IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SECURE NETWORK FOR DATA TRANSFER USING GENETIC ENCRYPTION

[1]Adwaith P A, Niyamol S Nair, Rihansha Rasheed, Sudeep S, [2]Prof. Salitha M K

[1]Final Year Students, Dept. of Computer Science and Engineering,
Musaliar College of Engineering and Technology, Pathanamthitta, India
[2]Assistant Professor, Dept. of Computer Science and Engineering,
Musaliar College of Engineering and Technology, Pathanamthitta, India

Abstract : One of the main problems the digital world is facing as a result of the rapid advancement of distributed system technologies is the security of private and sensitive data while it is being transported and stored.The most important method for protecting data is encryption. As a result, a variety of techniques, including DNA, are utilised to offer security, integrity, and authorised access. They still have some restrictions, though. Deoxyribose Nucleic Acid (DNA) contains a unique genetic code that is thought to be composed of deoxyribose nucleotides, which are monomers. Each nucleotide in a DNA molecule is made up of a nitrogen base, a phosphate group, and deoxyribose sugar. DNA molecules are made up of two long strands of nucleotides. The nitrogenous bases are A(Adenine), G(Guanine), C(Cytosine), and T(Thymine), which form bonds with both T and G bonds with C. Steganography is another technique used to protect the data within the image. Steganography is a technique for concealing sensitive information by integrating it into an image file. It is one of the techniques used to defend sensitive or secret data against nefarious attacks. Both steganography and cryptography are techniques used to conceal or safeguard secret data. However, they differ in that steganography conceals the existence of the data, whereas cryptography renders the data unreadable or hides the meaning of the data.

IndexTerms - Secure network for data transfer using genetic encryption , AES 256 encryption, DNA encryption, LSB algorithm, Steganography

CHAPTER 1

INTRODUCTION

A mathematical technique known as cryptology is used for security information management, including authentication, encryption, and data quality. To encrypt and decrypt private information that is represented by cryptography (Symmetric Algorithms, Asymmetric Algorithms, and Hybrid Algorithms), numerous popular encryption protocols, digital signatures, and hash functions are utilised. Protection difficulties exist for all of these present methods. Moreover, these techniques take a long time to generate cryptographic keys, retrieve keys, encrypt data, and decrypt data. Deoxyribose Nucleic Acid (DNA) cryptography has been improved through a number of studies and careful research, allowing for the concealment of sensitive information within DNA molecules to increase data security. DNA cryptography has been developed in order to meet the needs of DNA Cryptography systems, storage space, speed, and security against attack in the digital world. DNA sequences are accessible through databases maintained by the National Center for Biotechnology Information (NCBI, DDBJ, and EBI). Depending on the user's input, the DNA sequence can be randomly chosen, the biological process of DNA is difficult to dissect, and it lessens calculation complexity. These characteristics highlight the necessity of encoding DNA in cloud computing in order to achieve rapid calculation and increased complexity of cryptographic analysis.

A modern cryptographical prototype is DNA cryptography. DNA is a nucleic acid which contains instructions for genetics. Adenine (A), cytosine (C), guanine (G) and thymine (T) form the four bases present in DNA. Parallel processing capabilities are the greatest advantage of DNA cryptography. The approach to biomolecular cryptography based on DNA is planned. A new generation DNA-based key system is proposed to improve computation based on the DNA-based key expansion matrix using random key generation scheme speed. It proposes a novel and special technique based on biological simulation for DNA encryption and decryption. The plaintext is similarly split into two halves and translated for each session to DNA sequences using unique encoding table generation. After that, after applying suggested technique measures, the cypher text is produced. Some latest DNA Cryptography works are discussed and compared. Based on a secured symmetrical key generation, a new DNA cryptography algorithm is suggested. This encryption algorithm consists of encryption, random key generation and decryption in three steps. The text is translated to ASCII and then to DNA code at the encryption level. This initial cypher is translated to the final cypher by using random key-generated DNA sequences. The DNA-Genetic Encryption Technique (D-GET) is suggested in this paper. The hidden information was translated into binary data and then into DNA sequences in this technique. The D-GET is, moreover, an iterative algorithm. A round

is called an iteration, and the number of iterations is three or more. There are four in-round and it's iterative in nature. Iteration requires encryption, the method of reshaping and genetic operations. Furthermore, a symmetrical key is used. Any kind of data type can be used as the secret data, i.e. text, word document, pixel image, audio, and video. Experimental studies indicate that reconstructed information is a standard copy of secret information.They also show that the technique proposed maintains perfect security.

