ISSN (O) 2393-8021, ISSN (P) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⋇ Peer-reviewed & Refereed journal ⋇ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11795

# Social and Ethical Implications of Steganography: A case study Approach

**Yashaswini S[1], Dr Jasmine K S[2]**

PG Student, Master of Computer Applications, Rashtreeya Vidyalaya College of Engineering, Bengaluru- 560059[1]

Associate Professor, Department of Master of Computer Applications, Rashtreeya Vidyalaya College of Engineering, Bengaluru- 560059[2]

**Abstract:** Steganography, the ancient practice of concealing messages within other messages or media to avoid detection, has evolved significantly with advancements in technology. This paper explores the social and ethical implications of steganography, particularly in the digital age. Historically, steganography has been used for covert communication, from ancient Greece to World War II. In modern times, it has found applications in digital media, including images, audio files, and even software, raising concerns among governments and law enforcement agencies. The main ethical issue is to balance personal privacy and national security. While steganography can protect personal as well as sensitive information from being accessed illegally, malicious entities such as terrorists can also exploit it by trying to communicate undetected. This dual-use nature has led to debates on whether its use should be regulated or restricted. The paper also discusses the technical aspects of steganography, including various methods and tools used to embed and extract hidden information. Furthermore, it examines the potential consequences of misusing steganographic techniques, and the challenges faced by authorities in detecting and also preventing such misuse. Through a detailed analysis of historical and contemporary examples, the paper highlights the ongoing discussion on the benefits of steganography for personal privacy and the risks it poses to public safety. A case study on financial institution's client details is considered for the detailed analysis. The procedure follows a nuanced approach to regulation that considers both the ethical implications and practical challenges associated with steganography, advocating for continued research and development in detection/prevention techniques.

**Keywords:** Steganography, Ancient practice, Concealing messages, Covert communication, Digital age, Digital media, Personal privacy, Malicious entities, Embedding, Dual-use nature, Public safety, Nuanced regulation.

## I. INTRODUCTION

Steganography, derived from the Greek words "steganos" (covered) and "graphein" (writing), is the process of hiding the information within other non-secret text or data. This ancient technique dates back to at least the fifth century BCE, with the Greek historian Herodotus documenting early examples. In one instance, Demeratus used a wooden tablet coated with wax to send a hidden message warning Sparta of an impending Persian invasion. The message was concealed beneath the wax, allowing it to be transported without arousing suspicion. This early example underscores the aim of steganography: to avoid detection by hiding messages in plain sight.

In the digital age, steganography has evolved to utilize unused or insignificant areas of digital media files, such as images, audio recordings, and even software. By embedding secret information within these files, steganography enables covert communication over digital networks. For instance, an image of a space shuttle landing might conceal a private letter, or an audio recording might hide a company's confidential plans. The technique is also used in digital watermarking to protect intellectual property by embedding copyright marks within media files. The widespread availability of digital steganography tools has made it accessible to both individuals and organizations, raising important social and ethical questions.

The resurgence of interest in steganography is partly due to the increased media attention following events of 9/11 attacks. Concerns have been raised about the potential use of steganography by terrorists and other malicious actors to evade detection by law enforcement agencies.

This has led to a debate similar to that surrounding the use of strong encryption technologies, which balance personal privacy against national security interests. While encryption protects the content of a message, it fails to hide the evidence of the communication itself. Whereas Steganography hides the evidence of a message being sent, adding an additional layer of secrecy. This paper aims to explore the social and ethical implications of this powerful technique in today's interconnected world.

DOI: 10.17148/IARJSET.2024.11795

## II. BACKGROUND

Steganography is historically used in multiple forms across different civilizations. One amongst the earliest recorded uses was by the Greek tyrant Histiaeus, who sent a private message tattooed on a slave's scalp to his son-in-law. Ancient Romans used invisible ink made from substances like fruit juices and milk, which would become visible when heated. During World War II, steganography saw significant advancements with the invention of microdot technology, described by FBI Director J. Edgar Hoover as "the enemy's masterpiece of espionage." Microdots were tiny photographs capable of holding extensive data, cleverly disguised as periods in typed documents. These historical instances illustrate the continuous evolution of steganography technique to meet the demands of covert communication.

