Dr. Gaytri Devi, 2024, 12:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology
An Open Access Journal

Steganography and Its Role in Data Security: Techniques and Applications

Dr. Gaytri Devi[1], Dr. Renu Miglani[2], Anu Dahiya[3]
[1,2]GVM Institute of Technology & Management, DCRUST University, Murthal
[3]Tika Ram College , Sonipat ,Haryana

Abstract- In an era dominated by digital communication, ensuring the security and confidentiality of transmitted data has become increasingly critical due to rising cyber threats and pervasive surveillance. Steganography—the art and science of hiding information within seemingly innocuous media—offers a covert layer of protection that complements traditional encryption methods. This paper presents a comprehensive exploration of steganography, covering its historical evolution, fundamental principles, classification, and various embedding techniques and applications. It also investigates steganalysis, the countermeasure used to detect and analyze hidden information. Furthermore, the study includes a comparative evaluation of steganography techniques. Real-world case studies are presented to illustrate both the practical applications and potential misuse of steganography. Through a comprehensive analysis, we highlight steganography's growing role in modern data security as a discreet and powerful method for protecting information in diverse digital environments.

Keywords: Steganography, Information Hiding, Digital Security, Steganalysis, Embedding Techniques, Secure Communication.

I. INTRODUCTION

In today's digital world, cybercrime is a growing threat that affects individuals, businesses, and governments. Sensitive information is often stolen, leaked, or misused by hackers who use advanced methods to hide their activities [1]. As digital communication becomes faster and more common, it is important to find new ways to protect private and important data. One such method is steganography, which involves hiding information inside images, videos, or audio files so that it is not visible to others.

With rising concerns over cybercrime and data breaches, there is a growing need for advanced methods to protect sensitive information. As hackers become more skilled at stealing and leaking data, traditional security tools are sometimes not enough. steganography can be proved as a powerful tool for safeguarding sensitive information.

Unlike encryption, which makes it obvious that something is being protected, steganography hides the very existence of the message. This makes it especially useful in situations where secrecy is critical, such as military communication, personal privacy, and copyright protection[5]. As a result, steganography is becoming an important part of modern cybersecurity systems, working alongside encryption to strengthen digital defenses.

This paper explores how steganography is evolving to meet modern security needs and highlights its increasing relevance in today’s digital landscape. By analyzing various techniques, applications, and challenges, the study emphasizes the potential of steganography to play vital role in future secure communication systems.

The paper is organized as follows: Section 1 introduces the concept of steganography and its importance in the context of digital security. Section 2 outlines the fundamental concepts and categories of steganography, explaining the basic principles and various types based on media. Section 3 presents a literature review of previous research in this domain to establish the academic foundation. Section 4 discusses major steganographic techniques and compares them based on performance metrics like capacity, imperceptibility, and robustness. Section 5 examines steganalysis—the process of detecting hidden information Section 6 highlights challenges, real-world applications and case studies to demonstrate both practical uses and potential misuse of steganography. Finally, Section 7 concludes the paper with a summary of findings and suggestions for future research.

II. FUNDAMENTALS AND TYPES OF STEGANOGRAPHY

Steganography is the science and practice of hiding messages within other non-secret media such that the presence of the message is concealed. The term originates from the Greek words steganos (meaning "covered") and graphia (meaning "writing"). Steganography, unlike cryptography, hides the presence of a message [3]. Steganography aims to make the communication itself invisible, thus attracting less attention.

A typical steganographic system involves several core components:

- **Cover Object:** The carrier medium used to embed the secret message, such as an image, audio file, video stream, or text document.
- **Payload (Hidden Message):** The confidential data or message intended to be hidden within the cover.
- **Embedding Algorithm:** The method used to integrate the payload into the cover medium without arousing suspicion or noticeable distortion.
- **Stego Object:** The final product resulting from the embedding process, which looks nearly identical to the original cover object.
- **Extraction Algorithm:** The reverse process used to recover the hidden data from the stego object.

