Steganography: A Data Hiding Technique

A. Bhargavi[1], A. Sai Siddhartha[2], A. Varshitha Reddy[3], B. Bhavya[4]
[1,2,3,4]*Department of Computer Science & Engineering, Artificial Intelligence & Machine Learning*
[1,2,3,4]*Malla Reddy University, Hyderabad, India*

***Abstract*—Steganography is the practice of hiding information in such a way that the existence of the hidden message is concealed. It provides a stronger method of securing communication compared to cryptography, which only hides the content of a message but not the fact that a message exists. In this paper, we discuss how digital images can be used as carrier files to hide secret messages. By combining a secret image with a carrier image, a hidden image is produced, making the concealed information difficult to detect without proper extraction methods. This paper also explores fundamental steganographic concepts, its history, commonly used techniques, steganalysis, and applications such as digital watermarking.**

***Index Terms*—Steganography, Cryptography, Data Hiding, Digital Watermarking, Steganalysis, LSB, Covert Communication, Image Processing.**

I. INTRODUCTION

Internet users often need to store, send, or receive sensitive information securely. One common method is encryption — converting data so only authorized people can read it. However, encryption reveals that secret communication is occurring. To address this, another technique called steganography is used.

Steganography is the ancient practice of hiding messages so that their existence cannot be detected. Unlike encryption, which transforms a message's appearance, steganography hides the message within another medium. Steganography aims to conceal the existence of a message, while cryptography focuses on making the message unreadable.

The steganographic process involves three main steps:

1. Choosing a messenger capable of delivering the message securely.
2. Writing the message using notations that conceal the actual meaning.
3. Hiding the message so that even its presence cannot be predicted.

In steganography, information is hidden inside a normal-looking file called the cover carrier — digital files such as images, audio, video, or text. The resulting file is called a stego-carrier. The process is often protected by a stego key. The formula is:

Cover Medium + Message + Stego Key = Stego Medium

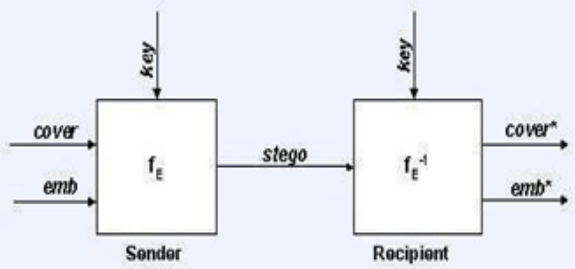

Fig. 1. Graphical Version of the Steganographic System

One key advantage of steganography is that it allows messages to be transmitted secretly without anyone realizing communication is taking place. By contrast, encryption, while securing content, can still signal that protected information is being exchanged.

II. HISTORICAL BACKGROUND

Steganography is believed to have been practiced as early as the Golden Age of Greece. People would melt wax from tablets, carve messages into the wooden surface beneath, and reapply the wax — allowing secret messages to be carried without suspicion.

Later, the Germans developed microdot technology, described by FBI Director J. Edgar Hoover as the enemy's masterpiece of espionage. Microdots are photographs reduced to the size of a printed period but containing the clarity of a full typed page. The first microdots were discovered in 1941.

Another technique was invisible ink, widely used during World War II. A normal-looking letter could contain a hidden message between the lines, using substances such as milk, vinegar, or fruit juices that become visible when heated.

III. APPLICATIONS OF STEGANOGRAPHY

Steganography has a broad range of real-world applications:

- Secure Storage: Sensitive data such as banking details or military information can be hidden within a cover file, undetectable to unauthorized parties.
- Digital Watermarking: Steganographic techniques embed ownership or copyright information into media files for rights protection.

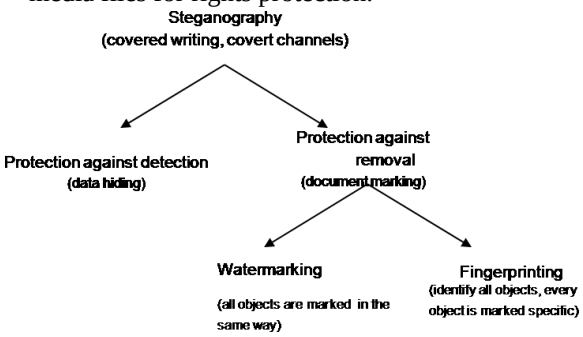

Fig. 2. Steganography Types

- E-Commerce Security: Biometric fingerprint authentication combined with steganography can embed a unique session ID into fingerprint images for secure transactions.
- Covert Communications: Governments and businesses use steganography to support national security and protect trade secrets.
- Secure Data Transportation: Steganography hides sensitive data within ordinary files, allowing information to pass through channels without raising suspicion — applicable to emails, images, and shared files.

