INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

# EXPLORING STEGANOGRAPHY: MEANING, TYPES, TECHNIQUES AND TOOLS

**Pratibha P. Parab[1], Hrishikesh R. Shelar[2]**

[1,2]Post-Graduate Student, MCA Department, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS34286

## ABSTRACT

Steganography, an ancient art of covert communication, has experienced a revival in the digital era, offering a unique approach to securing sensitive information within various digital mediums. This paper aims to comprehensively explore steganography, elucidating its meaning, types, techniques, and tools. Steganography involves concealing messages within seemingly innocuous carriers to evade detection, distinct from cryptography which focuses on encryption. The paper delves into different types of steganography, examining their principles, strengths, and limitations, providing a detailed classification of methods. Various techniques employed in steganography across digital mediums are explored, highlighting their complexities and practical applications. Additionally, the role of tools in facilitating steganographic processes is discussed. In summary, this research serves as a comprehensive guide to understanding steganography for researchers, practitioners, and enthusiasts interested in concealed communication. By explaining its fundamentals, types, techniques, and tools, the paper equips readers with essential knowledge to navigate this intriguing realm of information security.

**Keywords:** Steganography, types, techniques, data, message, information, hiding.

## 1. INTRODUCTION

Steganography, the practice of concealing information within other data, has gained significant attention in the field of digital security. The term “Steganography” originates from the Greek words “steganos” meaning “covered” and “graphia” meaning “writing”. This technique has been used for various purposes, including data hiding, secure communication, and digital watermarking.

### Meaning of Steganography

Steganography is the process of hiding information within other data, such as images, audio files or video files, to avoid detection. The hidden information is often referred as the “steganographic message” or “steganogram”. The main goal of steganography is to maintain the confidentiality and integrity of the hidden information, while ensuring that it remains undetected by unauthorized parties.

### Types of Steganography

Steganography encompasses a range of techniques designed to conceal information within different types of data. Text steganography involves manipulating text files by adjusting spacing, formatting, or character arrangements to embed hidden messages. Image steganography hides data within images through methods like modifying pixel values, using LSB replacement, or adjusting color palettes. Video steganography conceals information within digital video formats by altering discrete cosine transform (DCT) coefficients in frames or adjusting color and luminance values. Audio steganography hides data within audio files by modifying samples, adjusting frequencies, or using techniques like echo hiding. Additionally, network steganography involves concealing information within network transmissions, making it a covert method for communication [1]. Each type of steganography offers unique challenges and methods, showcasing the versatility of this field across various digital mediums.

### Techniques of Steganography:

Steganography techniques encompass several categories tailored to effectively conceal data within digital media. Spatial domain techniques focus on embedding data directly into the pixel values of an image while maintaining the cover image's visual integrity [2]. Transform domain techniques involve embedding message bits within transform domain coefficients, commonly used for creating robust watermarks and high-capacity steganography [6]. Statistical techniques involve altering cover properties by embedding message bits in blocks based on message size, minimizing modifications to maintain cover integrity [6]. Spread spectrum techniques disperse secret data across a wide frequency bandwidth, making detection challenging even if portions of the data are removed [6]. Distortion techniques conceal messages by applying sequence modifications to the cover, decoded by analyzing differences between the altered and original versions [6]. Masking and filtering methods embed information in image areas that stand out, suitable for

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

blending watermarks into images effectively [4]. Each technique offers unique approaches to covert communication, balancing concealment effectiveness with maintaining the integrity of the cover media.

**Tools used in Steganography:**

Tools and software developed for steganography offer diverse capabilities to conceal data within digital media effectively. Steghide, a popular tool, specializes in hiding data within image and audio files, providing features like data compression, encryption for security, and integrity checks [4]. OpenPuff, another professional-grade tool, allows secure storage of files within various media formats including images, audio, video, and flash files [5]. OpenStego combines data hiding and watermarking functionalities, prioritizing data concealment within image files of different formats like JPEG, JPG, BMP, GIF, and PNG [4]. Xiao Steganography is a widely-used free tool enabling users to hide secret files within both image and audio files [4]. Binwalk, on the other hand, specializes in scanning binary images to locate embedded files and executable code within firmware packages [6]. Lastly, ExifTool serves as a versatile utility for reading, writing, and manipulating metadata within images and media files through a command-line or graphical interface [6]. These tools provide essential support for various steganographic tasks, catering to different user needs and preferences in the realm of covert communication and information security.

