IJNRD.ORG ISSN : 2456-4184

International Research Journal
IJNRD
Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

IMAGE ENCRYPTION USING DYNAMIC DNA CRYPTOGRAPHY

[1]Arthiga, [2]Arya Roy

[1]B. Tech (ISDF) Student, [2]B. Tech (ISDF) Student,
[1]Department of Computer Science Engineering,
[1] Dr.M.G.R Educational and Research Institute University, Chennai, Tamilnadu, India

Abstract: Privacy protection for users is particularly crucial as image encryption plays a significant role in multimedia technology. Image encryption is crucial in order to give the user this level of protection and privacy and to safeguard against any unwanted user access. The goal of this research is to encrypt and decrypt image files using dynamic DNA cryptography. DNA (Deoxyribonucleic Acid) is a biological structure made up of the four fundamental nucleotides Adenine (A), Cytosine (C), Guanine (G), and Thymine. DNA Digital Coding is based on this biological structure (T). While sending sensitive information over the internet, encryption is always considered to be the most secure method. DNA cryptography and chaotic map approaches are suggested for this system to offer a digital image high-level security. Because of their size, digital images take a long time to process. The selective digital image encryption algorithm is used to speed up computing. This cryptosystem performs the permutation and diffusion process on a subset of the pixels in digital images. All DNA encoding rules depending on the pixel position of the digital medical image are used to build the DNA structure for digital images. The cypher picture is created by applying all DNA decoding rules based on the pixel value of the digital medical image.

Keywords **- Image encryption, DNA Cryptography, RGB, the Lorenz system, chaos.**

I. INTRODUCTION

The image is most frequently used as a communication tool in a variety of settings, including the medical field, laboratories, offices, military settings, etc. It is risky to send images over an unsecured internet. In order to prevent unwanted access to sensitive information, a secure channel must be used to transmit and receive the image. The secure transmission and storage of images over the internet are provided by the cryptography, which is a quiet image security methodology. Advanced systems include the medical profession, e-health, smart health, and telemedicine. End-to-end communication is accomplished by these technologies using digital information. Time is saved with digitization, yet it is open source. So, during transmission, hackers can manipulate the digital image. ensuring security, preserving an image's secrecy, and the two main problems are lowering the encryption algorithm's processing time. Cryptography, steganography, and watermarking are all used in various image encryption methods. The level of security that can be provided by these conventional techniques is insufficient.

II. LITERATURE SURVEY

Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang, and Mengmeng Wang proposed “Digital image encryption algorithm based on pixels” [1]. This study suggests a brand-new pixel-based image encryption technique. the process of watermarking, which makes it more difficult to decode, and finally by first pixel-by-pixel jumbling. To receive the final encrypted image, decide whether to view a camouflaged image or the pixels of the original image. The RGB pixel [2] displacement algorithm was another approach that Quist Kester and Koumadi created. This algorithm extracts the RGB value from the image. Then, individually reshape each RGB pixel into a 1-dimensional array, transpose the resulting matrix as "t," then once more reshape "t" into a 1-dimensional array, and finally transform the vector to a matrix with the same RGB dimension as the original image.

Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa proposed “Design of DNA-based Advanced coding customary” [3], They introduced the "Advanced Encryption Standard" with their DNA-based concept and implementation. Instead of using bits, they employed DNA to create their algorithm and all of its specifications (data, algorithm operations, and used functions).

Mansi Rathi, Shreyas Bhaskare, Tejas Kale,Niral Shah, Naveen Vaswani [4] proposed a new system that uses a transposition technique for the encryption process. In that they used fixed size block and the size of
Bahubali Akiwate, Dr. Latha Parthiban introduced a new method [5] A Dynamic DNA for Key-based Cryptography. The original message is converted to an ASCII character during the encryption process, followed by hexadecimal and binary conversions. Ciphertext communications will be produced using DNA Digital Coding and Key Combinations. A method that first retrieves an image and finds a hash value for this image was proposed by Manoj Dhande, Jay Bhatt, Paras Luvani, Yash Shah, and Mehulkumar Tandel [5]. The

image should then be divided into RGB values for each pixel, with DNA encryption performed on the RGB values. The encrypted image is eventually obtained.