Regarding digital technology, steganography has expanded its reach and capabilities. Digital steganography involves embedding information inside various means of digital media, such as images (JPEG, PNG), audio files (MP3, WAV), and even video files. A common approach is to modify the least significant bits (LSB) of pixel values in an image, a technique that is imperceptible to the human eye but can carry significant amounts of hidden data. This method has been employed for various purposes, from personal privacy protection to intellectual property management. Digital watermarking, a form of steganography, is used to embed copyright information within digital media, helping to prevent unauthorized copying and distribution. The ethical and social implications of steganography are profound and multifaceted. On one hand, it is a vital tool for protecting personal privacy and ensuring secure communication in an age where digital surveillance is pervasive, it also presents significant challenges for law enforcement and national security agencies. The ability to hide information within innocuous-looking files makes it difficult to detect and intercept communications that could pose threats to public safety. This dual-use nature of steganography has led to calls for regulation and control, though such measures are often met with resistance from privacy advocates and technologists who argue that restrictions could stifle innovation and infringe on individual rights.

## III. LITERATURE REVIEW

This literature review explores the historical evolution of steganography, examining its methods and applications from old times till the present digital age. The study shows development and significance of steganography in secure communication, analyzing key techniques and their impact on modern security systems.

### A. Historical Advancement of Steganography

Steganography, the art of hiding information to prevent the theft of hidden messages, uses methods like invisible inks, microdots, and digital signatures. Combining steganography with encryption enhances security by making hidden messages less detectable [1]. Since ancient Greece, steganography has involved embedding information within other data like hiding messages in company logos within emails. The main point here is to conceal information with minimal distortion, and the study discusses challenges and directions of future for improving security and invisibility [2]. Digital image mode steganography enables protected communication in modern applications, driven by advancements in power to process data and security awareness. Recent techniques and tools are reviewed, with a focus on deep learning-based methods and future research directions [3]. Historical roots of steganography include messages hidden within a hare’s body or tattooed on shaved heads, as recorded by Herodotus. The term "covered writing" reflects various innovative methods used throughout history to ensure secure communication [4]. This literature survey demonstrates the growth of steganography from ancient techniques to advanced digital methods, underscoring its crucial role in secure communication and highlighting notable challenges and advancements in the field [1-4].

### B. Comparison between different Steganographic Techniques

Steganography, referred to as the technique of hiding critical data in transmission medium, focusing on digital images as transmission carriers. This study compares the individual performance of common steganographic tools, emphasizing visual inspection and statistical comparison methods as key performance metrics [5]. The review covers different steganography techniques for information suppression, highlighting the need to concealing communications to improve data security. Image steganography, emphasized for its ability to hide critical information inside of images provides a higher-level security during data transfer [6]. With the increasing dependency upon internet and smart devices, data security is a critical concern. Image steganography, especially with JPEG images, offers a robust solution by hiding data where alterations are nearly undetectable, thus ensuring undetectability, robustness, and embedding storage capacity [7]. Furthermore, this study evaluates five different audio steganography techniques on Turkish audio recordings, highlighting the effectiveness of least significant bit technique (LSB) in maintaining high signal-to-noise ratios (SNR) and emphasizing the human auditory system's inability to notice hidden messages [8]. The comparison of steganographic techniques provides insights into their effectiveness and challenges, contributing to the creation of more secure and efficient methods [5-8].

DOI: 10.17148/IARJSET.2024.11795

### C. Steganography and Cryptography: Dual-Use for Enhanced Security

In today's digital age sophisticated data security measures is paramount. Cryptography encrypts messages to safeguard data, while steganography hides the data inside another medium to facilitate covert communication. Combining these techniques with advancements in AI, such as Generative Adversarial Networks (GANs), offers a comprehensive security system that enhances both privacy and integrity of information [9]. Encryption technology plays the main role in guaranteeing the privacy of electronic communications, protecting against various threats like hacking and industrial espionage. Despite challenges in controlling the export of encryption technology, powerful encryption products remain widely available and needed for maintaining data security [10]. The rise of cryptology during the European Renaissance marked significant advancements in cryptographic methods, influenced by historical developments and the rediscovery of classical techniques [11]. In the context of synthetic DNA sequences, DNA watermarks combined with error correction and encryption protocols ensure the authenticity and secure communication of synthetic DNA, highlighting the absolute need for digital signatures for public verification and traceability [12]. The dual-use of steganography and cryptography presents a robust solution for modern data security challenges [9-12].

