Key Creation for Steganography-Free

1stRojashree
dept. of Computer Science & Engineering
(VTU)
Rajeev Institute of Technology
(VTU)
Hassan, India
rose92grisha@gmail.com

2rdDr. Sharath.M.N.
dept. of computer Science & Engineering
(VTU)
Rajeev Institute of Technology
(VTU)
Hassan, India
sharath@gmail.com

***Abstract*—The creation of stego-key is a critical stage in the steganographic process. Steganography-Free employs DNA sequences to shift and flip the binary code representation, leading to the creation of the stego-key. Free Steganography is a technology that uses DNA-based key generation to improve security. Specific DNA segments are extracted, encoded digitally, and used as cryptographic keys, ensuring resilience against conventional cryptographic attacks. The study evaluates the integration of this method into the Free Steganography framework, comparing it with traditional encryption approaches to highlight its advantages.**

Keywords—Free Steganography, DNA-Based Key Generation, Cryptographic Security, Data Privacy.

I. INTRODUCTION

Technology has significantly advanced communication currently. People are more bonded by smartphones, the internet, cloud computing, and other sophisticated technologies. As a result, the security of data exchanged through networks is likewise threatened by this. Cryptography provides security by modifying text or image signals with a stego-key known only to the sender and recipient[1],[8]. In contrast to the concealed message in steganography, the encrypted message will raise suspicions.

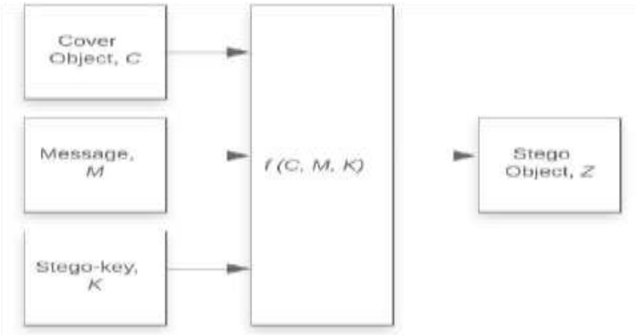


Fig 1.1. The basic steganography models

Key creation for steganography-free technology is frequently referred to the art of data concealment[8]. It involves hiding information in seemingly innocuous objects in a way that makes the information hidden from view. Free steganography safeguards the integrity and secrecy of hidden data in sensitive communications.

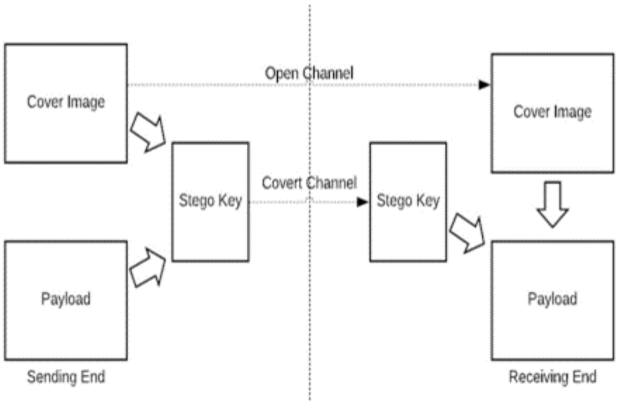


Fig 1.2. The basic principle of Free steganography

DNA cryptography is an exciting and emerging field that builds on the idea of DNA computing. Instead of using traditional methods to store and secure data, this approach uses DNA molecules to encode, carry, and protect information[2],[5]. Over the past 20 years, researchers have developed a variety of algorithms based on DNA, applying them to tasks like data encryption and cryptographic key generation[9]**.** This innovative blend of biology and computer science offers a completely new way to think about data security.

DNA, or Deoxyribonucleic Acid, is made up of six key components: a sugar molecule called deoxyribose, a phosphate group, and four nitrogenous bases—Adenine (A), Thymine (T), Cytosine (C), and Guanine (G)[5]. These components form two long strands that twist together into a structure known as the double helix, with the sugar and phosphate molecules creating the backbone of the strands[13].

DNA sequences are incredibly large and complex, making them ideal for storing large amounts of hidden data[5]. [13]To embed confidential information into DNA sequences, several techniques can be used—such as DNA insertion, DNA substitution, and DNA complementary algorithms[9]. Among these, the DNA insertion method stands out for its low probability of being cracked, making it more secure.

