International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 4, No. 2
May 2015

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 4, No. 2, May 2015

Research Paper

SECURED IMAGE TRANSFER THROUGH DNA CRYPTOGRAPHY USING SYMMETRIC CRYPTOGRAPHIC ALGORITHM

R Sridevi[1] and S Karthika[2]

Corresponding Author: **R Sridevi ✉ srinashok@gmail.com*

Information security has become crucial and it is getting difficult to secure the information using traditional methods. Internet and network applications are growing very fast, so that the needs to protect such applications are increased by using cryptographic methods. As security is the most important issue for data, the enhancement of cryptographic analysis and cryptography are considered as field of on-going research. This work proposes (Data Encryption Standard) DES based DNA Cryptography algorithm for secure transformation of sources. This method proposes a combination of traditional cryptographic method with DNA cryptography technique. The source considered for transmission is an image. The encryption and decryption of image is done using proposed DES based DNA cryptography. This method ensures the confidentiality and data integrity over the data transmission.

Keywords: Cryptography, DES, DNA, Encryption, Decryption

INTRODUCTION

Cryptography

Cryptography is the art of protecting information by transforming it into an unreadable format, called cipher text. Only the intended recipient can decipher the message into plain text using secret key. Cryptography is the science of securing data.

Cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key, a word, number, or phrase to encrypt the plain text. The same plaintext encrypts to different cipher text with different keys.

Goals of Cryptography

The main goals of cryptography are classified into four concerns:

[1] Department of Computer Science, PSG College of Arts &Science, Coimbatore, India.
[2] Department of CA&SS, Sri Krishna Arts and Science College, Coimbatore, India.

- Confidentiality
- Data Integrity
- Authentication
- Non-repudiation

Confidentiality

Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text.

Data Integrity

It ensures that the data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code or hashes.

Authentication

Authentication is a service related to identification. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

Non-repudiation

Non-repudiation prevents either sender or receiver from denying message. Thus, when a message is sent, the receiver can prove that the message was send by the alleged sender.

DNA CRYPTOGRAPHY

DNA means deoxyribonucleic acid. It has genetic information memory. Nucleotides strung into polymer chains, i.e., DNA strands. In DNA there are four types of nucleotides: Adenine (A), Guanine (G), Cytosine(C) and Thymine (T). DNA is double-stranded helix nucleotides which carries the genetic information of cell. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides will only combine in such a way that C always pairs with G and T always pairs with A.

DNA cryptography is a new branch of cryptography utilizes DNA as an informational and computational carrier with the aid of molecular techniques. It is relatively a new field which emerged after the disclosure of computational ability of DNA. In a DNA sequence consisting of four alphabets: A, C, G and T.Each alphabet is related to a nucleotide. It is usually quite long. For instance, the DNA sequence of “Litmus”, its real length is with 2856 nucleotides long.

ATCGAATTCGCGCTGAGTCACAATTGCGCTG
AGTCACAATTCGCGCTGAGTCACAATTGTGA
CTCAGCCGCGAATTCCTGCAGCCCCGAATTC
CGCATTGCAGAGATAATTGTATTTAAGTGCC
TAGATACAATAAACGCCATTTGACCATTCAC
CACATTGGTGTGCACCTCCAAGCTCGCGCAC
CGTACCGTCTCGAGGAATTCCTGCAGGATAT
CTGGATCCAC (Figure 1).