Categories of Steganography

Early classifications [4] formed the basis for categorizing steganographic media into text, image, audio, and network-based approaches and the domain in which the data is concealed:

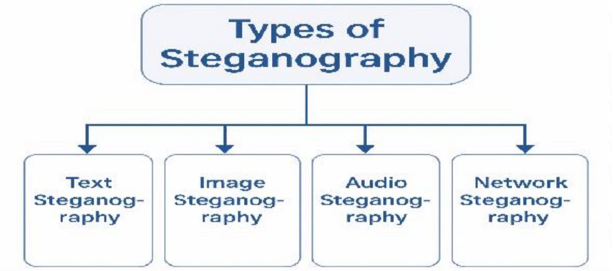


Figure 1 - Types of Steganography based on the nature of the cover object

- **Text Steganography:** This involves hiding information in text-based files by manipulating formatting elements such as spaces, font styles, line breaks, or using linguistic techniques like synonym substitution and semantic shifting. Although limited in capacity and prone to detection, it remains a simple and effective method for short messages.
- **Image Steganography:** One of the most widely used forms, it embeds data within image pixels, often using techniques like Least Significant Bit (LSB) modification. Image files provide high capacity and imperceptibility due to redundancy in visual data, making them ideal carriers for steganographic applications.
- **Audio Steganography:** This method conceals data within digital audio files. Techniques include phase coding, echo hiding, and spread spectrum methods. Audio steganography is challenging due to the high sensitivity of human auditory perception, but it allows for robust embedding when done effectively.
- **Video Steganography:** This combines image and audio steganography by embedding data across video frames or within audio tracks. The large file size and continuous frame flow of video allow for high-capacity and high-imperceptibility data hiding.
- **Network or Protocol Steganography:** Data is embedded in network traffic by manipulating protocol headers, timing patterns, or unused TCP/IP fields. This technique is increasingly relevant in covert channel communications, especially in cybersecurity and cyber defense contexts.

Each type of steganography serves unique use cases depending on the required capacity, robustness, and cover medium availability.

After understanding the fundamental components and various categories of steganography, it is essential to explore the complete lifecycle of a hidden message—from embedding to detection. Once a payload is embedded into a cover object using an embedding algorithm, the resulting stego object is transmitted across a communication channel. During this transmission phase, the message remains hidden from unintended observers, relying on the imperceptibility of the stego object. However, the existence of hidden data can still pose significant risks in certain contexts, particularly in cybersecurity, law enforcement, and digital forensics. This is where steganalysis enters the picture. Steganalysis is the adversarial discipline to steganography—it involves the detection, analysis, and possible extraction of hidden messages from stego objects.

A detailed examination of steganalysis techniques and tools is presented in Section 5. Together, steganography and steganalysis form a dynamic interplay in the domain of information security. Advances in embedding techniques drive the development of more sophisticated detection mechanisms, and vice versa. Understanding this duality is crucial for designing resilient steganographic algorithms and enhancing the overall robustness of secure communication systems. The following diagram illustrates the complete steganographic communication process—from message embedding to transmission, and ultimately to steganalysis and extraction.

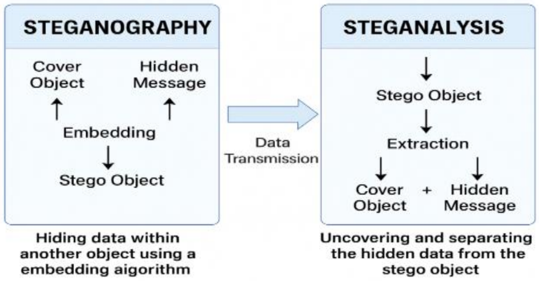


Figure 2: Diagram illustrating the contrast between steganography (embedding) and steganalysis (detection).

III. LITERATURE REVIEW

Steganography has evolved from simple text-based hiding schemes to sophisticated, AI-driven methods capable of operating across multiple domains, including image, audio, video, and network protocols.Researchers have extensively explored various techniques to enhance the imperceptibility, capacity, and robustness of steganographic systems, while also developing steganalysis as a parallel field to detect and counter these methods.

Petitcolas et al. (1999) in [2] offered one of the earliest and most comprehensive surveys of information hiding, outlining the conceptual underpinnings of steganography, watermarking, and anonymity. This foundational work has been instrumental in defining the research scope and challenges of the field.

The academic discourse surrounding steganography advanced notably with Johnson and Jajodia (1998)[4], who emphasized the distinctions between cryptographic secrecy and steganographic concealment. Their work also highlighted the significance of steganography in security-focused applications.Provos and Honeyman (2003)[3] contributed significantly by developing early detection models and illustrating the limitations of commonly used steganographic tools. Their insights into media classification and data embedding vulnerabilities broadened the analytical foundation of steganalysis.

