International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Steganography Hider System

[1]Nitesh Baranawal, [2]Herambh Sakpal, [3]Pranay Manoj, [4]Kaustabh Kadam, [5]Prof.Mohan Kumar
[1,2,3,4] Department of Data Engineering
[5]Professor, Department of Data Engineering Universal College Of Engineering, Kaman Road, India

Abstract- — The Steganography Hider System is a secure information-hiding solution designed to protect sensitive data by embedding it within digital images, making it imperceptible to unauthorized users. Unlike traditional encryption, which only disguises data, steganography conceals the very existence of the information, providing an additional layer of security. This system employs techniques such as Least Significant Bit (LSB) substitution, transform domain methods (e.g., DCT), or advanced neural network approaches to embed secret messages while maintaining the visual quality of the cover image. The proposed system allows users to securely hide and retrieve confidential information, ensuring data confidentiality, integrity, and robustness against common image processing operations such as compression, noise addition, and format conversion. This project serves as a practical demonstration of the importance of information security in today's digital communication era, providing a user-friendly interface that can be applied in various fields such as secure communications, copyright protection, and digital forensics.

Keywords- Steganography, Information Hiding, Data Security, Least Significant Bit (LSB), Digital Image Processing, Encryption, Cover Image, Secure Communication.

I. INTRODUCTION

Hider System is a technique used to hide secret information within digital media such as images, audio, or video files. It aims to protect sensitive data by concealing its existence rather than just encrypting it. This system uses algorithms like the Least Significant Bit (LSB) method to embed data without visibly altering the original file. Only the intended receiver with the correct key can extract the hidden message. It ensures data confidentiality, integrity, and secure communication over the internet. Unlike encryption, steganography doesn't attract attention since the carrier file looks unchanged. The system is useful in areas like military communication, digital watermarking, and copyright protection. By combining steganography with cryptography, it offers a double layer of security for information exchange. The Steganography Hider System is a specialized security solution designed to enhance the protection and confidentiality of digital information by embedding it within another medium, such as an image, in such a way that its existence remains completely hidden.

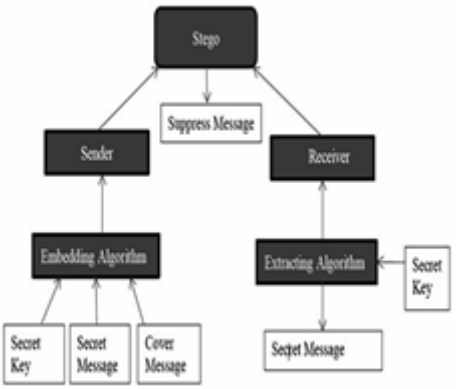

Figure 1.1 Steganography System Scenarios

II. APPLICATION OF STEGANOGRAPHY

Secure
Hide sensitive information (documents, credentials, classified data) inside images or audio files Send confidential messages through seemingly innocent media files

Intellection Property Protection:
Embed watermarks or ownership information in digital media
Track unauthorized distribution of copyrighted content

Copyright Protection:
Copy protection mechanisms that prevent data generally digital data, from being copied.

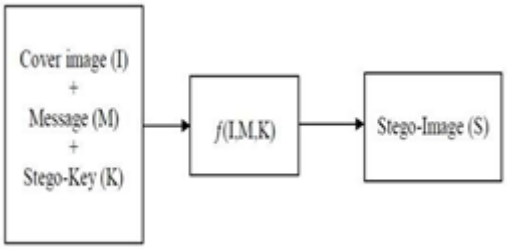

Figure 2.1 Simple Steganographic Model

III. SYSTEM MODULE

A Steganography Hider System typically involves storing, processing, and retrieving data related to hidden messages, media files, encryption details, and metadata.

Imange Steganalysis

The Steganography Hider System project aims to securely embed secret information into digital media such as images, audio, or video files. The project begins with requirement analysis in the first week to understand user needs, define system requirements, and determine technical feasibility. This is followed by system design in the second week, which includes designing the architecture, database schema, and embedding algorithm. Module development takes place in weeks three and four, involving coding of the steganography embedding and extraction modules, along with user interfaces. In weeks four and five, integration of all modules occurs, followed by rigorous testing to ensure the system works effectively without data loss or corruption. Deployment happens in week five to make the system operational. Finally, documentation is completed in weeks five and six, which includes user manuals, system diagrams, and project reports, ensuring clarity and maintainability for future enhancements.