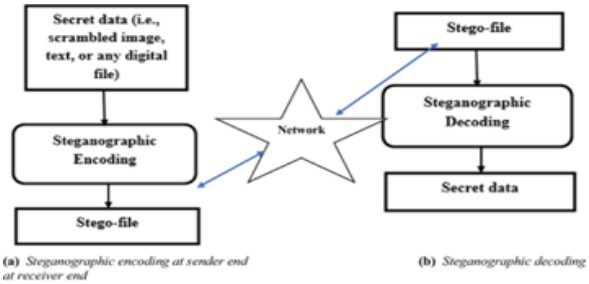

Fig. 3. Steganography on the Internet

IV. STEGANOGRAPHY AND CRYPTOGRAPHY

A. Comparison

Cryptography converts a message into an unreadable form, while steganography hides the existence of the message entirely. In cryptography, analysis compares plaintext with ciphertext. In steganography, comparisons are made between the original cover media and the stego-media.

B. Combination

For maximum privacy, encryption and steganography can be combined. When data is encrypted before being hidden, it becomes even more difficult to distinguish from normal data within the carrier medium. Several tools enable this dual-protection approach.

V. STEGANALYSIS

Steganalysis is the process of detecting steganography by examining irregularities in bit patterns or unusually large file sizes. Its objective is to analyze suspicious data streams, determine whether they contain hidden information, and, if possible, recover the concealed message. Unlike cryptanalysis, steganalysis operates in cases where the existence of a hidden message is not obvious.

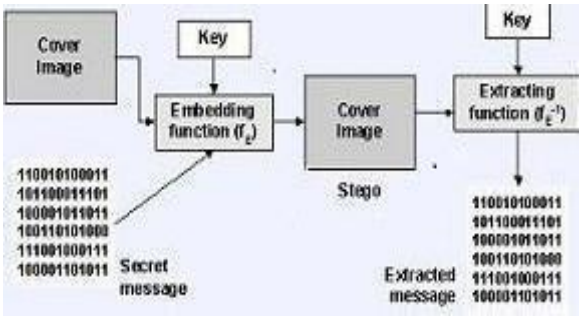

Fig. 4. Graphical Version of the Steganographic System

Steganalysis begins with a set of suspected information streams and uses statistical analysis and advanced techniques to identify unusual patterns or irregularities in the data.

VI. STEGANALYSIS TECHNIQUES

Hiding information within an electronic medium alters the medium's properties, resulting in degradation or

unusual characteristics. Common detection techniques include:

A. Unusual Patterns

Disk analysis tools can detect hidden information stored in unused partitions. Special filters can examine TCP/IP packets for hidden or invalid information within packet headers, where unused or reserved spaces are sometimes exploited to conceal data.

B. Visual Detection

Repetitive patterns in digital files can reveal hidden information. Comparing the original cover image with the stego image — a known-carrier attack — can expose changes. Image padding or cropping by steganography tools also acts as a visual indicator.

C. Detection Tools

When data is embedded using the Least Significant Bit (LSB) method, applying lossy compression can remove the hidden message. Dedicated tools such as *EnCase* (Guidance Software) and *ILook Investigator* (Electronic Crimes Program, Washington) are used for forensic steganalysis.

VII. IMPLEMENTATION AND RESULTS

In the implementation phase, the steganography technique was applied to sample images. A cover image was passed through an LSB embedding function along with a secret message and key, producing a stego image. The key encrypts the message before embedding and decrypts it after extraction.