### D. Challenges and Solutions in Steganalysis

This section investigates the main effects of pretraining Convolutional Neural Networks (CNNs) on their performance in steganalysis of digital images. Pretraining on large image datasets aids network convergence and enhances performance in steganalysis, even with unrelated pretraining tasks [13]. Contemporary steganalysis faces challenges due to new steganographic rich feature sets, which are powerful for supervised classification but less effective for unsupervised universal steganalysis. This study proposes feature extraction algorithms to improve performance, focusing on linear projections sensitive to stego content [14]. The historical context of digital steganography is rooted in the prisoners' problem, illustrating the importance for inconspicuous communication to avoid detection by monitors [15]. Forensic steganalysis offers a deeper insight into hidden messages beyond traditional binary steganalysis, identifying the steganographic algorithm used, estimating message length, and determining the stego key. This comprehensive review of forensic techniques highlights the need of advanced methods for digital image steganalysis and identifies future research areas to enhance steganalyzer capabilities [16]. The section on challenges and solutions in steganalysis addresses key issues and advancements in domain [13-16].

## IV. METHODOLOGY

In the realm of digital communication, steganography offers a sophisticated method for concealing information within various types of media. The following sections detail the critical steps in implementing steganography, from choosing the right medium to the final extraction of the hidden message. Each step plays a much needed in ensuring that information remains hidden and secure, providing a comprehensive guide to this intricate process.

### A. Understanding the Medium

The first step in employing steganography is to select an appropriate cover medium. This can be any digital file with enough redundant or insignificant data to hide the secret message without noticeable alterations. Common choices include images, audio files, and videos due to their large size and complexity. For example, digital images in formats like JPEG or PNG are particularly popular because of the abundance of pixel data that can be subtly modified without noticeable visual differences. Audio files, like MP3s, also offer vast amounts of data where slight alterations can go unnoticed by human ears. Videos, combining both audio and visual data, provide even more opportunities for hiding information which in turn makes them idealistic for more substantial or complex secret messages. Understanding the features of the chosen medium is crucial, as it determines the methods used for embedding and the robustness of the steganographic process.

### B. Embedding the Message

Once the cover medium is selected, embedding the secret message is the next step. This is typically done by altering the least significant bits of the data in cover medium. For instance considering an image file, the least significant bit of each pixel's color value can be modified to encode the message. This method, known as LSB steganography, ensures that changes are minimal and do not significantly alter the appearance of the image. Advanced techniques might involve manipulating more complex data structures within the medium, such as altering frequency components in audio files or specific frames in video files. The goal aims at making sure that the hidden message is imperceptible to human senses while being reliably retrievable by the intended recipient.

### C. Encryption (Optional)

To enhance security, the hidden message can be encrypted before embedding it inside the selected cover medium. This adds an additional layer of protection, ensuring that even if the hidden message is to be detected, it cannot be easily deciphered without the encryption key.

DOI: 10.17148/IARJSET.2024.11795

Encryption transforms the message to a format that is unreadable to unauthorized parties, making it much harder for an adversary to extract meaningful information. Common encryption algorithms, such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), can be made use to encrypt the message in its pre-embedded stage. This dual approach of encryption and steganography provides robust security, as it requires the interceptor to detect and break the encryption which is a significantly more challenging task.

### D. Transmission

After embedding the message, the modified cover object can be transmitted to the intended recipient. This may be done via various channels like email, file-sharing services, or social media platforms. The key is to ensure that the transmission method does not raise suspicion. For example, an image containing a hidden message can be uploaded to a photo-sharing site or sent as an attachment in an email. Using common and unsuspicious channels for transmission is crucial, as it reduces the likelihood of the medium being flagged for further scrutiny. Additionally, ensuring the cover medium blends seamlessly with regular content shared over these channels helps maintain the secrecy of the steganographic communication.

### E. Extraction

The final step is the extraction of the hidden message by the recipient. Using the appropriate steganographic software or algorithm, the recipient can extract the least significant bits from the cover medium to reconstruct the original secret message. The extraction process is essentially the reverse of the embedding process, where the hidden bits are identified and combined to reveal the message. If encryption was used, the extracted message must also be decrypted. This step requires the recipient to hold the necessary decryption key and knowledge of the encryption algorithm used. The accuracy of the extraction process depends on the robustness of the embedding method and the quality of the cover medium's transmission, ensuring that the hidden message remains intact and decipherable.

