Mini Project Report on



**Encryption and Decryption Using Digital Cryptography in Files**



Submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY IN

COMPUTER SCIENCE & ENGINEERING

Submitted by:

Student Name: SHRUTI AGARWAL University Roll No.2021456

***Under the Mentorship of* Mrs. Neha Tripathi**

**Assistant Professor**

****

Department of Computer Science and Engineering Graphic Era (Deemed to be University)

Dehradun, Uttarakhand January-2025



## CANDIDATE’S DECLARATION

I hereby certify that the work which is being presented in the project report entitled “Encryption and Decryption Using Digital Cryptography in Files”in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering of the Graphic Era (Deemed to be University), Dehradun shall be carried out by the under the mentorship of Mrs. Neha Tripathi, Assistant Professor, Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun.

Name: Shruti Agarwal University Roll no:2021456

# Table of Contents

**Chapter No. Description Page No.**

Chapter 1 Introduction 01-03

Chapter 2 Literature Survey 04-06

Chapter 3 Methodology 07-09

Chapter 4 Result and Discussion 10

Chapter 5 Conclusion and future work 11-12

References 13

# CHAPTER 1

# Introduction

**1.1 Definition and History**

**What is Steganography?**

Steganography is the art of hiding information within other non-suspicious data, such as images, audio, or even text, in a way that prevents detection. Unlike encryption, where the existence of the message is obvious, steganography aims to keep the presence of the hidden message secret.

In the modern world, steganography is mostly associated with digital files, especially images and videos, where small modifications to file attributes can encode hidden messages.

**History of Steganography**

The term "steganography" comes from the Greek words *steganos* (meaning "covered" or "hidden") and *graphein* (meaning "to write").

Historically, it has been used for centuries, from ancient Greek methods of hidden writing on wax tablets to more complex methods in the digital era.

The earliest documented use was during ancient Greece, where hidden messages were written on the back of wooden tablets, which were then covered with wax. Another famous example is from World War II, where hidden messages were encoded in microdots, invisible ink, and even in the ink of ordinary letters.

**1.2 Importance in Data Security**

**Confidential Communication**

Steganography allows for confidential communication without the risk of interception, making it a valuable tool in situations where privacy is crucial.

Unlike encryption, which might attract attention due to the encrypted data's existence, steganography ensures that the message remains hidden within plain sight.

**Use in the Modern Digital World**

With the rise of digital communication and information exchange, the need for secure data hiding techniques has grown. Steganography provides a solution for protecting sensitive information, such as intellectual property, personal data, and government communications.

It is used in a variety of applications, including watermarking, copyright protection, and even as a tool for secure communication in authoritarian regimes.

**1.3 Types of Steganography**

**Image Steganography**

This is the most common form of steganography in the digital world. It involves hiding messages within the pixel data of an image. The least significant bit (LSB) of each pixel is often altered to encode the message, ensuring that the changes are invisible to the human eye.

Image steganography is widely used due to the ease of embedding and extracting messages, as well as the wide availability of image files.

**Audio Steganography**

Similar to image-based steganography, audio steganography hides messages within sound files. It can involve altering the least significant bits in the audio file or embedding data in the frequencies that are inaudible to humans.

It is often used for hiding data in a way that ensures the audio quality remains unaffected to the human ear.

**Video Steganography**

Video files can carry both audio and visual steganographic content, making it a potent medium for hiding information.

Data can be embedded into individual frames of the video or in the sound layer, offering a more complex and secure method of communication.

**Text Steganography**

Text steganography involves hiding data within text files, using techniques like altering the spacing between words, using synonyms, or encoding information within the structure of the text.

Though less common than image-based methods, it can still serve as a simple form of data hiding in environments where images and audio files are not feasible.

**Network Steganography**

This involves hiding data within network protocols, making it harder for third parties to detect any hidden information during transmission. For example, data can be hidden in the header of network packets.

**1.4 Applications in Digital Communication and Media**

**Secure Communication**

One of the main applications of steganography is in secure communication, especially in high-risk environments where the confidentiality of information is paramount.

It allows users to exchange messages without the risk of interception, as no encryption or suspicious files are involved.

**Watermarking**

Steganography plays a role in digital watermarking, where information (e.g., copyright data or ownership) is embedded in media files such as images, videos, and audio.

This ensures that digital media cannot be copied or distributed without proper attribution.

**Digital Forensics**

In digital forensics, steganography is used to uncover hidden information in digital files during investigations. Detecting steganography can help law enforcement agencies find crucial evidence, especially in cybercrime cases.

