Secure Image Encryption Based On DNA Algorithm

Ms.N.Suneetha *[M.Tech, Ph.D.] *1,*
Boora Namratha Varshini#1**, Jagarapu JayaDeepika**#2**, Gampa Hema Aparna**#3 **, DevarasettyNirmal Sai**#4
**1Associate Professor CSE Department,*
#1, 2, 3, 4 students CSE Department, Lendi institute of engineering and technology,
VIZIANAGARAM, ANDHRA PRADESH, INDIA.
[1]namrathavarshini999@gmail.com [2]deepujagarapu@gmail.com [3]hemaaparna66@gmail.com [4]nirmalsai94@gmail.com

Abstract—**In our project, we propose a novel image encryption algorithm which uses the advantages of both image permutation and DNA based encryption. In the present day scenario it is known that, in the increasing of information threats it is really a challenging task for a user to transfer sensitive data over a unsecure channel. By keeping this in mind we had encrypted or proposed this technique. This provides multilevel security for the image. In the early stages we perform pixel permutation and then mathematical operations followed by DNA encoding for performing DNA encryption. Here DNA is built from four nucleic bases. They are A(adenine), C(cytosine), G(guanine), T(thymine).AT and CG are complemented to each other. Their values can be 00 10 01 11 respectively. a particular pixel intensity value is considered and converted into binary form and for that DNA coding is done where we will get the DNA sequence .In the second stage, for the DNA sequence random numerical values are assigned to each codon. For this, encryption is done using play fair cipher through which encrypted image is produced.**

Keywords— **DNA sequence, key generation, encryption, DNA addition, DNA complementary rule.**

I. INTRODUCTION

Now a days we are aware of that with the ever increasing growth of multimedia applications, security has become an important issue on communication and storage of images. People can easily transfer the various multimedia information through network. However, because of the openness of the network, people have to take more and more attention on security and confidentiality of multimedia information. traditional encryption algorithms, such as DES, IDEA, AES etc., are not suitable for image encryption. It has been noticed that traditional text encryption approaches fail to protect the image information effectively due to some special properties of the image and some specific requirements of image processing such as enormous size, strong redundancy of uncompressed data and high correlation coefficient. DNA cryptography is emerging as a new cryptographic field where DNA is used to carry the information. It is used as information carrier and the modern biological technology is used as implementation tool, and the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are explored for signature, and so on. DNA computing to solve the hidden insecurity problems existing when images are confused using the chaotic encryption technology, using the chaotic encryption technology. First, we confuse the digital image pixels using the chaotic encryption technology. We then diffuse the confused pixels using DNA encoding. The diffusion process is also applied to the chaotic encryption technology and, finally, we obtain the encryption result. DNA coding techniques is a method that has been verified via a large number of experiments and security analyses to prove the security and rationality of the algorithm.

II.EXISTING SYSTEM

The existing encryption algorithms such has the DES, AES, 3DES, Blowfish, RSA are the traditional methods and they are not suitable for encrypting an image. The drawbacks with these algorithms are due to the low computing effect and low avalanche effect and to send a long key. For this we are introducing DNA algorithm.

A. Analysis for Existing System:

DES is a block cipher that uses shared secret key for encryption and decryption. DES is algorithm as described by Davis R. The AES cipher is almost identical to the block cipher Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. Blowfish is one of the most common public domain encryption algorithms provided by Brucie Schneider. RSA is a public key algorithm invented by Rivest, Shamir and Adleman. The key used for encryption is different from (but related to) the key used for decryption. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

A. Limitations for existing systems

DES: Its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours.

It was recognized that DES was not secure because of advancement in computer processing power.

3DES: It is slower than other block cipher methods.

It has poor performance.

AES: AES in Galois/Counter Mode (GCM) is challenging to implement in software.

The size of the key length is too long that makes it complex sometimes.

Blowfish: It is block cipher 64-bit which can also be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits, default 128 bits.

It is compact as it can execute in less than 5 kb memory.

RSA: A disadvantage of using public key cryptography for encryption is speed: they are very slow in processing.

