International Journal of Research in Communication and Embedded Electronics
Volume1, Issue 4 2025

Cryptography Based on DNA Analysis

Mr.Naushad Alam[1], Khaja Uddin[2]
[1,2]Assistent Professor
Department of CSE-AIML, Lords Institute of Engineering & Technology.

Research Article

Date of Submission: 11-07-2025 **Date of Acceptance: 22-08-2025** **Date of Publication: 20-09-2025**

Abstract: These days, secure data transfer is a crucial and difficult issue. Cryptography and steganography techniques provide the safe and impervious transfer of verified data. Every day, new cryptographic algorithms are created as a result of technological advancements. Recent developments have produced a novel method known as DNA cryptography. This article ensures triple security by encrypting the plain text using the RSA algorithm, DNA cryptography, and steganography techniques. This combination will result in a stronger, more secure technique that makes it more difficult for an attacker to decipher the message.

Keywords: Steganography, RSA algorithm, DNA cryptography, secure data transfer, and triple security

INTRODUCTION

As is well known in today's technologically advanced world, where the majority of people interact with the internet, online transactions and commerce include private information. These facts are crucial to a person's existence. Hackers will always have the opportunity to corrupt, use, alter, and send sensitive data if it is not safeguarded.

Information technology's major goal is to maintain the security of systems and their contents. However, assaults on information systems happen every day, and as these attacks become more common, so does the demand for data protection. Therefore, the strongest and most effective idea must be used for network security management. This document makes recommendations for strengthening and increasing security standards. The primary concept put forward here is to provide critical data layered protection so that only authorized people may access or retrieve it.

DNA cryptography is the topic of the proposed paper. A new and very promising area of cryptography study is DNA cryptography. It offers a fresh promise for unbreakable algorithms and safe communication in the face of malevolent third parties. In plain

This work combines mathematics and security engineering to provide multi-layered data protection utilizing RSA, steganography, and DNA cryptography. Sensitive data that requires a secure key for communication is often secured using the RSA technique. Among the most well-known public-key cryptosystems is this one. Because RSA guarantees data privacy and authenticity, it is used in the majority of digital data, information, and telephone security applications. The RSA technique is primarily used to address the issue of key distribution for encryption and decryption.

The technique to conceal data using the DNA sequence is known as DNA cryptography. Adenine (A), Cytosine (C), Guanine (G), and Thymine (T) are nitrogen bases found in DNA (Deoxy Ribonucleic Acid), a lengthy polymer. The plain text's encoding and decoding depend heavily on these four bases. The picture is not secret and is visible to the viewer, but the text data, which takes the shape of a DNA sequence, is meant to be hidden within. Communication and a significant reduction in information leakage are both feasible with steganography. The steganography method described in this work protects confidential information against alteration, deletion, compression, and other threats. In the subject of study, steganography has grown to be both exciting and challenging. Therefore, this steganography allows for the possibility of adding a large amount of data and allows the concealed data to be more uniformly dispersed across the whole picture to strengthen it. Compared to previous cryptography techniques, the suggested approach in this work is quick and reliable.

This is how the paper is organized. The project's suggested technique is briefly explained in Section II. Section III provides a thorough description of the technique used, which combines steganography and encryption. Section IV discusses the experimental outcomes. Lastly, section V provides the conclusion and the scope for the future.

METHODOLOGY

With more people using the internet these days, data security is a big problem. An encryption model is suggested with the goal of safely transferring the data. This section explains the techniques used, such as chaotic neural networks and DNA

cryptography, and then provides a short explanation of the suggested encryption approach.