CHAPTER 2
SYSTEM DESIGN

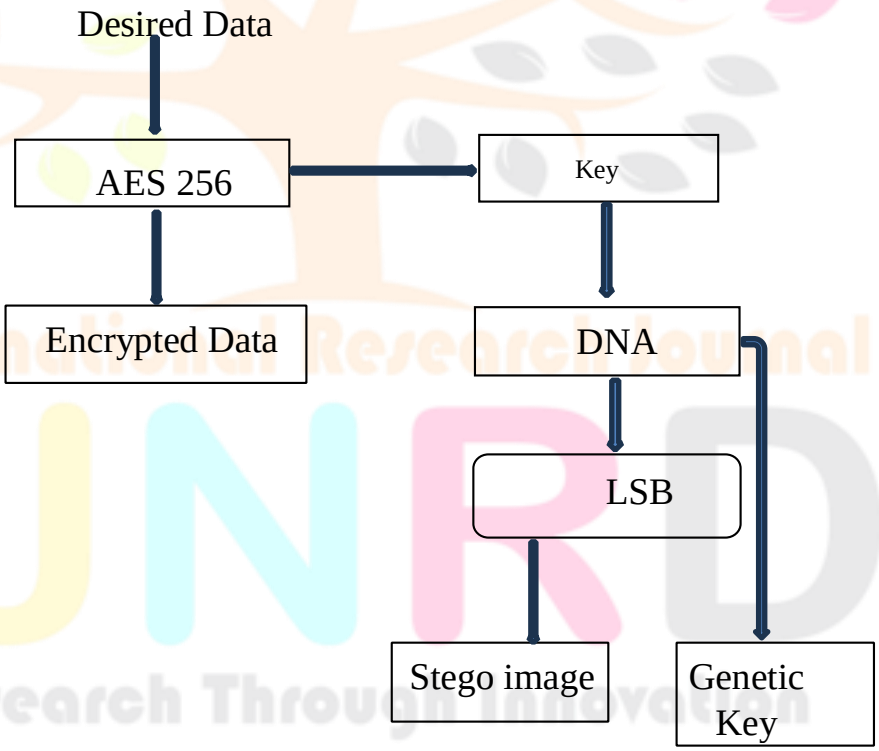
2.1 PROPOSED SYSTEM

Encryption is the most significant method for data protection. Therefore, many available encryption algorithms are used to provide security, integrity, and authorized access using many methods such as DNA. The DNA Cryptographic technique is a method, designed to improve cloud computing security. Initially the data to be protected is encrypted using AES256 Encryption technique. Then, the AES256 encryption algorithm generates a key. The generated key is then undergoes encryption process with the use of Genetic Encryption algorithm. After the encryption process, an image is selected to store the key within the image. Therefore, higher resolutional images are used to this process.

Image steganography is a method of concealing confidential or sensitive information in something that looks to be ordinary image. Steganography involves disguising text so that it appears to be an ordinary image or other file. When someone looks at an object that contains secret information, they are unaware that it is there.

2.2 SYSTEM ARCHITECTURE

2.2.1 Architecture of unit for the Motion.



The embedding procedure for the steganographic algorithm is as follows:
1) Read the cover image and secret image.
2) Use the Canny edge detector to detect the edges of the cover image.
3) Scramble the edge pixels of the cover image with a key.
4) Convert the secret image to a 1-D bit stream.
5) Scramble the 1-D bit stream of the secret image with a key.
6) Calculate the coherent bit length L for each edge pixel.
7) Encode the 1-D bit stream of the secret image using a Hamming (7, 4) encoder.
8) XOR the encoded data with 7 bits of random noise using a key.
9) Embedded the binary bit streams, coherent bit length L into the scrambled edge pixels.
Unscramble the edge pixels.

