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

DNA CRYPTOGRAPHY FOR SECURE DATA COMMUNICATION PROCESSING SYSTEM

[1]M. Maheswari , [2]Sundar Santhoshkumar
[1,2]Department of Computer Science, Alagappa University, Karaikudi, Tamil Nadu

Abstract- Data security is guaranteed by encrypting plain text with cryptographic algorithms and transforming it into an unreadable format. To provide secure communication over a network, cryptographic techniques are used to encrypt messages. It is critical for organizations and individuals to safeguard their information from attackers as well as hackers in order to ensure data privacy, integrity, and confidentiality.
DNA Computing is a new technique for securing data that makes use of the biological structure of DNA. Data can be stored and transmitted using DNA. The idea of using DNA computing in cryptography has been recognized as a possible technology that could usher in a new era of unbreakable algorithms.The primary goal of this paper is to provide data with a high level of security. The use of the four nucleotides in sequence is the most important aspect of the DNA-based data masking technique. These are the nucleotides A, C, G, and T. A DNA sequence can be formed by any combination of these nucleotides. The first step is to convert clear language to DNA code using predefined values. Then, using the Least Significant Bit (LSB) technique, encrypted text can be hidden within the image. The receiver will use the reverse operation for decryption to obtain the cipher text and plaintext. The experimental findings indicate that the proposed program gives a high level of security when sharing data.

Index Terms-DNA Cryptography, Data Hiding, DNA Conversion, Data Extraction,Steganography.

I. INTRODUCTION

Steganography is the practice of concealing hidden codes (hidden text) within seemingly innocuous everyday objects (cover text) to create a stego text [1]. The recipient of the stego text can recover the secret message from the stego text using his knowledge of the specific method of steganography used[2]. Steganography objective is toenable parties to hold a conversation covertly in such a way that an attacker cannot tell whether or not their conversation contains hidden meaning [3]. This distinguishes steganography from cryptography, which, while allowing for Personal communications can raise suspicion simply by Virtue of its use [4].G J Simmons defined modern steganography by describing the issue in terms of inmates trying to interact clandestinely in the existence of the warden [5]. Prisoners Alice and Bob are permitted to communicate, but only through the prison guard, Ward. Alice wishes to send hidden codes to Bob in such manner that Ward cannot determine the components of the messages or even that they are being sent. This problem can be seen today in national Intel agencies trying to detect general populace yet secretive interaction among terrorists, or communication among residents in oppressive states where cryptography is illegal [6].

Steganography Working Process

Steganography is the process of replacing unnecessary or unused bits in regular computer files (graphics, sound, and text) with bits of different and invisible information. Any other regular computer file or encrypted data can be used to conceal information. Steganalysis differs from cryptology in that it conceals the existence of the message, whereas cryptography conceals the message's content.Steganography is sometimes used in tandem with encryption. Even if an encrypted file is comprehended, this same metadata is not visible because it is hidden using steganography.