## 2. METHODOLOGY

The research methodology for this review paper on steganography involved an extensive examination of diverse sources to gather comprehensive information on steganographic techniques, tools, and applications.

Primary sources included academic papers, research articles, books, and credible online resources related to steganography. Official documentation, reputable academic journals, and specialized websites were consulted to ensure access to up-to-date information and recent advancements in steganographic methodologies.

In analyzing the gathered data, a systematic approach was adopted to categorize and synthesize the information. A chronological framework was applied to organize the historical evolution of steganography, highlighting key developments, techniques, and emerging trends over time. This structured presentation facilitated a clear narrative of steganography's progression and transformation in various digital media.

Furthermore, the gathered data underwent rigorous comparative analysis to identify patterns, similarities, and differences among different steganographic methods and tools. This comparative approach allowed for a nuanced exploration of the effectiveness, strengths, and limitations of various steganographic techniques.

Overall, the research methodology utilized a combination of literature review, primary sources, and critical analysis to provide a well-rounded understanding of steganography. By integrating insights from academic research and contemporary developments, this review paper aims to offer valuable insights into the complexities and applications of steganographic practices in modern information security contexts.

## 3. MODELING AND ANALYSIS

### I.WHAT IS STEGANOGRAPHY?

Steganography, in simple terms, is the art of hiding information in plain sight. It involves embedding a secret message within another seemingly innocuous object or communication, making it virtually undetectable to anyone not privy to its existence. However, for this clandestine method to work, the intended recipient typically needs to anticipate the receipt of a hidden message.[1]

Understanding steganography requires delving into its historical roots. Its origins trace back to ancient Greece, where the term itself finds its etymology.[1] Derived from the Greek words "steganos," meaning "covered or concealed," and "graphein," translating to "writing," steganography embodies the essence of concealing information within plain sight.[1]

An illustrative example from ancient times involves the Spartans, as documented by the Greek historian Herodotus. Spartan warriors employed steganography as a means to safeguard military intelligence from adversaries.[1] They would inscribe messages onto wooden tablets and coat them with wax, effectively concealing the content in case of interception by enemy forces.[1] The intended recipient could then scrape away the wax to reveal and decipher the hidden message, ensuring secure communication amidst the dangers of warfare.[1]