10) Apply the method of 2k correction to achieve better imperceptibility in the stego image. The new stego image is obtained.

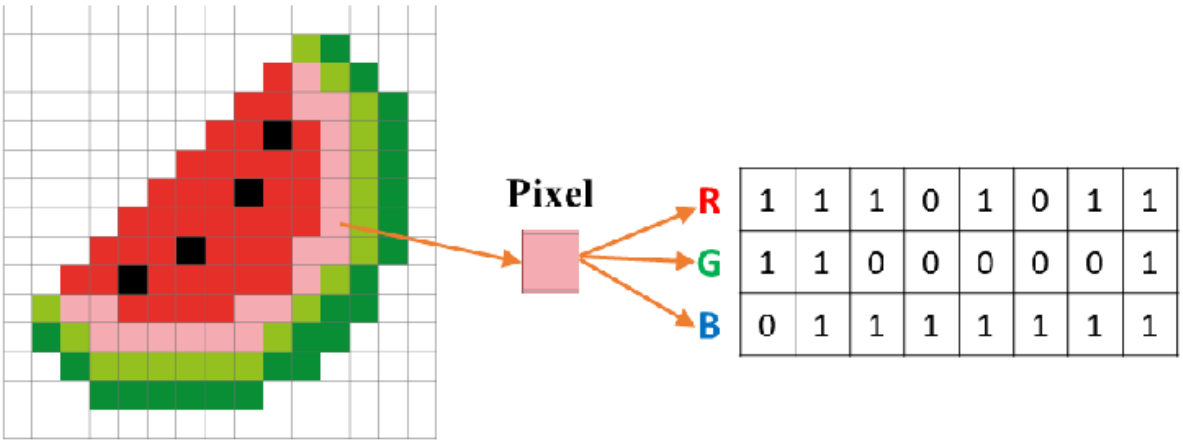


Fig 4.3.2: LSB Process

The Canny edge detector is used to detect the edges of the cover image because edges are typically the least noticeable parts of an image. By scrambling the edge pixels, the steganographic algorithm can hide the secret message without significantly affecting the quality of the cover image.

The Hamming (7, 4) encoder is used to encode the secret message because it is a very efficient way to encode data with a small amount of redundancy. This redundancy helps to protect the secret message from being detected by steganalysis algorithms.

The 2k correction method is used to improve the imperceptibility of the stego image by reducing the amount of noise that is introduced when the secret message is embedded.

The overall goal of the steganographic algorithm is to hide a secret message in a cover image without significantly affecting the quality of the cover image. The algorithm achieves this goal by using a combination of edge detection, scrambling, encoding, and noise reduction techniques.

CHAPTER 3
METHEDOLOGY

AES encryption algorithm and DNA cryptography can be used together to provide a secure way to transfer data. AES is a symmetric encryption algorithm that uses a key to encrypt and decrypt data. DNA cryptography is a method of storing data in DNA molecules. To use AES encryption algorithm and DNA cryptography to secure data transfer, the data is first encrypted using AES. After the encryption process, AES generates a key. To provide more security to the key, the key then undergo DNA encryption technique.

The AES 256 encryption process is as follows:

1) The data is divided into blocks of 128 bits.
2) A 256-bit key is used to encrypt the data.
3) The data is encrypted using a series of rounds.
4) Each round consists of the following steps:

- Substitution Bytes: The bytes in the block are replaced with new bytes using a substitution table.
- Shift Rows: The rows of the block are shifted by different amounts.
- Mix Columns: The columns of the block are multiplied by a matrix.
- Add Round Key: A round key is added to the block.

5) The final round does not include the Mix Columns step.
6) The encrypted data is the output of the last round.

The encryption process is reversible using the same key. To decrypt the data, the steps are performed in the reverse order. AES 256 encryption is very secure. It has been subjected to extensive cryptanalysis, and no practical attacks have been found. AES 256 is widely used in government and commercial applications. It is the default encryption algorithm for protecting classified information in the United States.

Here are some of the benefits of using AES 256 encryption:

- It is very secure.
- It is efficient in both software and hardware.
- It is widely supported by applications and operating systems.
- Here are some of the drawbacks of using AES 256 encryption:
- It can be computationally expensive, especially for large amounts of data.