## V. IMPLEMENTATION

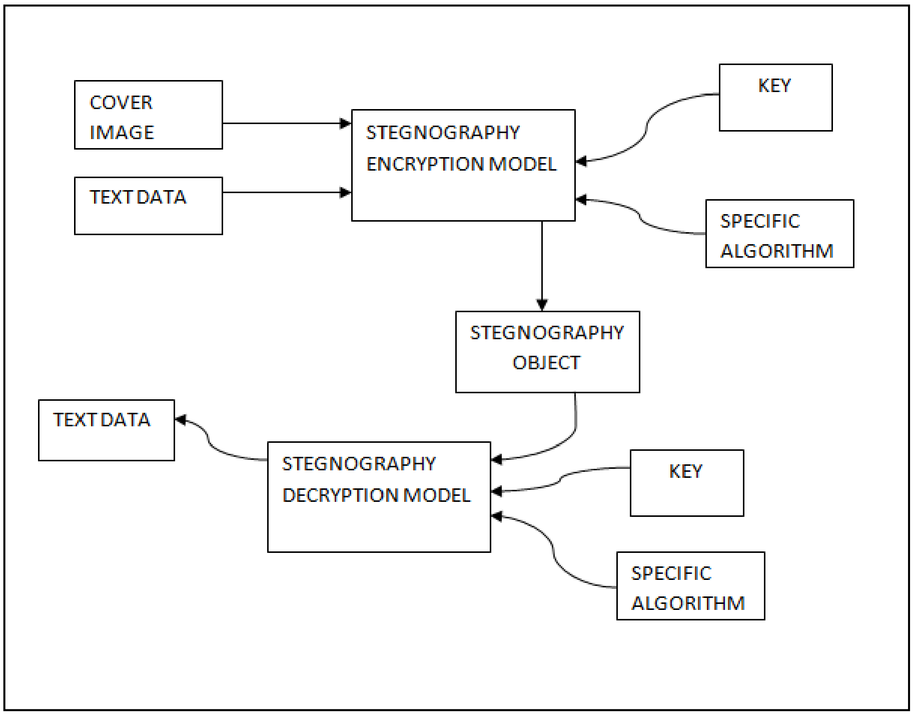


Fig. 1 Steganography Encryption and Decryption Process Flow

Fig. 1 illustrates the steganography process, highlighting how text data is embedded and extracted from a cover image. Initially, the cover image as well as text data acts as input to the Steganography Encryption Model, which utilizes a specific algorithm and a key to embed the hidden message. This encryption model modifies the cover image in order to create a Steganography Object that visually resembles the original image but contains the concealed text data. The steganography object can then be transmitted or stored discreetly, as it appears to be a regular image file. For extraction, the Steganography Object is fed into the Steganography Decryption Model, which also requires the same key and

DOI: 10.17148/IARJSET.2024.11795

algorithm used during encryption. This model deciphers the hidden text from steganography object, effectively reversing the embedding process. The final output is the original text data, now accessible to the intended recipient. Fig. 1 emphasizes the critical role of key and algorithm in maintaining security and integrity of the hidden message which ensures that critical information is securely embedded within and retrieved from digital media without detection by unauthorized parties.

In the modern digital age, critical sectors such as financial institutions require secure methods to send sensitive information, such as transaction details and confidential client data. Steganography technique has evolved to utilize various types of digital objects to covertly transmit this information without arousing suspicion. This technique involves embedding a hidden message inside of a seemingly innocuous file, such as image or audio file, making it an effective method for securing communication in the financial sector. Use case Considered: financial institution implemented steganography using the open-source software OpenStego v0.8.6 to securely transmit confidential client data.

A. Selecting the Cover Object

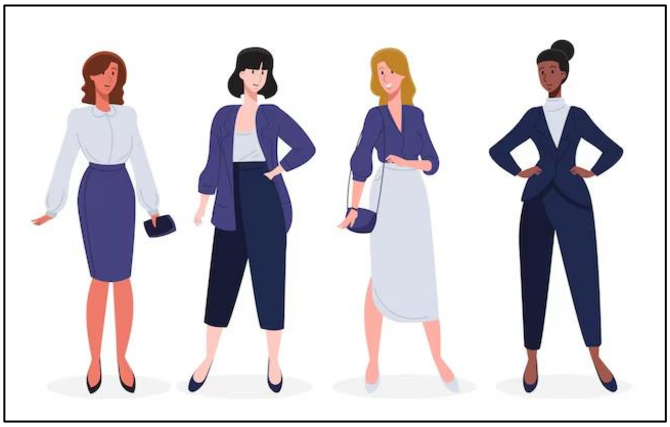
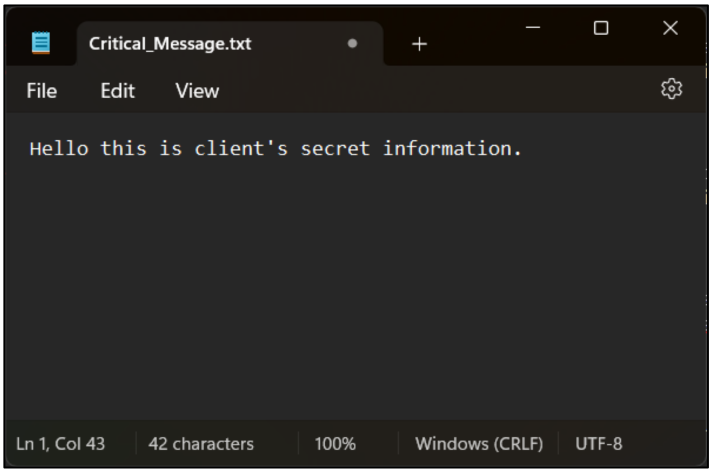