The digital image is split into two matrices in our system: matrix1 and matrix2. Then, matrix1 is permuted after matrix2 has been turned into a DNA-encoded matrix using some base rules. Then, using DNA XOR operation key matrix should be the same, shuffle matrix 1 and merge matrix 1 and matrix 2. They transpose and transform blocks of plaintext into ASCII values. A random key is simultaneously produced and transformed into a DNA sequence. The value of the transposed block and the value of the DNA sequence are then combined to create a new matrix. After that, they rotate the matrix's rows and columns. Next, change the ASCII to character (Cipher text).

III. DNA CRYPTOGRAPHY

DNA cryptography is a field where several studies have been conducted and are currently being conducted, and it is anticipated that more effective solutions will be found to address the challenges and issues of the modern period. PCR (Polymerize Chain Reaction), DNA synthesis, and DNA digital coding are examples of DNA cryptography technologies that are already widely used. Here, we used the DNA Digital Coding approach, which enables encoding and decoding using binary values 0 and 1. DNA (Deoxyribonucleic Acid) is a biological structure that is made up of the four fundamental nucleotides Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). The proposed system integrates the traditional, currently used cryptosystems, uses DNA Digital Coding, and converts digital data into biological DNA sequences and vice versa. The proposed method might be used in instances of digital transactions like credit card/debit card payments, email, and SMS (Short Message Service) encryption where customers need more secure communication. binary values are assigned to the building blocks of DNA. The binary values make use of two state levels, like mixtures of 0 and 1. Given that DNA employs four nucleotides (A, T, G, and C), these nucleotides can be initiated and assigned binary values as shown in Table I [1]. Each base has two bits, with A=00, T=01, G=10, and C=11 using ATGC as the starting key. We will combine one base with all other bases, i.e., key combination, and then assign random values in accordance with their corresponding pattern values in binary, as indicated in table II. [1] The hexadecimal value can be transformed into binary form, DNA digital code, and eventually the amplified message by employing this key combination table. Our ability to generate a total of 72-bit keys from Table II, which consists of 64 bits of key value from key combination addition and 8 bits of ATGC, is shown here. A random key will be generated at the sender and sent to the recipient using the initial key in the form of ATGC. In this system, a new key with a specific value can be generated at the sender each time for a separate communication or transaction.

IV. PROPOSED SYSTEM

The digital image in our system is split into two matrices, matrix1 and matrix2, for processing. Then, using some base rules, these two matrices are converted into DNA encoded matrices, and matrix 1 is subjected to permutation. Then, using DNA XOR operation, join matrix 1 and matrix 2 by shuffling matrix 1. They conduct transposition and convert blocks of plaintext into ASCII values. A random key is created and transformed into a DNA sequence simultaneously. The DNA sequence value and the transposed block value are then added to create a new matrix. The matrix is then rotated in both the row and column directions. Then convert the ASCII to character (Cipher text).

V. IMPLEMENTATION

Here we implement the code for DNA algorithm usingpython which encrypt and decrypt the image file whichcomprises following steps:

1. Import the image
2. Analyses the image
3. Manipulate the image
4. Output in which result can do altered image
5. Decrypting the encrypted image
6. Retrieving original image

