ISSN: 2393-8048

International Advance Journal of Engineering, Science and Management (IAJESM)

Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.

SJIF Impact Factor =8.152, January-June 2025, Submitted in March 2025

Cyber Security & Data Privacy by Using Steganography & Cryptography Algorithm

Ms. Pooja H. Rane, Computer Science, Aakar College of Management for Women, Hingna, Nagpur, India
Mrs. Roshani K. Kakde, Computer Science Aakar Institute of Management & Research Studies, Hingna, Nagpur, India
E-mail: asoleroshni16@gmail.com

Abstract

Data security has become a primary prerequisite and need in day to day life. Today's most of the systems can be hacked and it generates very high risks to our confidential files inside the systems. There are various security reasons; also we use various methods to save as possible data like forms, text pictures, videos etc. Data security used to provide Cryptography and steganography but both of them has a problem. In Cryptography the main problem is the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. In Steganography problem the presence of hidden information is revealed or even suspected, the message is become known. By using good security techniques of accession control. We can resolve many security problems. In this paper describes Steganography, Encryption/Decryption Algorithm, Cryptography technique and different algorithm used by these techniques. Steganography based on technical and non-technical steganography and also categorized based on its domain. High security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. This paper describes comparative study using various algorithms.

Keywords: Cyber Security, Steganography, Encryption/Decryption Algorithm, Cryptography,

Introduction:

As the digital world continues to expand, the importance of cyber security and data privacy has grown significantly, affecting individuals, organizations, and governments. With the rise of cyber threats like data breaches, hacking, and identity theft, the protection of sensitive information has become more critical than ever. While traditional security measures are helpful, they often face challenges in providing strong protection without compromising usability [1]. Cryptography, which is the practice of using mathematics to encrypt and decrypt data, plays a key role in securing information. It transforms readable data (plaintext) into an unreadable format (ciphertext) to protect messages. The term "cryptography" is derived from the Greek words "kryptós," meaning "hidden," and "gràphin," meaning "writing," thus translating to "hidden writing".Steganography, on the other hand, is the art of concealing a secret message within an ordinary one, such as an image, video, or audio file, so that the presence of the message remains undetected. At the destination, the hidden message can be extracted. Together, cryptography and steganography offer powerful solutions for securing digital data. While steganography hides messages within seemingly harmless data to mask their presence, cryptography encrypts data to make it unreadable without the correct decryption key. This research aims to explore and combine advanced cryptographic and steganographic algorithms to enhance both cyber security and data privacy.

Literature Review:

In today's digital age, cyber security and data privacy have become critical issues [11]. With the increasing frequency of cyber-attacks and data breaches, safeguarding sensitive information has never been more vital. Steganography and cryptography are two essential techniques that help address these challenges [5]. While each technique serves a unique purpose, together they provide a powerful means of protecting data, ensuring secure communication, and preventing unauthorized access [4]. This literature review delves into the roles of steganography and cryptography in enhancing cyber security and data privacy, examining their development, key methods, and practical uses.

Cyber Security:

Cyber security involves protecting systems, networks, and programs from digital threats. Its main objective is to stop unauthorized access to sensitive information, systems, and applications. Data privacy, however, focuses on protecting personal or sensitive data from being misused or accessed without permission. In today's digital world, where personal and financial information is frequently shared and stored online, the need for strong security measures is more critical than ever. To ensure cyber security and data privacy, a variety of techniques have been developed, with steganography and cryptography being two of the most commonly used methods.

Steganography:

Steganography is the technique of hiding information within seemingly harmless content, like embedding a message in an image or audio file. This practice has existed for centuries, with early examples including secret messages hidden on messengers' bodies or concealed within artwork. In today's digital era, steganography has advanced significantly, utilizing the large storage capacities and powerful processing abilities of modern computers.

3.1 Stenographic Techniques

Steganography can be classified into different types, including:

- **Image-Based Steganography**: This approach hides messages within the pixel data of an image. Techniques like Least Significant Bit (LSB) insertion are often used, where the smallest bits of the pixels are modified to embed the hidden message, causing little to no visible change in the image.
- **Audio-Based Steganography**: This method hides data in audio files by making tiny adjustments to the sound that are not detectable to the human ear. Common techniques include phase encoding and echo hiding.
- **Text-Based Steganography**: In this technique, messages are concealed within text using methods such as character encoding or creating specific word patterns that remain unnoticed by casual readers.
- **Video-Based Steganography**: Similar to image and audio steganography, this method involves embedding data within video files, leveraging the large file sizes to hide messages effectively.

