harder to crack. Due to the immense larger keyspace of the VG3 cipher, the exhaustive attack is nearly impossible on a standard colored digital image. Another imperative deliberation is the avalanche effect which means a small change in the encoding key will have huge effects on the ciphered image. It can be measured by the Number of Pixels Change Rate (NPCR), which designates the fraction of dissimilar pixels in different images [17]. The experiments reveal that NPCR for encoded images (with dissimilar keys) is approximately 99.6% i.e. the avalanche effect is not happening here. The correlation coefficient values in the encoded images are proximate to 0 which simply means that the neighboring pixels are not much related and do not reveal large information about the plain image. However, the correlation coefficient of the image before encryption is nearly 85%.

5.2. Timing Analysis
The efficiency of any enciphering algorithm depends not only on data safety but also on speed. Hence, the encoding and decoding timings of the proposed cryptogram must be as low as possible, so that speed must not be compromised. The encryption timings of VG3 cipher for multiple images are shown in the following table:

| Input Size (in Pixels) | Encryption Time (in seconds) |
|------------------------|-----------------------------|
| 512 * 512              | 38.6                        |
| 640 * 480              | 44.3                        |
| 700 * 400              | 51.7                        |
| 1920 * 1080            | 189.2                       |
Figure 8. Input Size vs Encoding Timings of VG3 Algorithm

The decryption timings of VG3 cipher for the same images are depicted in Table 3:

| Input Size (in Pixels) | Decryption Time (in seconds) |
|------------------------|-----------------------------|
| 512 * 512              | 36.4                        |
| 640 * 480              | 43.3                        |
| 700 * 400              | 49.9                        |
| 1920 * 1080            | 175.2                       |

Figure 9. Input Size vs Decoding Timings of VG3 Algorithm.

The above graphs also show that the encryption and decryption timings of VG3 cipher are increasing with increasing values of image size, hence the complexity of both processes are $O(n)$ i.e., linear in nature. The linear complexity of the proposed cipher ensures that the resource utilization of the algorithm will be optimal whether it is CPU time or memory, due to the fact that resources consumed by the algorithm is in accordance with the size of input data. It is a big advantage when compared to the other available encoding systems as VG3 cipher needs to do just one unit more work per item as the input size grows.

6. Conclusion and Future Work
The modern cryptography has turned the tables in the field of information security, but the attackers have also tried to gain an edge by modifying the tools according to the modern warfare techniques whether it is social engineering or hacking into someone’s bank account. Between this rat race of security personnel and attackers, there is always a requirement of newly fangled security solutions. In this paper, one such novel cryptographic approach is proposed which is based on DNA sequences and
Rubik’s Cube. The algorithm defined here makes use of DNA sequences present in the genetic databases to generate the secret keys which will be used to encipher and decipher the image. The Rubik’s cube is used to rotate the image in numerous ways so that it is distorted in a perplexed way. It is observed that the newly recommended encoding algorithm – VG3 cipher is quite secure due to the inclusion of several factors like biological sequences, rotation based on Rubik’s cube, and colossal keyspace. The speed test analysis also demonstrates that the proposed cryptogram has quite low execution timings and that too with linear complexity. Hence, it can be concluded that the VG3 cipher is pretty efficient and suitable for modern applications.

References
[1] Brummette, J., DiStaso, M., Vafeiadis, M., & Messner, M. Read all about it: The politicization of “fake news” on Twitter. Journalism & Mass Communication Quarterly, 2018, 95(2), 497-517.
[2] Gupta, L.M., Garg, H., & Samad, A. An improved DNA Based Security Model using Reduced Cipher Text Technique. International Journal of Computer Network & Information Security, 2019, 11(7), 13-20.
[3] Zhang, Y., Liu, X., Ma, Y., & Cheng, L. C. An optimized DNA-based encryption scheme with enforced secure key distribution. Cluster Computing, 2017, 20(4), 3119-3130.
[4] Know-It-All, An online article on Deoxyribonucleic Acid (DNA) structure available at URL: https://empoweryourknowledgeandhappytrivia.files.wordpress.com/2014/09/dna-structure1.jpg [Accessed 11-Sep-2020].
[5] Polfreman, R. and Oliver, B. “Rubik's Cube: Music's Cube", 2017.
[6] Rubik’s Cube Image, An online image available at https://www.dreamstime.com/photos-images/rubiks-cube.html [Accessed 16-Oct-2020].
[7] Buzady, Z. Resolving the Magic Cube of Effective Case Teaching: Benchmarking Case Teaching Practices in Emerging Markets–Insights from the Central European University Business School, Hungary. In Case Studies as a Teaching Tool in Management Education, 2017, pp. 79-103. IGI Global.
[8] Elayaraja, P. and Sivakumar, M. New Approach and Additional Security to Existing Cryptography Using Cubical Combinatorics, 2010.
[9] Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. A secure image encryption algorithm based on Rubik's cube principle. Journal of Electrical and Computer Engineering, 2012.
[10] Rawat, P. Mishra, R. and Upadhyay, A. Text Encryption By Rubik’s Cube Using Spatial Steganography, ISST Journal of Mathematics & Computing System, 7(2), 2016, 53-59.
[11] Helmy, M., El-Rabaie, E. S. M., Eldokany, I. M., & Abd El-Samie, F. E. 3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm. 3D Research, 8(4), 2017, 38.
[12] Zeng, D. X., Li, M., Wang, J. J., Hou, Y. L., Lu, W. J., & Huang, Z. Overview of Rubik's Cube and Reflections on Its Application in Mechanism. Chinese Journal of Mechanical Engineering, 31(1), 2018, 77.
[13] Dharavathu, K., & Mosa, A. Secure image transmission through crypto-OFDM system using Rubik's cube algorithm on an AWGN channel. International Journal of Communication Systems, 33(8), 2020, e4369.
[14] Zhang, Y., Liu, X., & Sun, M. DNA based random key generation and management for OTP encryption. Biosystems, 159, 2017, 51-63.
[15] De Lucia, M. J., & Cotton, C. A network security classifier defense: against adversarial machine learning attacks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, 2020, 67-73.
[16] Upadhyay, G., & Nene, M. J. One time pad generation using quantum superposition states. In 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016, 1882-1886, IEEE.
[17] Özkaynak, F. Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals. In 2017 International Conference on Computer Science and Engineering (UBMK), 2017, pp. 621-624, IEEE.