Fig. 2 Image as the cover object

You begin by selecting an appropriate cover medium. A high-resolution image as shown in Fig.2 is chose from the institution's promotional materials, knowing that its complexity and size provide ample space for hiding data. The image, depicting an organic flat business people collection, appears innocuous and will not arouse suspicion. This choice is critical, as it ensures the undetectability of steganographic steps.

B. Embedding the Critical Secret Message



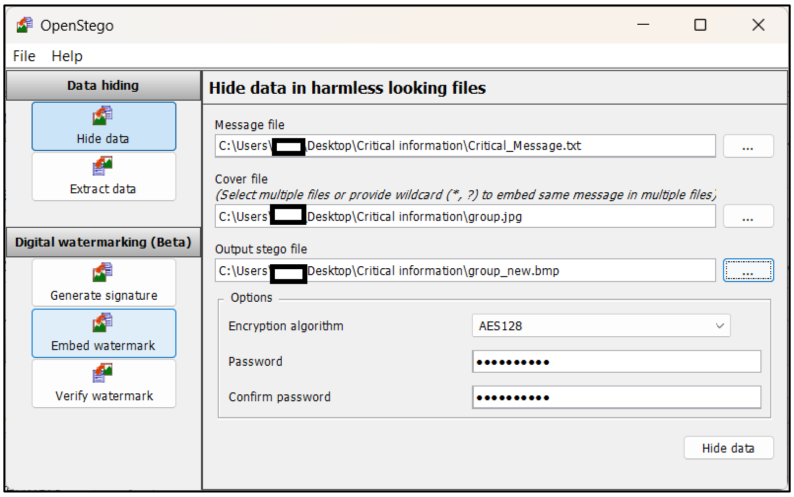
```
Hello this is client's secret information.
```

Fig. 3 Confidential client data

With the cover object ready, you use OpenStego to embed the confidential client data stored in a text file, as shown in Fig. 3, within the image. Meticulously, you alter least significant bit of each pixel's color value to encode the sensitive information. OpenStego’s user-friendly interface and advanced algorithms make this process efficient and secure, preserving the visual integrity of the image. To anyone else, it remains a normal picture, but to you, it now carries a hidden payload.

DOI: 10.17148/IARJSET.2024.11795

C. Encryption of the Critical Secret Message



Hide data in harmless looking files

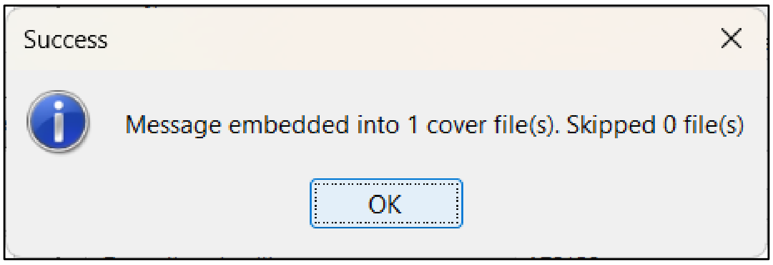
Message file
C:\Users\[redacted]Desktop\Critical information\Critical_Message.txt

Cover file
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
C:\Users\[redacted]Desktop\Critical information\group.jpg

Output stego file
C:\Users\[redacted]Desktop\Critical information\group_new.bmp

Options
Encryption algorithm: AES128
Password: ●●●●●●●●●●
Confirm password: ●●●●●●●●●●

Fig. 4 Embedding the AES128 encrypted hidden message inside image using OpenStego