Cheddad et al. (2010) [6] further organized the landscape by presenting a structured taxonomy of steganographic methods. Their classification into spatial and transform domain techniques has become a standard reference for evaluating the performance and limitations of steganographic algorithms.

The detection of Least Significant Bit (LSB) steganography was systematically approached by Zhang et al. (2003) [7], who proposed detection techniques focused on statistical inconsistencies introduced by LSB manipulation.

In the realm of steganalysis, Fridrich et al.(2001)[8] applied statistical models to effectively detect hidden data in both color and grayscale images. Similarly, Leu et al. (2005)[9] contributed to the development of automated detection systems, enhancing the ability to uncover covert communication without prior knowledge of the embedding method.

Together, these works form a solid theoretical and practical foundation for understanding and advancing the dual domains of steganography and steganalysis.

IV. STEGANOGRAPHIC TECHNIQUES

Steganographic techniques can be broadly categorized based on the domain in which they operate and the manner in which the secret data is embedded within the cover media. Each method offers unique advantages in terms of capacity, robustness, and imperceptibility, and the choice of technique often depends on the specific application and the nature of the cover object.

Substitution Techniques

Substitution techniques are among the simplest forms of steganography. These methods involve replacing insignificant parts of the cover object—typically bits that do not significantly affect perceptual quality—with the secret data. A common example is the Least Significant Bit (LSB) method used in image and audio files, where the least significant bits of pixel values or audio samples are modified. Although easy to implement and computationally efficient, substitution methods are highly susceptible to steganalysis and lossy compression, making them less robust for secure applications.

Transform Domain Techniques

In contrast to substitution methods, transform domain techniques embed information in the frequency components of the cover media. These methods often employ mathematical transforms such as the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). By embedding data in the transformed coefficients, these techniques offer improved robustness against compression, filtering, and other manipulations commonly applied to digital media. This makes them suitable for applications where durability of the hidden message is critical.

Spread Spectrum Techniques

Spread spectrum techniques distribute the secret data across a wide frequency spectrum of the cover signal, in a manner analogous to spread spectrum communication systems. This dispersion makes the embedded information less susceptible to noise, interference, and detection. Although these methods typically offer lower embedding capacity, they provide high robustness and are often used in secure and covert communication.

Statistical Methods

Statistical steganography modifies the statistical properties of the cover medium to embed information in a manner that avoids perceptual changes. Techniques in this category include histogram modification and block-based statistical embedding. By maintaining or mimicking the natural statistical characteristics of the cover, these methods are more resistant to detection through basic analysis, although advanced statistical steganalysis tools may still be effective.

Distortion Techniques

Distortion-based techniques encode secret data by intentionally introducing slight, controlled distortions to the cover object. These distortions are designed to be imperceptible to the human senses while still allowing for data recovery. Unlike other methods, extraction of the embedded message often requires access to the original, undistorted cover object. This dependency increases security but may limit practical deployment in certain scenarios.

Adaptive and Intelligent Steganography

Adaptive steganography leverages the characteristics of the cover media to optimize data embedding. Techniques in this category may utilize machine learning or statistical analysis to identify regions of the cover object that can tolerate modifications without noticeable degradation. Intelligent steganography systems dynamically adjust their embedding strategies based on local features such as texture or noise levels, significantly enhancing imperceptibility and resistance to steganalysis.

Coverless Steganography

Unlike traditional steganography, which embeds secret data into a cover object (such as an image, audio, or video), coverless steganography avoids using a cover medium altogether. Instead, it generates new media directly from the secret information, ensuring that there is no modification of an existing file that could be analyzed or detected.

Coverless methods often rely on generative models, such as Generative Adversarial Networks (GANs), to create content (e.g., images or texts) that inherently represent the hidden message. Since there is no alteration of a pre-existing file, statistical and structural steganalysis becomes ineffective, offering very high imperceptibility and robustness.

This technique is especially relevant in scenarios where traceability and forensic analysis need to be minimized. However, its application can be limited by the complexity of generation models and the capacity constraints associated with generating high-quality content.

Comparative Analysis of Steganographic Techniques:

Each steganographic technique offers a unique balance of robustness, payload capacity, and imperceptibility. While substitution methods like Least Significant Bit (LSB) are easy to implement and offer high capacity, they are relatively weak against image manipulations or statistical attacks. On the other hand, transform domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) improve robustness by embedding information into frequency components, but often at the cost of increased complexity.