- It can be difficult to implement correctly.

Overall, AES 256 is a very secure and efficient encryption algorithm that is widely used in government and commercial applications. The iterative algorithm known as the DNA-Genetic Encryption Technique (D-GET). Any type of data (such as a message,) can be encrypted. The main steps of the suggested technique include pre-processing, symmetric key encryption, reshaping, crossover, and mutation. They are clarified as follows.

1) Pre-processing Stage

This information has to be prepared after identifying the secret key, depending on its type. The ASCII values are translated in the case of a text file. Group them into 8-bit binary data. Each of the two adjacent bits is transferred to the four bases; adenine (A), cytosine (C), guanine (G) and thymine (T), located in the DNA. The table below shows DNA and bit representation :-

Bits	DNA
00	A
01	C
10	G
11	T

2) Encryption stage

Cryptographic algorithms fall into two categories: symmetric key algorithms and asymmetric key algorithms. In the symmetric scheme, a shared key is transmitted between the sender and the recipient. Asymmetric schemes have public and private keys that are mathematically related. The symmetric cryptographic algorithm's main benefit is high-speed encryption, which makes it more suited for encrypting huge amounts of data. The suggested method based on a DNA-based cryptography algorithm then employs the symmetric key.

After converting binary to DNA sequencing, encrypt the key. The solution could be a binary string or DNA sequence. The relevant DNA sequence elements are subjected to an exclusive OR operation and converted back to the DNA sequence if one or both of the DNA sequence key data and DNA sequence are converted to binary form.

Binary form of Key:
…… 00 10 11 11 11 11 00 1110 01 …….
XOR Result:
10 00 11 10 00 01 00 0110 10 …….

3) Reshaping Stage

After encryption, a basic genetic algorithm has three operators: replication, crossover, and mutation. The reshaping procedure is used to produce genetic material, in the form of the chromosomal population, that advances to the next activity and iteration. The first chromosome's number and length are established at this step. These numbers can be both constant and variable for every round. It can be reshaped by arranging the DNA sequence into rows to produce the parents' predetermined-length chromosomes (chromosome population). For example:

Secret key :

…….GCCCGCACCGGAACAACGGGCGTTCCGTCCGACCCCTTTCAACTATCAGTCTTGTCA

GGCTACCGATTATCAATGCGCT

Chromosome population:

GCCCGCACCGGAACAACGG
GCGTTCCGTCCGACCCCTTT
CAACTATCAGTCTTGTCAGG
CTACCGATTATCAATGCGCT

4) Crossover stage

After creating the parents' chromosomes, crossover is the following step.

There are two types of crossover. These can be applied in rounds of technique in succession. Parents are selected in the first one in the mating pool. The parents' first and last chromosomes are then crossed at a single spot, creating two new children by switching the heads of parent 1 and parent 2. The offspring therefore contain parts of the DNA codes of both parents. After the alignment of

the DNA sequence into rows for chromosomal formation, rotation is the second type of crossover. rotating left or right by applying a predetermined value. For instance:

Secret key:
…… 0 1101 1010 0101 0101 111 …….
Apply rotate Crossover:
0 1010 1111 0110 1101 001 …….
Apply one point Crossover:
Two parents:
11 0110 0100 1001 0010 11
…….
10 0100 0111 1011 1110 01 …….
Two offsprings:
11 0110 0100 1011 1110 01…….
10 0100 0111 1001 0010 11…….

5) Mutation Stage

The chromosomes are subject to mutation following the crossover process.