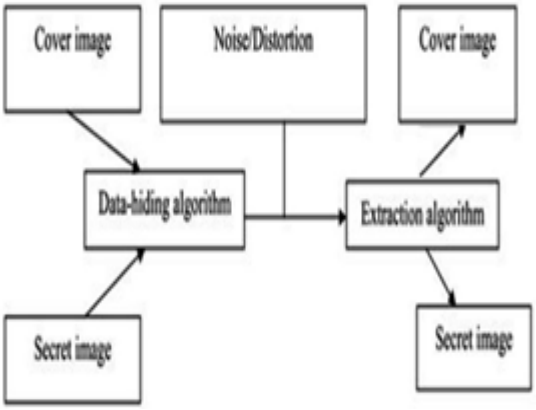

Figure 3.1Image Steganography System

IV. LITERATURE REVIEW

A literature survey was carried out to find various paper published in international journal such as IEEE, Springer, MDPI, Google Schoolar etc. related to tracing missing people using facial recognition to get the best algorithm for the same.

“RichardApau,MichaelAsante,FrimpongTwum,JamesBen HayfronAcquah,KwameOfosuhenPeasah” (Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review)[2024]

Information hiding in images has gained popularity. As image steganography gains releavance, techniques for detecting hidden messages have emerged. Statistical steganalysis mechanisms detect the presence of hidden secret messages in images, rendering images a prime target for cyber-attacks. The implication is that previously preferred traditional techniques such as LSB algorithms are receiving less attention.

“Heba Ragab, Hassan Shaban, Kareem Ahmed, Abd-Elmgied Ali” (Digital Image Steganography and Reversible Data Hiding: Algorithms, Applications and Recommendations)[2025]

Image steganography is a science that is interested in how to hide a secret message inside digital images in an imperceptible manner. An attacker listening to communication channel between the two communicating parties will never have any information about the existence of an embedded secret message. steganography, Reversible Data Hiding (RDH), watermarking, information hiding

“Abdullah Alenizi, Mohammad Sajid Mohammadi, Ahmad A. Al-Hajji, Arshiya Sajid Ansari” (A Review of Image Steganography Based on Multiple Hashing Algorithm) [2024]

Steganography is the method of concealing crucial data inside an innocent-looking file. Image steganography; multiple hashing algorithms; Hash-LSB approach; RSA algorithm; discrete cosine transform (DCT) algorithm; blowfish algorithm.

“Nagaraj V. Dharwadkar” (Unveiling the Hidden Pixels: A Comprehensive Exploration of Digital Image Steganography Schemes) [2025]

steganography, exploring a range of techniques, including Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Transform Domain methods, to evaluate their effectiveness

in real-world applications. Image steganography; cryptography; data compression; spatial domain; transform domain; dual approach.

"Isamadeen A. Khalifa, Salih Mustafa Saleem, Abdulkadir Sengur" (Multilayer Steganalysis in the Encryption Era:) [2026]

Steganography, Multilayer steganalysis, Cryptography, AEAD, AES–GCM.
We summarize the core principles and threat models and analyze symmetric, asymmetric, and hybrid encryp- tion (KEM+AEAD) in terms of its impact on the ciphertext entropy and payload efficiency. Moreover, we map the design space in terms of operational taxonomy that includes single-layer and onion-style pipelines, multi-carrier spreading, secret sharing with fragmentation, protocol- aware embedding, and a variety of different key-management techniques, some of which are post-quantum ready.

"Mazriha Akter Mohua" (A Review on the Integration of Cryptography and Steganography for Enhanced Information Security) [2025]

The rapid advancement in technology has revolutionized digital communications. This progress has also raised concerns regarding the security of transmitting sensitive data. The advancement of the Internet has made human beings more reliant on it, which on the other hand is vulnerable to attacks. Therefore, secure data communication is now becoming more challenging due to several specified and unspecified vulnerabilities in the information system. Cryptography, Steganography, Information Security, Data Hiding, Encryption, Decryption

"MAHADRISS, LAMIA BERRICHE, SIWAR REKIK" (Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions) [2025]

Internet of Things (IoT), steganography, covert communication, secure data transfer, resource-constrained devices. The Internet of Things (IoT) has raised significant security concerns, especially with regard to secure data transfer among resource-constrained devices. While effective, traditional encryption techniques are often computationally expensive and easily identifiable, making them unsuitable for many IoT applications. Steganography is an intriguing approach that allows hiding sensitive information within seemingly ordinary data, preventing unauthorized parties from detecting and accessing it.