A. Cryptography of DNA

Adenine (A), Cytosine (C), Guanine (G), and Thymine (T) are nitrogen bases found in DNA (Deoxy Ribonucleic Acid), a lengthy polymer. These four bases are crucial because they may be used to encode data that is a stream of 1s and 0s. DNA is used because of its enormous data storage and transmission capacity. The suggested method first converts the plaintext to the appropriate ASCII value. After that, each ASCII value is transformed into the appropriate binary format. The ATGC bases are then mapped to the binary pairs in order to convert the binary sequence into a DNA sequence.*Chaotic neural network*

The main reason to add a chaotic neural network in this paper is because of its captivating communication system. It includes high-speed information transmission, tolerance to noise, and broadband power spectrum. In general, cryptography is easy to frame up with a chaotic system. One main concept in a chaotic system is that it generates a secret key which is pseudorandom in nature. It is considered to be more protected since it is troublesome to integrate the chaotic neural network with time varying delay.

A. RSA Algorithm

RSA was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is an asymmetric cryptosystem and consists of two different keys Public and Private keys. The public key is to encrypt the message and can be shared with everyone, whereas the private key is to decrypt the message and must be kept secret. The plain text is encrypted using the public key whereas it can only be decrypted using the private key [1]. The steps involved in the algorithm are:

a) Key generation

It involves generation of two key pairs, public and private key. To generate the key following steps are to be followed.

- Choose two large distinct prime no's p and q • Compute n=p*q.
- Compute phi=(p-1)*(q-1).
- Choose public exponent e(co-prime) between the interval [1, phi].
- The public key pair (n, e) is generated.
- The private key d is calculated using the e value by computing d*e= 1 (mod phi). The private key pair (n, d) is generated.

Encryption

The encryption step involves the generation of the ciphertext by using the public key value e. Any user with the public key can encrypt the plaintext.

$$C = M^e mod n \quad (1)$$

b) Decryption

The end user only with the private key value d can decode the ciphertext.

$$M = C^e mod n \quad ()$$

B. Encryption process

The encryption process involves the RSA algorithm, chaotic neural network, DNA encoding, and steganography by guarantying triple layer security. The plain text is converted to a DNA sequence, which is wrapped by an image, upon which the RSA algorithm protects the data. The basic block diagram of the proposed method is shown in Fig 1. below.

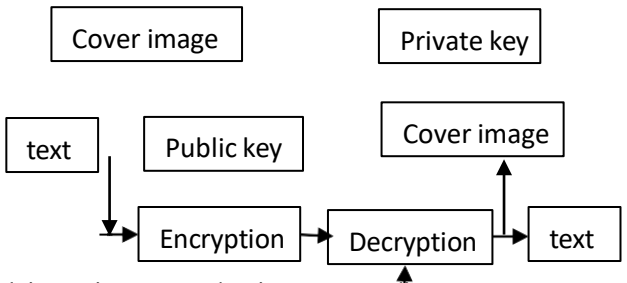


Fig 1. Basic block diagram of proposed method. Firstly, the plaintext is converted to its corresponding ASCII value. The binary equivalent (Bj) of the respective ASCII values is obtained. A random binary sequence is generated using a chaotic neural network. The Hopfield delay is first calculated by solving the differential equation of the delay function using the fourth-order Range-Kutta method by considering n=2 and step function h=0.01. After the calculation of the delay a random binary sequence generator, generates a random sequence of length 42 bit. Suppose say, the random binary sequence of length 42 bit generated is considered as 111011000111001110011000110011101011100011. The

sequence is then split into three subsequences. First 32 bits (Rj1) are used as a random key which is mainly used in XOR operations, the next 9 bits (Rj2) are used to set the number of shifts the binary sequences must undergo to create confusion to the intruder and the last bit is used to select the trajectory of the chaotic map. The sequence Rj1 and the binary equivalent of the ASCII value are subjected to left cyclic shifting by a certain bit specified by the sender.

The resultant sequences are then XORed, producing a 32bit stream of 1's and 0's (Ej).

$$E_j = R_j' \oplus B_j' \quad (3)$$

The resultant sequence (Ej) is then paired and mapped to DNA bases A, T, G and C respectively [4] by following Table 1, thus the plaintext is completely masked by DNA bases.

