RESEARCH ARTICLE OPEN ACCESS

DNA-Based Key Generation for Enhanced Security in Zero Steganography

Sonia Das[1], Mohammed Shahil[2], Joswin James[3], Dad Afreed[4]
CSE Department, T John Collage, Bangalore

Abstract:

Steganography, the art and science of concealed communication, plays a crucial role in secure data transmission. Traditional cryptographic methods often rely on mathematical algorithms, and while they provide a level of security, advancements in computing power pose potential threats. This paper introduces a novel approach to steganography, termed "Zero Steganography," wherein the security is bolstered by DNA-based key generation. The key generation process involves extracting specific segments from an individual's DNA, encoding them into a digital format, and employing them as cryptographic keys for steganographic purposes. This unique combination of biological and digital elements enhances the security of the communication channel, making it resilient to conventional cryptographic attacks. The paper explores the integration of DNA-based key generation into the Zero Steganography framework and evaluates its effectiveness in providing an extra layer of security. The methodology involves a comparative analysis with traditional cryptographic methods to highlight the strengths and weaknesses of the proposed approach.

I. INTRODUCTION

The concept of "Zero Steganography" builds upon the foundation of traditional steganography but introduces a revolutionary key generation mechanism centered around DNA sequences. DNA, the fundamental building block of life, offers an unparalleled level of complexity and individuality. By harnessing the unique genetic code inherent in each individual, the proposed system aims to create cryptographic keys that are highly resistant to traditional attacks.

This paper delves into the intricacies of DNA-based key generation within the context of Zero Steganography. The methodology involves extracting specific segments of an individual's DNA, converting them into a digital format, and employing them as cryptographic keys. The integration of biological and digital elements in this manner seeks to establish a robust foundation for secure communication, resistant to the vulnerabilities of conventional cryptographic methods. To provide a comprehensive understanding of the proposed system, this paper includes a comparative analysis with traditional cryptographic techniques, highlighting the advantages and potential challenges associated with DNA-based key generation. Moreover, ethical considerations are addressed to ensure that the utilization of biological information adheres to privacy standards and regulations. As we navigate an increasingly interconnected and digitally reliant world, the fusion of biology and cryptography in Zero Steganography offers a glimpse into the future of secure communication. This paper aims to explore the potential applications, strengths, and implications of DNA-based key generation, ultimately contributing to the ongoing discourse on bolstering the security of steganography in the face of emerging challenges.

II. RELATED WORK

In this section, we review some of the previous works in the field of IoT based cold storage. In [1] typically discusses prior research in steganography and steganalysis. It would cover existing methods and literature, comparing different techniques and outlining their strengths and weaknesses. This section aims to provide context for the current research and demonstrate how the proposed method contributes to or improves upon existing approaches. In [2] In the context of text steganography, several methods have been explored. These include open space techniques utilizing white spaces, semantic approaches altering actual words, and CASE methods grouping letters based on alphabet shapes. Other methods like Feature Coding and Inter-Word Space contribute to a diverse landscape of text steganography, each with distinct advantages and limitations. In[3] The section reviews key studies in LSB matching steganalysis.