**Copyright Protection**

Steganography can be used to protect intellectual property. Hidden messages in media files can assert ownership and prevent unauthorized distribution of digital content.

**1.5 Evolution of Steganography in the Digital Age**

**From Ancient to Modern Times**

Steganography techniques have evolved significantly with advances in technology. The move from manual methods like hidden ink or physical objects to digital systems has allowed for more sophisticated forms of data hiding.

**Steganography in the Internet Age**

With the advent of the internet, steganography has become more prevalent, especially in online communications. Digital files, including images, videos, and sound recordings, are prime candidates for embedding hidden information.

Modern tools allow for easier embedding and extraction of hidden messages, and steganography is now widely used in everything from social media to secure government communications.

# CHAPTER 2

# Literature Survey

**2.1 Secure Communication**

**Confidential Messaging**

Steganography is frequently used for secure communication between individuals or groups who need to keep their messages private. It allows messages to be hidden within seemingly innocuous files, making it difficult for adversaries to detect the communication.

This method is particularly useful in environments with high surveillance or in authoritarian regimes where censorship and interception of communication are a concern.

**Government and Military Use**

Governments and military organizations often employ steganography to send classified or sensitive information securely. The hidden messages can be embedded in innocuous-looking documents, images, or audio files, thus preventing detection by adversaries or surveillance agencies.

For example, a photo shared through social media could secretly contain critical intelligence, all while appearing to be just a normal image to the public.

**2.2 Digital Watermarking**

**Copyright Protection**

Steganography plays a crucial role in digital watermarking, which is used to protect intellectual property such as photographs, videos, music, and software. A digital watermark is a form of steganography where a copyright or ownership mark is embedded into the file, allowing the rightful owner to claim ownership.

Unlike visible watermarks that are overtly displayed on images or videos, digital watermarks can be hidden within the file and remain undetectable without specific software or tools.

These watermarks are often used by artists, content creators, and businesses to track unauthorized copies of their digital assets.

**Broadcast Monitoring and Anti-Piracy**

Digital watermarking is also widely used by broadcasters and streaming services to protect content from piracy. Watermarks can be used to track the source of illegal copies and help identify the point of leakage.

For example, a video streaming service might embed a unique identifier in every stream of their content. If the video is pirated, the watermark can trace the source of the leak.

**2.3 Digital Forensics and Evidence Preservation**

**Forensic Investigation**

In digital forensics, steganography can be used to hide evidence or protect the integrity of files during investigations. Law enforcement agencies use steganography to preserve data without altering it, ensuring its admissibility in court.

Investigators may use steganography to embed important metadata or forensic evidence within digital files, such as images or documents, which can be crucial for proving the authenticity of evidence in legal cases.

**Tracking and Identifying Criminals**

In some cases, criminals might use steganography to hide illicit messages or instructions, and forensic experts can use steganalysis to uncover these hidden communications. The ability to detect hidden data can assist in criminal investigations by revealing important clues that would otherwise remain concealed.

**2.4 Data Integrity and Authentication**

**Message Authentication**

Steganography is used to embed a unique authentication code within digital files to verify their integrity. This helps in confirming that the data has not been tampered with during transmission. For instance, an image or document might contain a hidden signature that verifies its origin and authenticity.

**Data Fingerprinting**

Data fingerprinting is a technique that involves embedding unique identifiers or “fingerprints” into files, such as images, videos, or even software. These fingerprints can be used to verify the authenticity of the file and to track its distribution.

This technique is often used in software piracy prevention, as it helps companies track the illegal distribution of their products.

**2.5 Hiding Malware and Malicious Code**

**Advanced Persistent Threats (APT)**

Steganography is sometimes used by cybercriminals and hackers to hide malicious code, viruses, or ransomware within otherwise normal files. These files are often used as a delivery mechanism, and once opened by the target system, the hidden malware is executed without detection.

The hidden nature of this code makes it difficult for traditional antivirus software to detect it, as the files appear to be benign. By using steganography, the malware can bypass firewalls and security checks.

**Covert Communication for Hacking Groups**

In the context of cyber-attacks, steganography allows hacking groups to communicate covertly. For example, during a cyberattack, hackers may embed secret instructions in files that are later retrieved by accomplices. These hidden messages can include commands for executing further malicious activities or coordinating attack strategies.

Law enforcement agencies and cybersecurity firms use steganalysis to detect and stop these activities by identifying hidden communication channels used by cybercriminals.

**2.6 Social Media and Information Hiding**

**Privacy and Personal Security**

Individuals can use steganography to hide private information, such as passwords or personal notes, in social media posts, images, or videos. This allows them to communicate securely without revealing sensitive information to the public.