The alteration of a string's elements is known as mutation. It employs two types of mutation. Convert the data to a binary vector in the first case, then specify two points of mutation between the first and end bits. The bits between these points are then complements, meaning that a single point of mutation can change from 1 to 0 or vice versa. Change each of the four bits to two DNA bases (1010□CG) for the second type of mutation. After conversion, convert it into a vector of DNA bases and identify two points between the first and last bases, then shift the DNA bases to eachother. (i.e., C□G).
DNA bases and Representation of bits

DNA	Bits	DNA	Bits	DNA	Bits	DNA	Bits
TA	0000	GA	0100	CA	1000	AA	1100
TC	0001	GC	0101	CC	1001	AC	1101
TG	0010	GG	0110	CG	1010	AG	1110
TT	0011	GT	0111	CT	1011	AT	1111

The following example illustrates the proposed technique's mutation operations.
For instance:
Apply Mutation complement:
Before mutation:
11 0110 0100 1001 0010 11 …….
After mutation:
…… 11 0101 1011 0110 1010 11 ……..
Apply Alter Mutation:
Before mutation:
……GGACTGCGAT…….
After mutation:
……AAGTCATAGC……..

Crossover and mutation operations occur 100% of the time. Data must be encrypted and reshaped in order to advance. A predetermined number of iterations determines how many rounds there will be. Transmit the text/image file containing the encrypted data. Binaries received the data at the receiving end and converted it to DNA sequencing before reshaping, decrypting, crossing across, mutating, and reshaping it back to the original format. The scenario of the stages of D-GET serves as an example of the stages D-GET in order.

CHAPTER 4

EXPERIMENT AND RESULT ANALYSIS

4.1 SOFTWAREE SETUP

This secure network has the exact protection we need. The network is equipped with AES 256 encryption, DNA encryption and LSB algorithm. It can prevent any type of attack.