III.PROPOSED SYSTEM

The growth of computers and communication systems brought with it a demand from the private sector for means to protect information in digital form and to provide security services. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Some of data may be secret information which is candidate to unauthorized user away variety of techniques have been used such as cryptography and data hiding. . A cipher is a plain of algorithms that create the encryption and the decryption.

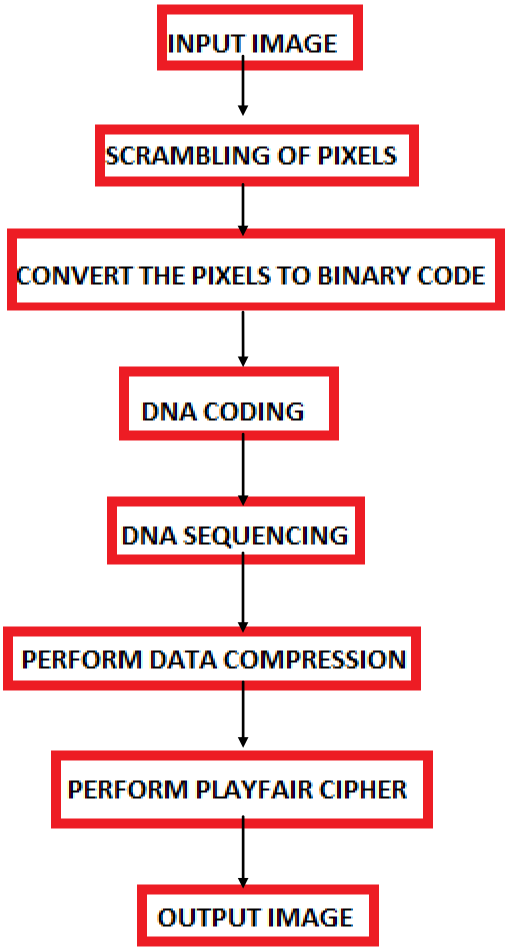
Steganography is the art of science of writing hidden messages with in another seemingly innocuous message, or carrier. In biology Deoxyribonucleic acid (DNA) is the master molecule whose structure encodes all the information needed to create and direct to the chemical machinery of life. In 1953, the structure of DNA was correctly pre defined. DNA Based Data Encryption and Hiding Using Play fair and Insertion Techniques dictated by Watson and Francis crick that DNA module consists of two long polynucleotide chains each of these chains is known as DNA chain, or DNA stands which is made from simple subunits, called nucleotides. Each nucleotide consists of sugar phosphate molecule with a nitrogen-containing side group, or bases .The bases are of four types ATCG (Adenine, Cytosine, and Thymine, Guanine), corresponding to four distinct nucleotides, labeled

A. Algorithmic Specification:

To simplify the discussion, we start with the most basic version and give a simple example. The more complicated version of our method will be presented after this basic one is given. Suppose the secret message M is 01001100. Let S be ACGGTTCCAATGC. Our coding steps are as follows:

1. We first code S into a binary sequence by using the binary coding scheme. Thus the sequence S will now become 00010101111010100001110 01.
2. Divide S into segments whereby each segment contains k bits. Suppose k is 2. Then we have the following segments: 00, 10, 11, 11, 01, 10,11, 10, 01.
3. Insert bits from M, once at a time, into the beginning of segments of S. The result is as follows: 0000, 1110, 0101, 0111, 1010, 1100, 0001, 0110, 01. We should ignore those segments without any secret message inserted. Thus, we will have the following segments: 0000, 1110, 0101, 0111, 1010, 1100, 0001, 0110. Concatenating the above segments, we have the following binary sequence: 00001110010101111010110000010110.
4. We use the binary code scheme to produce the following faked DNA sequence S’=AATGCCCTGGTAACCG. As the reader can see, this sequence is quite different from S.
5. We send the above sequence S’ to the other irrelevant sequences.

