International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST52310269

A Novel Image Encryption Algorithm Using DNA Cryptography

B.V.V.H. Chandra Sekhar[1], P. Gayathri Reddy[2], U. Mohan Rama Subramanyam[3], A.Akhila Reddy[4], M. Bhuvana[5]

[1] Assistant Professor, Department of Information Technology, Kallam Haranadha Reddy Institute of Technology, Chowdavaram, Guntur (Dt), Andhra Pradesh, India

[2, 3, 4, 5]B. Tech Students, Department of Information Technology, Kallam Haranadha Reddy Institute of Technology, Chowdavaram, Guntur(Dt), Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted: 15 March 2023
Published: 05 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
388-392

ABSTRACT

Many different technologies are used to encode and decode photos. However, the DNA cryptography method is the most significant of all of these. The study of DNA computing has given rise to a brand-new instinctive cryptographic field called DNA cryptography. Data transfers in today's environment require the highest level of security because they can be insecure. To safeguard the data from unauthorized recipients, our picture encryption technology either modifies the original image's pixels or inserts information inside them using the image as a cover. The image's pixels are transformed into DNA molecules of the form A C G T before being shared with recipients, who may then use decryption techniques to access the data.

Keywords : Encryption, Decryption, DNA Cryptography, Security, Privacy.

I. INTRODUCTION

These days, all financial and electronic transactions take place on the internet. Communication in a timely manner is crucial for both business and personal dealings. in a very secure way. In mathematical cryptography, numerous methods and systems have been created for encoding and decoding plain text. These approaches are thwarted by DNA cryptography methods and procedures. Many algorithms and systems have been published to incorporate the security of the shared content. In the course of normal business operations, text files including images are typically sent over an unprotected network, where anyone with access to your system can view them. With the help of our algorithm, we have attempted to protect all image transmissions against use or viewing by parties other than the intended recipients. Deoxyribonucleic acid, or DNA. DNA sculpts living things. It holds all of the details of any organism's physical characteristics. Each person's experience is different. Deoxyribonucleotides

are the monomers that make up the polymer known as DNA. Deoxyribose sugar, a phosphate group, and a nitrogenous base make up each nucleotide. There are two types of nitrogenous bases: purines (adenine and guanine), and pyrimidines (cytosine and thymine). The letters A, G, C, and T stand for these bases: adenine, guanine, cytosine, and thymine. (thymine). G and A are bonded to one other and to C. In procedures involving DNA like DNA computing and DNA cryptography, these bases and bonding are crucial. The use of bioinformatics in DNA computing and DNA cryptography is crucial.

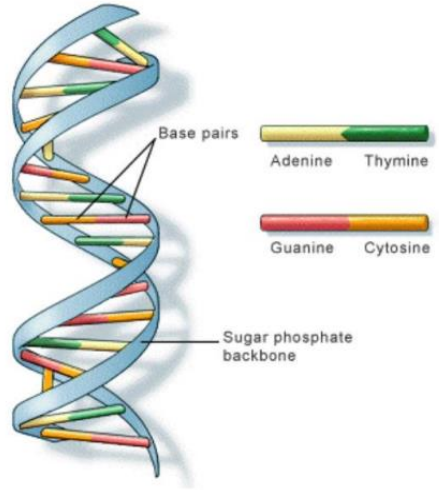


Figure 1.1 DNA structure

There is a great need to keep personnel information private in this day of abundant information. This data may comprise financial transactions, commercial agreements, and other such items. Steganography and cryptography are two methods that are frequently employed to safeguard data on a page. Steganography involves concealing the data, such as storing the secret data by slicing the least important bits of bytes from a picture without altering the image noticeably. While in cryptography, a number of methods have been employed to render the data incomprehensible to attackers. A key is used in cryptography to encrypt and decrypt data. Further categorization of cryptography is done into two groups. The same key is used for encryption and decryption in symmetric cryptography (also known as private key cryptography).THE other is asymmetric cryptography (or public key cryptography), in which there are two keys. Public key is used for encryption while private key is used for decryption. The key used for encryption is made public because it cannot be abused easily like trapdoor function.