A	T	G	C
00	11	10	01

Table 1. DNA mapping

The DNA sequence obtained is to be hidden in an image using a steganographic process. The proposed work is based on the LSB steganography method, in which the cover image is captured in real-time with the aid of a web camera. The cover image captured is an RGB image and has to be converted to a greyscale image for the ease of computation. The greyscale is chosen over an RGB image because the greyscale image consists of an 8-bit plane and is easy to extract them whereas the RGB image consists of a 24-bit plane and it may require more computational step to extract the bit plane. The DNA sequence is then mapped back to the binary. The bit plane in which the sequence to be hidden is selected. The pixel value of that bit plane is extracted to which the binary sequence is appended at the least significant bit place. The DNA sequence hidden in the image is referred to as stegno-image, which is transmitted to the end-user.

C. Decryption process

The Steganographic image can only be decrypted by an end-user with access to private key. Firstly, the steganographic image is obtained by providing an accurate private key d. The next step is to decrypt the steganographic image in order to retrieve the DNA sequence. At first, the bit plane in which the sequence is hidden is extracted from the greyscale image. The pixels of the image are then obtained is converted to binary values, the least significant bits are recognized and are grouped. In the proposed method three least significant bits are considered. If the bit range increases a noise or distortion in the steganographic image can be noticed hence choosing three least significant bits is efficient. Thus, the DNA sequence is retrieved back from the image [6].

The DNA sequence is decoded using Table 1 resulting a binary sequence (Ej). The sequence Ej is then XORed with the random sequence (Rj'), (Bj') is obtained as a result. Right cyclic shift operation is performed on Bj', which yields (Bj) the binary equivalent of the ASCII code. The plain text is retrieved by considering the generated ASCII values.*Binary Sequence Generator*

A random binary sequence is generated based on chaotic neural network which is identical in nature. The binary sequence generated randomly depends on the trajectories of chaotic map [7]. Consider a chaotic map x(.) generating a binary sequence in the interval k=[s,t] can be defined as,

$$x_{t-s} \equiv \underset{t-s}{0}.\, a1(x).\, a2(x). \ldots\ldots ai(x), x \in [s,t] \quad (4)$$

where ai(x) ϵ {0,1} and

$$ai(x) = -\sum_{j=1}^{2^i-1} (-1)^{j-1} \emptyset(t-2)(j \div 2^i) + s^y \quad (5)$$

where, ∅(t) is the threshold function. The random binary sequence is generated by nth iteration.

A. Encryption process

The popular RSA algorithm followed by DNA coding is used to encrypt the message. The public key pair and private key pair are generated by using the RSA algorithm. The plain text is then encrypted by using the public key (e), which yields the ciphertext. The DNA encoding is achieved by the means of a chaotic neural network [8], the steps followed in the encryption process is shown in Fig 2.

Step1: A random binary sequence of length 42-bit is generated. Which is then split into three sections. The first 32 bit can be used as key; the next 9 bits are used by the sender to set the decimal value for the shifting operations and the last bit is used as a trajectory.

Step2: The binary equivalent value of the ASCII code of the plain text is then XORed with the random binary sequence generated by a chaotic neural network (here the sequence are subjected to left shift by j times before XOR operation, j is the decimal value generated by the random binary sequence

generator), which yields a stream of binary sequence [9].

Step3: The resultant binary sequence after performing XOR operations is then grouped into pairs. The pairs are then mapped into DNA sequence by simple substitution for 00 as A, 01 as C, 10 as G and 11 as T as shown in Table 1.