For instance, people might upload a photo to a social media platform, knowing that it contains a hidden message that only the intended recipient can decode.

**Protest and Political Speech**

In politically oppressive environments, steganography is used to hide messages that would otherwise be censored. Activists or dissidents may use steganography to communicate messages without alerting authorities.

By embedding protest messages or political content in images or audio files, these individuals can share important information without being detected.

**2.7 E-Commerce and Consumer Protection**

**Brand Protection**

E-commerce platforms and brands use steganography to prevent counterfeiting and protect brand identity. For instance, a company may use steganographic techniques to embed a hidden watermark or identifier within its products (e.g., images of the product) to confirm that they are genuine and not counterfeit.

**Product Tracking**

Retailers might use steganography to track the origin and distribution of their products. Hidden data within product images or barcodes could contain important details like manufacturing batch numbers or shipping routes, helping prevent fraud and ensure authenticity.

**2.8 Steganography in Artificial Intelligence and Machine Learning**

**Data Hiding for AI Models**

AI models often require large amounts of data for training. Steganography can be used to hide training data within larger datasets, ensuring the integrity and confidentiality of sensitive information while still allowing the AI to learn from it.

**AI-Powered Steganalysis**

Machine learning techniques are increasingly being used to detect hidden messages in files. AI-powered steganalysis tools can scan large volumes of data to identify patterns that suggest the presence of hidden information, making it more difficult for steganographers to hide messages undetected.

# CHAPTER 3

# Methodology

The core idea of steganography is to manipulate a cover medium (such as an image, audio, or video) in such a way that the hidden message does not alter the medium significantly. The goal is to encode the message in a way that it is not noticeable to the human eye or ear.

The message is typically hidden in the least significant bits (LSB) of a pixel in an image, or the LSBs of a sound wave in audio. These changes are typically so small that they do not noticeably change the overall appearance of the image or the quality of the audio.

**3.1 Redundancy of Media**

Digital files, especially images and audio, contain redundancy. Redundancy means that there are parts of the data that can be altered without noticeably changing the file. Steganography exploits this redundancy to hide messages.

For instance, in an image, most pixel values vary only slightly, meaning minor changes in their least significant bits can encode information without disrupting the image's integrity.

**3.2 Encoding Methods in Steganography**

**3.2.1 Least Significant Bit (LSB) Encoding**: LSB encoding is one of the most commonly used techniques in steganography. It involves replacing the least significant bit of the cover file (like an image or audio file) with the bits of the secret message.

**3.2.2 In Images**: An image consists of pixels, each containing RGB (Red, Green, Blue) values. Each color channel can be encoded with a single bit of information. The least significant bit of each channel is altered to hide a message. This results in an imperceptible change to the image.

**3.2.3 In Audio**: In audio steganography, the least significant bit of each sample is altered to hide the message. Since audio files often have a high number of samples, minor changes are difficult to detect by the human ear.

**Spread Spectrum:**Spread spectrum encoding involves spreading the hidden message over a wide range of data points. Rather than altering one pixel or sample to carry the message, the data is spread out across multiple locations.

This technique makes it harder for attackers to detect the presence of a hidden message, as the changes are more dispersed and subtle.

**Transform Domain Techniques:**This method involves encoding the message in the frequency domain (for example, using Discrete Cosine Transform (DCT) in JPEG images or Discrete Fourier Transform (DFT) in audio).

Transforming the data into a different domain (from pixel or sample values to frequency values) makes it harder to detect changes, as the message is encoded in frequencies rather than direct pixel values.

It is especially useful in compressed files like JPEGs, as it allows for hiding data without affecting the compression process.

**Patchwork:**This technique is used in images, where patches of pixels are selected randomly, and each patch is altered to encode a portion of the message.

This method makes the changes less predictable, which increases the security of the steganographic method.

**3.3 Decoding Methods in Steganography**

**3.3.1 Extracting Information from LSB**

To retrieve the hidden message, the decoding process involves reading the least significant bits of the image or audio file and reconstructing the original message from these bits.

The decoder must know where the hidden data starts and the format of the message. In the case of images, this might involve reading the LSBs of each RGB value and combining them to recreate the binary representation of the message.

**3.3.2 Reversing Spread Spectrum**

Spread spectrum decoding involves collecting the scattered bits of the message and putting them together. This process can be more complex due to the dispersion of the message, and requires knowledge of the spread pattern used during encoding.