3.2 Applications of Steganography in Cyber Security

Steganography is especially valuable in situations where it is crucial to keep the existence of a message hidden. Some key uses include:

- **Covert Communication**: Enables secure communication in situations where encryption might draw unwanted attention, making it particularly useful for confidential intelligence communication.
- **Digital Watermarking**: Involves embedding hidden information, such as copyright or ownership details, within digital media to safeguard intellectual property.
- **File Integrity Verification**: This involves embedding checksums or digital signatures into files to verify that they haven't been tampered with during transmission or storage.

Cryptography:

Cryptography has a rich history, starting in ancient times when simple ciphers were used for military communication. Over the centuries, cryptographic methods have advanced from basic substitution ciphers to complex algorithms designed to secure data in today's digital world. The introduction of public-key cryptography in the 1970s was a game-changer, enabling secure communication over untrusted networks without the need for a shared secret key. Cryptography is the practice of studying secure communication techniques to prevent unauthorized access to private data, information, or messages [6]. It encompasses key areas of information security, including data confidentiality, integrity, and authentication (CIA), as well as non-repudiation, which are central to modern cryptographic practices [3].

2.2 Cryptographic Algorithms and Techniques

Cryptographic techniques can be generally divided into two main types:

- **Symmetric Cryptography**: This method uses the same key for both encrypting and decrypting data. Examples include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). AES, in particular, is widely used in both academic research and real-world applications due to its strong security and efficiency.
- **Asymmetric Cryptography (Public-Key Cryptography)**: This approach uses two keys: a public key for encrypting data and a private key for decrypting it. Popular algorithms in this category include RSA and Elliptic Curve Cryptography (ECC). Public-key cryptography is essential for secure online communication, such as in SSL/TLS protocols for securing web traffic.
- **Hashing**: This technique ensures data integrity by generating a fixed-size hash value based on input data, like SHA-256 or MD5. The hash acts as a unique identifier or fingerprint for the data. If the data is altered, the hash value will change, notifying the recipient of any potential tampering.

Combining Steganography and Cryptography for Enhanced Security

While steganography and cryptography are both effective on their own, combining them creates a more robust approach to securing data. These techniques complement each other in several ways:

- **Confidentiality and Integrity**: Cryptography ensures that the hidden message remains confidential and intact, while steganography adds an extra layer of concealment, making it more difficult for attackers to detect or alter the message.
- **Multilayered Security**: Cryptography can first encrypt the hidden message before it is embedded into a file using steganography. This creates two layers of protection, making it harder for attackers to break both the encryption and the steganographic method at once.
- **Secure Data Transmission**: Using both techniques together ensures secure communication over public networks, ensuring that the message stays both hidden and unreadable, even if intercepted.

Many studies and real-world applications have shown the advantages of using these techniques together. For example, researchers have developed methods for embedding encrypted messages within image files, where cryptographic algorithms protect the message and steganography conceals its presence. These approaches are commonly used in military and intelligence settings, where secure and covert communication is essential.Here is a diagram that illustrates how Cyber Security & Data Privacy, Steganography, and Cryptography algorithms are interconnected. It emphasizes how these techniques work together to strengthen data protection.

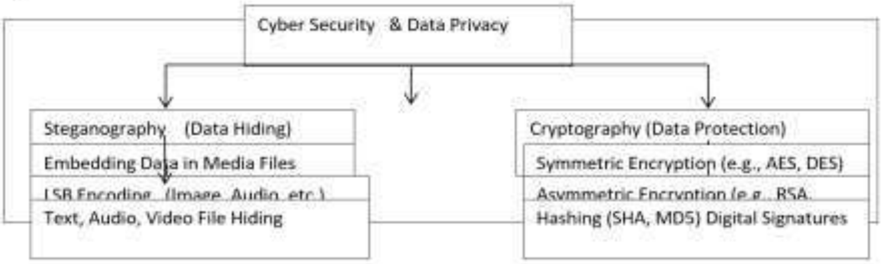
Cyber Security & Data Privacy
Steganography (Data Hiding)
Embedding Data in Media Files
LSB Encoding (Image, Audio, etc.)
Text, Audio, Video File Hiding
Cryptography (Data Protection)
Symmetric Encryption (e.g., AES, DES)
Asymmetric Encryption (e.g., RSA,
Hashing (SHA, MD5) Digital Signatures