Fig1.3. Structure of DNA

In this paper, we propose an improved version of the DNA insertion algorithm aimed at further reducing the likelihood of the hidden information being detected or tampered with. This enhancement is designed to make the fake DNA sequence even harder to decipher, increasing the overall security of the data hiding process[13],[9].
This illustrates an explanation of classic steganography. Without sacrificing the quality of the cover object, the sender can hide the secret message inside it by using a stego-key[1]. The stego object is the output of this procedure.

It is inevitable to leave modifications in the stego-image when using the traditional steganography technique. As a result, it is challenging for the stego-picture to avoid being discovered by image steganalysis algorithms. If the message is detected, a steganographic method is deemed untrustworthy.

II. Literature Review

[2]Recent studies have shown that when DNA binds to minerals, it becomes more stable and can survive much longer in the environment. These DNA-mineral associations can act like natural gene banks, preserving genetic material over long periods. What's especially fascinating is that this DNA isn't just preserved—it can still be taken up by other, unrelated organisms through a process known as horizontal gene transfer (HGT). In this piece, we propose that minerals may play a much bigger role in spreading genetic material than previously thought, carrying DNA across different environments and time periods. We suggest that this mineral-mediated transfer of genes has had a profound impact on the evolution of life on Earth.

[4]This paper explores a recently developed image encryption algorithm that leverages evolutionary computation techniques. It proposes a novel hybrid encryption model that integrates DNA masking, a genetic algorithm (GA), and a logistic map. In this approach, DNA encoding and logistic maps are used to generate an initial set of DNA masks. The genetic algorithm then optimizes this set to select the most effective mask for encrypting the image. The main advantage of this method lies in its ability to enhance the quality and suitability of the DNA masks, ensuring better compatibility with the original (plain) images. Experimental results and simulations demonstrate that the proposed encryption scheme not only delivers strong security performance but also effectively withstands a range of common cryptographic attacks.

[8]Instead of embedding the secret image into another image, our approach feeds the secret image into a generative model database, which produces a new, natural-looking image that appears unrelated to the original. This generated image is then sent to the receiver. On the receiving end, the same generative model is used to reconstruct an image that visually resembles the original secret image. Data security studies frequently employ cryptography, particularly key creation.

III. EXISTING SYSTEM

The research presented several noteworthy contributions in enhancing the security and efficiency of the Crypto-Stego method for image confidentiality.

Direct Implementation on Color Images: Instead of converting color images into grayscale, the proposed method directly applied the security mechanism to the original color images. This approach ensured the preservation of visual information while maintaining security measures.

Elimination of Separate Key Distribution Mechanism: The Crypto-Stego method eliminated the need for a separate key distribution mechanism during decryption. by doing away with the need for the sender and recipient to exchange keys during the encryption and decryption process.

Parallel-Processing Approach: A parallel-processing strategy was used in the study to improve execution time and effectiveness. By effectively utilizing system resources, multiple tasks were executed simultaneously, resulting in improved overall performance.

Extensive Experimental Validation: The effectiveness of the proposed Crypto-Stego method was rigorously validated through extensive experiments[4]. To assess the scheme, a range of RGB photographs with varying sizes and resolutions were used. Strong scores in the Structural Similarity (SSIM) index showed that the approach was effective in preserving picture confidentiality.

The steganography systems, secret data is embedded within digital media such as images, audio files, or videos by altering the least significant bits (LSBs) of pixel or sound data. These systems rely on minor modifications that are usually imperceptible to human senses but can still be detected by advanced steganalysis tools or result in degradation of the original media. While effective, these methods are not ideal for text-based communication, where any change to the content or structure may be more noticeable.

Text-based steganography has also been explored in various forms, including methods like whitespace manipulation, font change encoding, and misspelling-based hiding. However, many of these methods are detectable by spell-checkers or formatting tools and can be easily disrupted when the text is copied, reformatted, or passed through text filters.

The results demonstrated the efficacy of the method in maintaining image confidentiality, as indicated by high scores in the Structural Similarity (SSIM) index. It was confirmed by the low Mean Squared Error (MSE) statistics that hostile people could not identify the stego data in the cover image.The suggested approach was found to be effective, as evidenced by the negligible changes in the pixel intensity histogram[4]. The study also highlighted the average efficiency of 77% achieved through parallel processing, along with a 1.5 times speed-up factor, providing additional evidence of the method's effectiveness in ensuring image confidentiality.

Hiding messages is not new. Before the advent of the internet, messages might be concealed using invisible ink, delicate paper creases, Morse code signals sewn into garments or even messages tattooed beneath messengers' hair.

