Advancements in Modern Steganography Techniques for Enhanced Data Security: A Comprehensive Review

Shresty Bohra
Computer Science Engineering
Pandit Deendayal Energy University
Gandhinagar, India
shresty73@gmail.com

Charmi Naik
Computer Science Engineering
Pandit Deendayal Energy University
Gandhinagar, India
charminaik27@gmail.com

Rashi Batra
Computer Science Engineering
Pandit Deendayal Energy University
Gandhinagar, India
rashibatra78@gmail.com

Kinshu Popat
Computer Science Engineering
Pandit Deendayal Energy University
Gandhinagar, India
kinshu.pce21@sot.pdpu.ac.in

Hargeet Kaur
Computer Science Engineering
Pandit Deendayal Energy University
Gandhinagar, India
hargeet.kaur13@gmail.com

***Abstract*—Information security has become a major concern in today's digital world with the rapid growth of the internet. To confront this challenge, various techniques like cryptography and steganography have developed in the fields of computer security for protecting sensitive data from unauthorized access. The review paper explores modern steganography techniques, providing valuable information about their applications in data security. It analyzes the emerging field of DNA-based steganography. The paper also examines the dynamic domain of audio steganography, focusing on the challenge of developing strong, high-capacity systems for secure communication. Additionally, it focuses on evaluation of digital image steganography methods.**

***Keywords*—DNA steganography, Image steganography, Audio steganography, Prisoners' problem, Cracking probability, SNR, Temporal Domain, Transform Domain, LSB, RGB, Discrete Cosine Transform, Stego-Image.**

I. Introduction

This research highlights on the growing interest in DNA-based steganography and its importance in enhancing data protection. There are various policies and protocols to secure patients' data, and its security and privacy is a main key issue that remains for EHR systems. In this paper, according to privacy and security, we discuss the basics of DNA steganography to protect the confidential data from cybercriminals and attackers in the field of communication and data security [1].

The properties of digital audio media are used against human auditory system limitations for hiding information within audio files in Audio Steganography. It is used in communications, such as telephone or video conference conversations, where the cover audio signal appears harmless. Also, embedding an information into a digital audio file in an imperceptible manner is a difficult task. It is the science of hiding confidential data in a digital audio file which enables the invisibility of hidden data. Varieties of techniques have been established from the last few years for embedding secret information in digital audio files. This paper presents basics of audio steganography and some audio steganography techniques for information hiding [2].

The paper contains various popular image steganography algorithms like LSB substitution [3] that provide information about their strengths and weaknesses. Image Steganography is a highly utilized field to secure data due to its prevalence on the internet. For example, we can easily hide confidential information binary code in image binary code , where some enable invisibility of hidden data [4].

The ultimate goal of this research is for secure communication. This review paper aims to gather the findings from these distinct steganography domains, providing a comprehensive understanding of their significance and future research challenges in order to secure and digital communication.

Fig. 1 explains a typical Steganographic system is described using the Prisoner's Problem [5] where two prisoners Rashi and Kinshu are making an escape plan. The warden, Charmi observes communication between the two and would put them in isolation if she finds them communicating secretly.

Thus, Rashi and Kinshu must communicate in such a manner that Charmi does not get to know their secret communication. So, they need to hide messages in the form that Charmi does not come to know of its very existence [6]. Steganalysis is the set of techniques by which it is possible to check for the existence of steganographic content in an object.

978-93-80544-51-9/24/©BVICAM, New Delhi, India

Charmi can check through steganalysis whether there is any communication between Rashi and Kinshu.

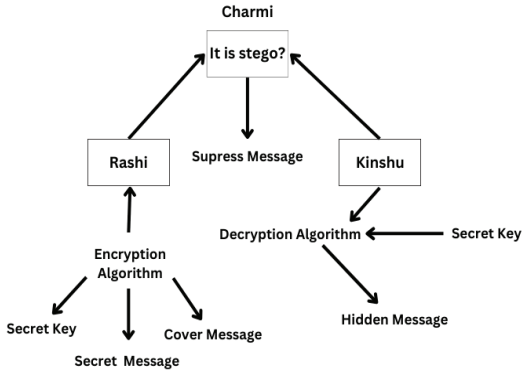

Fig. 1. Prisoners' Problem [5]

II. Literature Review

In this section of paper, we will discuss in brief about three types of steganography namely DNA, Image, Audio with its technique.