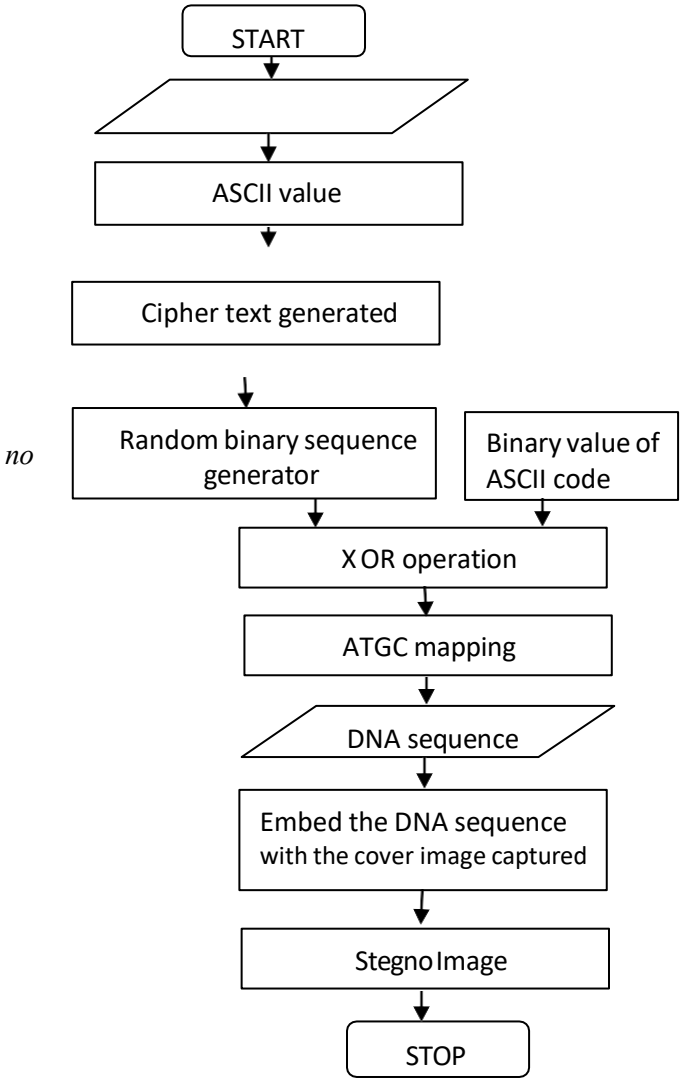


Fig 2. Flowchart of the encryption process

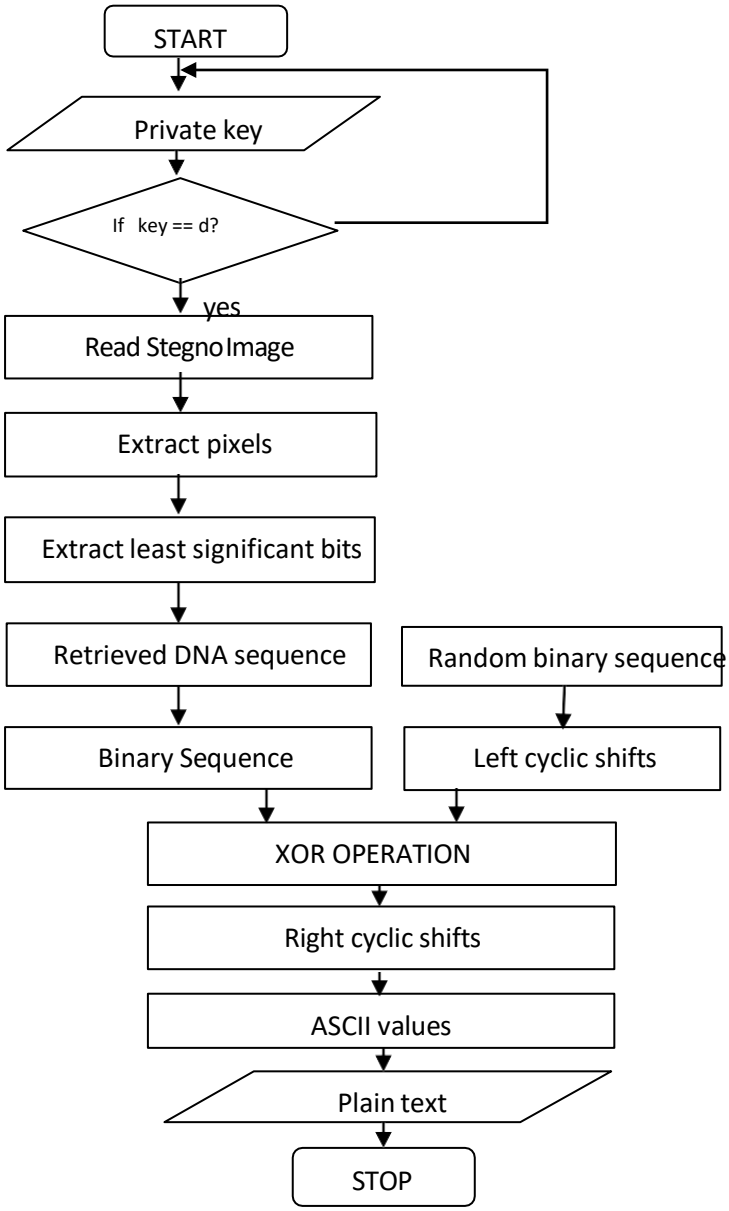
Step4: The DNA sequence formed, is then embedded into an image [10] by following the Steganographic method.