Statistical and distortion-based methods aim to make detection more challenging by preserving or altering statistical properties in imperceptible ways. Adaptive and intelligent steganography—leveraging machine learning and content-aware embedding—strikes a balance between undetectability and adaptability but can be computationally intensive.

The following table presents a comparative evaluation of these techniques across core parameters: Robustness – resistance to compression and noise, Imperceptibility – visual/auditory undetectability ,Payload Capacity – how much data can be hidden and Complexity – implementation difficulty[3][6].

Table 1: Comprative Analytics of steganographic techniques based on domain, applicable media, performance indicators, and their resilience against steganalysis

.

Technique	Domain	Applicable Media	Capacity	Robustness against Steganalysis	Imperceptibiliy	Complexity
LSB Substitution	Spatial	Text, Image, Audio	High	Low	Medium	Low
DCT / DWT Embedding	Transform	Image, Audio, Video	Medium	High	High	Medium
Spread Spectrum	Frequency	Audio, Video	Low–Medium	High	Medium	Medium–High
Statistical Methods	Statistical	Image, Network	Medium	Medium	High	Medium
Distortion Techniques	Distortion	Image, Audio	Medium	High	Medium	Medium
Adaptive Steganography	Hybrid	Image,Vide oGenerated Media	Medium	High	Very High	High

Technique	Domain	Applicable Media	Capacity	Robustness against Steganalysis	Imperceptibiliy	Complexity
Coverless Steganography	Generated (GAN)	AI-generated Text/Image	Medium	Very High	Very High	Very High

V. STEGANALYSIS

Steganalysis is the counterpart to steganography—it is the process of detecting, analyzing, and potentially recovering hidden information from stego objects. While steganography focuses on embedding a message in such a way that its existence remains secret, steganalysis aims to uncover that hidden communication, often without prior knowledge of the original embedding method or key.

Steganalysis techniques typically rely on statistical analysis, pattern recognition, machine learning, and signal processing to detect anomalies introduced by data embedding. It plays a crucial role in digital forensics, cybersecurity, and surveillance, where detecting covert communication can prevent malicious activities.

Types of Steganalysis

Steganalysis techniques are broadly classified into two categories:

Passive Steganalysis: This approach seeks to detect the presence of hidden information without altering the stego object. It is primarily used in monitoring and forensic contexts where the integrity of the file must be preserved.

Active Steganalysis: This involves deliberately altering or attacking the stego object to extract or disrupt the embedded message. Active methods are more aggressive and are used in counterintelligence or defensive scenarios.

Common Detection Techniques

To expose steganographic content, various analytical approaches are employed:

Visual Attacks: Involve manual or automated inspection of media for visible anomalies introduced during embedding (e.g., distortion in LSB-embedded images).

Statistical Attacks: Utilize statistical methods to detect irregularities in the pixel distribution, frequency spectrum, or noise patterns. Techniques like RS analysis, Chi-square testing, and histogram comparison are often used.

Structural Attacks: Exploit predictable changes in the structure of file formats or metadata fields. For example, unexpected shifts in file size or header inconsistencies can signal steganographic activity.

Machine Learning-Based Detection: Increasingly, steganalysis leverages AI/ML models trained to identify subtle patterns and anomalies introduced by embedding techniques. Deep learning models such as CNNs have shown high accuracy in detecting stego content, especially in large-scale datasets.

VI. APPLICATIONS, CHALLENGES AND CASE STUDIES

Applications of Steganography in Data Security

Steganography plays a vital role in modern digital communication by enabling the concealment of information within various media formats. Its ability to mask the very existence of a message makes it especially valuable in domains requiring confidentiality, data authenticity, and covert communication.

Steganography has found diverse applications across multiple domains due to its ability to discreetly embed information in digital media. One of its primary uses is in secure communication, where it enables the hidden transmission of sensitive information. This is especially valuable in surveillance-heavy or censored environments, such as journalists working in authoritarian regimes who need to exchange critical data without detection.

Another major application lies in digital watermarking, where steganographic methods are employed to embed ownership or copyright data into multimedia files. This helps media publishers track content distribution and prevent unauthorized use.

In the field of cybersecurity, steganography is both a tool and a threat. It can be used to build covert channels for secure system testing, but it also plays a role in unethical activities such as data exfiltration by malware.

