VIPKBIET Digital Steganography and Watermarking for Digital Images

Nayana Ghalme, Revati Deshmukh, Gauri Jadhav, Divya Lokhande.
*Department of Computer Engineering, VPKBIET Baramati, SPPU University, Pune, Maharashtra, India.

ABSTRACT

Steganography and watermarking is used to hide important data in an another data so that hidden important data is only known by receiver or only known to that person who is belonging to that data and not known by any attacker that's why this technique (tech) is also known as security based tech. Methods of steganography and watermarking are designed that implement embedding in digital objects hidden information sequences for various purposes. The development of information technology has led to a significant increase in the share of multimedia traffic in data networks. This has necessitated to solve the following information security tasks in relation to multimedia data: protection against leakage of confidential information, as well as identifying the source of the leak; ensuring the impossibility of unauthorized changes; copyright protection for digital objects. To solve such kind of problems, methods of steganography and watermarking are designed that implement embedding in digital objects hidden information sequences for various purposes. In this paper, an overview of promising research in the specified area is provided. In this paper, First of all, we provide basic information about this field of research .Next, we provide the Literature Survey (Summary of referred existing papers related to our topic).Then we provide the Proposed method (Subpoints : architecture (Design), algorithms, experimental setup). After that there is results of Steganography and watermarking including screenshot also. Then we provide the performance analysis. Then last, there are Discussions , Conclusion and References this points are included.

INTRODUCTION

Steganography is the practice of concealing a message or information within another non secret data in a way that the existence of the hidden message is not apparent to an observer. It involves embedding data, such as text, images, or audio, into another medium, such as an image or audio file, without altering the apparent features of the medium.

Watermarking, on the other hand, is a technique used to embed information, such as a logo, text, or digital signature, into digital content to verify its authenticity or protect it from unauthorized use. Watermarks are typically visible or invisible markings applied to images, videos, audio, or documents, serving as a form of digital identification or proof of ownership.

Steganography and watermarking are both techniques used to conceal information within digital content, but they serve different purposes and have distinct methods of implementation. Steganography involves hiding secret messages or data within other non-secret data in such a way that the existence of the embedded information is concealed. The primary goal of steganography is to ensure that the existence of the secret message is undetectable to anyone except the intended recipient. This technique can be applied to various types of digital media, including images, audio, video, and text. On the other hand, watermarking is a technique used to embed visible or invisible markings, typically in the form of text, logos, or unique identifiers, into digital content to signify ownership, copyright information, or authentication. Watermarks are often used to deter unauthorized use or distribution of digital assets and to provide a means of identifying the owner or creator of the content. While both steganography and watermarking involve embedding information within digital content, they serve different purposes: steganography focuses on hiding the existence of information, while watermarking focuses on providing a visible or invisible mark to identify ownership or authenticity.

The history of steganography and watermarking dates back centuries:

⇨ <u>Steganography:</u>

- Ancient Practices: Steganography has ancient origins, with historical examples including the use of invisible inks, hidden messages in wax tablets, and secret compartments in physical objects.
- Medieval Period: During the medieval period, various methods such as invisible writing and microdots were employed for covert communication.
- World War Era: Steganography saw significant use during World War II, with techniques like microphotography being utilized for espionage and covert messaging.
- Digital Age: In the digital age, steganography has evolved to include embedding messages within digital media such as images, audio, and video files. Modern techniques leverage digital algorithms and data hiding methods for secure communication and data protection.

⇨ <u>Watermarking:</u>

- Paper Watermarks: Watermarking originated with papermaking in the Middle Ages, where unique designs were embedded into paper sheets as a form of identification or authentication.
- Printed Materials: Watermarks became prevalent in printed

materials such as currency, stamps, and official documents to prevent counterfeiting and establish authenticity.

- Digital Era: With the advent of digital media, watermarking transitioned into the digital realm, where it serves purposes such as copyright protection, content authentication, and digital rights management.
- Throughout history, both steganography and watermarking have adapted to advancements in technology and have been utilized for various purposes, including espionage, security, authentication, and content protection. Their evolution continues to shape the landscape of digital communication and content management in the modern era.

LITERATURE SURVEY

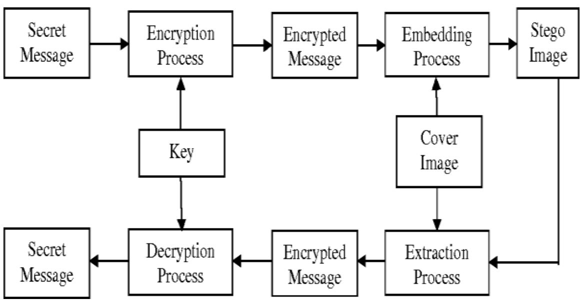
Author	Project Title	Description
Jessica Fridrich	Steganography in Digital Media.	This project focuses on various techniques for embedding data within digital images, videos, and audio files while minimizing perceptible changes to the media.
Ingemar Cox, Matthew Miller, and Jeffrey Bloom	Digital Watermarking.	This project explores methods for embedding imperceptible marks or signatures into digital media files to assert copyright, authenticate content, or track usage without significantly degrading the quality of the media.
Neil F. Johnson and Sushil Jajodia	Steganography: Seeing the Unseen.	This project delves into the theory and practice of steganography, covering various approaches for concealing information within digital media, including images, audio, and text.