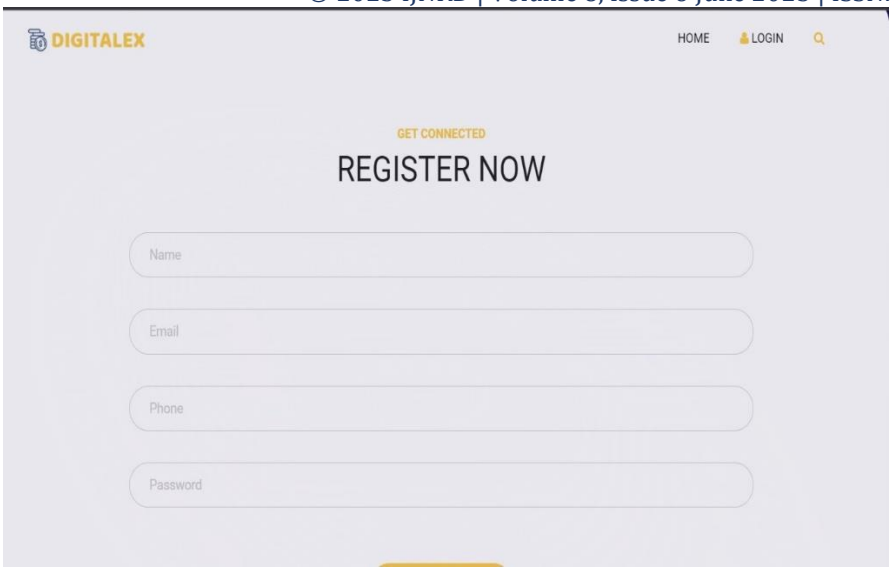


Fig 4.1.1 : Registration process

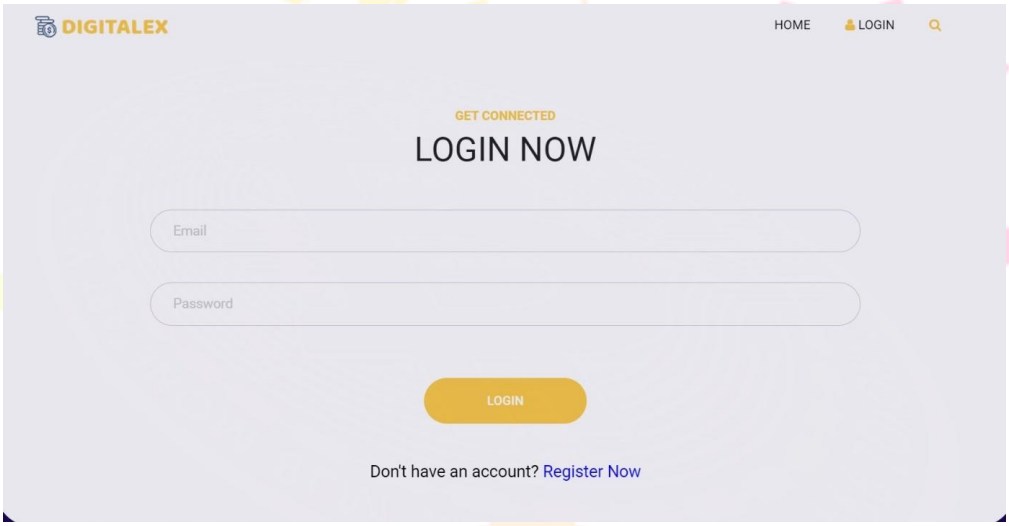


Fig 4.4.2: User Interface

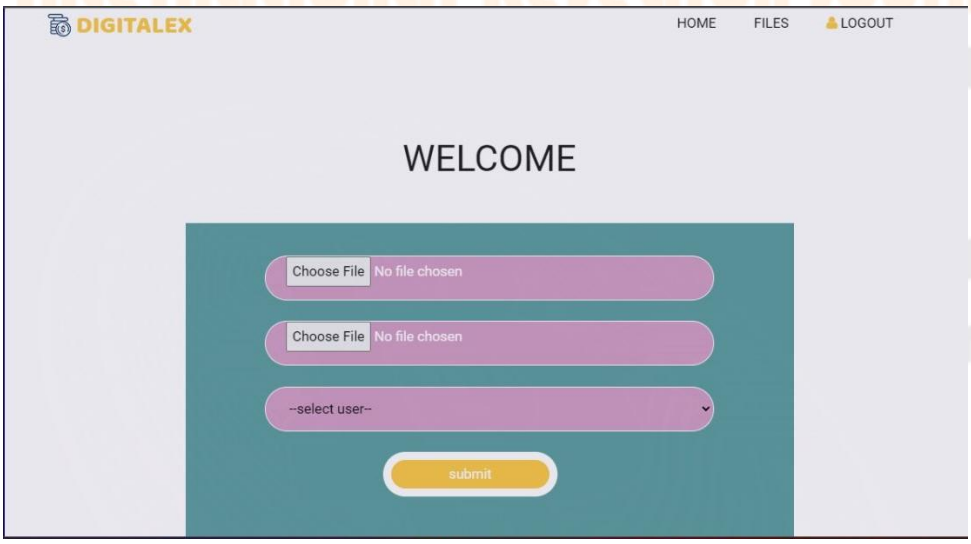


Fig 4.4.3: Encryption process

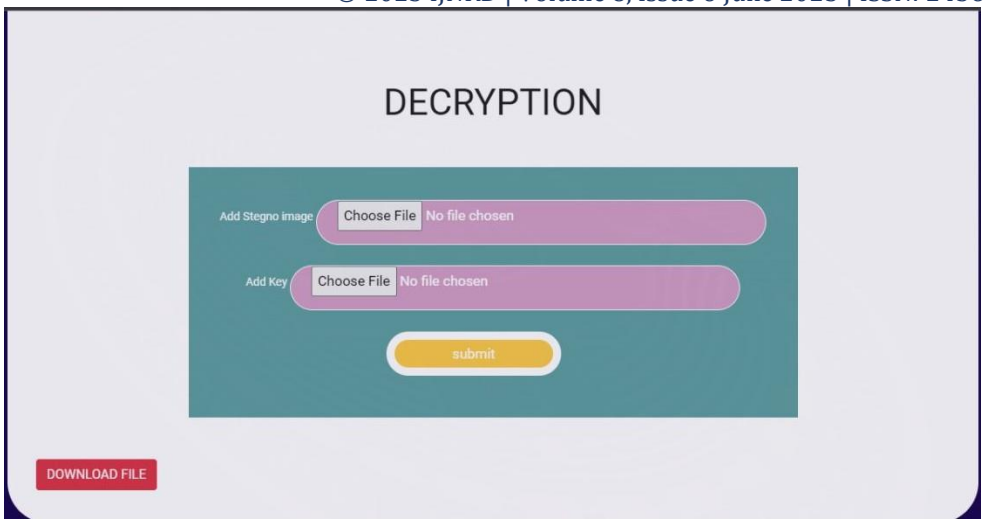


Fig 4.4.4: Decryption process

4.2 Result Analysis

DATA	DATA TYPE	PROCESSING TIME
PDF	TEXT	45sec
PNG	IMAGE	4sec
JPG	IMAGE	3sec
AUDIO	AUDIO	1.4min

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

A promising new technology for safe data transfer is DNA encryption. It has a number of benefits over conventional encryption techniques, including the fact that DNA encryption is based on the special DNA structure, which makes it very challenging to crack. AES Encryption algorithm is used to encrypt the data. It's crucial to create a key before using AES to encrypt data. A password or a random number generator can be used to create a key. Any of the several AES encryption libraries that are available can be used to encrypt data after the key has been generated.

After the AES encryption process the key undergo DNA Encryption. DNA is the perfect medium for high-speed data transfer since it can be processed very fast. To increase the speed of calculation based on the DNA-based key expansion matrix, a new generation DNA-based key system is proposed. The three steps of this encryption algorithm are encryption, random key creation, and decryption. At the encryption stage, the key is converted to DNA code. Using randomly produced DNA sequences as keys, this initial cypher is converted into the final cypher. Additionally, the D-GET is an iterative method. Iterations have three or more rounds and are referred to as rounds. It is iterative in nature and has four rounds. Encryption, reshaping, and genetic operations are required for iteration. Additionally, a symmetrical key is employed. Any type of data format, including text, word documents, pixel images, audio files, and videos, may be used as hidden data. Reconstructed information is a conventional copy of secret knowledge, according to experimental investigations. Additionally, they demonstrate that the suggested technique retains full security.