Military and intelligence operations also benefit from steganography, using it to embed mission-critical data into innocuous-looking files such as drone footage or image files, ensuring secure data exchange without arousing suspicion.

In healthcare and legal domains, the technique is applied for privacy-preserving data sharing, such as embedding patient information within diagnostic images or confidential legal data in routine-looking documents. This ensures confidentiality without compromising accessibility.

In emerging technologies like blockchain and decentralized systems, steganography is leveraged to hide metadata or transaction records, enhancing traceability and ensuring the authenticity of records without bloating the blockchain.

Social media and messaging platforms present another critical area of application. Users may circumvent censorship or surveillance by embedding covert messages within memes or altered videos shared online.

Steganography is also widely used in education and research, serving as a practical teaching and experimentation tool in fields like cybersecurity, digital forensics, and secure communication systems. These diverse use cases highlight the flexibility and significance of steganography in modern digital infrastructures.

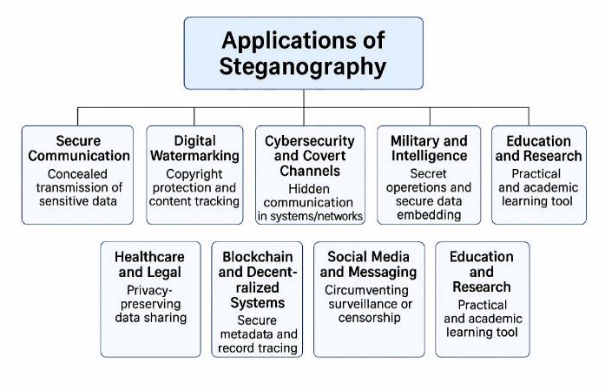

Applications of Steganography
Secure Communication
Concealed transmission of sensitive data
Digital Watermarking
Copyright protection and content tracking
Cybersecurity and Covert Channels
Hidden communication in systems/networks
Military and Intelligence
Secret operetions and secure data embedding
Education and Research
Practical and academic learning tool
Healthcare and Legal
Privacy-preserving data sharing
Blockchain and Decent-ralized Systems
Secure metadata and record tracing
Social Media and Messaging
Circumventing surveillance or censorship
Education and Research
Practical and academic learning tool

Figure 3: Applications of steganography

Challenges in Steganography

Despite its potential in secure communication and digital privacy, steganography faces several critical challenges that limit its widespread and reliable application. These challenges arise from the evolving nature of security threats, technological constraints, and the adversarial dynamics with steganalysis.

Detection by Steganalysis

Modern steganographic systems are constantly at risk of being detected by increasingly sophisticated steganalysis techniques. Tools based on machine learning, statistical analysis, and signal processing can identify hidden patterns, especially in predictable or poorly implemented hiding methods. Ensuring undetectability remains a core difficulty.

Trade-Off Between Capacity, Robustness, and Imperceptibility

A fundamental limitation in steganography is balancing three competing goals: Capacity (amount of data that can be hidden), Robustness (resistance to attacks or compression), and Imperceptibility (undetectability to human senses or statistical analysis). Improving one often weakens the others, making optimal system design complex.

Format Sensitivity and Media Compression

Lossy compression formats (e.g., JPEG, MP3) often discard or alter hidden data, especially if the embedding method isn't robust. This poses a challenge in real-world applications where media is frequently edited, resized, or compressed during transmission.

Platform and Device Limitations

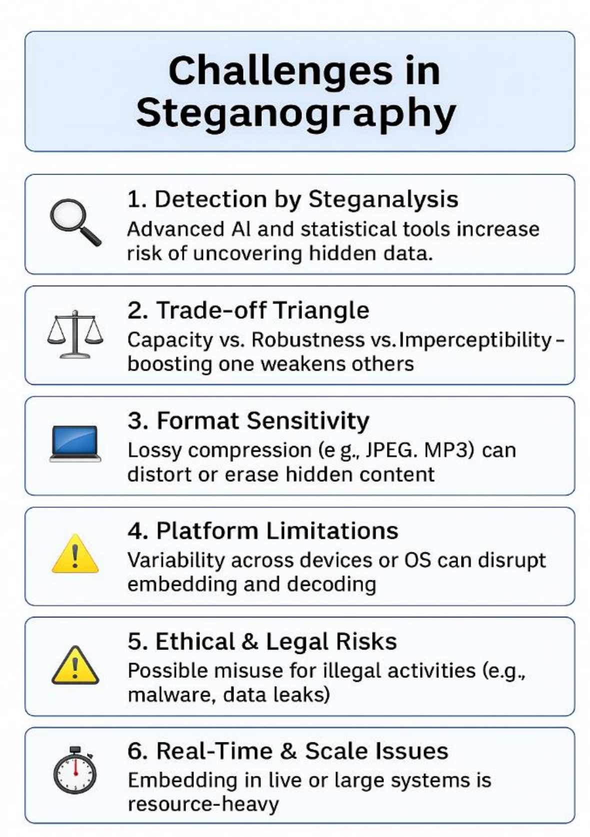
Embedding and extracting hidden data may not function consistently across different platforms, devices, or software environments. Hardware inconsistencies (e.g., camera sensors, audio codecs) can affect the integrity of stego objects.