"Javier Guaña-Moya, Yolanda Borja López, Gutiérrez Constante, Paulina Jaramillo Flores" (Information security vulnerabilities using steganography as the art of hiding information) [2024]

Steganography is the art of hiding information and an effort to hide the existence of the embedded information, it serves as a better way to protect the message than cryptography, which only hides the content of the message, not the existence of the message, allowing the original message is hidden within a digital medium that serves as transport, so that the changes that occur in it are not de tectable. Digital archive, hidden file, cryptography, steganography.

"SAHAR A. EL-RAHMAN, AHMED E. MANSOUR, MANAL ABDULLAH ALOHALI"(C-HIDE:A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES) [2025]

Coverless image steganography conceals information without modifying the carrier image, addressing vulnerabilities in traditional methods. However, existing approaches often require transmitting metadata, raising suspicion and security risks. To overcome these limitations, we propose Coverless Hybrid Image Data Encryption (C-HIDE), a robust steganographic method integrating Advanced Encryption Standard (AES) for data confidentiality and Elliptic Curve Cryptography (ECC) for secure key exchange. The system ensures secure transmission without altering cover images, making embedded data harder to detect. C-HIDE eliminates metadata transmission by enabling both sender and receiver to independently generate synchronized coverless image datasets (CIDs) using random seeds. Encrypted secret data is mapped to images whose hash sequences correspond to segments of the message, with Speeded-Up Robust Features (SURF) ensuring reliable image matching. Steganography, coverless image steganography, information hiding, information security, concealed communications, cryptography, embedding, encryption technique.

V. SYSTEM ARCHITECTURE

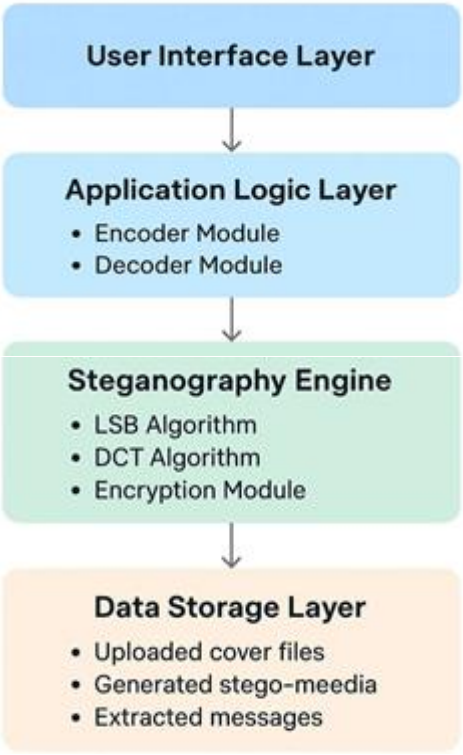

Figure 5.1 Simple Steganographic Model

VI. PROPOSED SYSTEM

The proposed Steganography Hider System is designed to provide a secure and efficient method for hiding sensitive information within a cover medium such as an image, audio, or video file. The system uses advanced steganographic techniques to embed the secret data in a way that is imperceptible to human senses and resistant to detection by steganalysis tools. It integrates an encryption module to add an extra layer of security, ensuring that even if the hidden data is detected, it cannot be easily interpreted without the proper key. The system consists of an embedding process that carefully modifies the cover media without significantly affecting its quality, and an extraction process that retrieves the hidden data accurately. The proposed system aims to achieve high imperceptibility, data integrity, robustness, and efficiency, making it suitable for applications where confidential communication is critical. This approach ensures secure transmission of sensitive information while maintaining the visual or auditory quality of the original media.