As the next level of security, steganography process is used. Information is concealed within an image file using the technique of image steganography. The image selected for this purpose is known as the cover image, and the image acquired after steganography is known as the stego image. Text, pictures, or videos can all contain the hidden information. It is concealed such that a human eye cannot see it. Visually, the cover image and stego image are identical. Spatial domain steganography, one of the major types of picture steganography utilised here, conceals the secret information by altering the least significant bits (LSBs) of the pixels in the cover image. Because it is simpler to execute and uses fewer computer resources, spatial domain steganography is more popular.

5.2 FUTURE SCOPE

Using DNA cryptography and image steganography, secure data transit has a bright future. Although DNA cryptography is a young field of study, it has the potential to be substantially more secure than current encryption techniques. This is due to the complexity and difficulty of breaking DNA. Data is concealed within images via a process called image steganography. This can be used to convey covert communications or to prevent unauthorised access to sensitive data. Using image steganography and DNA cryptography together can offer extremely high levels of security. This is because it can be exceedingly challenging to find hidden data in an image. In addition, even with the most powerful computers, DNA cryptography is incredibly difficult to crack.

CHAPTER 6
REFERENCES

[1]. **"**A technique for DNA cryptography based on dynamic mechanisms" (Md. Rafiul Biswas a, Kazi Md. Rokibul Alama, Shinsuke Tamura b, Yasuhiko Morimoto, 2019)
[2]. " A hybrid DNA based cryptography algorithm using chaos method"(Paulin Rachel C, Dr. Sampath Kumar,2018)
[3]. "DNA cryptography for secure data storage in cloud" (Sreeja Cherillath Sukumaran, Misbahuddin Mohammed,May 2018)
[4]. " Three reversible data encoding algorithms based on DNA and amino acids' structure"
(Mona Sabry, Mohamed Hashem, Taymoor Nazma, September 2012)
[5]. "A hybradized model for image encryption through genetic algorithm and DNA sequence"(saswat k pijari, gargi bhattacharjee, soumyakanta bhoi, 2018)
[6]. H.M. Mousa, " DNA-genetic encryption technique", Int. J. Comput. Netw. Inf. Secur

2016

[7]. A. Aieh, A. Sen, S.R. Dash, S. Dehuri, "Deoxyribonucleic Acid (DNA) for a Shared Secret Key Cryptosystem with Diffie Hellman Key Sharing Technique", 2015

[8]. S. Kalsi, H. Kaur, V. Chang, " DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation", J. Med. Syst. 2018