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

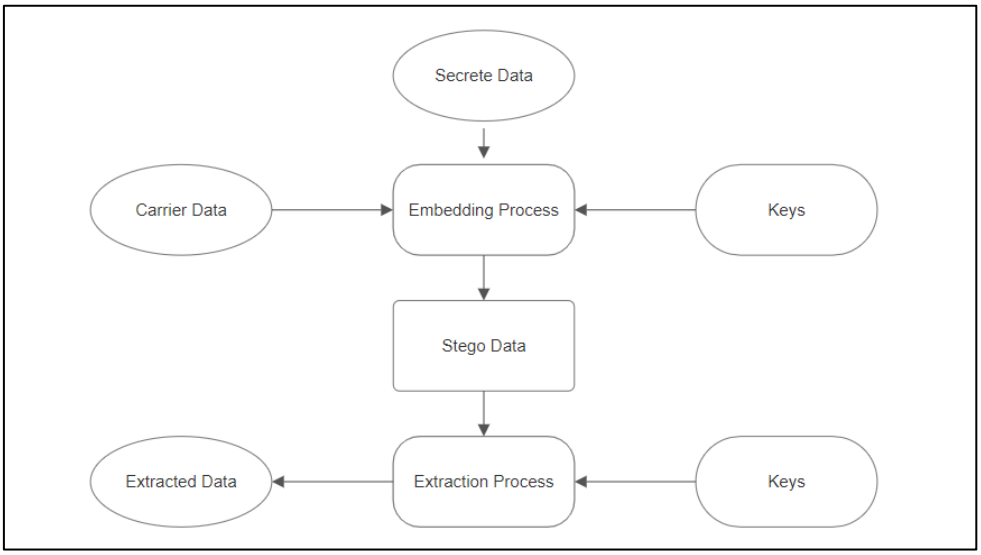


**Figure 1:** Steganography Process

**TYPES OF STEGANOGRAPHY**

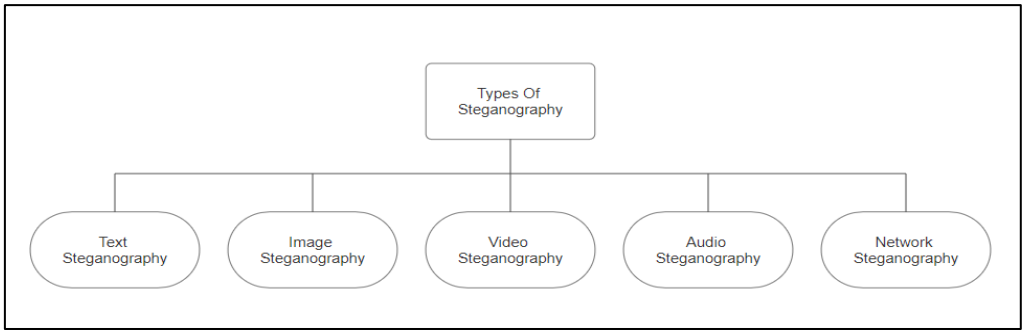


**Figure 2:** Types of Steganography

**A. Text Steganography:**

Text steganography conceals secret messages within plain text, employing techniques like whitespace manipulation, word substitution, and formatting adjustments. By embedding information in seemingly innocuous content, it prioritizes hiding the existence of a message over content secrecy. Additional methods include letter case alterations and metadata concealment. Detecting such covert communication is challenging due to subtle alterations, often necessitating advanced analysis tools. Text steganography serves diverse purposes, from espionage to digital watermarking, where discreet communication is essential. Its applications extend to secure data transmission and copyright protection, highlighting its significance in both clandestine operations and legitimate endeavours.

**B. Image Steganography:**

Image steganography involves concealing secret information within digital images. Unlike cryptography, which encrypts the message, steganography hides the message itself within the image, making it imperceptible to the human eye. Techniques include LSB (Least Significant Bit) insertion, where data is embedded in the least significant bits of the image pixels, and spread spectrum, which distributes the message across the entire frequency spectrum of the image. Detection of such hidden messages often requires specialized software and algorithms. Image steganography finds applications in covert communication, digital watermarking, and copyright protection, among other fields, where discreet data transmission is crucial.

**C. Video Steganography:**

Video steganography is the practice of concealing secret information within digital video files. Similar to image steganography, it aims to embed data within the video content without altering its perceptual quality significantly. Techniques for video steganography include LSB (Least Significant Bit) insertion, where data is hidden in the least significant bits of video frames, and spread spectrum methods, which distribute the information across the video's frequency spectrum. Detection of hidden messages within videos often requires sophisticated algorithms and tools capable of analyzing video frames and detecting subtle changes. Video steganography is utilized in applications such as covert communication, digital watermarking, and copyright protection, where discreet data embedding is essential.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

**D. Audio Steganography:**

Audio steganography involves hiding secret information within digital audio files. Unlike cryptography, which encrypts the message, steganography embeds the message within the audio content itself, making it imperceptible to the human ear. Techniques include LSB (Least Significant Bit) insertion, where data is concealed in the least significant bits of audio samples, and spread spectrum methods, which distribute the information across the frequency spectrum of the audio signal. Detecting hidden messages in audio files typically requires specialized software and algorithms capable of analysing audio samples and identifying subtle alterations. Audio steganography is used in applications such as covert communication, digital watermarking, and copyright protection, where discreet data transmission is essential.

**E. Network steganography:**

Network steganography involves concealing secret information within network communications, such as internet traffic or network protocols. Unlike encryption, which scrambles the message to make it unintelligible, steganography hides the very existence of the message within seemingly innocuous network traffic. Techniques include embedding data within unused fields of network packets, manipulating timing or packet size, or encoding information in seemingly random variations of packet headers. Detection of network steganography often requires advanced analysis tools capable of detecting patterns or anomalies in network traffic. This method finds application in covert communication, data exfiltration, and evasion of network security measures.