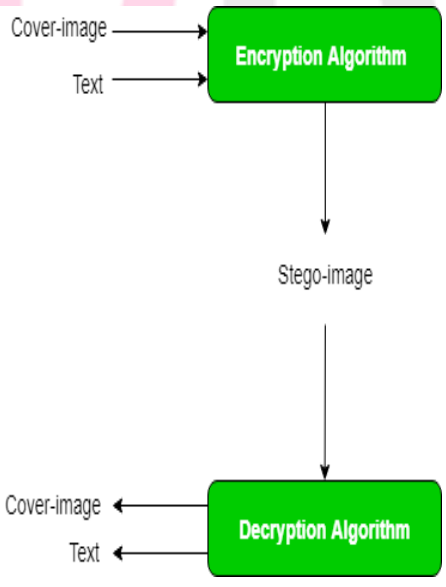

Fig 1: Basic Steganography layout

II. RELATED WORK

Chia-Hung Lin, et.al., [7] Implement a framework that includes an RFID system that is vulnerable to both passive and active attacks. Hackers may disassemble protocol knowledge and decide how that is system operates in order to obtain data, allow entry, or tamper with data. Cryptographic algorithms to permutation and substitution methods, or a combination of both, have been proposed for digital medical records in medical signal and image security; such methodologies involve reorganizing mathematical / pixel positions and changing numerical / number of pixels. Permutation cipher methods can rearrange their positions in an encrypted data sequence without changing the numerical / pixel values.Substitution cipher-based methods, on the other hand, replace plain messages with letters, numbers, or specific symbols that change the numerical / pixel values in the entire encrypted data sequence by using the transformation function or combining the replacement and transposition methods. To improve communication security, methods such as shift cipher, affine cipher, exclusive (XOR), Hill cipher, play fair cipher, and hash function can be combined with a multi-round cryptography protocol. Encrypted messages that use iterated or replacement methodologies with repaired private keys as continual control factors in the synchronous cryptography protocol, on the other hand, are easily broken by either active or passive cyber security threats that intercept message content to adjust, steal, and copy by unauthorized behaviour, resulting in theft cases and security threats.

Zhongyun Hua, et.al.,[8] presents the S-box generation method and analyses this same performance and efficiency of its generated S-box develops an image encryption algorithm using the construct evaluates the security performance of the encryption algorithm concludes this document. In general, an S-box is a matrix that takes a variety of input bits and transforms them into the identical number of output bits. It is among the most important sections in a symmetric-key encryption algorithm and has the ability to randomly change an image's pixel positions. As a result, the level of security of a cryptographic algorithm is heavily influenced by the S-box it employs.Many security attacks may easily break the encryption algorithm in the absence of a high-performance S-box. As a result, one important aspect of working to develop image encryption is to create a high-performance S-box. Until now, scientists have devised a variety of methods for building S-boxes. A chaotic system is widely used to develop S-boxes because it can generate randomly distributed sequences. A two-dimensional chaotic map, for example, is used to build a high-performance S-box. Once nonlinearities are used to build S-boxes, the chaotic system's properties heavily impact the performance of the built S-boxes. A dynamic system to poor performance could result in the constructed S-box having a low security level.Many techniques are combined with chaotic systems to design S-boxes in order to avoid the negative effects of chaotic systems. Security analyses revealed that S-boxes built using combined method outperformed those built solely with chaos theory.

Zhongyun, et.al., [9]Many researchers have introduced pressure changes (CS) technology into image encryption to conduct image compression and encryption at the same time. For example, the authors of first used the CS to compress a plain image, and then encrypted the compressed image by scrambling and diffusing image pixels. To increase security, the authors have proposed a parallel CS (PCS) technique to resist a chosen plain attack. These encryption schemes can condense and decryption a plain image at the same time, making them useful in a variety of situations. However, they also convert plain images into unrecognizable cipher images, which do not deter attackers.To address the shortcomings of the first two types of data encryption, the third type intends to encode an unobtrusive as possible to a cipher image to visual security. These encryption algorithms typically have two stages: encryption and embedding. The encryption stage converts an unobtrusive as possible to an encrypted image, which is then embedded into a cover file to create the final visually constructive cipher image. The scheme in, for example, first encrypts a plain image to create an unrecognizable secret, and then embeds the secret image into a carrier image by substituting a portion of the carrier image.To reduce the embedding size, an encryption scheme based on CS and discrete wavelet transform was proposed (DWT). A plain image is first compressed using CS, then encrypted to become a secret picture, and finally embedded into a carrier image of the same size as the plain image. The relevant in today the encryption framework by introducing a new CS counter mode and integer wavelet transformation to improve the security level and quality of the reconstructed image.

Dhivya Ravichandran, et.al., [10]Implemented technological innovations are blowing up far above. Telecommunication advancements have paved the way for more convenient information transmission over the internet. Several types of data, such as digital images, videos, and records, are transferred around the world in a matter of seconds. Telehealth is the most outstanding solution to the current healthcare crisis in the medical field. Electronic healthcare images are images of human body parts that are used for accurate diagnosis and treatment. Because of cybercrime, healthcare professionals must exercise extreme caution when dealing with sensitive patient information. Encryption techniques are required in this scenario to ensure the secure data transmission of highly classified medical information.Encryption is the method of encoding data with the aid of a secret key so that it can only be accessed by authorised parties. Because of the bulk pixel capacity and high redundancy, traditional security mechanisms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are inefficient for encrypting medical images. These algorithms require a significant amount of supercomputing time to finish the encryption process. Because of its high randomness performance, a chaotic

system has recently piqued the interest of several researchers for use in various cryptosystems. Due to insufficient key performances, single-dimensional chaotic maps are insufficient for achieving a secure method.Medical images have inherent characteristics such as big data sizes, correlated pixel density, pixel size, and high redundancy. As a result, a new block cipher based on DNA is needed to address these growing security problems.