A. *DNA Steganography*

DNA based steganography has gained a lot of consideration and study over the time due to its huge storage capacity one gram of DNA can store 108 tera-bytes [7-8] and its computational abilities. DNA act as novel carrier for huge data and its security due to the following reasons

- DNA is made up of nucleotide sequences of Adenine (A), Cytosine (C), Guanine (G), and Thymine (T) [9-10] which are used for manipulating to encode the hidden data.
- It also supports complement base pairing of A with T and C with G which is also used to encode messages.
- There are amino acid codons which use triplets of nucleotide sequence to encode amino acids which are altered to encode messages [11].
- There is an inbuilt error correction option due to DNAs ability of self-correcting mechanism.
- Biological cover and biological invisibility are used to cover data and blend it with DNA sequences.

There are twelve algorithms [11] based on different criteria such as binary coding rules, use of encryption, data hiding and lastly whether they are blind or not. The evaluation focuses on factors like cracking probability, advantages, and disadvantages. The concept of cracking probability is used to measure the difficulty of the algorithm.

B. *Audio Steganography*

Audio steganography is a technique which conceals data within audio data. Various techniques used in audio steganography

- Temporal domain includes bit encoding and echo hiding.
- Transform domain includes methods like tone insertion, phase coding amplitude modification and spread spectrum; it leverages the auditory characteristics of humans and manipulates audio frequencies.
- Wavelet domain uses wavelet coefficients for data embedding [12].
- Encoder domain works by embedding data within audio codec parameters.

The evaluation process employs the signal to noise ratio (SNR) as a parameter to check the impact of data embedding on the audio signal quality.

A. *Image Steganography*

Image steganography involves hiding data using the visuals of an image. Image serves as a carrier for concealing messages.

They are represented as a grid of pixels [13] where each pixel is given numerical value. The most prominent color mode of digital images is RGB (Red, Green, Blue). There are 16 million possible color pallets [14] which highly helps in data concealing.

The popular formats used are GIF, JPEG, PNG. The latter two are more advanced as it provides lossy compression and advanced encryption

The few popular techniques of image steganography are:

- JPEG compression and Discrete Cosine Transform: In these DCT [15] is applied on JPEG compression to convert it into frequency domain.
- Wavelet transform domain techniques are used for discontinuous images such as medical and satellite images. It involves modifying wavelet coefficient to embed data.
- Spread spectrum techniques use the idea of covering images as noise and adding pseudo-noise as hidden data. The hidden data is not easily detectable by both observer and analyst.

III. Results and Discussion

The main principal idea is to use the Steganography technique for hiding the secret information and transmit hidden messages digitally without suspicion of unauthorized third parties. In Steganography public media files like audio, video, image are used and as time passes more secure techniques are used to secure data using DNA.

Hiding sensitive information using audio file, video file, image files and DNA give more security because it is not observable through the human eye. DNA Steganography is a new and emerging field of securing important data from hacking and transfer of undetectable secret data.

Using DNA Steganography, we can achieve high protection and powerful security to hide data in natural SPNs.

Another potential of the DNA Steganography for securing data is DNS' incredibly high capacity and computational power.

This paper intends to discuss the overview of DNA Steganography and some basic techniques to securing data using DNA in real-time. The main principal idea of DNA Steganography is to encrypt the secret data in the large number of DNA strands, so no third party can decode it.

Audio Steganography is also used as the DNA Steganography to hide the secret data but in Audio Steganography public song files are used to hide the secret data for securing it from hacking.