**TECHNIQUES USED IN STEGANOGRAPHY**

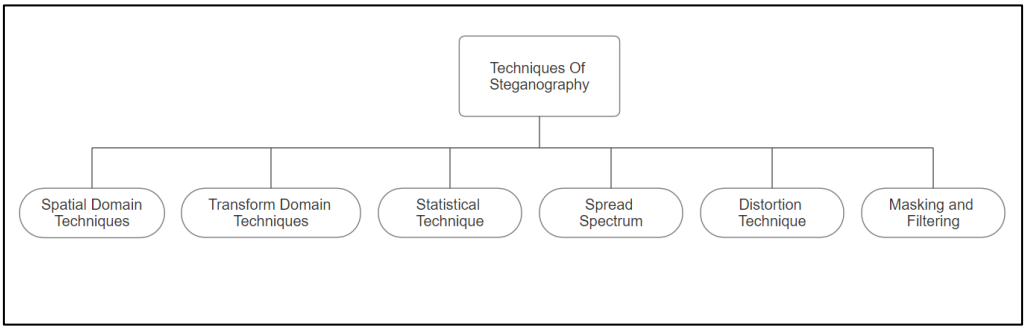


**Figure 3:** Techniques Of Steganography

**A. Spatial Domain Techniques:**

Spatial domain techniques in steganography involve directly manipulating the pixels of an image or the samples of an audio signal to embed hidden information. These techniques operate directly on the spatial representation of the cover media without transforming it into another domain, such as frequency or wavelet.

Common spatial domain techniques include:

1) **Least Significant Bit (LSB) insertion:**
   This method involves replacing the least significant bits of the cover media (such as image pixels or audio samples) with the bits of the secret message [2]. Since changes in the LSBs are often imperceptible to human senses, this method can embed a significant amount of data while minimizing noticeable degradation of the cover media.
2) **Random Pixel Manipulation:**
   Randomly altering the values of selected pixels in the cover image to encode the secret message. This method aims to minimize perceptual changes in the cover image while still providing space for data embedding.
3) **Pixel-Value Differencing (PVD):**
   PVD involves calculating the difference between adjacent pixel values and using these differences to encode the secret message [2]. By modifying the differences between neighboring pixels, this technique can hide information while maintaining the visual quality of the cover image.
4) **Spatial LSB Matching:**
   This technique modifies the LSBs of pixels in a way that ensures their values match those of neighboring pixels. By maintaining local statistical characteristics, spatial LSB matching can make the embedded data less detectable.

   Spatial domain techniques are relatively simple and efficient but may be vulnerable to detection by steganalysis algorithms. Balancing data embedding capacity with perceptual transparency is crucial to ensure that the hidden information remains undetectable to human observers while resisting detection by steganalysis techniques.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

**B. Transform Domain Techniques:**

Transform domain techniques in steganography involve manipulating the transformed representation of the cover media, such as the frequency domain or wavelet domain. These methods typically transform the cover media into a different domain where the embedding of hidden information can be performed more effectively or with less perceptual impact.

Common transform domain techniques include:

1) **Discrete Cosine Transform (DCT) Steganography:**
   This method applies the DCT to the cover image, breaking it down into frequency components [2]. The secret message is then embedded into the coefficients of the DCT, typically in the higher-frequency components where changes are less perceptible.
2) **Discrete Wavelet Transform (DWT) Steganography:**
   DWT decomposes the cover image into different frequency bands or scales. The secret message is embedded into the wavelet coefficients, often in the higher-frequency sub bands or in coefficients with lower perceptual significance.
3) **Fast Fourier Transform (FFT) Steganography:**
   FFT transforms the cover media into its frequency representation. Hidden information is embedded by modifying the magnitude or phase of the frequency components, aiming to minimize perceptual changes in the cover media.
4) **Quantization Index Modulation (QIM):**
   QIM modifies the quantization levels in transformed domains such as DCT or DWT to embed the secret message. This technique exploits the quantization process used in compression algorithms to hide information imperceptibly.