1.2 DNA and Cryptography

DNA cryptography involves enciphering the plaintext using DNA computational techniques. Most of the cryptographic algorithms involve a large memory and computations like, One Time Pad in which there are non-repeating very large text pads, this technique will be very useful. A gram of DNA contains 1021 DNA bases and can store 108 terabytes of memory [2]. One trillion bits of binary data can be stored in one cubic decimeter of DNA solution [3].Moreover DNA based computations take very less time compared to other algorithms. The task of any cryptography algorithm is to secure the data for very large duration of time. In this technique, bases of DNA are arranged in random order and plaintext bits can be stored successfully using these bases. As this technique employs one time pad which is perfectly random cryptographic technique, the data can be secured for very long periods of time. In addition to memory, DNA molecules show parallel computation, which means DNA based processes are capable of intense processing. DNA chains have large scale of parallelism and its computing speed could reach up to 1 billion times per second computations [3]. DNA based computers also have very less power consumption, which is equal to one – billionth of a traditional computer [3].

II. LITERATURE REVIEW

2.1 Ancient Techniques :

The science of securing important messages and information from outsiders is very old. The two methods used for data security are steganography and

cryptography. Steganography was used by Histiaeus in 5th century BC. He sent his messages by tattooing shaved head of a slave and sending him as a carrier when the hair grew back [6]. As for the cryptographic methods of data security many ciphers had developed like Ceaser Cipher, One Time Pad Cipher, Transposition Cipher and many more.

2.2 Modern Techniques There are several cryptographic algorithms like AES, DES and RSA, which are used for securing data from eavesdroppers. Steganography is used in slicing least significant bits for hiding the information. As far as the DNA cryptography is concerned, the Pioneering work is done by

Ashish Gehani et al and Amin et al after L. M. Adleman showed the capability of molecular computation in 1994 [7]. Ashish Gehani et al used DNA cryptography technique using one time pad. They implemented DNA cryptography using two techniques; DNA cryptosystem using substitution and DNA cryptosystem using XOR OTP. The latter technique has been discussed here. For XORing the message bits with OTP random bits, the Vernam Cipher [9] has been used. Now suppose S is the sequence of R uniformly distributed bits known as a one-time pad. Sender and the receiver have the copy of sequence S. L is the number of bits of S that have not been used for encrypting a message. Two binary inputs give 0 if they are same, when they are XORed and give 1 if they are different. When a plain text binary message has to be sent, each bit has to b XORed with the bits of sequence S. If M is the message and C is the ciphered message then Ci = Mi XOR Si where i = 1,2,…..n. After encryption the cipher text is sent. At the receiver's end, the same sequence S will be used to decrypt the cipher text to obtain the plain text. Cipher text C is XORed with bit sequence of S to obtain the plain text i. e. Mi = Ci XOR Si.

To implement Vernam Cipher using DNA molecules,

the following steps are required.

i. Encipher the message
ii. Create one time pad using DNA
iii. Realization of XOR operation These operations are realized using DNA tiling implementation. In this tiling long chains of inputs and outputs are created. DNA tiles are multi-strand complexes which have two or more double helical domains in a way that individual oligonucleotide chains might base pair in one helix then cross over and base pair in another helix. Complexes involving cross overs create tiles which are thermally stable

DNA Lookup table			
A=CGA	K=AAG	U=CTG	0=ACT
B=CCA	L=TGC	V=CCT	1=ACC
C=GTT	M=TCC	W=CCG	2=TAG
D=TTG	N=TCT	X=CTA	3=GCA
E=GGC	O=GGA	Y=AAA	4=GAG
F=GGT	P=GTG	Z=CTT	5=AGA
G=TTT	Q=AAC	<space>=ATA	6=TTA
H=ATG	R=TCA	,=TCG	7=ACA
I=ATG	S=ACG	.=GAT	8=AGG
J=AGT	T=TTC	:=GCT	9=GCG

And hence the encryption and decryption can be done using the above table. Both sender and the receiver should have this lookup table for encryption and decryption. The simplified diagram of their implementation of this scheme is as follows:

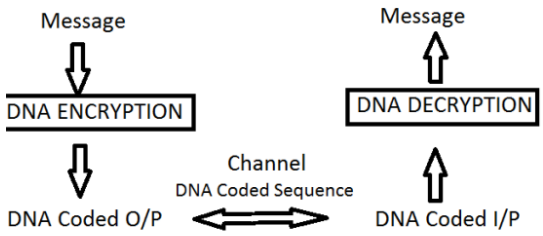


Figure 2.3 Encryption using Lookup Table

III. PROPOSED MODEL /ALGORITHM

Image Encryption Algorithm, Section 3. Figure 1 shows the overall encryption procedure. The procedures for encryption are as follows, assuming that the size of the initial grayscale image I is M N:

Image I, the logistic map's starting values of a0 and b0, the parameters a and b, the Chebyshev's map's initial values of z0 and q0, and the parameters wz and wq are all inputs.

The encrypted image is the output.

Step 1: Create a two-dimensional matrix called I from the original grayscale image I. Let's call two arrays R and C. These are used to record the rows and columns of picture I, respectively.

Step 2: Create the two one-dimensional descending index sequences using logistic mapping (3) to exchange the rows and columns of matrix I, respectively. thus, we

Step 3. Convert image I into a binary two-dimensional

matrix I. The size of I is $M \times N$rows and eight columns.

Step 4. Generate a storing unit P using (7) of the Chebyshev mapping. Get a sequence of iterations C with P. Then, generate a random integer $r2$ from one to six. Thus, we can decide which rule to use among the six types of complementary base pairs rules. Finally, according to each value of ci, we can decide the method to replace the nucleotides xi in the DNA sequence X. The method of iterative substitution is as follows: switch ci; case 0, do not change xi; case 1, $xi = L(xi)$; case 2, $xi = L(L(xi))$; case 3, $xi = L(L(L(xi)))$. The complementarily substituted DNA sequence is X.

IV. Experimental Results

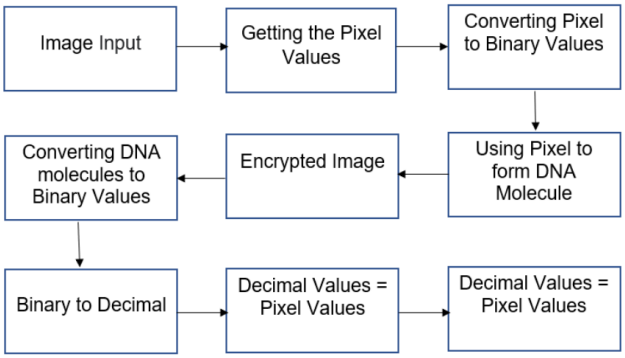
In our experiment, we first set the initial values and parameters of the logistic map: $a0 = 0.3575123321123321$, $b0 = 0.5575123321123321$, $\mu a = 3.775123321123321$, and $\mu b = 3.875123321123321$. For Chebyshev's map, we set $z0 = 0.6398711122233345$, $q0 = 0.2298711122233345$, $wz = 5.299233234567891$, and $wq = 4.289233234567891$. The size of the original grayscale image was 256×256.

V. WORK FLOW OF THE ALGORITHM

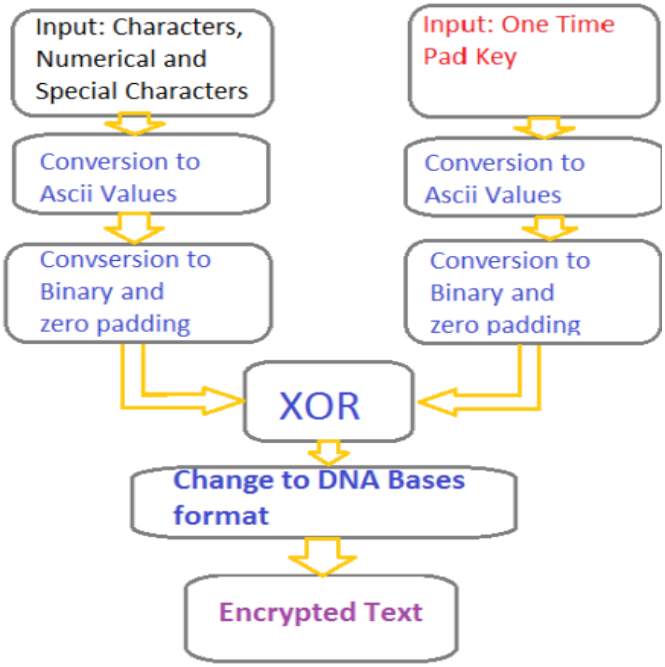
Algorithm and the Workflow

- As Input, We can take any image as of our need.
- Using python inbuilt function we will be getting the pixel values of the image and converting them into binary using inbuilt binary function.
- Once we have the binary values of the pixels then we will be using DNA molecules: adenine (A), cytosine (C), guanine (G), and thymine (T) and its binary coding to encrypt the image/pixel data.
- Using the above DNA-binary coding we will be encrypting our pixel values in the form of DNA molecules.
- This algorithm comprises of the encryption part of our project.

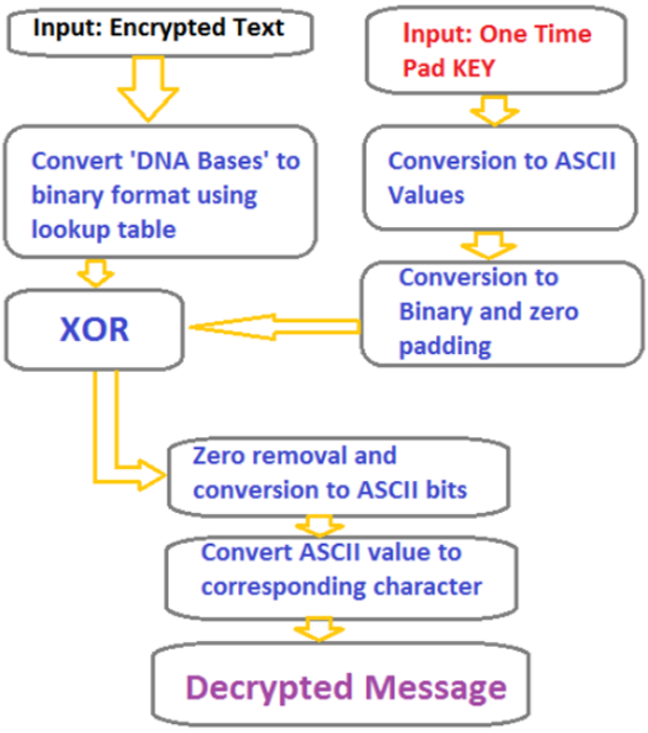
VI. BLOCK DIAGRAM



VII. DNA ENCRYPTION FLOW CHART



VIII. DNA DECRYPTION FLOW CHART



IX. CONCLUSION AND CHALLENGES

Despite being computationally demanding, cryptographic techniques have facilitated solutions to a variety of security issues in image and video processing. Even though the different applications come with different challenges, it is clear that the signal processing community will have to face three main challenges in future work. First, the utility and limitations of cryptography are not very well known to the community, which hampers the widespread consideration of cryptographic solutions for security problems in image and video processing. Second, cryptographic operations are often computationally expensive. Efficient usage of cryptographic protocols is therefore imperative. And third, certain cryptographic techniques cause ciphertext expansion of two orders of magnitude, such as public-key encryption of image pixels. Efficient data packing strategies and operations are then needed.

X. REFERENCES

[1]. Javier Resano, "A Hardware Implementation of the Smith-Waterman Algorithm for DNA Comparison", IEEE 2012.

[2]. Radu Terec et al, "DNA Security using Symmetric and Asymmetric Cryptography", IJNCAA (ISSN 2220- 9085), 2011 [3] Yunpeng Zhang and Liu He Bochen Fu. "Research on DNA Cryptography, Applied Cryptography and Network Security", Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0218-2, InTech, 2012. [4] Zhihua Chen et el. "Efficient DNA Sticker Algorithms for DES", IEEE 3rd international conference on Bio-inspired computing, 2012

[3]. Taylor C. et al, "Hiding Messages in DNA Microdots", Nature 1999

[4]. M. Reza Najaf Torkaman et al, "Innovative Approach to Improve Hybrid Cryptography by using DNA Steganography", IJNCAA 2012

[5]. L. M. Adleman, "Molecular Computation of Solutions to Combinatorial Problems", Science-266:1021 {1024}, 1994

[6]. Ashish Gehani et al, "DNA Based Cryptography", DIMACS Series in Discrete Mathematics and Theoretical Computer Science Volume 54, 2000

[7]. David Kahn, "The Codebreakers", Macmillan, NY, 1967

[8]. Naveen Jarold K. et al, "Hardware Implementation of DNA Based Cryptography", IEEE (Conference of ICT), 2013.

Cite this article as :
B.V.V.H. Chandra Sekhar, P. Gayathri Reddy, U. Mohan Rama Subramanyam, A. Akhila Reddy, M. Bhuvana, "A Novel Image Encryption Algorithm Using DNA Cryptography", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 2, pp. 388-392, March-April 2023.
Available at doi : https://doi.org/10.32628/IJSRST52310269
Journal URL : https://ijsrst.com/IJSRST52310269