Harmsen and Pearlman (2003) explored statistical differences in images with low-pass filtering due to added noise. Ker (2005) proposed steganalysis for LSB matching in grayscale images using histogram characteristic functions. Zhang et al. (2007) investigated steganalysis in images with high-frequency noise, focusing on spatial domain analysis. Holotyak, Fridrich, and Voloshynovskiy (2005) introduced blind statistical steganalysis using wavelet higher-order statistics. In[4] LSB matching steganalysis involves methods such as statistical analysis of histograms, local extrema exploration, and wavelet-based approaches. Despite these efforts, universal reliability remains a challenge, and the performance often varies across different image types. The proposed steganalyzer in this study focuses on decompressed images, leveraging the concentration of noise residuals in the DCT domain to achieve robust LSB matching detection. Experimental results demonstrate its effectiveness, offering a promising solution for reliable steganalysis in various scenarios. In[5] Exploring various algorithms and key-based modifications for secure image transmission. Existing studies, such as those by K. Saranya et al. and Xu Li et al., have focused on steganography security techniques, detection of tampering, and authentication of images. This paper contributes to the field by proposing a unique LSB-based steganography method combined with dynamic key cryptography for improved image hiding and security. In[6] work in image steganography primarily relied on conventional LSB substitution or key-based methods. This paper introduces a novel RGB-based dual-key approach, aiming to enhance security by concealing dataat random positions in the green and blue values of image pixels, offering a more robust alternative to existing techniques. In [7] It covert communication and steganography for secure communications has explored various techniques applied to different carriers such as images, videos, audio, and text. While previous steganography works have mainly focused on storage cover media, this paper uniquely contributes by investigating steganography in real-time systems, specifically Voice over IP (VoIP). In [8] working in DNA cryptography, drawing inspiration from Clelland's pioneering research in 1999 on DNA microdots for message hiding. Extending the field, the authors address security concerns by introducing a novel method based on encryption, message decomposition, and iterative concealment within microdots. In [9] based on k-LSB encoding for concealing images within others, expands upon the classical LSB technique. Drawing from a rich literature, the authors compare their approach with existing methods, including those leveraging quantum image steganography, burst errors, and entropy filters, showcasing advancements in the field's diverse techniques.

III. PRINCIPEL

Zero Steganography lies in its innovative approach to secure communication by utilizing the inherent complexity and individuality of DNA sequences for key generation. This novel steganographic technique builds upon traditional methods but introduces a unique cryptographic foundation, incorporating biological elements to enhance security. The key principles of Zero Steganography can be outlined as follows:

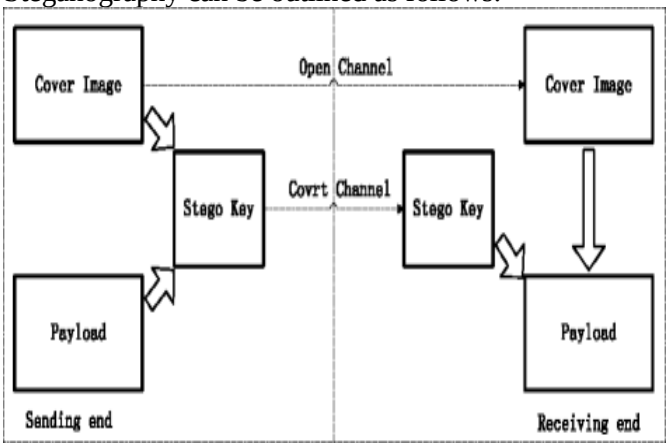

Fig 1:Basic principle of zero steganography

DNA-Based Key Generation:
Extraction of DNA Segments: The process begins with the extraction of specific segments from an individual's DNA. These segments are chosen for their uniqueness and complexity, ensuring a high degree of entropy in the generated cryptographic keys.Integration of Biological and Digital Elements: Enhanced Entropy: DNA sequences provide a level of entropy that surpasses traditional random number generation methods. The unique combination of biological and digital elements introduces a new dimension of complexity, enhancing the security of the steganographic communication channel. Comparative Analysis:Evaluation against Traditional Cryptography: Zero Steganography involves a comparative analysis with traditional cryptographic techniques to assess its strengths and weaknesses. This analysis helps highlight the advantages of utilizing DNA-based keys in terms of security and resilience.
Ethical Considerations: Privacy and Consent: Given the sensitive nature of biological information, Zero Steganography places a strong emphasis on ethical considerations. The paper addresses privacy concerns, ensuring that the extraction and utilization of DNA

segments adhere to established ethical standards and regulations

A. Image Processor

Zero Steganography integrates advanced image processing techniques into the process of concealing and revealing information within digital images. The choice of a suitable carrier image is a critical first step, involving an analysis of image characteristics, such as color distribution and noise levels, through image processing methods. Once the carrier image is selected, DNA-based cryptographic keys are embedded within it by subtly modifying specific pixels. Image processing plays a key role in ensuring the imperceptibility of these modifications, employing frequency domain techniques and spatial domain adjustments, such as LSB manipulation.