Audio Steganography is a methodology of transmitting hidden messages by modifying audio bits and audio signals in a cryptic manner, also before plaintext and stego text will have the same characteristics.

This paper highlights some techniques that are used in Audio Steganography for real-time and the most famous technique is LSB method. The main principal idea of Audio Steganography is to hide information in the audio file that is unidentical to the human ear and save data from third parties.

Image Steganography is also a Steganography technique that secures data. It transmits secret information using Image files without altering their visual appearance to the human eye. Image Steganography serves as a stealthy communication method, providing the means to communicate digitally without causing suspicion to unauthorized third parties.

In fig. 2 a simple process of Image Steganography is shown. In Image Steganography secret information is embedded into image files by altering the values of pixels or RGB value, which are chosen by an Encryption algorithm. The receiver of the image file with the hidden information should also know the Decryption algorithm to know which pixels they must select to extract the secret information.

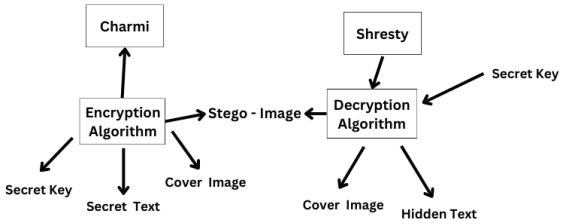

Fig. 2. Process of Image Steganography

A. DNA Steganography

a) Trends:

- Rapid Development in DNA Sequencing: DNA sequencing technologies have played an emerging role in the field of DNA steganography, which allows for more efficient encoding and decoding of hidden data in DNA strands.
- Security Purpose: DNA steganography serves various applications such as authentication, watermarking and secure communication.

b) Patterns:

- Integration with DNA Computing: Researchers in both DNA computing and DNA steganography seek to harness the potential of molecules, leading to multiple applications in information security.
- Diversity in Algorithms: There exist a wide variety of steganographic algorithms that focus on error correction and data hiding capacity.

c) Controversies:

- Legal and Ethical Concerns: Misuse of biotechnology has been one of the major concerns in DNA steganography. Data is concealed in DNA strands, which might be interpreted as a way to obscure potentially deleterious information.
- Effect on the Environment: DNA Steganography requires resources and processes related to genetic material, which results in environmental consequences. A major concern for most of the researchers is the impact of using DNA as a medium for data storage.

B. Audio Steganography

a) Trends:

- Enhanced Indistinguishable: Audio steganography focuses on enhancing the imperceptibility of hidden data. Various researches have been done to make the changes to audio signals virtually which are undetectable to human ears.
- Strength in the Real-world Environment: Audio Steganography resolves real world challenges to ensure that hidden data remains intact.

b) Patterns

- Diverse Embedding Techniques: Audio Steganography includes various techniques such as LSB, Spread Spectrum and phase coding.
- SNR Evaluation: Signal to Noise Ratio (SNR) is used as an evaluation metric. Various researchers evaluate the impact of data embedding in audio quality using SNR to recognize the trade-offs.

c) Controversies:

- Security and Privacy Concerns: Data Privacy and Security is one of the major concerns raised by Audio Steganography like other steganographic methods. If utilized for malicious purposes, it can easily convert communication thereby leading to illegal activities.
- False Positives in Detection: The efficacy of detection methods can be disputed producing false positives.

C. Image Steganography

a) Trends:

- Compliant Techniques: Image Steganography trends emphasizes on adoption of compliant techniques which astutely selects pixels for embedding. These methods

improve the trade-off between data capacity and perceptibility.

- Integration of Machine Learning: Machine learning is widely used in embedding and detection. Neural networks play a role in enhancing data concealment against detection.

b) Patterns:

- Exploiting Image Formats: Characteristics of common image formats like JPEG and PNG can be accomplished by steganographic techniques. These formats led to challenges such as lossy compression and encoding methods.
- Statistical Analysis: Image Steganography performs statistical analysis to determine the suitable pixel for data embedding ensuring data coherently blends into the image.

c) Controversies:

- Concealed messages: Compressed file might find difficulties in embedding the information. The major concerns in image Steganography are to hide the information without degrading the quality of file.