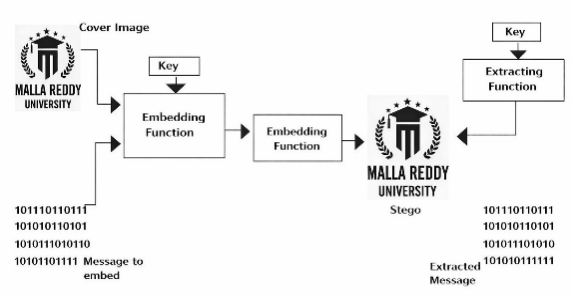

Fig. 5. Steganography Procedure

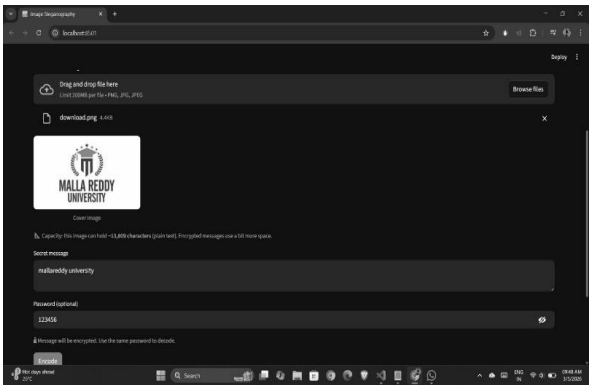

Fig. 6. Stego Image with Embedded Message

Histogram analysis was performed on both the cover image and the stego image. The results showed measurable differences between the two histograms, confirming that the embedding process introduces statistical changes detectable by steganalysis tools.

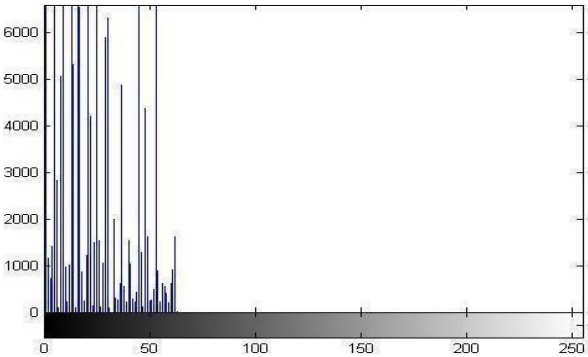

Fig. 7. Histogram of Stego Image

VIII. DIGITAL WATERMARKING

Digital watermarking embeds information into a digital signal in a way that is difficult to remove. If the signal is copied, the watermark travels with it. There are two main types:

A. Visible Watermarking

The embedded information is clearly visible, typically as text or a logo identifying the owner — for example, a broadcaster's logo displayed in the corner of a video frame.

B. Invisible Watermarking

Information is embedded as digital data imperceptible to users. It may function as steganography — hiding a secret message — or as a copyright marker readable only by specialized watermark-reading software. Applications include identity card certification,

passport authentication, and copyright protection for media content.

IX. RESULTS AND CONCLUSION

Steganography is a powerful technique for transmitting secret information by hiding it within ordinary-looking files. Digital image steganography is becoming increasingly popular across many applications.

The most significant future application of steganographic techniques is likely to be digital watermarking. Content creators need reliable methods to identify and track ownership of digital material. At the same time, steganography may face legal restrictions as governments work to prevent misuse for covert criminal communications.

Future application directions include:

- Hiding data on the network in case of a security breach.
- Peer-to-peer private communications without interception.
- Posting secret communications on the web to avoid transmission interception.
- Embedding corrective audio or image data to prevent corruption from poor connections.

REFERENCES

[1] S. Baluja, "Hiding Images in Plain Sight: Deep Steganography," NeurIPS, 2017.
[2] J. Zhu et al., "HiDDeN: Hiding Data with Deep Networks," ECCV, 2018.
[3] K. A. Zhang et al., "SteganoGAN: High-Capacity Image Steganography with GANs," arXiv:1901.03892, 2019.
[4] J. Boroumand et al., "Deep Residual Network for Steganalysis of Digital Images," IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1181–1193, 2019.
[5] J. Ye et al., "Deep Learning Hierarchical Representations for Image Steganalysis," IEEE Trans. Inf. Forensics Security, 2017.
[6] F. Kreuk et al., "End-to-End Optimized Speech Steganography," IEEE ICASSP, 2020.
[7] M. Tancik et al., "StegaStamp: Invisible Hyperlinks in Physical Photographs," IEEE CVPR, 2020.
[8] R. Zhang et al., "Invisible Steganography via Generative Adversarial Networks," Multimedia Tools and Applications, 2019.
[9] N. Subramanian and O. Elharrouss, "Deep Image Steganography: A Survey," ACM Computing Surveys, 2022.
[10] X. Luo et al., "Reversible Image Steganography Based on Deep Learning," Signal Processing: Image Communication, 2018.
[11] A. Rehman et al., "End-to-End Trained CNN for Image Steganography," Pattern Recognition Letters, 2018.
[12] S. Weng et al., "Secure Steganography Based on Adversarial Learning," IEEE Access, 2021.
[13] J. Li et al., "Transformer-Based Image Steganography for Secure Communication," Future Generation Computer Systems, 2023.
[14] Y. Zhang et al., "Transformer-Based High-Capacity Image Steganography," IEEE Trans. Inf. Forensics Security, 2024.
[15] L. Chen et al., "Robust GAN-Based Image Steganography Against Deep Steganalysis," IEEE Access, 2024.