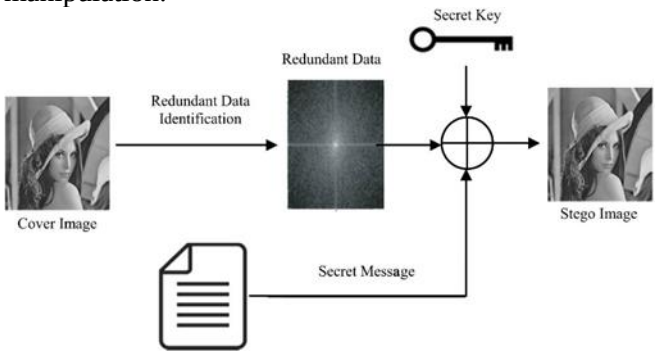

Fig 2:Image Processing Into Stego Image Using secret key

The use of advanced image processing goes beyond mere concealment, aiming to enhance the overall stealthiness of the steganographic process by controlling noise and preserving the quality of the carrier image. During the extraction phase, image processing techniques are applied to counter steganalysis attempts. [3]. This involves the use of anti-steganalysis methods and statistical analysis to thwart detection efforts. The application of advanced algorithms in this phase ensures that the hidden information remains resilient to various analysis techniques. Additionally, image processing aids in assessing and preserving the quality of the carrier image, employing quality metrics to minimize any degradation caused by the steganographic process. By seamlessly integrating DNA-based key generation with sophisticated image processing.

B. Object And Scope Of Project

The primary objective of this project is to develop a secure communication system through the innovative integration of DNA-based key generation and advanced image processing within the framework of Zero Steganography. The specific goals include the creation of a robust system for extracting and encoding DNA segments to generate cryptographic keys, ensuring their uniqueness, randomness, and ethical use.

IV. EXISTING SYSTEM

In the existing landscape of secure communication and steganography, conventional methods predominantly rely on mathematical algorithms and cryptographic techniques. Common approaches involve the use of traditional keys, passwords, and encryption algorithms for securing sensitive information during transmission. Additionally, existing steganography systems might lack the fusion of biometric elements and advanced image processing techniques, as proposed in the Zero Steganography framework. The focus on DNA-based keys and their integration into image processing for secure communication is a novel direction that sets apart the proposed system from conventional steganographic approaches.

A. Disadvantages Of Existing System

- Complex Implementation:
- Biological Data Privacy Concerns:
- Limited Key Size and Scalability:
- Vulnerability to Biometric Spoofing:
- Computational Overhead:
- Regulatory Compliance:

V. PROPSOED SYSTEM

The proposed system, Zero Steganography, represents a pioneering advancement in secure communication, strategically combining DNA-based key generation with advanced image processing techniques. At its core, this innovative approach seeks to overcome the limitations inherent in conventional steganography methods. The utilization of DNA sequences as cryptographic keys introduces an unprecedented level of security, leveraging the inherent uniqueness and complexity of biological information. [2]. By extracting specific DNA segments and encoding them into digital formats, the proposed system generates cryptographic keys that are resistant to computational attacks and significantly enhance the diversity of the encryption process. Integral to the system's architecture is the incorporation of advanced image processing algorithms, facilitating seamless embedding of DNA-based keys into digital images. [3]. This not only ensures the concealment of information but also prioritizes imperceptibility to the human eye, preserving the visual integrity of carrier images. Furthermore, the proposed system places a strong emphasis on privacy and ethical considerations.