Figure 1: Structure of DNA

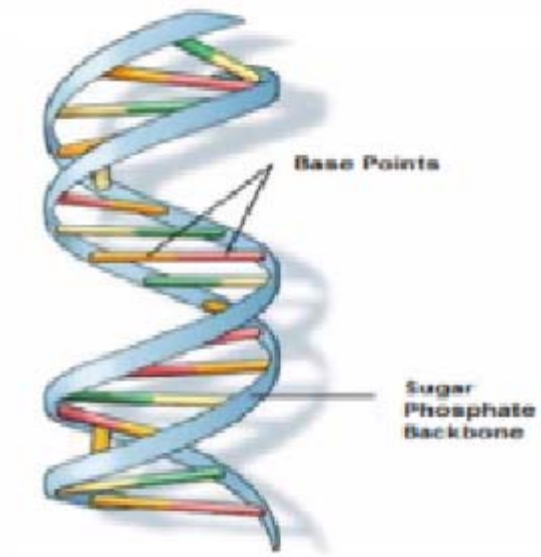
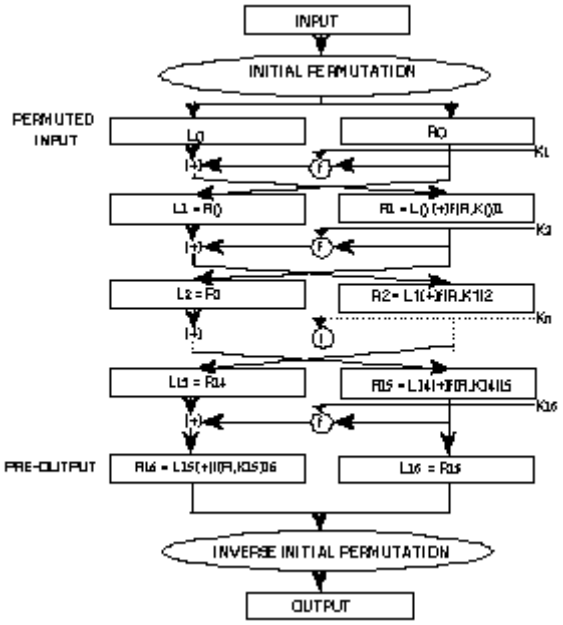


Table 1: DNA Features			
	StorageMedium	**Storage Capacity**	**TimeComplexity**
TraditionalCryptography	ComputerChips	1 gram of silicon chipcarries 16MB	≤ few seconds
DNA cryptography	DNA Stands	1 gram of DNA carries10^8 TB	≤ few hours

DNA cryptography gains attention due to the vast storage capacity of DNA, which is the basic computational tool of this field. One gram of DNA is known to store about 108 tera-bytes. This surpasses the storage capacity of any electrical, optical or magnetic storage medium.

The storage medium for traditional method is computer chips (16 MB) whereas in DNA cryptography is DNA strands (10^8 TB). The time taken for traditional cryptography is less when compared to DNA cryptography. DNA cryptography provides two way securities. One by computational difficulty and other by biological difficulties. These properties make DNA cryptography and DNA computing very beneficial.

Figure 2: General Depiction of DES Encryption Algorithm



DES ALGORITHM

The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key.

DES is the archetypal block cipher an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits as in Figure 2 used. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key consists of 64 bits and only the first 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is never quoted as such. Every 8th bit of the selected key is discarded, that is, positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64 bit key leaving behind only the 56 bit key.

Principles of DES

It is a symmetric encryption system that uses 64-bit blocks, 8 bits of which are used for parity

checks (to verify the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to the key therefore has a "useful" length of 56 bits, which means that only 56 bits are actually used in the algorithm. The algorithm involves carrying out combinations, substitutions and permutations between the text to be encrypted and the key, while making sure the operations can be performed in both directions (for decryption). The combination of substitutions and permutations is called a product cipher.

The key is ciphered on 64 bits and made of 16 blocks of 4 bits, generally denotedk_1 to k_{16}. Given that "only" 56 bits are actually used for encrypting, there can be 2^{56} (or $7.2*10^{16}$) different keys.

DES BASED DNA CYPTOGRAPHIC ALGORITHM

In this algorithm the image is first encrypted using traditional cryptography algorithm that is DES and then the encrypted form of bits are again encrypted using DNA Sequence. In this proposed algorithm the encryption process is done double the time so that the security for data transmission is increased. This technique provides high security and confidentiality over data transformation.

Encryption:

Step1: The input image is used under the pixel format for encryption.

Step2: These numbers are then grouped in blocks and encrypted in using a traditional method of DES algorithm, will form a 2 level encryption.

Step3: This encoded message is then changed to binary format.

Step4: Then these digits are grouped into two and substituted as A for 00, T for 01, G for 10, and C for 11.

Step 5: Return the encrypted cipher image.

Decryption:

Step 1: The input is taken as DES based DNA encrypted image

Step 2: The ATGC characters are substituted accordingly (00, 01, 10, and 11 respectively)

Step 3: Then the binary code is recovered from DNA sequence.

Step 4: Finally original image is recovered by decryption of obtained binary code by reverse process of DES.