VII. CONCLUSIONS

In conclusion, the Steganography Hider System provides an effective and secure solution for hiding sensitive information within digital media. By integrating encryption with advanced steganographic techniques, the system ensures that hidden data remains confidential and resistant to detection or tampering. The proposed system achieves high imperceptibility, preserving the quality of the cover media while embedding information in a way that is invisible to the human eye or ear. It offers accurate data extraction, maintaining the integrity of the hidden message. With its robust performance, minimal distortion, and strong security features, the system serves as a reliable method for secure communication and data protection. This project demonstrates the potential of steganography as a valuable tool in modern information security, paving the way for future enhancements and practical applications in diverse fields such as digital forensics, secure communication, and data privacy.

REFERENCES

1. STEGANOHIDE: An Information Hiding System using Steganography Technique — Shobhit Sharma, Shivam Sharma, A. Charan. Journal of Research in Engineering and Applied Sciences, 2024. Looks at LSB encoding and steganalysis, proposes improvements without using a secret key in some parts.
2. Recent Advances in Steganography — Mahmud Ahmad Bamanga, Aliyu Kamalu Babando, Mohammed Ahmed Shehu. IntechOpen, 2024. A survey chapter covering workflows, applications, challenges, and future directions.
3. "Cross: Diffusion Model Makes Controllable, Robust and Secure Image Steganography" (2023) This paper introduces Cross, a steganography framework that leverages diffusion models to achieve controllable, robust, and secure image steganography. The framework utilizes Stable Diffusion and other open-source tools to improve the controllability and diversity of container images, enhancing the security and robustness of the hidden data.
4. "A Novel Approach to Image Steganography Using Generative Adversarial Networks" (2024) This research explores the use of Generative Adversarial Networks (GANs) in image steganography to create stego-images that are visually indistinguishable from their original counterparts.
5. "A Novel and Efficient Digital Image Steganography Algorithm Incorporating LSB Substitution with MultiLevel Encryption" (2025) This research introduces a

steganographic algorithm that combines LSB substitution with multi-level encryption techniques. The approach enhances data security by encrypting the secret message before embedding it into the cover image, making unauthorized extraction more challenging.

6. "An Effective Steganographic Technique for Hiding the Image" (2025) This paper discusses a Least Significant Bit (LSB) based steganography method enhanced with user-specific detection mechanisms. It aims to improve security by ensuring that hidden data can only be detected by authorized users.
7. "RichardApau,MichaelAsante,FrimpongTwum,JamesBen HayfronAcquah,KwameOfosuhenPeasah"(Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review) [2025]
8. "Heba Ragab, Hassan Shaban, Kareem Ahmed, Abd-Elmgied Ali" (Digital Image Steganography and Reversible Data Hiding: Algorithms, Applications and Recommendations) steganography, Reversible Data Hiding (RDH), watermarking, information hiding. [2025]
9. "Abdullah Alenizi, Mohammad Sajid Mohammadi, Ahmad A. Al-Hajji, Arshiya Sajid Ansari" (A Review of Image Steganography Based on Multiple Hashing Algorithm) Steganography is the method of concealing crucial data inside an innocent-looking file. [2024]
10. "Nagaraj V. Dharwadkar" (Unveiling the Hidden Pixels: A Comprehensive Exploration of Digital Image Steganography Schemes) Image steganography; cryptography; data compression; spatial domain; transform domain; dual approach. [2025]
11. "Isamadeen A. Khalifa, Salih Mustafa Saleem, Abdulkadir Sengur" (Multilayer Steganalysis in the Encryption Era:) Steganography, Multilayer steganalysis, Cryptography, AEAD, AES–GCM. [2026]
12. "Mazriha Akter Mohua" (A Review on the Integration of Cryptography and Steganography for Enhanced Information Security) Cryptography, Steganography, Information Security, Data Hiding, Encryption, Decryption [2025]
13. "MAHADRISS, LAMIA BERRICHE, SIWAR REKIK" (Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions) Internet of Things (IoT), steganography, covert communication, secure data transfer, resource-constrained devices. [2025]
14. "Javier Guaña-Moya, Yolanda Borja López, Gutiérrez Constante, Paulina Jaramillo Flores" (Information security vulnerabilities using steganography as the art of hiding information) Digital archive, hidden file, cryptography, steganography. [2024]
15. "SAHAR A. EL-RAHMAN, AHMED E. MANSOUR, MANAL ABDULLAH ALOHALI" (C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES) Steganography, coverless image steganography, information hiding, information security, concealed communications, cryptography, embedding, encryption technique. [2025]