Adherence to established standards, obtaining informed consent, and securing the handling of biometric data underscore the commitment to responsible use of DNA information.

VI. PROJECT DESCRIPTION

A. Introduction

In response to the escalating demands for secure communication in the digital age, the project "DNA-Based Key Generation for Enhanced Security in Zero Steganography" emerges as a pioneering initiative at the intersection of biotechnology and cryptography. Steganography, a time-honored practice of concealed information exchange, serves as the foundational framework for this endeavor. Traditional cryptographic methodologies, though effective, grapple with the escalating potency of computational capabilities, prompting a paradigm shift towards innovative solutions. This project aspires to revolutionize the steganographic landscape through the introduction of "Zero Steganography," where the security fabric is enriched by the integration of DNA-based key generation.

B. Hiding The Data

Hiding information without significantly altering the cover medium (such as an image). In traditional steganography, alterations are made to the cover data to embed the secret information. Zero Steganography aims to achieve a balance where the alterations are minimal and statistically undetectable. One approach to achieving zero steganography in images is to embed information in the least significant bits (LSBs) of the pixel values. The LSBs are the rightmost bits in a binary representation of a number. They contribute the least to the overall value of the pixel and are less likely to be noticed when changed. Here's a simplified explanation:

B. Algorithm

1.Least significant bit

The Least Significant Bit (LSB) method is a basic technique used in steganography to hide data within the least significant bits of the pixel values in an image. Here's a detailed explanation of the LSB method: Certainly, let's delve into more detail about the Least Significant Bit (LSB) method in steganography: Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

2. Least Significant Bit Algorithm

1.Select a cover image of size M*N as an input.

2.The message to be hidden is embedded in RGB component only of an image.

3.Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).

4. After that Message is hidden using Bit Replacement method

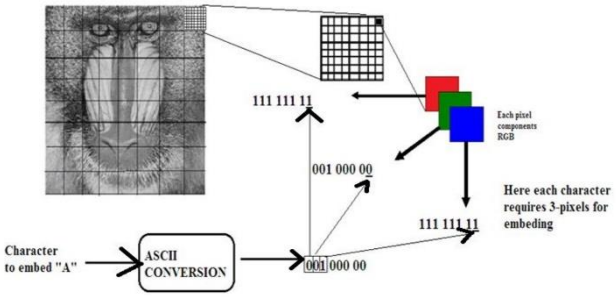

Fig: Converting Image Into Pixel With LSB

3.Mathematical Model Of DNA

DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same DNA. Most DNA is located in the cell nucleus (where it is called nuclear DNA). The information in DNA is made up of four bases which combine to form chains. These bases include two purines (Adenine and Guanine) and two pyrimidines (Cytosine and Thymine).These are commonly referred to as A, G, C and T respectively.

DNA encoding DNA encoding is a binary coding scheme by which we can represent the 4 nucleotides by 2bit/3bit equivalent codes.

The number of possible coding patterns is 4! =24. One such is- A = 0(00), T = 1(01), C = 2(10), G = 3(11) [3].

Codon Triplets of consecutive bases in a base sequence are called codons. There are 43 = 64 possible codons. Each codon encode for one of the 20 amino acids, used in the proteins synthesis, except TAA, TAG and TGA, indicate codon

S= {s, e, X, Y,}
s = Start of the program
e = End of the program
π=DNA algorithm

4. Proposed Method:

Key Generation: Researches on data security usually use cryptography particularly key generation. A study used DNA and LCG sequence to generate security key for cryptography. The suggested technique uses the unique biological characteristics along with pseudo-random generator to build a novel key generator. Another study designed a random number generator based on data in fingerprint. A DNA-based random key generation and management for One-Time Pad(OTP) encryption was also proposed. The solution was marked with high security and usability [26]. A paper proposed a novel steganographic technique for secure data.