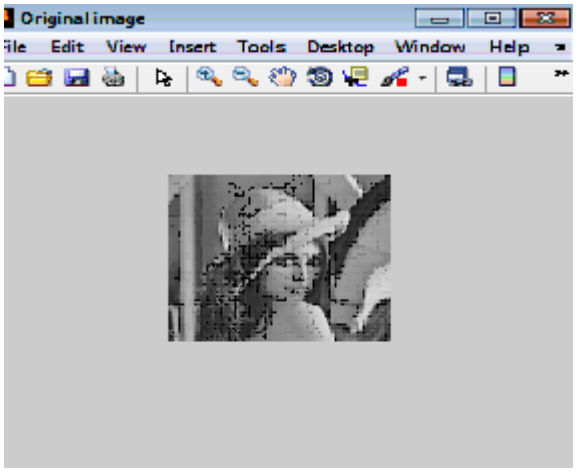
Step 5: Return the Original image.

PROCESS DESCRIPTION

Image Conversion into Digits

In this process (Figure 3) an input image is first converted into Pixels. Each pixel is then converted into DataStream & DataStream is saved in Code book. The codebook contains the bit series of each pixel in the same location and this location

Figure 3: Sample Input Image



is important because the same locations' bit series will give the same pixel so these locations should be matched when applying Encryption and Decryption.

Image Encryption using DES based DNA Cryptographic Algorithm

The image encryption using proposed DES based DNA cryptography algorithm provides high security because the encryption process is performed double the time (Figure 4). First, the image is encrypted using DES algorithm then the encrypted bits of DES will be again encrypted using DNA sequence.

The 8-bit transformation of image will have 256 pixels so we have 256*8 bits, but actually the DES implementation will require 64 bits for this, so apply the DES to the group of pixels so for 64 bits' group we take 8 pixels at a time.

The DES loop will be Re-apply to another 8 pixels so 64*32 bits will covers in 32 loops. The bit number D (1) to D (32) will first processed and then D (33) To D (64) and so on up to D (2013) to D (2048) bit in 32 loops. The results of DES are performed based on the DNA nucleotide table to transfer it into cipher image.

In Figures 5 and 6 the input image is converted into pixels. The corresponding binary code is