   Transform domain techniques offer advantages such as increased embedding capacity and improved resistance to steganalysis compared to spatial domain techniques. However, they may require more computational resources and may introduce perceptual distortions if not applied carefully. Balancing embedding capacity with perceptual transparency remains important to ensure the effectiveness of transform domain steganography.

**C. Statistical Technique:**

Statistical techniques in steganography subtly modify statistical properties of cover media to hide secret information. They analyse pixel or sample statistics to embed data in areas where changes are less noticeable. Some methods employ statistical models of cover media, while others use randomized embedding to increase complexity. Countermeasures may also be integrated to resist statistical steganalysis. These techniques require a deep understanding of cover media statistics and advanced algorithms to ensure hidden data remains undetectable. Balancing imperceptibility with robustness against steganalysis is key for their effectiveness

**D. Spread Spectrum:**

Spread spectrum techniques in steganography spread the hidden message across a wide frequency spectrum, making it difficult to detect. Methods like Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) modulate the secret information onto carrier signals using pseudo-random sequences or frequency hopping. Chirp Spread Spectrum (CSS) uses linearly changing frequencies. These techniques enhance resistance to interception and jamming but require sophisticated encoding and decoding algorithms. Balancing robustness against detection with computational complexity is crucial for effective spread spectrum steganography.

**E. Distortion Technique:**

Distortion techniques in steganography involve subtly altering the cover media to embed hidden information. These methods aim to introduce imperceptible changes to the cover media while ensuring that the hidden message remains concealed.

Common distortion techniques include:

1) **Perceptual Masking:**
   Exploiting characteristics of human perception to hide information by embedding it in regions where changes are less likely to be noticed. Perceptual masking takes advantage of limitations in human sensory perception to make alterations less detectable.
2) **Error Diffusion:**
   Propagating quantization errors from one pixel to neighboring pixels to hide information. This technique distributes the distortion caused by embedding across the cover media, making it less noticeable.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

**3) Noise Injection:**

Adding noise to the cover media to mask the embedded information. By introducing random variations, noise injection can obscure the presence of hidden data.

**4) Distortion Compensation:**

Adjusting other parts of the cover media to compensate for the distortion caused by embedding the hidden message. This technique aims to maintain the overall quality of the cover media while concealing the hidden information.

### F. Masking and Filtering:

Masking and filtering are techniques in steganography used to conceal hidden information within cover media by exploiting properties of human perception or by altering specific components of the media.

**1) Masking:**

In masking, the embedded information is hidden within areas of the cover media where changes are less likely to be detected by human senses. This technique leverages perceptual limitations, such as visual or auditory masking effects, to make alterations less noticeable. For example, in image steganography, the hidden data may be embedded in regions with high texture or complex patterns, where slight modifications are less likely to be perceived.

**2) Filtering:**

Filtering involves applying modifications to specific frequencies or components of the cover media to embed the hidden information. This can include techniques such as low-pass filtering, where high-frequency components are attenuated to make room for the embedded data. Filtering methods aim to ensure that the modifications introduced to the cover media are subtle and imperceptible to human observers.

Both masking and filtering techniques require careful consideration of perceptual characteristics and signal properties to ensure that the embedded information remains hidden while minimizing perceptual distortions in the cover media. Additionally, they may need to withstand detection by steganalysis techniques, which analyse statistical properties or anomalies in the cover media to detect the presence of hidden data.

## TOOLS USED FOR STEGANOGRAPHY

### A. Steghide:

Steghide serves as an accessible and user-friendly steganography tool suitable for beginners. Compatible with both Windows and Linux operating systems, it was developed by Stefan Hetzl in 2003 and has since found utility in Capture The Flag (CTF) competitions [6].

This tool operates by concealing fragments of a data file within the least significant bits of another file, rendering the presence of the hidden data undetectable and challenging to authenticate [6].

Offering portability and versatility, Steghide boasts a range of features, including the ability to conceal data within BMP, JPEG, WAV, and AU file formats [6]. Additionally, it supports blowfish encryption, employs MD5 hashing to convert passphrases into blowfish keys, and utilizes pseudo-random distribution techniques to embed hidden bits within container data [6].