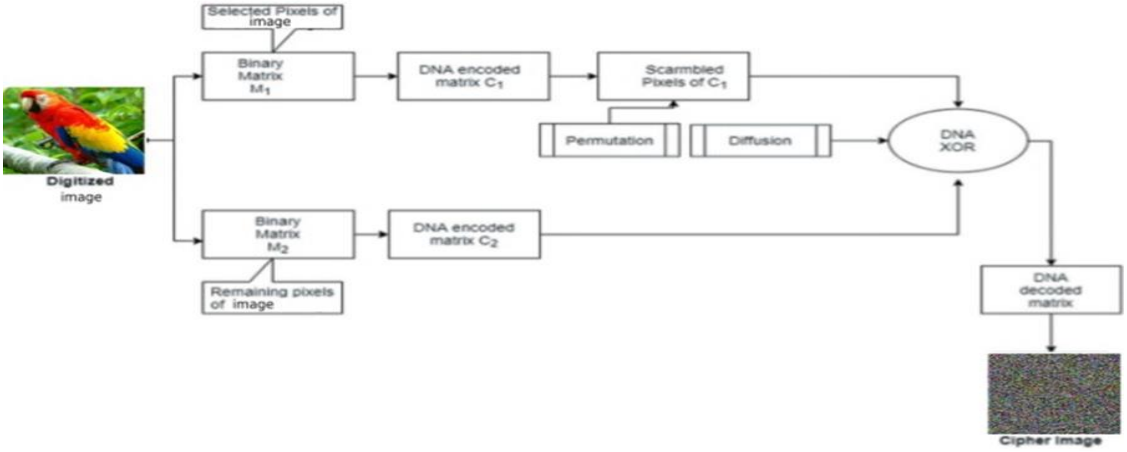

Fig. 1: Block Diagram

1. Import the image

Select the image for which you want to perform the encryption. Get the location where the image isbeing saved. Various types of the image can be selected is grey scale image and various image with format like jpeg and jpg.

2. Analyses the image

After selection of the image, analyze the image i.eSplit the image into three parts i.e (Red, Green, Blue).

3. Manipulate the image

Once the RGB split image is obtain apply the DNAalgorithm on each RGB (Red, Green, Blue) image simultaneously in order to obtain the encrypted image

4.Output in which result can do altered image Oncethe encrypted image is being obtained send it to the receiver through TOR socket.

5.Decrypting the encrypted image

Receiver receive encrypted image through TOR socket and apply DNA decryption

6.Retrieving original image

Receiver gets RGB simultaneously, merge RGBvalue & gets original image

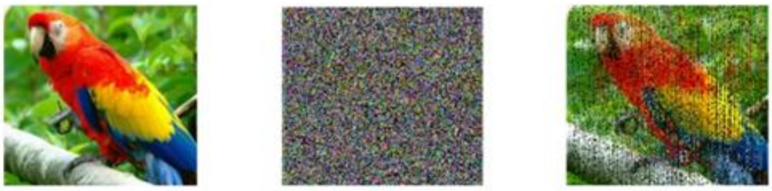

Fig.Input Image

Fig.Encrypted Image

Fig.Decrypted Image

Fig. 2: Sample Results

VI. CONCULSION

In this paper, a selective digitized image encryption using Taylor-Chirikov map and DNA sequencing is proposed. The original medically digitised image is first refurbished into two DNA-encoded matrixes, C1 and C2, utilising only the DNA rules based on the pixel index value. The Taylor-Chirikov map's system variables and parameters are used to generate the chaotic sequences. The chosen pixels of the encoded DNA matrix C1 are muddled using the Taylor chirikov map. The DNA-encoded matrix C1 and matrix C2 are mixed together using the DNA XOR method. To create a cypher image, the combined DNA-encoded matrix is converted from binary to grayscale to binary utilising all DNA decoding rules. The performance analysis demonstrates how the SIDE method improves security while simultaneously thwarting differential, exhaustive, and statistical attacks. For telemedicine, smart health, and e-health applications, the proposed SIDE approach requires less computational time.

ACKNOWLEDGMENT

We are really very thankful and we will also like to display our sincere recognition for our Head of the Department Dr S Geetha and our project guide Sayan Karmakar for the guidance and support in making this Research possible. Their Valuable guidance from initial to final level helps us to achieve to complete this research paper. Our sincere thanks to all the faculties who helped us to complete this and gave their valuable advice and made it easy to complete this.

VII. REFERENCES

[1] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang, and Mengmeng Wang. Digital image encryption algorithm based on pixels. October 2010.

[2] QuistKester and Koumadi. Cryptographic technique for image encryption based on rgb pixel displacement. *IEEE 4th ICAST*, 2012.

[3] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, and Mohamed Essam Khal- ifa. Design of dna-based advanced coding customary. *The Seventh IEEE International conference on Intelligent Computing and Information Systems (ICICIS)*, 7, December 2015.

[4] Mansi Rathi, Shreyas Bhaskare, Tejas Kale, Niral Shah, and Naveen Vaswani. Data security using dna cryptography. *IJCSMC*, 5:123–129, October Bahubali Akiwate and Dr. Latha Parthiban. A dynamic dna for key- based cryptography. *IEEE CTEMS*, 2018

[5] Manoj Dhande, Jay bhatt, ParasLuvani, Yash Shah, and Mehul Kumar Tandel. Image encryption using dynamic DNA cryptography. *International Research Journal of Engineering and Technology (IRJET)*, 7, may 2020.