IV. PROPOSED SYSTEM

The primary goal of the suggested approach is to improve data security while it is being transmitted. This is achieved by manipulating the positions of elements within the original input data, specifically numeric data. Through this manipulation, modified numeric data is generated and used as input for the encryption algorithm. involves designing a method for creating and managing secret keys used to hide or extract hidden messages within media files. With the AES implementation, the cipher text is obtained in hexadecimal format and has a very long length. All of the keys are used to encrypt all of the data. Two distinct keys—the encryption key and the data concealing key—are utilized for image encryption and information hiding, [2]we partially hide the encrypted information in the image and with the help of the remaining part of the encrypted message we generate two keys.

The encryption algorithm takes the modified numeric data as input and produces cipher text, which can be decrypted by the receiver. Upon decryption, the receiver generates the modified numeric data. To obtain the original plaintext, the receiver rearranges the positions of the modified numeric data accordingly. The fundamental idea behind the design of merging two distinct techniques is to distort the message and conceal its presence, and to recover the original message, reverse the distortion process and reclaim the distorted original message.

To ensure successful conversion between the modified numeric data and the original plaintext, it is crucial for the sender and receiver to share the encryption and decryption key. The procedure of getting the updated numerical data and precisely converting it back to the original plaintext is made easier by this key sharing technique.

The challenges associated with steganography include the concealment of data and the ability to avoid detection by steganalysis algorithms. [14]One approach called zero steganography allows for data concealment without modifying the cover image. This research concentrates on the development of a stego-key, which plays a pivotal role in the steganographic procedure. The proposed method employs DNA sequences and incorporates shifting and flipping operations to represent binary code[2]. Based on experimental findings, the key generation algorithm demonstrates a minimal risk of being cracked and fulfils the avalanche requirement. Create and put into use a safe, free key generation system for steganographic applications that can embed and retrieve concealed data from digital media while also withstanding brute-force attacks.

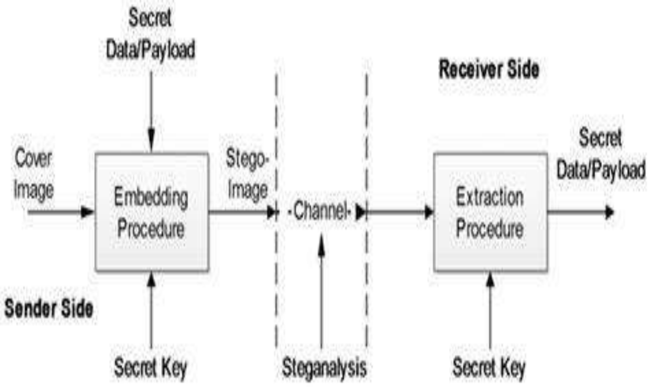


Fig 4.1. The key generation algorithm using DNA

Using zero-width Unicode characters (such as zero-width space, zero-width non-joiner, and zero-width joiner) to insert hidden messages within ordinary text is the focus of this project. This technique is called Zero Steganography[8]. Because these characters are invisible to the human eye, confidential information can be kept in plain view without changing the text's appearance.

The objective is to use zero-width characters to encode and decode concealed messages in an effective and safe manner. While accurately recovering the embedded message, the system must guarantee that the cover text stays intelligible and visually unaltered. The technique should also have a high embedding capacity, be impervious to casual scrutiny, and possibly offer encryption for further protection.

V. KEY GENERATION

Data security studies frequently employ cryptography particularly key creation. [3]The suggested approach uses unique biological characteristics and a pseudo-random generator to generate a novel key generator. A random number generator was developed in another investigation using fingerprint data. Additionally, it was proposed to use DNA to create and maintain random keys for One-Time Pad (OTP) encryption[2]. The solution was rated as having high security and usability. [1]In a publication, a novel steganographic technique for safe data transfer was created by fusing image steganography with secret key cryptography[14].