ZhongyunHua,et.al. [11]The majority of research focuses on determining the mathematical definitions of chaos theory or assessing their initial states and chaotic signals under certain conditions. A hybrid regularized echo state network, for example, was tried to introduce to predict multi - variable chaotic signals using past observation states. In general, chaotic systems with discontinuous chaotic distances and imperfect output distributions are prone to the above situations. If some important information about a chaotic system's equation or chaotic signal can be estimated, the system may end up losing the essential properties of chaos, which may have a negative impact on its applications. Many works, as reviewed in, have indeed been dedicated to addressing the flaws of established chaotic systems.One common strategy is to increase the sophistication of chaotic signals by changing their parameters or directly interfering with their chaotic systems using noise or arbitrary numbers. Chen et al., for example, use noise to scurry the output characteristics of a modified Maps in. This method can produce chaotic signals with a high degree of randomness. However, there are some drawbacks to this strategy for increasing the complexity of chaotic signals.

PI-YUN CHEN, et.al., [12]Improve diagnosing accuracy and efficiency for effectively utilising and managing medical data, such as biomedical parameters, medical images, and care in the context. Medical imaging has become an important component of the majority of diagnostic procedures, as well as a major component of the health infrastructure. Medical imaging techniques, including such X-ray image analysis, magnetic resonance imaging (MRI), ultra-zoography, echocardiography, and computed tomography, are used to create two-dimensional (2D) or three-dimensional (3D) images of human organs for diagnostic and treatment applications in digital health (CT). Since 2018, Taiwanese academic institutions have gradually created cross-hospital medical image datasets for research and artificial intelligence applications such as lung disease, meningioma, breast tumour, liver tumour, and heart disease treatment.

Medical images from 46,540 patients were collected, totaling more than 5 million clinical data in Taiwan. In this study, the hash transformation function is used to convert graphic data (any image) into sequence data, which is then mixed with a sequence of hash weighting values and a sequence of secret key data to encrypt internet transmissions in a health information system. To generate the spread spectrum signal, a chirped signal is used as a multi-secret key, which embeds an encryption in the ROI. Then, optimization automated process controllers such as the linear regression (GD) and particle swarm optimizing (PSO) algorithms are used to iteratively search for the decryption weighting parameter.

Aashiq Banu,et.al., [13]It is critical to protect medical data from cyber-attacks once safe transmission of medical data has been implemented. DICOM is the most widely used standard in medical image storage, retrieval, processing, and transmission. To transfer patient information between health-care facilities, a secure network should be established. Encryption is one of the best techniques to use to overcome privacy concerns and ensure reliable transmission. Encryption can be achieved through the use of suitable ambiguity and diffusion mechanisms. To protect text data, established encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Triple DES are well suited. Large data sizes, high-intensity repetition, and pixel interdependences distinguish digital medical images.As a result, traditional cryptographic protocols are ineffective for securing DICOM images. Because of prominent characteristics such as immense high ergodicity, high parametric range, and sensitivity to initial seeds, chaotic maps are widespread used in several MRI images cryptosystems. Nonetheless, 1D and multi-dimensional chaos - based have flaws such as an insufficient and discontinuous range of lackluster performance, a restricted non-uniform data structure, and so on.

Rethinam Sivaraman, et.al., [14]Despite the fact that responsiveness to initial state serves as the foundation for series data generation via chaotic maps or attractors, the selective chaotic region limits the random range width. Attacks on chaos-based ciphering techniques are becoming more common. Norouzi and Mirzakuchaki recently performed cryptanalysis on turmoil greyscale image encryption, where the method was compromised by the plaintext attack. Dou et al. also conducted a decryption on logistic maps that combined a DNA-based combined picture encryption scheme. Their work could be cracked using an innovative chosen-plaintext attack. For chaotic maps, a random image or a synthetic image generated by hardware appears to be an option. Any viable alternative must be able to replicate the effect of confusion as well as diffusion produced by chaos-influenced maps.Because of the problems in arriving at a specific mathematical model, odd parts acquired through unique hardware features can withstand attacks. In the proposed DNA - Chaotic image encryption work, a key image was produced using Matlab 7.1's randint (size) command. This synthetic image, however, was found to have a low correlation. True random generators (TRNGs) have been used in previous works for image diffusion, including a ring oscillator (RO)-based synthetic image recorded using IC 7404 converters rings. This random image was produced by a near-uniform histogram with thermodynamics of 7.954 nearer to 8. Another study made use of a synthetic image generated by PLLs driven by beat frequency detection.