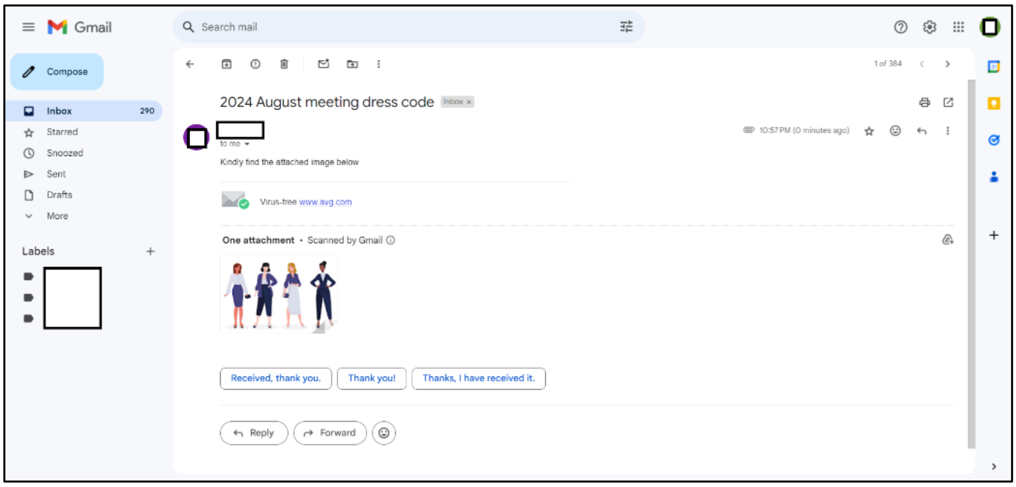
Success

Message embedded into 1 cover file(s). Skipped 0 file(s)

Fig. 5 Confirmation pop-up after embedding is completed

To enhance the secrecy of hidden message, OpenStego allows you to set a password before embedding the data. This step transforms the information into an unreadable format without the correct password. It uses Advanced Encryption Standard (AES) encryption algorithm with 128-bit and 256-bit encryption as shown in Fig. 4 This ensures that even if hidden message is detected, it cannot be easily deciphered. OpenStego's integration of this feature simplifies the encryption process, making it straightforward and effective.

D. Transmitting the Steganographic Object



2024 August meeting dress code

[redacted]
to me
10:57 PM (0 minutes ago)

Kindly find the attached image below

Virus-free www.avg.com

One attachment • Scanned by Gmail

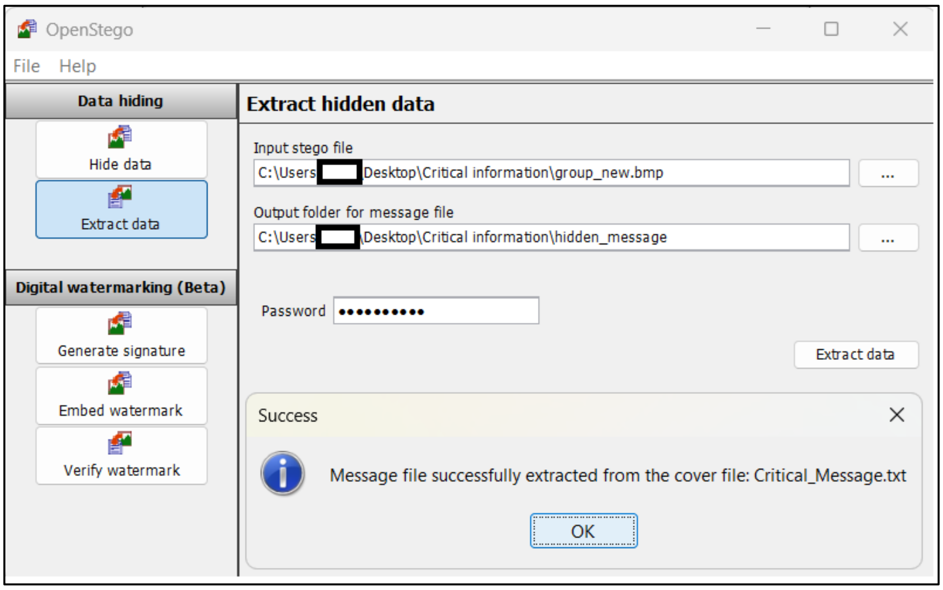
[redacted]

Fig. 6 Steganographic object sent to the intended receiver through an email service

DOI: 10.17148/IARJSET.2024.11795

You then prepare to send the steganographic object – the image with embedded, encrypted client data. Opting for secure email services, you embed the image in a regular business communication. The transmission is successful if the image appears as a routine attachment, raising no alarms. You also ensure the email is sent over an encrypted connection, adding another layer of protection during transit.