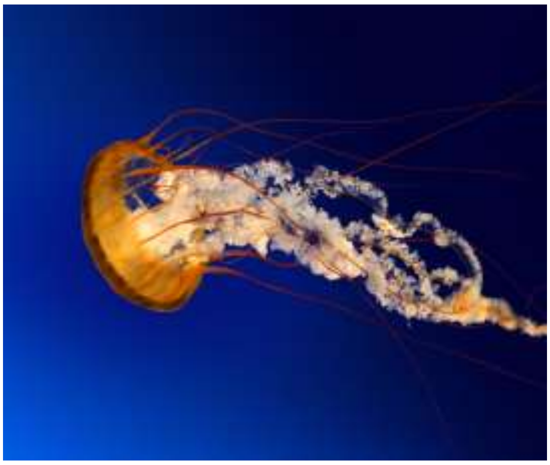
PROPOSED ARCHITECTURE



A.Advantages

- Speed - Conventional computers can perform approximately 100 MIPS (millions of instruction per second).
- Minimal Storage Requirements - DNA stores memory at a density of about 1 bit per cubic nanometer where conventional storage media requires 12 10 cubic nanometers to store 1 bit. In essence, mankinds collective knowledge could theoretically be stored in a small bucket of DNA solution.
- Minimal Power Requirements - There is no power required for DNA computing while the computation is taking place. The chemical bonds that are the building blocks of DNA happen without any outside power source. There is no comparison to the power requirements of conventional computers.

A. FOR ORIGINAL IMAGE:



B. IMAGE AFTER SCRAMBLING:

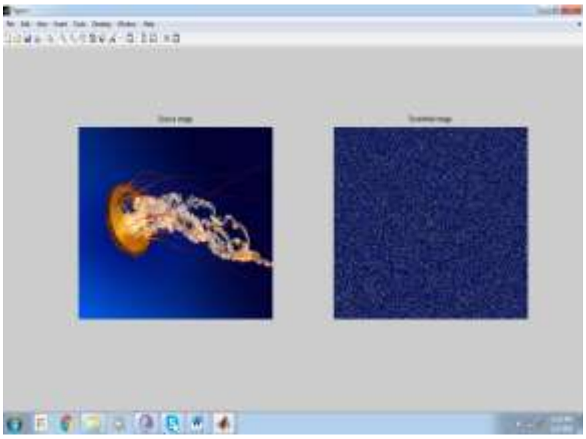


FIG.2. Complete scrambled image

C. CHANGING THE PIXEL INTENSITIES:

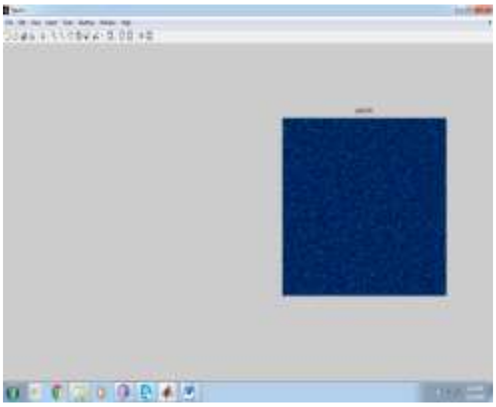


FIG 4. This is the resultant image when the pixel intensities are changed from darker to brighter and higher to darker side.

D. HISTOGRAM EQUILIZATION

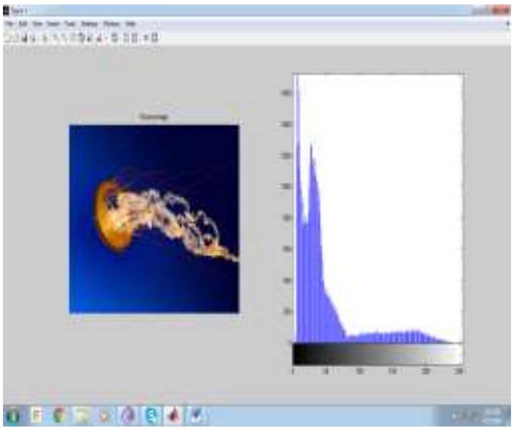


FIG.4.histogram formation of the original image

E. CONVERSION TO GRAYSCALE IMAGE:

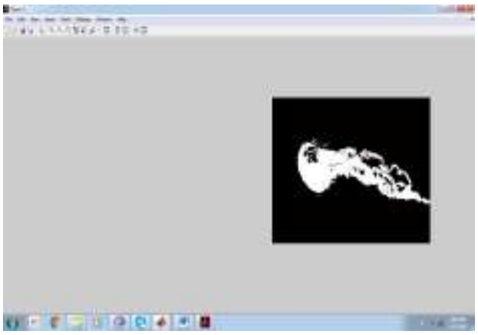


FIG.6. Conversion of the image from color to grayscale image

F.CONVERSION TO BINARY VALUES:

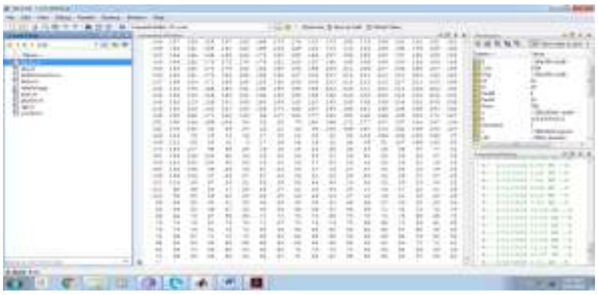


Fig.8. Original pixel values

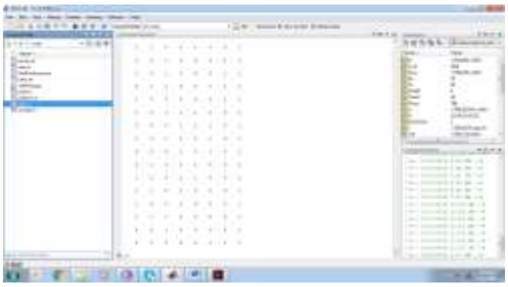


FIG.8. Pixel values after conversion of binary values

G. GENERATION OF DNA SEQUENCE:

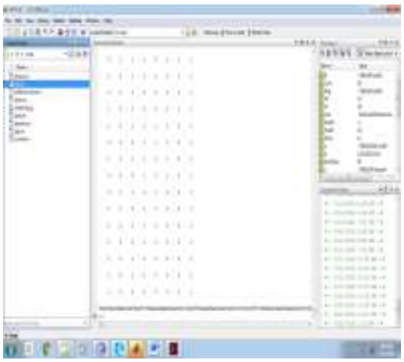


FIG.9. Formation of DNA sequence for the obtained binary values

H.ENCRYPTED OUTPUT

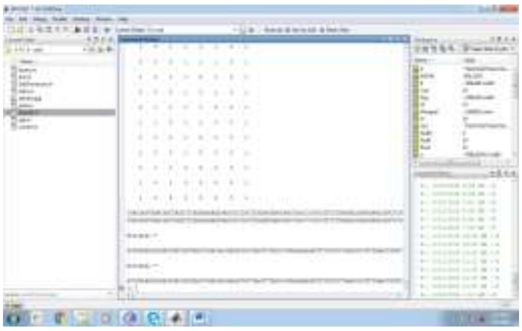


FIG..9. resultant image when the DNA sequence is encrypted using playfair cipher

IV. CONCLUSION

“DNA Based Image Encryption” has been successfully completed. Here we are using the play fair cipher technique to encrypt the image.

In this project, initially we perform the pre-processing technique steps such as scramble the pixels then changes the intensities. After that we converting the pixel values to binary values then generate the DNA sequence according to binary values by using four DNA bases.

Finally we are applying the PLAY FAIR cipher technique.

This project has been implemented successfully on a standard images because it gives less execution time whereas real time images takes more to execute which have high resolution

REFERENCES

1. H.Z Hsu and R.C.T.Lee, “DNA Based Enryption Methods”, The 23rd workshop on Combinatorial Mathematics and Compution Theory, National Chi Nan University Puli, Nantou Hsiees, Taiwan 545, Aapril 2006.

2. Amal Khalifa and Ahmed Atito. “High-Capacity DNA-based Steganography”, In the 8th International Cionferebce and informatics and systems (INFOS 2012), IEEE, May 2012.

3. United states Code: Title 44,3542. Definitions|LII/Legal Information Institute. Cornell University-Law school.(Online)(cited:71, 2011). http:/www.law.cornell.edu/uscode/44/3542.html.

4, A,Menezes, P. van Oorschot, S.Vanstone, Handbook of applied Cryptography,, 1997.

5. William Stalling,s Cryptogrphy and Network Security Principles and practies, fourth Edition,2005.