HEGUI ZHU, et.al., [15]Many picture encryption techniques, such as chaos cryptology, DNA software, and quantum theory, have been proposed. Chaos cryptography is an interdisciplinary subject that incorporates chaos theory into cryptography and is better suited for cryptography with distinct characteristics. There are two types of chaotic maps: each (1D) chaotic maps and high-dimensional (HD) chaotic maps. Logistic, Sine, and Chebyshev maps are instances of 1D chaotic maps. Even so, 1D chaotic maps have several drawbacks, including simple structures and very few variables. With little extracted information, their chaotic orbits, parameters, and initial values can be predicted.As a result, digital chaotic maps really aren't dominant in the field of security. Because HD chaotic maps have much more complex systems and better chaos performance than 1D chaotic maps, they are an excellent choice for encryption. For example, TD-ERCS chaotic system was proposed and used to produce two sequence for image encryption. Hua et al. proposed a very one (1D) multiple linear regression model (1D-NLM) for generating discrete-time chaotic maps in one dimension.These freshly created chaotic maps have had much wider chaotic ranges, more random outputs, higher degree of freedom attractors, and more sensitive initial states than existing ones. They designed two high-level chaotic maps, Cosinus-Arcsinus and Sinus-Power Logistic map, for colour encrypted images that had improved results with low calculation administrative costs and less co - relation among adjacent pixels in the permuted image.

Chunlai Li, et.al., [16]have discovered the existence of robust chaos in constant chaos theory with unlimited parameter space. These parameters can regulate the amplitude of the system signal on a regular basis, and the Nonlinear exponent remains constant. As a result, this type of system is a strong contender for the practical implementation of chaos encryption and chaotic communication. However, to the greatest of our knowledge, no study on robust chaos of a separate chart with unlimited parameter space has been reported in the literature, leaving the field open and challenging. So, in an attempt to solve the dilemma of existing discrete maps, we introduce a two-dimensional smooth map and an optimal control scheme.First, we discover that when some system parameters and state variable scales vary in infinite real space, the Lyapunov exponents of this discrete map remain invariant and the signal amplitudes change regularly following some functional relationship. Then, using matching condition of iteration range and the definition of Lyapunov exponent, a compound operation-based optimization control method of complexity is introduced. Theoretical analysis shows that as the control parameters vary in real space, the values of the Lyapunov exponent increase in logarithmic form. As a result, the chaotic sequence becomes more complex.

III. BACKGROUND OF THE WORK

Steganography may be a solution that allows individuals to send information and news without fear of being censored or having their messages intercepted and traced back to them. Steganography can also be used to simply store information about a location [17]. Several information sources, such as with us private bank details and some military secrets, could be stored in a cover source, for example. Watermarking can also be accomplished using steganography. Watermarks are stored in data using a variety of steganographic techniques. The main distinction is the purpose of steganalysis is to conceal information, whereas watermarking is simply to augment the cover source with additional information [18].Cryptography is the art of encrypting and decrypting data using mathematics. Cryptography allows you to keep sensitive data or transfer this across insecure networks (such as the Internet) so that no one but the intended recipient can read it.

Cryptography is the art of securing data, whereas cryptanalysis is the science of analyzing and breaking secure communication [19]. Classical cryptanalysis entails an intriguing combination of analytical thinking, mathematical tool application, pattern recognition, perseverance, determination, and luck. Cryptanalysts are also referred to as attackers. Cryptology includes cryptography as well as cryptanalysis [20]. Fig 2 displays the secure communication system

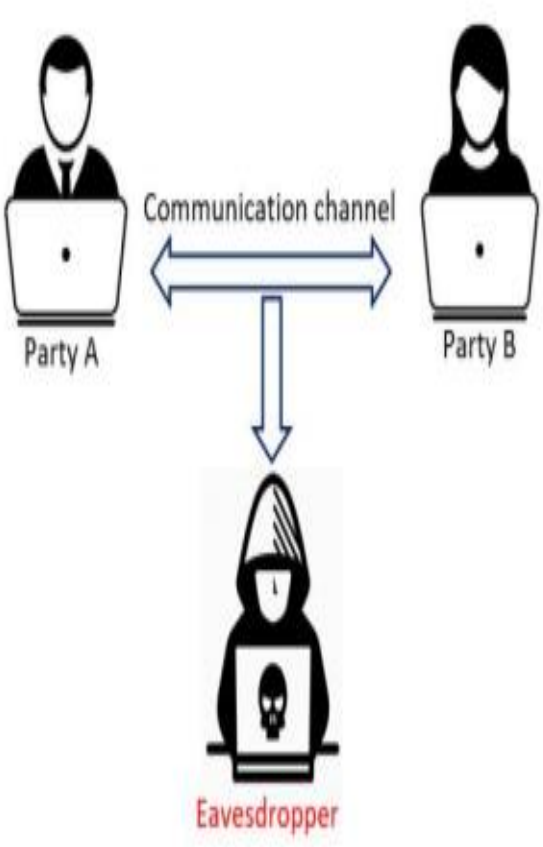

Fig 2: Secure communication channel

IV. PROPOSED WORK

The science of secret writing is known as cryptography. It aids in the encryption of plain text messages, rendering them unreadable. It is a very old art, going all the way back to that when Egyptian scribes was using non-standard inscriptions in an inscription. Steganography is a security system obscurity method

that involves concealing the presence of a text between the recipient and intended recipient. This technique has been used to conceal secret messages in a variety of documents, including digital images, audio, and video. The most common use of steganography is to safeguard the data from one file within the information of another.Wrap carriers, including such images, sound, video, text, or code depicted digitally, for example, hold the secret knowledge so that its existence is not discovered by a third party or an unintended receiver. Clear text, block cipher, images, or information hidden in a bitstream are all examples of hidden information. A stego-carrier is formed by the cover carrier and the hidden information. The covered image with the hidden message is known as STEGO, and it aids in the reduction or elimination of suspicion.

Steganography is a system for disguising a message in a reasonable holder, such as a picture, sound, or video document. The steganography network is heavily influenced by the flag and image handling networks.Some less successive obligations from the cryptographic protocols and information hypothesis networks don't always use the same wording, which can make it challenging to see the connections between various works.

A new encryption algorithm based on DNA patterns is proposed in the proposed system. DNA Coding is a novel method for securely storing large amounts of data in small fragments of DNA. The DNA structure allows for massive parallelism, exceptional energy efficiency, and exceptional storage capacity. Genetic material can be employed to encrypt data for storage and transmission, as well as to perform computation. The primary function of DNA cryptography is to generate a DNA sequence. The knowledge carrier and biological technology are used to create the DNA sequence.The paper proposes using DNA sequences to implement data hiding. To encrypt the message, both the concept of encryption approach based on modified RSA and data hiding are used, and sample DNA sequencing is considered. The encrypted message will then be hidden with image data using the LSB technique. The receiver will receive both the DNA sequence and the encrypted data, which will be extracted from the image to obtain the original message. In this method, both the sender and the receiver will use the same Sequence of DNA for encryption and decryption.This algorithm has three stages: DNA Sequence, Cryptography, and Data Hide. The text entry message was converted into DNA layout using a DNA sequence table in the first stage. In the second stage, the Genomic DNA is encrypted using the DNA coding method. The third stage of the data hiding process, which is based on the LSB technique, occurs.

This is a steganography technique in which a message is hidden inside an image by replacing the image's least significant bit with the message's hidden bits.A secret message can be inserted, and the picture made unnoticeable by modifying only the first most right bit of a picture, but if the message is too large, this will start changing the second rightmost bit and so on, and an attacker will notice the changes in the picture. This same least important provision (LSB) insertion method is a common and simple way to embed data in an image. The LSB of a bit of data is replaced with an M's bit in this technique. The stego image appears the same to the carrier image to the naked eye. An image is simply a file that displays different colors and light intensity of illumination on various areas of an image to a computer.

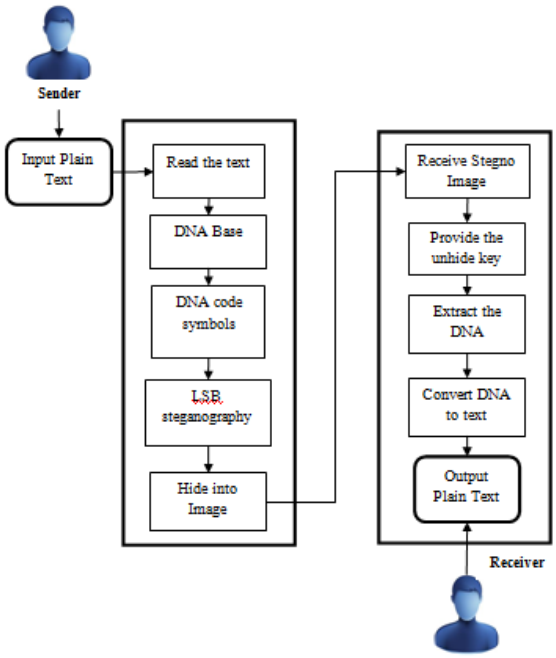

Fig: 3 Proposed Framework

Communication Framework

Because of the rapid growth of transmission applications, information security is regarded as the most critical issue in communication systems. In the proposed framework, sender and receiver will communicate in a secure manner using DNA conversion, encryption, and data hiding techniques.

Apply Dna Conversion

Using a DNA sequence table, the input text can be transformed into a DNA sequence. Cryptographic technique introduces an improved technique for storing large amounts of data in a small segment of DNA while maintaining data integrity and security. DNA cryptography is the practice of concealing data in a DNA sequence. In DNA sequence, the four types of nitrogen bases are adenine (A) and thymine (T) or cytosine (C) and guanine (G).

Data Hiding Within Image

This module describes the data hiding process. The encrypted message may be concealed within an image file. This procedure increases the confidentiality of the shared message. The LSB technique was used to implement the hidden process. With the help of LSB, the encrypted message was completely hidden within the image file. During the hidden process, the sender could generate a secret key for identifying the shared message.

Data Extraction Process

The method for extracting an able to share secret message on the receiver side is known as data extraction. First, the message reaches the receiver in the form of a hidden message within an image. The hidden message will be delivered to the recipient using the shared secret key. The decryption process is then used to obtain the DNA sequence. Decryption is the process of returning encrypted text to its original form. Only an authorised user can decrypt the data. The encrypted message first reaches the receiver in the shape of strings usually contains numbers and DNA sequences.

Least Significant Bit Insertion

The most well-known algorithm for image steganography is Least Significant Bit (LSB) insertion, which involves modifying the image's LSB layer. The message is stored in the LSB of the pixels in this technique, which could be considered random noise. As a result, changing them has no discernible effect on the image.

Masking And Filtering

Masking and filtration techniques work best with images that are 24 bits or greyscale. They conceal information in a manner similar to paper watermarks and are occasionally used as electronic watermarks. The images are changed when they are masked. To make sure that changes are undetectable, make them in numerous small proportions. Masking is more robust than LSB masking, and masked images pass cropping, compression, and some image analysis. Masking combines information in key areas, making the hidden message more integrated into the cover picture than simply hiding it in the "loud sound" level. The above makes it more suitable for use with lossy JPEG images than LSB.

Redundant Pattern Encoding

Redundant pattern code is similar to the spread spectrum technique in some ways. The text is scattered throughout the image using an algorithm in this technique. This technique renders the image unusable for crop rotation and rotation. Even if the stegano-image is manipulated, numerous small images with redundancy increase the chances of recovery.

Encrypt And Scatter

The message is hidden as white noise using encryption and scatter techniques. Storm is an example of a spectrum sensing and frequency hopping application. Prior window size and data connection are employed to generate a random number, and this random number, message is scattered across all eight channels. Each channel rotates, swaps, and interlaces with all others. Because each channel represents one bit, there are many unaffected bits in each channel. It is extremely difficult to extract the real statement from a stegano-image using this technique. This method is more secure than LSB because it requires both an algorithm and a key to decipher the awareness means from the stegano-image.

Algorithms And Transformations

If any type of compression is applied to the resulting stego-image, such as JPEG or GIF, the LSB modification technique holds true. JPEG images are compressed using the discrete cosine transform. Because cosine values cannot be calculated exactly, DCT is a lossy compression transform, and repeated calculations with limited cellsbased introduce rounding errors into the final result. The differences between original and restored data values are determined by the technique used to calculate DCT.

V. EXPERIMENTAL WORK

A steganography technique in which a message is hidden inside an image by replacing the image's least significant bit with the bits of the message to be hidden. A secret message can be inserted and the picture made unnoticeable by modifying only the first most right bit of an image, but if the message is too large, it will start changing the second rightmost bit and so on, and an attacker will notice the changes in the picture. The lowest important provision (LSB) insertion method is a common and simple way to embed data in an image. The LSB of a byte is replaced with an M's bit in this technique. The stego image appears the same to the carrier image to the naked eye. An image file is simply a file that displays various shades and intensities of light on different areas of an image to a computer. A 24 Bit BMP (Bitmap) image is the best type of image file to hide information inside. Despite the fact that 24 Bit photos are best for concealing data because of their size. Some people may prefer 8 Bit BMPs or the other image layout such as GIF. The reason for this is that posting large images onto the internet may raise eyebrows. The eighth bit, the least significant bit, is employed to change to a bit of a secret message.

In this chapter, we will incorporate the system in real-time and layout the framework with C#.NET as the front end as well as SQL SERVER as the back end.

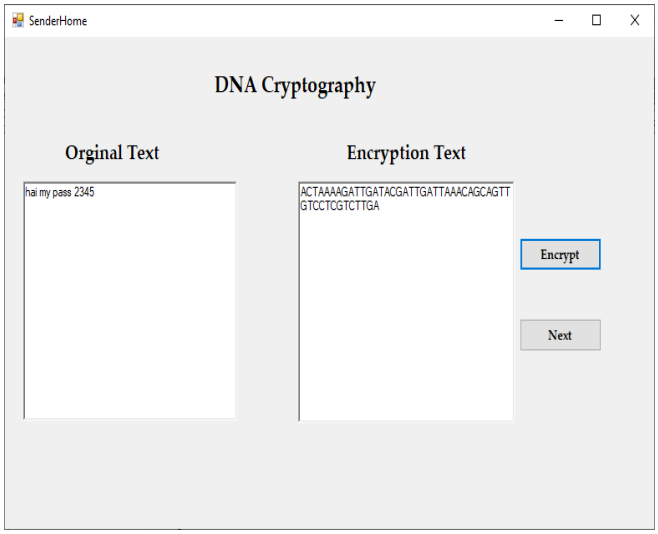

Fig 4: Dna Coding

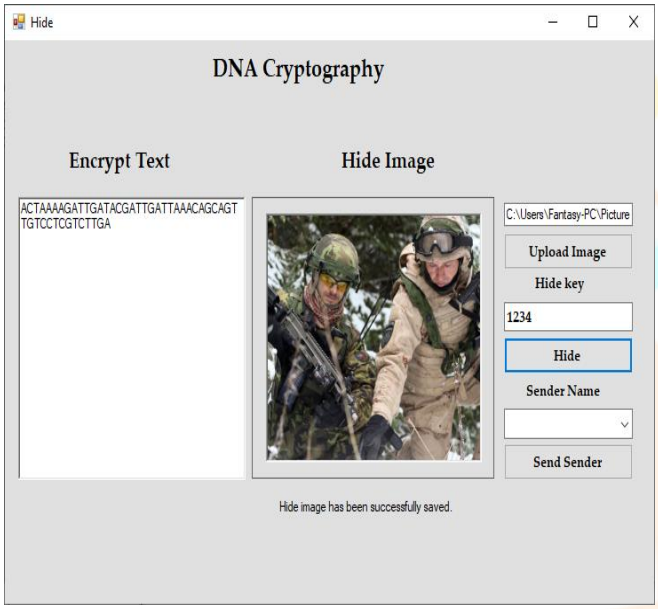

Fig 5: Data Hiding

Fig 6 : Unhide The Data

Fig 7: Message Extraction

VI. CONCLUSION

The extraction of data now begins with a comparison of the Target DNA and number strings. The DNA base code is then applied and converted to binary values, from which the ASCII values are represented, and the corresponding text, which is nothing but original data, is obtained.Money transfers, medical and personal records, and other sensitive information are transmitted via public communication facilities. The security of sensitive information is jeopardized by such an unintended recipient. Cryptographic techniques aid in the protection of such sensitive data. Cryptology allows the sender to safely store or transfer sensitive data all over unsecured network so that only the intended recipient can understand it. A cryptographic system encrypts the information and generates an encrypted output that is pointless to an unplanned user who does not know the key. Decryption requires knowledge of the key.

REFERENCES

[1] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." In *ISSA*, vol. 1, no. 2, pp. 1-11. 2005.

[2]Banerjee, Indradip, Souvik Bhattacharyya, and Gautam Sanyal. "Novel text steganography through special code generation." In *Proceedings of International Conference on Systemics, Cybernetics and Informatics (ICSCI-2011), Hyderabad, India*. 2011.

[3] Tiemann, Thore, Sebastian Berndt, Thomas Eisenbarth, and Maciej Liskiewicz. "" Act natural!": Having a Private Chat on a Public Blockchain." *Cryptology ePrint Archive* (2021)..

[4]Jegadeesan, S., K. S. Naghulkirthic, and K. Akash. *Multi Secret Sharing with Encrypted Data Hiding for Secure Communication*. No. 5256. EasyChair, 2021.

[5] Mazurczyk, Wojciech, Steffen Wendzel, Mehdi Chourib, and Jörg Keller. "Countering adaptive network covert communication with dynamic wardens." *Future Generation Computer Systems* 94 (2019): 712-725.

[6] Lissaris, Euthimios, Georgios Giataganas, Dimitrios Kavallieros, Dimitrios Myttas, and Emmanouil Kermitsis. "Terrorist Activities in the Dark and the

Surface Web." In *Dark Web Investigation*, pp. 49-84. Springer, Cham, 2021.
[7]Lin, Chia-Hung, et al. "Symmetric cryptography with a chaotic map and a multilayer machine learning network for physiological signal infosecurity: Case study in electrocardiogram." IEEE Access 9 (2021): 26451-26467.
[8] Hua, Zhongyun, et al. "Design and application of an S-box using complete Latin square." Nonlinear Dynamics 104.1 (2021): 807-825.
[9] Hua, Zhongyun, et al. "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing." Signal Processing 183 (2021): 107998.
[10] Ravichandran, Dhivya, et al. "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain." Medical & Biological Engineering & Computing 59.3 (2021): 589-605.
[11] Hua, Zhongyun, Yinxing Zhang, and Yicong Zhou. "Two-dimensional modular chaotification system for improving chaos complexity." IEEE Transactions on Signal Processing 68 (2020): 1937-1949.
[12] Chen, Pi-Yun, et al. "Medical image infosecurity using hash transformation and optimization-based controller in a health information system: Case study in breast elastography and X-ray image." IEEE Access 8 (2020): 61340-61354.
[13] Aashiq Banu, S., and Rengarajan Amirtharajan. "Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach." Multimedia Tools and Applications 79.39 (2020): 28807-28824.
[14] Sivaraman, Rethinam, et al. "Ring oscillator as confusion–diffusion agent: A complete TRNG drove image security." IET Image Processing 14.13 (2020): 2987-2997.
[15] Zhu, Hegui, Yiran Zhao, and Yujia Song. "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption." IEEE Access 7 (2019): 14081-14098.
[16] Li, Chunlai, et al. "Dynamics and optimization control of a robust chaotic map." IEEE Access 7 (2019): 160072-160081.
[17] Oyaniyi, Lawrence Olanrewaju. "Design And Implementation Of Digital Image Tool For Forensic Analysis." Phd Diss., Federal University Of Technology, Akure, 2019.
[18] Ahvanooey, Milad Taleby, Qianmu Li, Xuefang Zhu, Mamoun Alazab, and Jing Zhang. "ANiTW: A novel intelligent text watermarking technique for forensic identification of spurious information on social media." *Computers & Security* 90 (2020): 101702.
[19] Younes, Mohammad Ali Bani. "A Survey Of The Most Current Image Encryption And Decryption Techniques." *International Journal Of Advanced Research In Computer Science* 10, No. 1 (2019).
[20] Bos, Joppe, and Martijn Stam, eds. *Computational Cryptography: Algorithmic Aspects of Cryptology*. Vol. 469. Cambridge University Press, 2021.