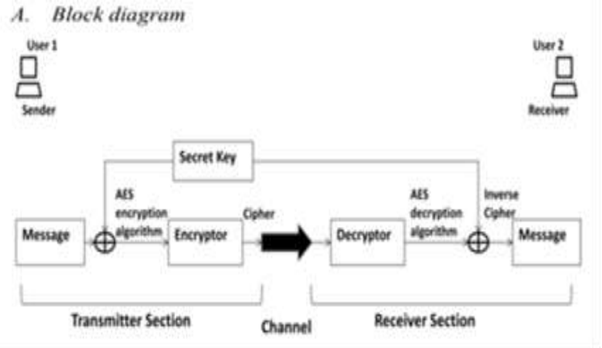
Symmetric Keys

Symmetric keys are typically used to encrypt and decrypt data. Like physical keys, they work to safely "lock" away information (i.e., encrypt it) so that only the key holder may "unlock" (i.e., decrypt it)[8]. For encryption and decryption, the same key is utilized, hence the word "symmetric."[2]

Keeping symmetric keys hidden, long, and random is necessary for them to be deemed secure, or "strong." An attacker, even if they know the encryption algorithm that was employed, cannot decipher the data without this secret key. Not even a very powerful computer that can attempt millions of key guesses per second can "brute force" (guess) a strong key and a high-quality symmetric encryption algorithm in an acceptable length of time.

Asymmetric Keys

Frequently, asymmetric keys are found in pairs, each of which is made up of a mathematically connected "public key" and "private key." The public key is meant to be shared with the public, but the private key needs to be kept confidential. These keys enable "public key cryptography"[2].



Everyone can encrypt data using the public key, but due to the characteristics of asymmetric keys, only the owner of the private key can decrypt or decode it. Since all they need is your public key, sending someone a private message is advantageous[7].

The benefit of sending someone a private message is that they only require your public key.

Asymmetric keys can also be used to verify the authenticity of a message. Using a device known as a "hash function," the message is first compressed to form a "digital signature," and the resulting "fingerprint" is then encrypted using the private key. In order to verify that this signature yields the same result as hashing the message themselves, anyone can then quickly and easily decode it using the sender's public key; if not, the owner of the corresponding personal key can sign it.

VI. ALGORITHM

As seen in the below figure, the suggested method uses an encrypt, decrypt, or secret key at the transmitter and receiver sections over a network channel. User 1 sends a cipher-based message to the receiver part via the channel by encrypting the transmitter component. By decrypting the cipher into the inverse cipher, User 2 is able to obtain the original message.

The system makes use of the secret key. The user can access the message across the channel.Start the input by entering the age. Applying the supplied messages encryption method (AES)[6]. Kowtowing serves as a medium for an encrypted message.With the AES decryption technique, the original message can be recovered.

Key creation for steganography-free algorithms often involves leveraging existing cryptographic techniques to secure the data before embedding it within a cover medium. This often involves utilizing encryption algorithms such as AES or RSA to secure the confidential communication, and subsequently, maybe applying a distinct steganographic technique to conceal the encrypted information within a more extensive file or medium.

AES Encryption Algorithm

128 bits of a plaintext block will be considered as 16 bytes in AES as it uses bytes for all of its operations instead of bits[6], and these 16 bytes are set up in 4 rows and 4 columns for matrix processing[2].

Figure4.1: Transfer secret key between encrypt to decrypt

It adds 128 bit input message.
• The four operations shift rows, mix columns, add round key, and s-box are carried out in a sequential fashion[2].
• Mix columns were not operated in the previous round.
• The encrypted message or 128 bit cipher is acquired in the final round, or the tenth round.

AES Decryption Algorithm

This AES decryption algorithm uses the same secret key to reverse the encryption process and transform ciphertext back into its original plaintext[6].
• A 128-bit cipher are added.
• Inverse shift rows, inverse box, inverse mix columns, and inverse add round key are the four operations that are carried out sequentially.
• At the final round the mix columns operation is not carried out on the key schedule from k10, e is equal to k0, d upto k0, e is equal to k10[2].
• In the final round or the tenth round the starting message or 128-bit inverse cipher is obtained[2].

VII. EXISTING SYSTEM

The research presented several noteworthy contributions in enhancing the security and efficiency of the Crypto-Stego method for image confidentiality[7].

Direct Implementation on Color Images: Instead of converting color images into grayscale, the proposed method directly applied the security mechanism to the original color images. This approach ensured the preservation of visual information while maintaining security measures.

Elimination of Separate Key Distribution Mechanism: The Crypto-Stego method eliminated the need for a separate key distribution mechanism during decryption. [6]By doing away with the need for the sender and recipient to exchange keys during the encryption and decryption process.

Parallel-Processing Approach: A parallel-processing strategy was used in the study to improve execution time and effectiveness. By effectively utilizing system resources, multiple tasks were executed simultaneously, resulting in improved overall performance.