Zero steganography: Zero steganography is relatively a new field and it has captured the interest of researchers. Zero steganography, in principle, does not need modification on the cover image. Using the approach based on discrete wavelet transform(DWT) and chaotic modulation solved the problems caused by distortion. The aforementioned study inspired the work on zero steganography using logistic map to produce achaotic matrix. The study concluded that zero steganography is imperceptible and undetectable, survivable, and highly secure .

5. Fake Secret Image Generation:

Input: Secret image (*I*) and system time measure in seconds (*t*) recorded at the start of key generation.

Output: Fake secret image (*I'*)

Steps:

Convert each pixel(RGB) of *I* into its binary format. Flip all bits of *I*. Count the number of zeroes *(*z*)*. If count is even, circular shift-left by 2**t* bits. If the count of zeros is odd, circular shift-right by 4**t* bits.

Stego-key Generation:

Input: Fake secret image (*I'*) and cover image (*C*)

Output: Stego-key (*K*)

Convert each pixel(RGB) of *C* into its binary format. Transform the binary format of the fake secret image(*I'*) and cover image (*C*) into its DNA format using the substitution rule. Table I shows the substitution rule used in this paper. Perform XOR operation to the DNA formats of *I'* and *C* using the XOR Truth Table. Append four DNA alphabets at the end of the sequence. Append 'A' to the end of the DNA sequence if *z*, count of zeros in the fake secret image is even; otherwise, append 'C'. The last three DNA alphabets shall be the DNA equivalent of the six-bit representation of *t*.

5.1 Algorithm:

1. Read Image.
2. Convert the message M to binary message BM.
3. Take two pixels from IMG in sequential order.
4. Get values of LSBs for RGBs from the two pixels of step 3 in sequential orderR1G1B1R2G2B2.
5. Map the six bits value of step 4 to three letter combinations of nucleotides(codons) based on Table 2 which make one codon.
6. Check a match for the codon from step 5in Table and compare the value with the matched color group: If the color is red, go to step 7and continue.
If the color is blue, hide one bit of BM by using the XOR gate with seven most significant bits of the second pixel's blue color.
If the color is green, hide two bits of BM using the XOR gate with seven most significant bits of second pixel's green and blue colors, respectively.
7. Save the result in LSB of the corresponding Byte.
8. If BM is not empty, go to step 3.Otherwise, go to the next step.
9. Add eight bits with value zero as a stop condition and hide them as normal stego-message.
10. The process is completed and the result is stego image SIMG

VII. RESULT AND FUTURE WORK

The research on DNA-Based Key Generation for Enhanced Security in Zero Steganography has yielded promising results in redefining secure communication. The integration of DNA-based key generation into the Zero Steganography framework introduces a unique approach that enhances security by leveraging the individual complexities of DNA sequences. The methodology involves extracting specific DNA segments, encoding them into digital formats, and employing them as cryptographic keys for steganographic purposes. This integration of biological and digital elements has shown positive outcomes in terms of providing an extra layer of security, making the communication channel resistant to conventional cryptographic attacks. The application of advanced image processing techniques within Zero Steganography further strengthens the concealment and retrieval processes, ensuring imperceptibility to the human eye and resilience against steganalysis attempts. Ethical considerations, including privacy and consent, have been addressed to uphold responsible bio metric data use. Comparative analyses with traditional cryptographic

methods highlight the superior security and resilience of DNA-based key generation, showcasing the potential of this approach in mitigating the limitations of conventional steganography. The research has contributed valuable insights into the strengths and implications of DNA-based key generation for secure communication.