Step4: Select a bit plane (from 1 to 8-bit planes) to hide the DNA sequence.

Step5: Compute the segment of the cover image.

D. Decryption process

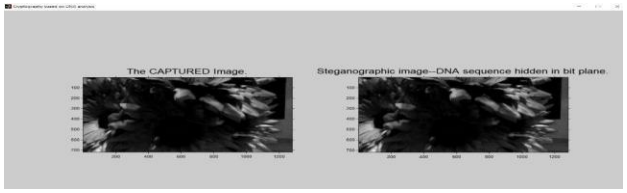
the cover image by considering the bit plane in which the sequence is hidden. The steps followed in decoding the DNA sequence is shown in Fig 3 and is explained below



Steganographic process

A real-time captured image is used as a cover image to hide the DNA sequence. The least significant bits (LSB) method is used to hide the DNA sequence in the cover image. The method involves replacing the least significant bits of the cover image pixels of a given byte. LSB method is significant and easier, but if the bits exceed more than three bits place a small distortion noticed in the steganographic image [11], Fig 2 explains the steps involved in steganography. The steps followed in embedding the DNA sequence with the cover image are:

Step1: Capture the cover image by the means of a web camera. The captured image will be a color image.



Step2: Convert the cover image to greyscale image by using an image conversion unit by selecting any channel, in this paper a green channel is selected.

Step3: Convert the DNA sequence to the stream of bytes by mapping back to binary sequence referring the

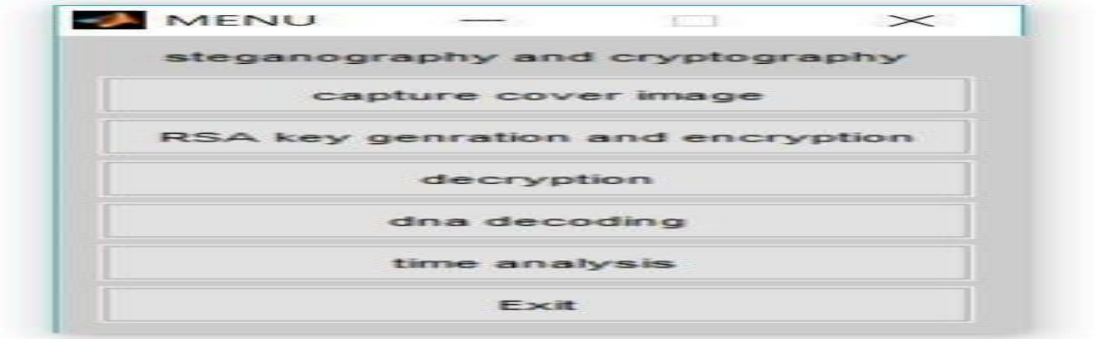




Fig 4. (a) menu displaying all the steps involved in the program (b) RSA key generation (c) Plaintext masked into the DNA sequence. (d) Generation of Steganographic image by hiding the DNA sequence in any one of the bit planes of the greyscale image.