### B. OpenPuff:

OpenPuff distinguishes itself as a premier steganography tool, offering unparalleled features not available in any other free or commercial software [10]. This professional-grade tool is not only 100% free but also tailored for the covert transmission of highly sensitive data [10]. Notable features include deniable steganography, carrier chains, and layers of security and obfuscation, ensuring robust protection for concealed information [10]. Moreover, OpenPuff supports multiple carrier formats, providing flexibility in data concealment methods. Its portability enhances convenience, and as freeware, it remains accessible to all users [10].

Key Highlights of OpenPuff:

**1) Deniable Steganography:**

OpenPuff incorporates deniable steganography, enabling users to conceal top-secret data using less sensitive information as a decoy, enhancing overall security.

**2) Carrier Chains:**

The tool employs carrier chains, splitting data across multiple carriers. Only the correct sequence of carriers allows for unhiding, providing an added layer of protection. Additionally, up to 256Mb of data can be hidden, given sufficient carriers, with the last carrier filled with random bits for indistinguishability.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1047-1054

3) **Supported Formats:**
OpenPuff supports a diverse range of carrier formats, including images, audios, videos, flash, and Adobe files, ensuring flexibility in data concealment across various media types.

4) **Layers of Security:**
Prior to carrier injection, data undergoes encryption, scrambling, whitening, and encoding, bolstering security measures and mitigating risks of unauthorized access.

5) **Portability and Freeware:**
OpenPuff is portable and ad-free, offering users the convenience of usage across different platforms without any cost implications. Additionally, it is open-source, relying on the libObfuscate system-independent library for enhanced security and transparency.

In essence, OpenPuff stands as a reliable and feature-rich steganography solution tailored for users seeking unparalleled levels of data concealment and security.

**C. OpenStego:**

OpenStego stands out as an open-source steganography tool revered for its capability to conceal information within a variety of file types, spanning images, audio, and video files [9]. Renowned among steganography enthusiasts for its intuitive interface and robust encryption support, it garners popularity owing to its user-friendly design and reliance on solid encryption algorithms [9].

Key Features of OpenStego:

1) **Diverse File Format Support:**
OpenStego accommodates multiple file formats for embedding and extracting hidden data, encompassing images, audio files, and video files.

2) **Advanced Encryption Capabilities:**
The software boasts advanced encryption techniques, including support for AES and Blowfish encryption algorithms, revered for their efficacy in safeguarding confidential data.

3) **Intuitive User Interface:**
OpenStego presents users with a user-friendly interface designed for seamless data hiding and extraction within files. Its intuitive layout ensures swift and straightforward navigation through the software.

4) **Command-Line Interface:**
In addition to its graphical user interface, OpenStego caters to advanced users with a command-line interface, offering flexibility for those who prefer command-line tools.

5) **Open-Source Nature:**
Being open-source, OpenStego is freely accessible to the public, enabling users to modify and tailor the software to their specific requirements, fostering a collaborative and adaptable environment.

**D. Xiao Steganography:**

Xiao Steganography emerges as a lightweight and freely available multi-platform software solution crafted specifically for concealing private files within BMP images or WAV files [8]. Its intuitive interface makes usage straightforward: users simply launch the program, import any BMP image or WAV file into the interface, and then incorporate the desired files for hiding [8]. Additionally, it offers encryption functionality, empowering users to select from a diverse array of encryption algorithms to enhance security and confidentiality [8].

**E. Binwalk:**

Binwalk is a specialized tool designed to scan binary images for embedded files and executable code, particularly within firmware packages [6]. It is tailored to identify various types of files and code integrated into firmware [6]. Compatibility with magic signatures designed for the Unix file utility is a notable feature of Binwalk, as it leverages the libmagic library for this purpose [6].

Moreover, Binwalk incorporates a dedicated magic signature file, enhancing its ability to detect commonly encountered files within firmware images. These may include compressed or archived files, firmware headers, Linux kernels, bootloaders, file systems, and more.

**F. ExifTool:**

ExifTool, a prominent application within the Kali Linux suite, empowers users to inspect and manipulate image metadata effortlessly [7]. With images carrying a wealth of information such as device details, ISO settings, timestamps, lens specifications, and flash configurations, ExifTool enables extraction and modification of this metadata seamlessly [7].