Ethical and Legal Concerns

Steganography can be used for malicious purposes, such as concealing malware or illegal communication. Its covert nature raises concerns about misuse, surveillance evasion, and legal accountability. These ethical issues necessitate responsible research and application.

Real-Time and Scalable Implementation

Applying steganography in high-throughput or real-time systems (e.g., live video streaming or secure VoIP) remains a challenge due to processing overhead and delay. Scalability in large systems, such as blockchain or cloud environments, also requires lightweight yet secure techniques.



Challenges in Steganography

1. Detection by Steganalysis
Advanced AI and statistical tools increase risk of uncovering hidden data.

2. Trade-off Triangle
Capacity vs. Robustness vs.Imperceptibility - boosting one weakens others

3. Format Sensitivity
Lossy compression (e g., JPEG. MP3) can distort or erase hidden content

4. Platform Limitations
Variability across devices or OS can disrupt embedding and decoding

5. Ethical & Legal Risks
Possible misuse for illegal activities (e.g., malware, data leaks)

6. Real-Time & Scale Issues
Embedding in live or large systems is resource-heavy

Figure 4: Challenges in steganography

Case Studies: Real-World Applications and Misuse of Steganography

To further illustrate the practical implications of steganography, this section presents selected case studies that highlight both legitimate uses and malicious exploitation.
Steganography has proven effective in a variety of practical domains. However, its covert nature also opens doors for malicious misuse. Below, we categorize real-world case studies to illustrate both the advantages and potential threats posed by steganography.

In legitimate applications, companies like Netflix and YouTube have adopted invisible digital watermarking to trace pirated content. These watermarks are imperceptibly embedded into video streams and remain intact even after screen recording or file conversion, enabling platforms to identify the source of content leakage and reinforce copyright protection. Similarly, in the defense sector, military drones (UAVs) have utilized image steganography to embed mission-critical information directly into surveillance footage, thereby reducing the risk of interception and ensuring the secure transmission of sensitive data. In the healthcare industry, medical steganography is used to embed patient information within diagnostic imaging files (such as DICOM images), offering privacy-preserving solutions compliant with regulations like HIPAA.

On the other hand, steganography has also been exploited for malicious purposes. A notable example is the alleged use of image-based steganography by Al-Qaeda operatives, who reportedly concealed communication within pornographic images shared via online forums to evade detection. Although the details remain speculative, the case raised significant global concern over steganography's misuse. In cybercrime, sophisticated malware such as Vawtrak and Turla employed steganographic methods to embed command-and-control instructions in benign-looking image files.

Once downloaded, these hidden payloads bypassed antivirus detection, making them a growing threat in the realm of "stegomalware." Furthermore, Operation Shady RAT, a high-profile cyber-espionage campaign, was reported to have leveraged steganographic techniques to exfiltrate sensitive government and corporate data without raising suspicion. These diverse cases underscore the dual-edged nature of steganography: while it can safeguard information in legitimate contexts, it can also pose serious cybersecurity threats when misappropriated.[10][11].