IV. Conclusion

DNA steganography, Audio steganography and Image steganography all three are powerful evolving techniques that plays a crucial role in hiding secret information without causing any suspicion.

After comparing all three steganography we can conclude that DNA steganography gives more security and can hide large amounts of data than Audio steganography and Image steganography.

V. Future Scopes

The main challenges in the future for image steganography are hiding data with high security in order to make it hard to find data against attackers with high capacity. Researchers are still working on this field but they have not completely achieved the outcomes.

DNA Steganography, an emerging field supports data transmission through untrusted channels. The main objective is to get secure from attacks like masquerade attack, brute force attack, ciphertext only attack, known plaintext attack and man-in-the-middle attack.

The process of extending research in image steganography has to be carried out to accomplish the task of high data embedding. It is done by manipulating two or more LSB without compromising the security.

References

[1] M. A. Farahat, A. Abdo and S. K. Kassim, “A Systematic Literature Review of DNA-Based Steganography Techniques: Research Trends, Data Sets, Methods, and Frameworks,” Digital Transformation Technology, vol. 224, pp. 495-505, 2022.

[2] P. P. Balgurgi and S. K. Jagtap, “Audio Steganography Used for Secure Data Transmission,” Proceedings of International Conference on Advances in Computing, vol. 174, pp. 699-706, 2013.

[3] S. Arivazhagan, W. Sylvia Lilly Jebarani, S. T. Veena and E. Amrutha, “Extraction of secrets from LSB stego images using various denoising methods,” Int. j. inf. tecnol., vol. 15, pp. 2107-2121, 2023.

[4] P. Akshita and P. P. Amritha, “Enhanced Security Layer for Hardening Image Steganography,” Congress on Intelligent Systems, vol. 111, pp. 753-765, 2022.

[5] G. J. Simmons, “The prisoners’ problem and the subliminal channel," Annual International Cryptology Conference, pp. 51-67, 1983.

[6] M. Kharrazi, H. T. Sencar and N. D. Memon, “Image Steganography: Concepts and Practice,” Polytechnic University, USA, 2004.

[7] B. Anam, K. Sakib, Md. A. Hossain and K. Dahal, “Review on the Advancements of DNA Cryptography,” enprint arXiv:1010.0186, 2010.

[8] L. Ceze, J. Nivala and K. Strauss, “Molecular digital data storage using DNA,” Nat Rev Genet, vol. 20, pp. 456–66, 2019.

[9] K. Gábor, “How to teach the history of cryptography and steganography,” Education Plus vol. 20, no. 2, pp. 13–23,2018.

[10] N. Nandy, D. Banerjee, and C. Pradhan, “Color image encryption using DNA based cryptography,” Int. j. inf. tecnol., vol. 13, pp. 533-540, September 2021.

[11] G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba, “Comparative Study for Various DNA Based Steganography Techniques with the Essential Conclusions about the Future Research,” 2016 11th International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, pp. 220-225, 2016.

[12] G. Swain, "Very high-capacity image steganography technique using quotient value differencing and LSB substitution," Arb. J. Sci. Eng., vol. 44, pp. 2995-3004, 2019.

[13] N. Cvejic and T. Seppanen,” A wavelet domain LSB insertion algorithm for high-capacity audio steganography,” Proceedings of 2002 IEEE 10th Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop., Pine Mountain, GA, USA, pp. 53-55, 2002.

[14] R. Roy, S. Changder, A. Sarkar and N. C Debnath, “Evaluating Image Steganography Techniques: Future Research Challenges,” 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Ho Chi Minh City, Vietnam, pp. 309-314, 2013.

[15] R. Patel, K. Lad and M. Patel,” Novel DCT and DST based video steganography algorithms over non-dynamic region in compressed domain: a comparative analysis”, Int. j. inf. tecnol., vol. 14, pp. 1649-1657, 2022.