E. Extraction and Decryption of Critical Hidden Message



Extract hidden data

Input stego file
C:\Users[redacted]Desktop\Critical information\group_new.bmp

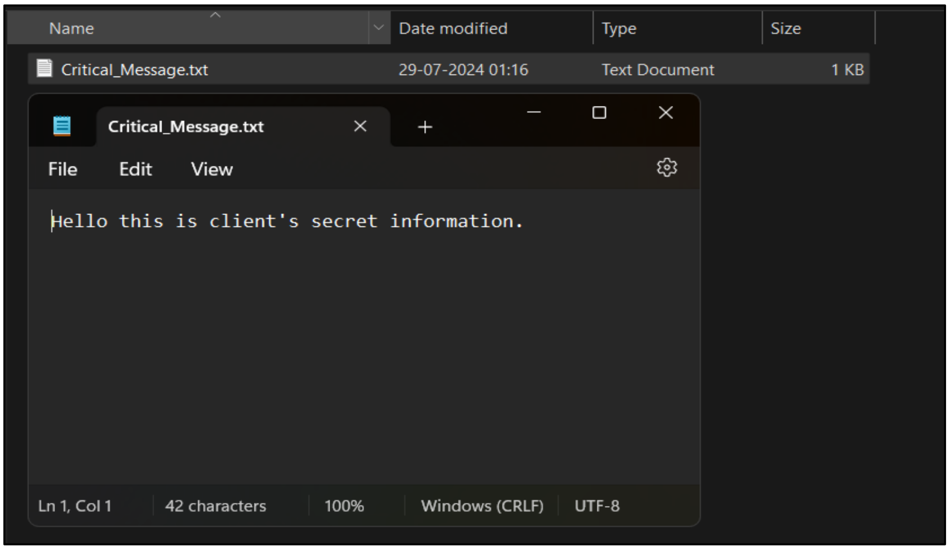
Output folder for message file
C:\Users[redacted]Desktop\Critical information\hidden_message

Password ••••••••••

Success

Message file successfully extracted from the cover file: Critical_Message.txt

Fig. 7 Extracting the hidden text from the Steganographic object after receiving it



| Name | Date modified | Type | Size |
|---|---|---|---|
| Critical_Message.txt | 29-07-2024 01:16 | Text Document | 1 KB |

Critical_Message.txt

```
Hello this is client's secret information.
```

Ln 1, Col 1 | 42 characters | 100% | Windows (CRLF) | UTF-8

Fig. 8 The extracted text file from the Steganographic object

Upon receiving the email, the cybersecurity officer at the branch office, follows the protocol to extract and decrypt the critical hidden message.

Using OpenStego, he retrieves least significant bits from the image, reconstructing the encrypted client data as shown in Fig. 7 With the correct password, he decrypts the information, restoring it to its original, readable format as shown in Fig. 8 The entire process is smooth and secure, ensuring that the confidential client data remains protected throughout its journey.

DOI: 10.17148/IARJSET.2024.11795

## VI. CONCLUSION

The dual-use nature of steganography presents a significant ethical dilemma that requires a nuanced approach. On one hand, steganography offers a powerful tool for protecting personal privacy and securing sensitive information. This is particularly important in an era where data breaches and unauthorized access to personal data are rampant. Individuals and organizations can utilize steganography to ensure their communications remain confidential, enhancing overall security. However, the same technology can be misused by malicious entities, such as terrorists, to coordinate activities without detection, posing a substantial threat to national security.

The challenges faced by law enforcement agencies in detecting and preventing the misuse of steganography are formidable. Traditional surveillance and monitoring techniques are often inadequate in identifying hidden messages embedded within seemingly innocuous media. The sophistication of modern steganographic methods further complicates detection efforts. Hence, there is an urgent need for ongoing research/development in advanced detection techniques. This will require collaboration between technologists, policymakers, and law enforcement agencies to develop effective countermeasures without infringing on personal privacy rights.

Ultimately, addressing the ethical implications of steganography requires a balanced regulatory approach. Overly restrictive regulations could stifle legitimate uses and innovation, while insufficient oversight could leave societies vulnerable to the risks associated with undetectable communication by malicious actors. Policymakers must consider both the benefits and risks, crafting regulations that protect public safety while respecting individual privacy. Continued dialogue and cooperation among stakeholders are required to navigate the complex landscape of steganography, ensuring that its potential for good is maximized while mitigating its potential for harm.

## REFERENCES

[1] Amirtharajan, Rengarajan and John Bosco Balaguru Rayappan. “Steganography-Time to Time: A Review.” *Research Journal of Information Technology* 5 (2013): 53-66.