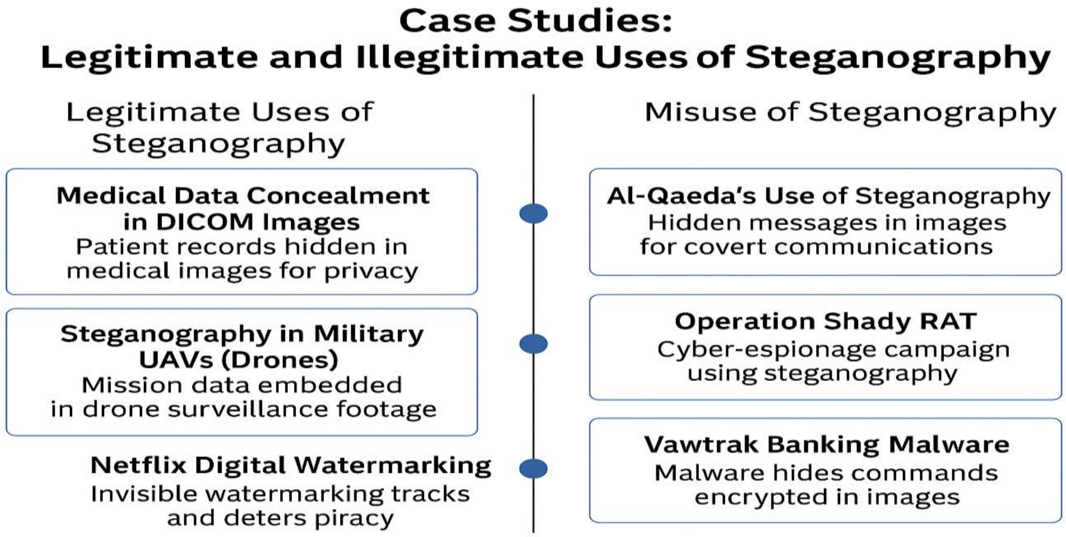

Case Studies:
Legitimate and Illegitimate Uses of Steganography
Legitimate Uses of Steganography
Misuse of Steganography
Medical Data Concealment in DICOM Images
Patient records hidden in medical images for privacy
Al-Qaeda's Use of Steganography
Hidden messages in images for covert communications
Steganography in Military UAVs (Drones)
Mission data embedded in drone surveillance footage
Operation Shady RAT
Cyber-espionage campaign using steganography
Netflix Digital Watermarking
Invisible watermarking tracks and deters piracy
Vawtrak Banking Malware
Malware hides commands encrypted in images

Figure 5: Case Studies

VII. CONCLUSION

Steganography plays an increasingly important role in modern data security. As digital information becomes easier to share and more vulnerable to breaches, the ability to hide data within other digital content offers a practical layer of protection. Alongside traditional methods like encryption and access control, steganography provides a subtle and effective way to keep information safe.

This paper has discussed various techniques, applications, and challenges of steganography, including both classical and modern approaches. Techniques like LSB and DCT are still widely used, while newer approaches such as GAN-based and coverless steganography offer better security and invisibility. However, these advances must be matched by progress in steganalysis and ethical standards to prevent misuse.

In the future, our research will focus on integrating steganography with machine learning and AI, exploring its role in blockchain-based and decentralized systems, developing deep learning-based embedding and extraction methods, and investigating the possibilities of quantum steganography. With continued development and responsible use, steganography will remain a key technology for protecting digital data in an increasingly connected world.

REFERENCES

1. Devi, Gaytri and Vats, Muskan, “The Threat of Cyber Squatting:Understanding the Risks of Digital Identity Theft” (August 3, 2024). SSRN: https://ssrn.com/abstract=4915086
2. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A survey. Proceedings of the IEEE, 87(7), 1062–1078.
3. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32–44.
4. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. IEEE Computer, 31(2), 26–34
5. Gaytri Devi, & Sukhija, V. (2024). IPR and digital space. International Journal of Scientific Research in Science, Engineering and Technology, 11(2), 535–543.
6. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). Digital image steganography: Survey

and analysis of current methods. Signal Processing, 90(3), 727–752.

7. Zhang, T., & Ping, X. (2003). Reliable detection of LSB steganography based on the difference image histogram. Lecture Notes in Computer Science, 2846, 434–441.
8. Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color and grayscale images. IEEE Multimedia, 8(4), 22–28.
9. Lyu, S., Farid, H. (2005). Steganalysis using higher-order image statistics. IEEE Transactions on Information Forensics and Security, 1(1), 111–119.
10. Subramanian, N., Elharrouss, O., Al Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. IEEE Access, 9, 34309–34330.
11. Bamanga, M. A., Babando, A. K., & Shehu, M. A. (2024). Recent advances in steganography. IntechOpen. https://doi.org/10.5772/intechopen.1004521