Renowned for its utility in generating steganographic challenges and facilitating open-source intelligence tasks, ExifTool finds widespread use among students and professionals engaged in Capture The Flag (CTF) competitions [7].

Notably, ExifTool offers advanced capabilities, including the embedding of command injection payloads into image files, expanding its utility beyond metadata manipulation [7].

Some noteworthy command features include:

1) Extracting GPS coordinates with "exiftool | grep GPS": This command reveals embedded GPS coordinates in image files, offering insights into the geographical origins of the image.
2) Extracting thumbnail images using "exiftool -ThumbnailImage >": This command facilitates the extraction of thumbnail images embedded within files, enabling users to access miniature representations of the original images.
3) Verbose mode activation with "exiftool -v": By appending [-v] to the exiftool command, users can access verbose mode, which provides comprehensive and detailed information about the processes being executed, enhancing transparency and insight into ExifTool's operations.

## 4. CONCLUSION

In conclusion, steganography, the art of covertly embedding information within seemingly innocuous data, has evolved into a sophisticated field crucial for digital security and communication. Rooted in ancient practices, modern steganography encompasses various techniques spanning text, image, video, audio, and network domains. Spatial and transform domain methods, statistical techniques, spread spectrum, distortion, and masking/filtration strategies offer diverse approaches to concealment. A plethora of tools such as Steghide, OpenPuff, OpenStego, Xiao Steganography, Binwalk, and ExifTool provide users with versatile capabilities, ranging from basic data hiding to advanced encryption and metadata manipulation. This review elucidates the rich tapestry of steganographic methodologies, emphasizing their significance in safeguarding sensitive information and enabling covert communication across digital mediums. As steganography continues to evolve, it remains an indispensable asset in the arsenal of modern information security practices.

## 5. REFERENCES

[1] Praveen, “A Guide to Steganography: Meaning, Types, Tools, & Techniques,” Cybersecurity Exchange, Mar. 27, 2024. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-steganography-guide-meaning-types-tools/

[2] H. Kaur, J. Rani, and CSE Department, GZSCCET Bathinda, Punjab, India, “A Survey on different techniques of steganography,” journal-article, 2016. doi: 10.1051/conf/2016.

[3] Prof. Sheela, Prof. Komal, and Prof. Sonali, “DIFFERENT TYPES AND TECHNIQUES OF STEGANOGRAPHY-REVIEW,” Mar. 2018. [Online]. Available: https://ijcrt.org/papers/IJCRT1802865.pdf

[4] A. Kolla, “List of 10 best steganography tools to hide Data,” Geek Dashboard, Jun. 11, 2020. https://www.geekdashboard.com/best-steganography-tools/

[5] A. Choudary, “Steganography Tutorial – a complete guide for beginners,” Edureka, Jun. 02, 2023. https://www.edureka.co/blog/steganography-tutorial

[6] L. T. Philip, “Best Tools for Steganography | Lipson Thomas | Medium,” Medium, May 26, 2023. [Online]. Available: https://lipsonthomas.medium.com/best-tools-for-steganography-9f74cf238973

[7] A. B. Vahab and A. B. Vahab, “Top 3 Steganography tools in 2024,” Wattlecorp, Dec. 08, 2023. https://www.wattlecorp.com/top-3-steganography-tools/

[8] C. Gong, J. Zhang, Y. Yang, X. Yi, X. Zhao, and Y. Ma, “Detecting fingerprints of audio steganography software,” Forensic Science International. Reports, vol. 2, p. 100075, Dec. 2020, doi: 10.1016/j.fsir.2020.100075.

[9] N. Siddhardha, “‘Unlocking the Secrets of Steganography: A Comprehensive guide to OpenStego.,’” Medium, Dec. 04, 2023. [Online]. Available: https://nandasiddhardha.medium.com/unlocking-the-secrets-of-steganography-a-comprehensive-guide-to-openstego-552a185154dd

[10] Darknet, “OpenPuff – professional steganography tool,” Darknet - Hacking Tools, Hacker News & Cyber Security, Sep. 02, 2017. https://www.darknet.org.uk/2017/07/openpuff-professional-steganography-tool/