Fig. 1 Relationship between Cyber Security & Data Privacy, Steganography, and Cryptography algorithms

By combining both steganography and cryptography, the diagram shows a comprehensive approach to secure communication and data protection. Steganography hides the message in plain sight, while cryptography ensures that even if intercepted, the message cannot be understood without the proper key.

Comparative Study:

Feature	Steganography	Cryptography
Primary Goal	Conceal the presence of the message	Make the message unreadable without the proper key
Visibility of Message	Hidden in plain sight within files or media	The message is visible but encrypted
Data Integrity	Does not have a built-in way to check if the data has been altered	Ensures data integrity through hashing or digital signatures
Capacity for Data	Limited by the size of the medium (e.g., an image or audio file)	Can encrypt large volumes of data
Resistance to Detection	Susceptible to techniques that detect hidden data (steganalysis)	Vulnerable to cryptanalysis and attacks targeting encryption keys
Computational Overhead	Low, particularly for simpler methods	High, especially with more complex encryption like asymmetric methods
Applications	Used for covert communication, digital watermarking, and hidden data storage	Applied in securing online transactions, protecting passwords, and ensuring data integrity

Conclusion:

In today's digital world, protecting sensitive information is more crucial than ever. Cyber security and data privacy are key areas that need strong solutions to guard against unauthorized access, theft, and tampering. The combination of steganography and cryptography provides a powerful and effective approach to securing data. Cryptography works by transforming data into an unreadable format, ensuring that only authorized parties can access it. It's widely used to secure communications, financial transactions, and personal information, proving its effectiveness. Cryptographic methods like AES, RSA, and hashing are essential for preventing unauthorized access and maintaining data integrity.

On the other hand, steganography offers an extra layer of security by concealing the very presence of the message. This technique is ideal for covert communication, where it's just as important to hide the existence of the message as it is to protect its content. When used together, cryptography and steganography form a strong, two-pronged security approach. Cryptography keeps the contents of the data secure, while steganography hides its existence. This combination makes it much harder for attackers to both detect and decode sensitive information. Despite their strengths, there are challenges, such as vulnerabilities to advanced cryptanalysis and steganalysis methods, as well as the computational cost of implementing complex cryptographic algorithms. However, ongoing improvements in both fields are leading to more efficient and secure solutions. As cyber threats continue to grow and evolve, the importance of steganography and cryptography will only increase. By integrating these techniques into modern security systems, individuals and organizations can significantly enhance the confidentiality, integrity, and authenticity of their data, offering better protection against emerging cyber risks.

References:

[1] Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications*, *7*(6).

[2] Pant, V. K., Prakash, J., & Asthana, A. (2015, October). Three step data security model for cloud computing based on RSA and steganography. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 490-494). IEEE.

[3]Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.
[4] ALRikabi, H. T. S., & Hazim, H. T. (2021). Enhanced data security of communication system using combined encryption and steganography. *iJIM*, *15*(16), 145.
[5] Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. *Computers and Electrical Engineering*, *102*, 108205.
[6] Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63-87.
[7] Hosam, O., & Ahmad, M. H. (2019). Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. *International Journal of Computational Science and Engineering*, *19*(2), 153-161.
[8] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Mohammed, K. I., Albahri, O. S., Albahri, A. S., & Alsalem, M. A. (2021). PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. *Multimedia tools and applications*, *80*, 14137-14161.
[9] El-Emam, N. N. (2007). Hiding a large amount of data with high security using steganography algorithm. *Journal of Computer Science*, *3*(4), 223-232.
[10] CHOUDHARY, S., & HUSAIN, S. (2023). Analysis of cryptography encryption for network security and image steganography technique. *algorithms*, *7*(10).
[11] Dubey, R., Saxena, A., & Gond, S. (2015). An innovative data security techniques using cryptography and steganographic techniques. *IJCSIT) International Journal of Computer Science and Information Technologies*, *6*(3), 2175-2182.