Extensive Experimental Validation: The effectiveness of the proposed Crypto-Stego method was rigorously validated through extensive experiments[4]. To assess the scheme, a range of RGB photographs with varying sizes and resolutions were used[7]. Strong scores in the Structural Similarity (SSIM) index showed that the approach was effective in preserving picture confidentiality[12].

The steganography systems, secret data is embedded within digital media such as images, audio files, or videos by altering the least significant bits (LSBs) of pixel or sound data[7]. These systems rely on minor modifications that are usually imperceptible to human senses but can still be detected by advanced steganalysis tools or result in degradation of the original media. While effective, these methods are not ideal for text-based communication, where any change to the content or structure may be more noticeable.

[14]Text-based steganography has also been explored in various forms, including methods like whitespace manipulation, font change encoding, and misspelling-based hiding. However, many of these methods are detectable by spell-checkers or formatting tools and can be easily disrupted when the text is copied, reformatted, or passed through text filters.

The results demonstrated the efficacy of the method in maintaining image confidentiality, as indicated by high scores in the Structural Similarity (SSIM) index. It was confirmed by the low Mean Squared Error (MSE) statistics that hostile people could not identify the stego data in the cover image[7]. The suggested approach was found to be effective, as evidenced by the negligible changes in the pixel intensity histogram[4]. The study also highlighted the average efficiency of 77% achieved through parallel processing, along with a 1.5 times speed-up factor, providing additional evidence of the method's effectiveness in ensuring image confidentiality.
Hiding messages is not new. Before the advent of the internet, messages might be concealed using invisible ink, delicate paper creases, Morse code signals sewn into garments or even messages tattooed beneath messengers' hair.

VIII. CONCLUSION

It presents an innovative approach that utilizes a combination of algorithms for simultaneous encryption and decryption processes, supplemented by steganography to enhance security. This steganography-free employed are not only for security purpose but also flexible and user-friendly. Steganography-free is applicable in various domains, including private companies, government organizations, aeronautical agencies, research and development organizations, and intelligence agencies. [10]Steganography-free approach provides an advanced level of data protection and confidentiality, benefit diverse sectors and ensuring secure communication and information exchange. From ancient methods of concealing messages in wax tablets to modern digital techniques embedded within multimedia files, steganography has evolved to meet the changing demands of covert communication.

REFRENCES

[1] Zhella Anne Nisperos, Bobby Gerardo, Alexander Hernandez, "Key Generation for Zero Steganography Using DNA Sequences", 2020, International Conference on Electronics, Computers and Artificial Intelligence (ECAI).

[2] M.Natheera Banu, "FPGA Based Hardware Implementation of Encryption Algorithm", IJEAT,2014.

[3] Paweł Okal, "Computer Simulation of Percolation in a Two-dimensional Square Network", NAP, 2020.

[4] Liliang Zhang , Dejian Huang, "Novel High-Throughput Assay for Antioxidant Capacity against Superoxide Anion" 2009.

[5] Jiyun Zhou , Qin Lu , Ruifeng Xu, Lin Gui, and Hongpeng Wang, "EL_LSTM: Prediction of DNA-Binding Residue from Protein Sequence by Combining Long Short-Term Memory and Ensemble Learning", IEEE, 2020.

[6] DIVYA SHARMA, CHANDER PRABHA, MD MEHEDI HASSAN, "Securing X-Ray Images Into Cover Images Using Hybrid EBS Steganography With Five-Layer Cryptography", IEEE, 2024.

[7] SAHAR A. EL-RAHMAN, AHMED E. MANSOUR, LEILA JAMEL, "C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC", IEEE Explore, 2025.

[8] D. Bai, X. L. Chen, and M. Tian, "A satellite communication zero steganography algorithm," Multimed. Tools Appl., 2017.

[9] S. M. Hussain and H. Al-bahadili, "A DNA-Based Cryptographic Key Generation Algorithm," Int'l Conf. Secur. Manag., 2016.

[10] O. A. Al-Harbi, W. E. Alahmadi, and A. O. Aljahdali, "Security analysis of DNA based steganography techniques," SN Appl. Sci., 2020.

[11] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," Opt. Lasers Eng., 2014.

[12] Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," Soft Comput., 2019.

[13] X. Duan, H. Song, C. Qin, and M. K. Khan, "Coverless steganography for digital images based on a generative model," Comput. Mater. Contin., 2018.

[14] Malathi Pa*, Manoaj Ma,Manoj Ra, Vaikunth Raghavana,Vinodhini R Ea, "Highly Improved DNA Based Steganography", 2017.