[2] Abdul-wahab, Shams N., Mostafa Abdulghafoor Mohammed, and Omar A. Hammood. "Theoretical Background of steganography." *Mesopotamian Journal of CyberSecurity* 2021 (2021): 22-32.

[3] Mandal, Pratap Chandra, Imon Mukherjee, Goutam Paul, and B. N. Chatterji. "Digital image steganography: A literature survey." *Information sciences* 609 (2022*)*: 1451-1488.

[4] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "A comparative analysis of steganographic tools." *In Proceedings of the Seventh IT&T Conference. Institute of Technology Blanchardstown, Dublin, Ireland. 25th*, pp. 29-37. 2007.

[5] Arora, Himanshu, Cheshta Bansal, and Sunny Dagar. "Comparative study of image steganography techniques." *In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN),* pp. 982-985. IEEE, 2018.

[6] Watni, Dipti, and Sonal Chawla. "A comparative evaluation of jpeg steganography." *In 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 36-40. IEEE, 2019.

[7] Aslantaş, Funda, and Cemal Hanilçi. "Comparative Analysis of Audio Steganography Methods." *Journal of Innovative Science and Engineering* 6, no. 1 (2022): 122-137.

[8] Maiti, Anamitra, Subham Laha, Rishav Upadhaya, Soumyajit Biswas, Vikas Choudhary, Biplab Kar, Nikhil Kumar, and Jaydip Sen. "Boosting Digital Safeguards: Blending Cryptography and Steganography." *arXiv preprint arXiv:2404.05985* (2024).

[9] Strasser, Gerhard F. "The rise of cryptology in the European Renaissance." *In The History of Information Security*, pp. 277-325. Elsevier Science BV, 2007.

[10] Berezin, Casey-Tyler, Samuel Peccoud, Diptendu M. Kar, and Jean Peccoud. "Cryptographic approaches to authenticating synthetic DNA sequences." *Trends in Biotechnology* (2024).

[11] Butora, Jan, Yassine Yousfi, and Jessica Fridrich. "How to pretrain for steganalysis." *In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security*, pp. 143-148. 2021.

[12] Pevný, Tomáš, and Andrew D. Ker. "The challenges of rich features in universal steganalysis." *In Media Watermarking, Security, and Forensics* 2013, vol. 8665, pp. 203-217. SPIE, 2013.

[13] Böhme, Rainer, and Rainer Böhme. "Principles of modern steganography and steganalysis." *Advanced Statistical Steganalysis* (2010): 11-77.

[14] Chutani, Shaveta, and Anjali Goyal. "A review of forensic approaches to digital image Steganalysis." *Multimedia Tools and Applications* 78, no. 13 (2019): 18169-18204.

DOI: 10.17148/IARJSET.2024.11795

[15] Bateman, Philip, and Hans Georg Schaathun. "Image steganography and steganalysis." *Department Of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom,* 4th August (2008).

[16] Rafat, Khan Farhan, and Muhammad Junaid Hussain. "Secure steganography for digital images." *International Journal of Advanced Computer Science and Applications* 7, no. 6 (2016): 45-59.

[17] Hassaballah, M., Mohamed Abdel Hameed, and Monagi H. Alkinani. "Introduction to digital image steganography." *In Digital Media Steganography*, pp. 1-15. Academic Press, 2020.

[18] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." *Signal processing* 90, no. 3 (2010): 727-752.

[19] Abduallah, Wafaa Mustafa, and Abdul Monem S. Rahma. "A review on steganography techniques." *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)* 24, no. 1 (2016): 131-150.

[20] Oolo, Egle, and Andra Siibak. "Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 7, no. 1 (2013): 7.

[21] Nicolás-Sánchez, Alejandro, and Francisco J. Castro-Toledo. "Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective." *Crime Science* 13, no. 1 (2024): 11.

[22] Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6, no. 3 (2012): 168-187.

[23] Artz, D., 2001. "Digital steganography: hiding data within data." *IEEE Internet computing*, 5(3), pp.75-80.

[24] Nicolás-Sánchez, Alejandro, and Francisco J. Castro-Toledo. "Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective." *Crime Science* 13.1 (2024): 11.

[25] Haji, Mohammed Suliman, et al. "A Survey on Digital Image Steganography and Steganalysis." *Journal of Computational and Theoretical Nanoscience* 17.7 (2020): 3256-3263.

[26] Balogun, Aishat. "Cybersecurity: Introduction to Steganography." *Journal of Technology-Integrated Lessons and Teaching* 1.2 (2022): 18-23.