Figure 4: Image Encryption using DES Algorithm

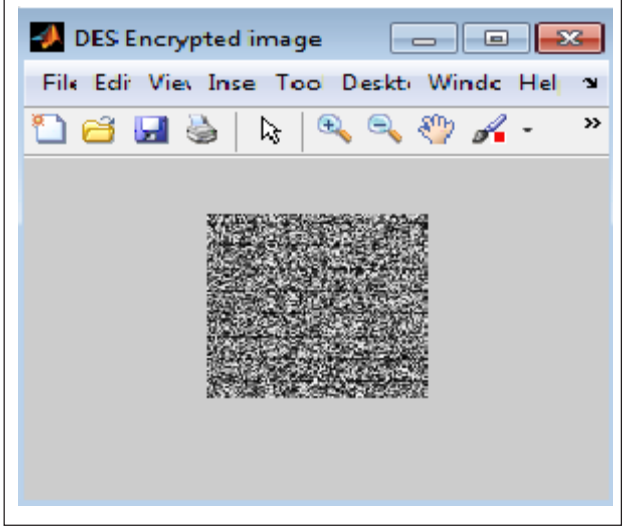


Figure 5: Image Encryption using DES Based DNA Cryptographic Algorithm

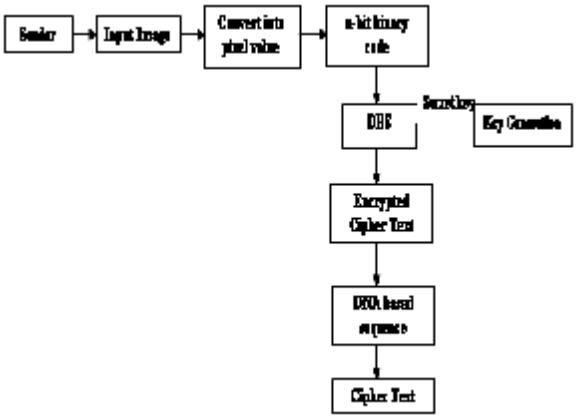
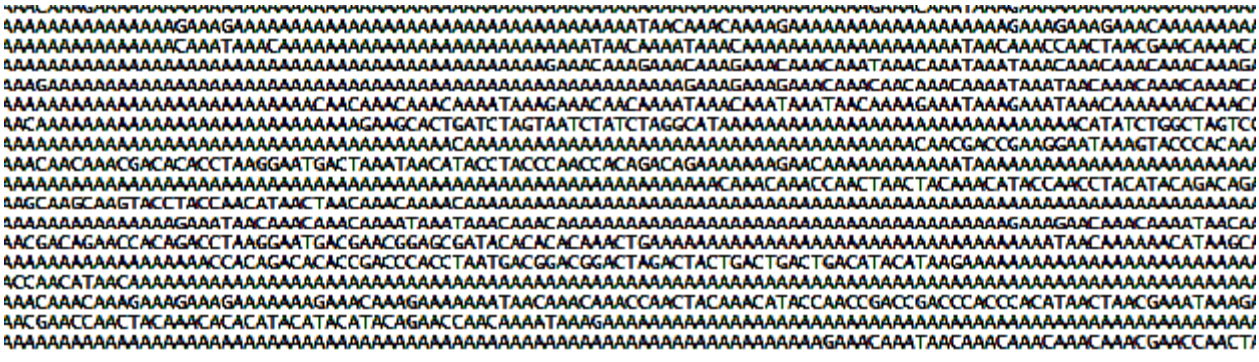


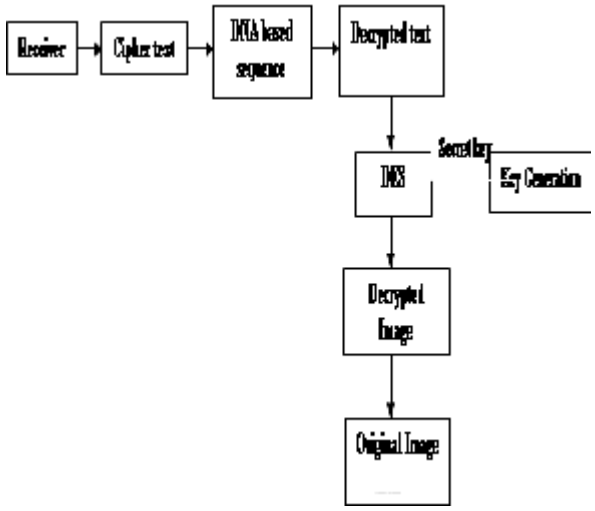
Figure 6 : Encrypted Cipher Text Using DNA Algorithm



generated for each pixel. The binary code will be given as an input to DES algorithm. Cipher text code will be generated by using the secret key.

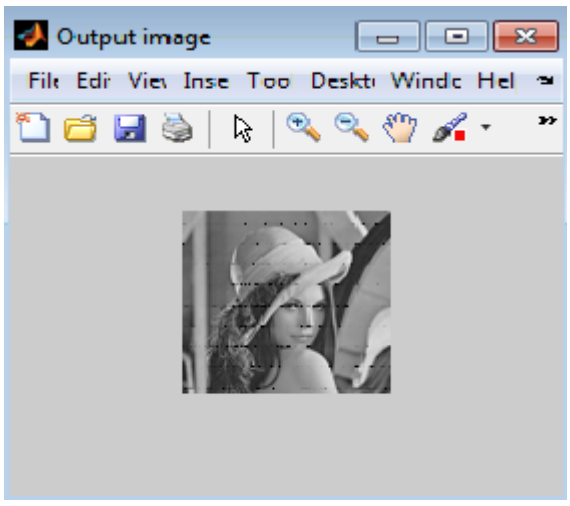
Decryption of Image Using Proposed Algorithm

Figure 7: Image Decryption using DES Based DNA Cryptographic Algorithm



For decryption, the reverse process of encryption is made to acquire the original image. The cipher text will be decrypted using DNA nucleotide sequence then it is again decrypted using DES algorithm. The secret key is used to decrypt the original image in DES algorithm. Figures 7 and 8 denotes the descryption on an image using proposed algorithm.