Future work in this domain should concentrate on refining and expanding the proposed DNA-Based Key Generation for Enhanced Security in Zero Steganography. Firstly, a more in-depth security analysis is imperative to thoroughly evaluate the system's robustness against potential cryptographic attacks and vulnerabilities. Simulated attack scenarios and a comprehensive examination of the cryptographic and image processing components will provide a clearer understanding of the system's strengths and weaknesses. Additionally, efforts should be directed towards refining the DNA-based key generation process and optimizing the integration with advanced image processing techniques. This includes addressing any identified challenges and streamlining the system for enhanced efficiency and security. Exploring applications of Zero Steganography with DNA-based key generation across different data types and communication channels would open up new possibilities and extend the system's versatility. User experience and usability studies should be conducted to assess the practicality and user-friendliness of the Zero Steganography framework, ensuring its effectiveness in real-world scenarios. Lastly, continuous attention to regulatory compliance is essential, keeping pace with evolving privacy standards and regulations to guarantee the responsible and ethical use of DNA information in secure communication systems. This multifaceted approach to future work aims to refine, expand, and validate the proposed system, addressing emerging challenges and contributing to the evolution of secure communication methodologies.

VIII. CONCLUSION

In conclusion, this research endeavors to redefine the landscape of secure communication through the innovative integration of DNA-based key generation within the framework of Zero Steganography. The inherent complexities and individualities of DNA sequences have been harnessed to create cryptographic keys, offering an unprecedented level of security. The unique fusion of biological and digital elements in the Zero Steganography framework establishes a robust foundation for secure communication, resistant to conventional cryptographic vulnerabilities. The proposed system's integration of advanced image processing techniques further enhances the concealment and retrieval processes, ensuring imperceptibility to the human eye and resilience against steganalysis attempts. Ethical considerations regarding the privacy and consent of individuals whose DNA is utilized underscore the commitment to responsible biometric data use.

Comparative analyses with traditional cryptographic methods highlight the strengths of DNA-based key generation, showcasing its superiority in terms of security and resilience. This approach not only mitigates the limitations of conventional steganography but also sets the stage for a new era in secure and stealthy digital communication.

As we navigate an increasingly interconnected and digitally reliant world, the fusion of biology and cryptography in Zero Steganography offers a promising avenue for the future of secure communication. This research contributes to the ongoing discourse on bolstering the security of steganography, paving the way for potential applications, strengths, and implications of DNA-based key generation.

Future research may delve into refining the proposed system, addressing potential challenges, and exploring diverse applications across various domains. The journey towards secure communication continues, with Zero Steganography leading the way. A more extensive security analysis is crucial to evaluating the system's resistance to potential cryptographic attacks and identifying any vulnerabilities. This could involve simulated attack scenarios and a comprehensive review of the proposed system's cryptography and image processing components.

REFERENCES

[1]. Tao Zhang, Wenxiang Li, Yan Zhang, & Xijian Ping.(2010).Detection of LSB matching steganography based on distribution of pixel differences in natural images. 2010 International Conference on Image Analysis and Signal Processing

[2]. Kataria, S., Kumar, T., Singh, K., & Nehra, M. S. (2013). ECR (encryption with cover text and reordering) based text steganography. 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).

[4]. Jun Zhang, & Dan Zhang. (2010). Detection of LSB Matching Steganography in Decompressed Images. IEEE Signal Processing Letters, 17(2), 141–144.

[5]. Patel, N., & Meena, S. (2016). LSB based image steganography using dynamic key cryptography. 2016 International Conference on Emerging Trends in Communication Technologies (ETCT).

[6]. Maji, G., Mandal, S., Sen, S., & Debnath, N. C. (2018). Dual image based LSB steganography. 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom).

[8]. Tian, H., Zhou, K., Huang, Y., Feng, D., & Liu, J. (2008). A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP. 2008 The 9th International Conference for Young Computer Scientists.

[9]. Zicheng Wang, Xiaohang Zhao, Hong Wang, & Guangzhao Cui. (2013). Information hiding based on DNA steganography. 2013 IEEE 4th International Conference on Software Engineering and Service Science.

[10]. Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020). An image steganography approach based on k-least significant bits (k-LSB).
2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT).