International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

IMAGE ENCRYPTION USING DYNAMIC DNA CRYPTOGRAPHY

Asmit Pawar[1]
Department of Computer Engineering
Datta Meghe College of Engineering, Airoli, Thane, Maharashtra, India

Samida Mahind[2]
Department of Computer Engineering
Datta Meghe College of Engineering, Airoli, Thane, Maharashtra, India

Aishwarya Manje[3]
Department of Computer Engineering
Datta Meghe College of Engineering, Airoli, Thane, Maharashtra, India

Prof. Nusrat Parveen[4]
Department of Computer Engineering
Datta Meghe College of Engineering, Airoli, Thane, Maharashtra, India

Abstract

A dynamic DNA for key-based Cryptography that encrypt and decrypt plain text characters, text file, image file and audio file using DNA sequences. Cryptography is always taken as the secure way while transforming the confidential information over the network such as LAN, Internet. But over the time, the traditional cryptographic approaches are been replaced with more effective cryptographic systems such as Quantum Cryptography, Biometric Cryptography, Geographical Cryptography and DNA Cryptography.

Keywords – Encryption, Decryption, cryptography, DNA

1. INTRODUCTION

The image is most widely used communication mode in the different areas like medical area, research area, business area, military area, etc. The important image transfer will take place over an unsecured Internet network. Thus, there is need of proper security for the image to avoid the unauthorized person's access the important information. The cryptography is a kind of image security method that offers the secure transmission and storage

method for the image over the internet DNA Cryptology combines cryptology and modern biotechnology. DNA stores memory at a density of about 1 bit/nm3 where conventional storage media requires 1012 nm3/bit. No power is required for DNA computing while the computation is taking place DNA Cryptography can be defined as a hiding data in terms of DNA Sequence.

1.1 Objectives

1. To protect the digital data confidentiality.
2. It helps keep information secure.

2. LITERATURE REVIEW

Today, the world is going to be digitalized in all the ways. Every business unit, government and private sectors, research units are using the digital image as transferring mode for every critical data. These images over the internet which will not be secure. Therefore, there is a need of image security.

Currently, there exists various image security techniques like encryption, watermarking, steganography, etc. There are various image encryption systems to encrypt and decrypt data, and

there is no single encryption algorithm satisfies the different image types. Image stitching and image steganography security can be provided to any image which has to absent over the network or transferred using any electronic mode.

There is a message and a secret image that has to be sent. The secret image is divided into parts. After DNA was introduced as the most advanced form of information representation, different algorithms were developed and proposed by the researchers to provide better security. This section highlights some of the algorithms which used nucleotide sequence in order to encrypt the digital data.

The main idea behind our project is being taken from our observation that there are many security algorithms for text but very few algorithms for image security. Various algorithms are available for image security but they are very complex algorithm.

2.1 Digital Image Encryption Algorithm Based on Pixels

Working Scrambling the image pixels, then through the method of watermark increasing the difficulty of its decoded. At last, choose a camouflaged image to vision or the pixels of the true image, getting the final encryption image. The key parameters are encrypted by Elliptic Curve Cryptography (ECC). We verify and analyze the algorithm security, reliability and efficiency with an experiment the experiment results and algorithm analyses indicate that the new algorithm possesses a large key space and high-level security and the time needed for encrypting the interactive image tends to +00. It provides a new access to satisfy high level security of interactive information requirements in the fields of aerospace, military, confidential, financial and economic, national security and so on [3]

Advantages

- Use of watermark which increases difficulty of decoding the image

Disadvantages

- Use of complex encryption algorithm
- Use of camouflaged image

2.2 Data Security Using DNA Cryptography

Working

Each block size in this algorithm is taken as 16 bytes. The size of the key matrix is also the same that is 16 bytes. The values of the Key Matrix are randomly generated and these values range from 0 to 127. In this algorithm, the concept of poly alphabetic substitution is followed. This algorithm also makes use of the Byte-Rotation technique [4]. The encryption of the key is done with the help of DNA Sequencing.

Advantages

- Use of polyalphabetic substitution
- Block size and key matrix is of 16byte

Disadvantage

- Transposition may lead to complications
- Difficult to implement

2.3. Cryptographic Technique for Image Encryption Based on The RGB Pixel Displacement

Working

Step1: -Import data from image and create an image graphics object by interpreting each element in a matrix. Extract the red, green, blue component as ′r′,’g’,’b’.

Step2: - Reshape red, green, blue into I-dimensional array as ′p′,’1’,’y’

Step3: - t= [y;1; p]

Step4: -Transpose ′t′

Step5: - Let 1 =f 1 “part of n): (1/3rd part of n) as 1 dimensional array Let y = (1/3 rd. part of n):

(2/3rd. part of n) as I-dimensional array Let p = (2/3rd part of n): (nth) as 1-dimensional array

Step6: - Transform 1, p, and y from vector to matrix with the same dimension of ′r′ or ′g′ or ′b′ of

the original image.

Step7: - Finally the data will be converted into an image format to get the encrypted image.[5]

Advantages

- Simply uses image data to encrypt the image

Disadvantages

- Size of the image should be known.
- Data in the image can be lost.

2.4 Problem Statement

The system's main aim is to transfer the image over the internet in a secure manner. The system should use a strong algorithm and it should generate a unique pattern. On every image successful transmission. The system should also take care that there is no data loss in the image. The system will also understand if someone changes the data of the image in between sender and receiver.

3. PROPOSED SYSTEM

3.1 Algorithm

We used Dynamic DNA Encryption Algorithm to encrypt an image we will see how Dynamic DNA Works DNA digital coding is required in which we are considering DNA basic nucleotides assigned with binary values. The binary values use two state levels such as combinations of 0 and 1. As the DNA digital coding uses four nucleotides (A, T, G, and C) can be initialized and assigned with binary values as shown in table

Binary Value	DNA Digital Coding
00	A
01	T
10	G
11	C

Table 1 - DNA DIGITAL CODING

Using ATGC as an initial key, every base has 2 bits like A=00, T=01, G=10, and C=11.We are going to combine one base with all other bases i.e. key combination and later assigning of random values can be made respectively with their equivalent pattern values in the form of binary is as shown in table from the table II, here we are able to generate total of 72-bit keys that is 64 bits key value from key combination adding along with 8 bits of ATGC. The initial key in the form of ATGC will be used to produce a random key at the sender will be submitted to receiver. In this system, every time we can generate key at sender with particular value will be randomly changed for different communication or transaction.

Key Combination	Patterns	Value
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	2
TA	1111	6
TT	0111	15
TG	1001	7
TC	1010	9
GA	0100	10
GT	1000	4
GG	1100	8
GC	1110	12
CA	1011	14
CT	0000	11
CG	1101	0
CC	1111	13

Table 2 - KEY COMBINATION

Binary value:

01011100011101010011000001100101001100000101110001
11010100110000011000010110000101011100011101010011
00000011001000110000001100100011000001011100011101
01001100000110010100110000010111000111010100110000
01100001011000010101110001110101001100000110001000
11011001011100011101010011000001100101001100000101
10001110101001100000110000101100001010111000111010
10011000001100010011001100101110001110101001100000
11001010011000001011100011101010011000001100001011
00001010111000111010100110000011000100011011 1

After the binary value it can be now converted to DNA digital coding format.

DNA Digital coding:

From table I, we can write

TTCATCTTACAATGTTACAATTCATCTTACAATGATTGATTTCATCTTACAAACAGACAAA
CAGACAATTCATCTTACAATGTTACAATTCATCTTACAATGATTGATTTCATCTTACAATG
AGACTGTTCATCTTACAATGTTACAATTCATCTTACAATGATTGATTTCATCTTACAATGA
GTGTGTTCATCTTACAATGTTACAATTCATCTTCATGATTGATTTCATCT
TACAATGAGACTC

Now from table II, by using the DNA digital coding and the key combination we can generate amplified message that can be transferred over the network as shown below.

Amplified Message:

11111110100111110010010101111111001001011111111010011111001001010111001101110011111
11110100111110010010100110001001001010010000100100101111111110100111110010010101111
11110010010111111110100111110010010101110011011100111111111010011111001001010111000
01001001111111111010011111001001010111111100100101111111101001111100100101011100111
01110011111111101001111001001010111000101110111111111010011111001001010111111110011
00101111111101001111100100101011100110111001111111110100111
11100100101011100010010 1001

3.2 Details of hardware & software

- Python3
- TOR
- Linux
- Computer

3.3 Methodology

DNA encoding and decoding for image

A DNA sequence contains four nucleic acid bases A (adenine), C (cytosine), G.(guanine), T (thymine), where A and T are complementary, and G and C are complementary. In the binary, 0 and 1 are complementary, so 00 and 11 are complementary, 01 and 10 are also complementary. In this paper, we use C, A, T, G to denote 00, 01, 10, 11, respectively. For 8-bit grey image each pixel can be expressed a DNA sequence whose length is 4. For example: If the first pixel value of the original image is 173, convert it into a binary stream as T10101101U, by using the above DNA encoding rule to encode the stream, we can get a DNA sequence TTTGAU. Whereas using 00, 01, 10, 11 to denote C, A, T, G, respectively, to decode the above DNA sequence, we can get a binary sequence T10101101U.

4. Implementation Details

4.1 Module & Description

Our system mainly contains of these module

1. Import the image

2. Analyses the image

3. Manipulate the image

4. Output in which result can do altered image

A. Import the image

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

B. Analyses the image

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

C. Manipulate the image

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

D. Output in which result can do altered image Once the encrypted image is being obtained send it to the receiver on the internet.

5. TESTING

Test case ID	Objective	Steps/ Description	Input	Expected Output	Actual Output	Result	Remark
TID1	Fetching the image from storage.	1.Go to the folder 2. select the image	Image	Image Should be selected	Image Fetched	Successful	Test Case Pass
TID2	Splitting the image pixels into RGB values	1.Select the pixels row wise 2. Split it to individual RGB values	Pixel Values	Getting RGB value of each pixels	Individual RGB value	Successful	Test Case Pass
TID3	Applying DNA Encoding	1.Create Key for Encryption. 2.Apply Encryption-key on the binary pixel values.	Pixels Binary values	Encrypted image.	Image encrypted d.	Successful	Test Case Pass
TID4	Send the encrypted image to receiver's end		Image	Sending encrypted image successfully	Image Send.	Successful	Test Case Pass
TID5	Applying DNA Decoding	1.Apply Encryption-key on the binary pixel values.	Pixels Binary value	Decrypt image	Image Decrypt ed	Successful	Test case pass

6 Result & Analysis

We have successfully encrypted the image and we have transmitted the encrypted image on the internet. After receiver has successfully received the encrypted image then it will split the image into RGB and then we will get the decrypted image we have also analysed that the image with less size requires less time to encrypt and there is no data loss .

7. CONCLUSION AND FUTURE SCOPE

In this work we have implemented the image encryption using dynamic DNA cryptography. Here it applies DNA cryptography algorithm on the image. Thus, we are taking advantage of the DNA cryptography for image encryption. Thus, we have developed a DNA image Encryption to provide security on the image data structure. Then we can provide this algorithm to the country's military & special agency where images are important data structure. Example: Sending the military Map or weapons model from one military point to another military point

8. REFERENCES

[1] Naveen Jarold, P Karthigaikumar, N M Sivamangai, Sandhya R, Sruthi BAshok,"Hardware Implementation of polymer primarily based Cryptography",Conference on data and Communication Technologies, IEEE, pp. 696-700,2013.

[2] M R Saranya,Arun K Mohan and K.Anusudha, "Algorithm for Enhanced Image Security Using polymer and Genetic Algorithm", IEEE, April 2015.

[3] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang ,Mengmeng Wang "Digital Image Encryption Algorithm Based on Pixels"

[4] Mansi Rathi, Shreyas Bhaskare, Tejas Kale, Niral Shah, Naveen Vaswani ,"Data Security Using DNA Cryptography" IJCSMC, Vol. 5, Issue. 10, October 2016, pg.123 – 129

[5] Quist Kester, Koumadi "Cryptographic Technique for Image Encryption based on RGB pixel Displacement " 2012 IEEE 4th ICAST

[6] Prajapati Ashishkumar B and Hindu deity Barkha, "Implementation Of DNA cryptography In Cloud Computing and exploitation Socket Programming", IEEE, Jan 2016.

[7] Ajit Singh and Reena Singh, "Information concealment Techniques supported DNA Inconsistency: AN Overview", IEEE, May 2015.

[8] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa, "Design of DNA-based Advanced coding customary", IEEE, pp. 390-397,2015.

[9] Deepak Singh Chouhan,R.P.Mahajan, "An subject area Framework for Encryption & Generation of Digital Signature victimization DNA Cryptography", IEEE,pp. 743-748, June 2014