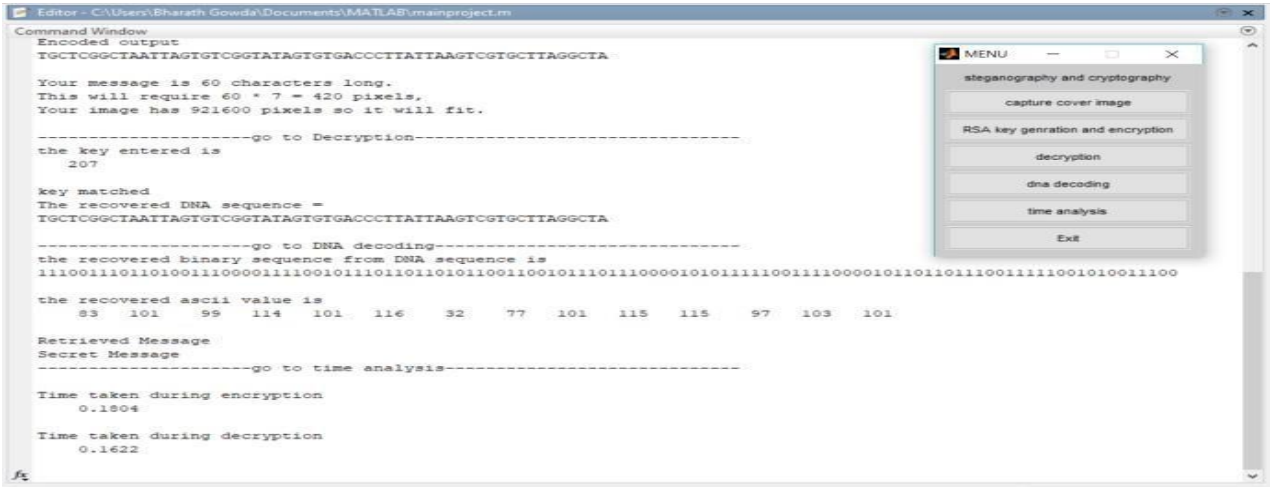


Fig 5. Decryption of the plaintext

CONCLUSION

The proposed paper is based on the combination of cryptography with steganography, which produces a more dependable and secure method. We may use DNA and the RSA technique to provide multi-layer reliability for the private data. This technique may be used in a number of ways to safeguard the data. Text may be incorporated into audio or video recordings, and polymerase chain reaction (PCR) can be employed to enhance DNA encryption methods.

REFERENCES

Taki, A. E., Deen, E., & Gobran, S. N. (2014). Digital Image Encryption Based on RSA Algorithm, 9(1), 69–73.

Yu, Wenwu, and J. Cao. "Cryptography based on delayed chaotic neural networks," Physics Letters, vol. A 356.4, pp. 333-338, August 2006.

C. Fu, Z. Zhu, "A chaotic image encryption scheme based on circular bit shift method.", in The 9th International Conference for Young Computer Scientists. pp. 3057–3061, 2008.

Qiang Zhang, Xianglian Xue, and XiaopengWei, "A Novel Image Encryption Algorithm Based on DNA Subsequence Operation", The Scientific World Journal, 2012, Volume 2012, Article ID 286741

Ms. Pallavi Hemant Dixit," Arm Implementation of LSB Algorithm of Steganography" Submission, Shivaji University,
Kolhapur, Maharashtra, India

Sajisha K S, Dr. Sheena Mathew, "An Encryption based on DNA cryptography and Steganography", IEEE, 2017.

T. Kohda, A. Tsuneda, "Statistics of chaotic binary sequences," IEEE Transactions on information theory, vol. A 43.1, pp. 104- 112, January 1997

A. Khare A, B. Shukla P, C. Silakari S. Secure and Fast Chaos based Encryption System using Digital Logic Circuit. Int J Comput Netw Inf Secur [Internet]. 2014; 6(6): 25–33.

Tian Tian Zhang, Shan Jun Yan, Cheng Yan Gu, Ran Ren and Kai Xin Liao, "Research on Image Encryption Based on DNA Sequence and Chaos Theory", IOP Conf. Series: Journal of Physics: Conf. Series 1004 (2018)