**3.3.3 Reverse Transform Domain Techniques**

In transform domain techniques, the decoder works by performing the inverse of the transformation (e.g., using Inverse Discrete Cosine Transform (IDCT) or Inverse Discrete Fourier Transform (IDFT)) to retrieve the message embedded in the frequency domain.

This method is more robust against detection as it hides data in the less obvious frequency components of the file.

**3.4 Key Factors Affecting Steganography**

**3.4.1 Capacity**

The capacity refers to the amount of data that can be hidden within the cover medium. It is influenced by the size of the file, the type of encoding used, and the properties of the medium.

Larger cover files like high-resolution images or high-quality audio files can hold more data, but the more data that is hidden, the more likely it is to be detectable.

**3.4.2 Robustness**

Robustness is the ability of the steganographic method to resist attempts at detection or removal. If the cover medium is altered (e.g., resized, compressed, or cropped), a robust steganographic method ensures that the hidden data remains intact.

Techniques such as transform domain encoding and spread spectrum tend to offer better robustness compared to simple LSB encoding.

**3.4.3 Imperceptibility**

The imperceptibility of the hidden message is a measure of how undetectable the changes are to the human eye or ear. In image steganography, this means that the encoded image should look nearly identical to the original. In audio steganography, the hidden message should not distort the audio quality.

Techniques like LSB are favored because they leave minimal changes to the cover file, ensuring that the hidden data is difficult to detect.

**3.5 Security Considerations in Steganography**

**3.5.1 Steganalysis**

Steganalysis refers to the process of detecting the presence of hidden messages in files. It can be challenging to detect steganography, especially with robust methods, but advancements in machine learning and statistical analysis have made steganalysis more effective.

Common techniques in steganalysis involve analyzing patterns in the pixel values, noise levels, or frequency components of files that are indicative of data being hidden.

**3.5.2 Ethical Implications and Misuse**

While steganography has legitimate uses in secure communication, it can also be misused for illegal activities such as hiding malicious code or illegal content. This has led to concerns in law enforcement and cybersecurity.

It is important to balance the use of steganography for security with the potential risks of misuse.

## CHAPTER 4

## Result and Discussion

Building the steganography project provided valuable insights into both the technical and conceptual aspects of information hiding. Some of the key learnings include:

**Understanding Steganography**: A deeper understanding of how steganography works, specifically in encoding and decoding messages within images. This includes how binary data is embedded into image pixels and how to retrieve it without disturbing the image's perceptible content.

**Working with PIL and Image Processing**: Gained hands-on experience in image manipulation using Python’s Pillow (PIL) library to read, modify, and save images in various formats, as well as processing pixel-level data.

**Web Development with Django**: Developed skills in full-stack web development with Django, focusing on building secure, user-friendly interfaces to handle file uploads, image processing, and serving results. The project involved both frontend and backend components to create an integrated web application.

**Security Concerns and Ethical Implications**: While implementing steganography, the potential risks and ethical issues surrounding its use were brought to the forefront, helping understand the importance of ensuring that such technologies are used responsibly.

Throughout the project, several challenges were encountered and overcome:

**Handling File Uploads and Image Encoding**: Ensuring that the uploaded files were properly handled, and the images were successfully processed without corruption, was a challenge. Special care was needed to ensure that the encoding/decoding of data didn’t compromise the quality or integrity of the image.

**Error Handling**: Implementing robust error handling mechanisms was necessary to deal with user inputs, such as large images or invalid files, which could potentially break the system or cause unexpected behaviour.

**Message Size Limitations**: One of the early challenges was to ensure that the messages were small enough to be embedded into the image without distorting the original content. This required careful management of the binary data size and adjusting for image dimensions.

**Web Interface and User Experience**: Designing a clean and intuitive user interface using Bootstrap for the web application took time to ensure it was user-friendly, especially for non-technical users.

**Security Aspects**: While the project focuses on the hidden encoding of messages, ensuring that these hidden messages were secure from detection by others required research into steganographic techniques and the potential vulnerabilities of different methods.

## CHAPTER 5

## Conclusion and Future Work

The “Encryption and Decryption Using Digital Cryptography in Files” website project successfully merges modern web development practices, creating an interactive platform that allows users to encrypt and decrypt. Through a well-structured design utilizing HTML, CSS, Django, Tailwind CSS and JavaScript, the website offers an engaging and user-friendly experience, ensuring smooth navigation and accessibility across various devices and browsers.

Looking ahead, the project has significant scope for expansion, enhanced interactivity, and community features, which can further enrich user engagement and satisfaction. Overall, this project exemplifies how combining encryption and decryption with contemporary web design can create a compelling digital experience that tach as well as help new audiences.