Figure 8: Decrypted Image using DES based DNA Cryptography



CONCLUSION

The present work consists of DES based DNA cryptographic algorithm for encryption of images. Due to the development and advance of science, the possibilities are rapidly growing. DNA in cryptography is a fast developing interdisciplinary area. DNA has dense information storage capacity and massive parallelism it is used for computations. Transforming the data through DNA makes it more secure. In addition to DNA encryption, DES algorithm is included for obtaining the robust security among various attacks. Proposed methodology of DES based DNA cryptography will have different combinations of data which is very difficult to change in the middle. Choosing binary values for the nucleotides we get four factorial different possibilities, instead of assigning fixed binary values. This method of research adds some artificial features to make the resulting cipher texts difficult to break. The theoretical analysis shows that this method is powerful against certain attacks. This method ensures the confidentiality and data integrity over the data transmission.

FUTURE ENHANCEMENT

DNA cryptography is a new promising direction in cryptography research that emerged with the evolution of DNA computing field. DNA computing is currently one of the fastest growing fields in both Computer Science and Biology and its future looks extremely promising. DNA cryptography is basically hiding of data in terms of DNA sequences. The future work will consist of analyzing and comparing the performance of

asymmetric cryptographic algorithm based DNA cryptographic techniques for secure data transmission processes. Asymmetric cryptographic algorithm used two different keys for encryption and decryption. Public key is used for encryption and Private Key is used for decryption process. This scheme will provides better security and efficiency.

REFERENCES

1. Abhishek Majumdar and Meenakshi Sharma (2014), "Enhanced Information Security Using DNA Cryptographic Approach", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Vol. 4, Issue 2, pp. 72-76.
2. Alani M M (2010)," A DES96 - improved DES security ", 7th International Multi-Conference on Systems, Signals and Devices, Amman, 27-30 June 2010..
3. Aradhana Soni and Anuja Kumar Acharya (2012), " A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis", *International Journal of Computer Applications (0975 – 8887)*, Vol. 47– No. 23.
4. Beenish Anam, Kazi Sakib, Md.Alamgir Hossain and Keshav Dahal (2010), "Review on the advancements of DNA Cryptography", arXiv:1010.0186v1 [cs.CR] 1 Oct 2010.
5. Bibhash Roy and Atanu Majumder (2012), "An Improved Concept of Cryptography Based on DNA Sequencing", *International Journal of Electronics Communication and Computer Engineering,* Vol. 3, Issue-6 (Nov 2012).
6. Bochen Fu and Xianwei Zhang (2012), "DNA cryptography based on DNA Fragment assembly", in the IEEE proceedings of 8th International Conference on Information Science and Digital Content Technology (ICIDT), Vol.1, pp. 179-182.
7. Bonny B Raj, Panchami (2014), "DNA Based Cryptography Using Permutation and Random Key Generation Method", *International Journal of Computer Application,* Vol. 3, Special Issue 5, July 2014.
8. Cui G Z, Qin L M, Wang Y F and Zhang X C (2007), "Information Security Based on DNA Computing", 2007 IEEE International Workshop on Anti-Counterfeiting Security, Identification, pp. 288-291.
9. Dhanraj Nandini C and Mohd Tajuddin (2011), "An Enhanced Approch for Secret Key Algorithm baata Encryption Standard", *International Journal of Research And Review in Computer Science*, August 2011.
10. Grasha Jacob and Murugan A (2013), "An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images", *IEEE.*
11. Guangzhao Cui , Limin Qin, Yanfeng Wang and Xuncai Zhang, "An Encryption Scheme Using DNA Technology", College of Electrical Information Engineering, Zhengzhou University of Light Industry.
12. Gyanadeep N, Dinesh Kumar P V S, Girish Kumar K, Madhu Viswanatham V (2014), "Secure Speech Transformation using Enhanced DNA Cryptography", *International Journal of Applied Engineering Research,*

ISSN 0973-4562, Vol. 9, No. 18, pp. 5171-5180

13. Hsu H Z and Lee R C T (2006), "DNA Based Encryption Methods, "The 23rd Workshop on Combinatorial Mathematics and Computation Theory", National Chi Nan University Puli, Nantou Hsies, Taiwan 545, April 2006.

14. Leier A, Richter C, Banzhaf W and Rauhe H (2000), "Cryptography with DNA Binary Strands", *BioSystems*, Vol. 57, pp. 13–22.

15. Radhana Soni and Anuja Kumar Acharya (2012), "A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis", *International Journal of Computer Applications* (0975 –8887), Vol. 47, No. 23, June 2012.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com