**Functional Steganography System**: The project successfully implements both encryption (embedding data into an image) and decryption (retrieving hidden data from an image) functionalities.

**Interactive Web Interface**: The Django-based web interface enables users to upload images and messages, and retrieve steganographic results with a clean, responsive design.

**Educational Component**: The “Learn Steganography” section adds value to the project by educating users on the principles and techniques behind steganography.

**User Authentication**: Integrating user authentication could allow users to create accounts and securely store encrypted images or messages for future use.

**File Format Support**: Expanding the project to support other file formats (e.g., audio, video) for embedding hidden messages, making it more versatile.

**Advanced Steganographic Techniques**: Investigating more advanced techniques for data hiding, such as using algorithms for encryption before embedding, to improve security and robustness.

**Performance Improvements**: Enhancing the performance for large files or large messages, ensuring that the system scales effectively as the user base grows.

**Mobile Application**: Developing a mobile version of the steganography tool using frameworks like React Native or Flutter to make it accessible on smartphones for better convenience.

Steganography plays an important role in modern security, particularly in the context of **privacy protection** and **covert communication**. As digital communication becomes increasingly scrutinized, the need for hidden channels of communication grows, especially in sensitive environments like:

**Government and Military Applications**: Where secure, hidden communication is critical.

**Digital Privacy and Anonymity**: Allowing individuals to preserve their privacy in oppressive environments.

**Anti-Censorship and Whistleblowing**: Protecting those who need to reveal information without detection.

However, while steganography is essential for privacy, it also poses **ethical and legal challenges**. The same methods that protect individuals can also be used by malicious actors to hide criminal activities, making it a double-edged sword in modern security discussions.

While the current project offers a fundamental implementation of image-based steganography, there are several potential areas for further research and development:

**Machine Learning for Steganography**: Leveraging AI and machine learning algorithms to develop adaptive steganographic systems that can automatically optimize encoding methods to avoid detection.

**Steganography in Video and Audio**: Extending the concept of steganography to more complex file formats such as audio and video, where data can be hidden in sounds, frequencies, or even video frames.

**Robustness Against Steganalysis**: Investigating how to make steganographic systems more resistant to detection by advanced forensic tools. This involves researching methods to detect and counter steganalysis attacks that try to identify hidden data.

**Blockchain Integration for Security**: As mentioned previously, incorporating blockchain for verifying and securing steganographic data could lead to a decentralized, tamper-proof storage system for hidden messages.

**Steganography for IoT Devices**: Researching how steganography could be applied to Internet of Things (IoT) devices, ensuring secure communication between smart devices in a way that is invisible to unauthorized parties.

**Ethical and Legal Frameworks**: As steganography’s use grows, there’s a pressing need to develop frameworks to balance security, privacy, and ethics, ensuring that the technology is not misused for illicit purposes.

### References

1. **Katzenbeisser, S., & Petitcolas, F. A. (1999).** *Information hiding techniques for steganography and digital watermarking*. Artech House.
2. **Fridrich, J. (2009).** *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press.
3. **Provos, N., & Honeyman, P. (2003).** "Hide and Seek: An Introduction to Steganography." *IEEE Security & Privacy*, 1(3), 32-44.
4. **Johnson, N. F., Duric, Z., & Jajodia, S. (2000).** *Information hiding: Steganography and watermarking - attacks and countermeasures*. Springer.
5. **Anderson, R. J., & Petitcolas, F. A. (1998).** "On the Limits of Steganography." *IEEE Journal on Selected Areas in Communications*, 16(4), 474-481.
6. **National Institute of Standards and Technology (NIST).** *Cryptographic Standards and Guidelines*. Retrieved from <https://www.nist.gov/cryptography>
7. **Computerphile. (2018, June 12).** *What is Steganography?* [Video]. YouTube. Retrieved from <https://www.youtube.com/watch?v=TWEXCYQKyDc>
8. **ScienceDirect.** *Research Articles on Steganography and Digital Forensics*. Retrieved from <https://www.sciencedirect.com/>
9. **OWASP Foundation.** *Information Security Risks and Countermeasures*. Retrieved from <https://owasp.org/>
10. **IEEE Xplore Digital Library.** *Research on Steganography and Cryptography*. Retrieved from <https://ieeexplore.ieee.org/>.
11. **The Hated One. (2020).** *Image Steganography Explained*. [Video]. YouTube. Retrieved from <https://www.youtube.com/watch?v=8PSfDjvbnjI>