PROPOSED METHODS

1. Architecture (Design) :-

The architecture or design of steganography and watermarking systems can vary depending on factors such as the application scenario, the type of media involved (images, audio, video, etc.), and the specific requirements of the system (robustness, imperceptibility, capacity, etc.). Here, outline of the general architecture for both steganography and watermarking systems:

❖ Steganography :-



⇨ Payload Embedding Module:

- This module is responsible for embedding the secret message or payload into the cover media (image, audio, video, etc.).
- It employs various techniques such as LSB substitution, LSB matching, or frequency domain manipulation to hide the payload while minimizing perceptual distortion.
- The embedding process should ensure that the changes introduced to the cover media are imperceptible to human observers.

⇨ Payload Extraction Module:

- This module is responsible for extracting the hidden payload from the stego media.
- It reverses the embedding process by detecting and extracting the hidden information while minimizing errors or false positives.
- Techniques such as statistical analysis or machine learning-based approaches may be used for payload extraction.

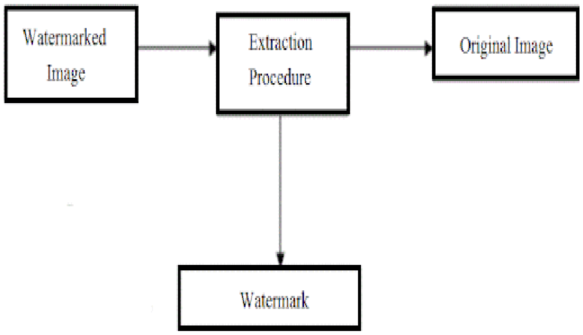
⇨ Key Management and Security Module:

- This module handles key management, encryption, and authentication to ensure the security of the hidden payload.
- It may involve encryption of the payload before embedding and decryption during extraction to protect against unauthorized access.

⇨ Quality Assessment Module:

- This module evaluates the quality of the stego media by comparing it with the original cover media.
- It assesses factors such as perceptual quality, distortion level, and robustness against attacks to ensure the effectiveness of the steganography technique.

❖ Watermarking :-



⇨ Embedding Module:

- This module embeds the watermark or identifier into the host media (image, audio, video, etc.).
- It utilizes techniques such as spatial domain modulation, frequency domain modulation, or transform domain modulation to insert the watermark while maintaining its imperceptibility and robustness.
- The embedding process may involve key-based operations to enhance security and prevent unauthorized removal of the watermark.

⇨ Detection and Extraction Module:

- This module detects and extracts the watermark from the watermarked media.
- It employs detection algorithms to locate and isolate the watermark signal while minimizing false positives.
- Techniques such as correlation-based detection or statistical analysis may be used for watermark extraction.

⇨ Robustness Enhancement Module:

- This module enhances the robustness of the watermark against common attacks such as compression, noise addition, and geometric transformations.
- It may involve error correction coding, spread spectrum techniques, or redundant embedding to improve the resilience of the watermark against intentional or unintentional alterations.

⇨ Authentication and Verification Module:

- This module verifies the authenticity and integrity of the watermarked media by validating the embedded watermark.
- It compares the extracted watermark with the original reference to determine if the media has been tampered with or manipulated.
- Authentication techniques such as digital signatures or cryptographic hashes may be employed for verification.

2. Algorithm :-

Steganography Algorithms:

1. Input:

- Cover Medium(e.g. image, audio, video)
- Message to be hidden.

2. Prepare the Message:

- Convert the message into a binary format.

3. Select Embedding Method:

Choose a technique to embed the message into the cover medium:

- Least Significant Bit (LSB) substitution for images.
- Frequency domain techniques for audio.

- Spatial domain techniques for videos.

4. Embed the Message:

- Modify the cover medium according to the chosen embedding method to hide the binary message.
- Ensure the modifications are imperceptible or have minimal impact on the quality of the cover medium.

5. Output:

- Obtain the stego-medium (the cover medium with the hidden message).

6. Optional:

- Encrypt the hidden message for added security.

7. Transmission or Storage:

- Transmit or store the stego-medium.

8. Extraction (for recipient):

- Use the reverse of the embedding method to extract the hidden message from the stego-medium.

9. Decode the Message:

- Convert the binary message back into its original format (text, data, etc.).

<u>Watermarking Algorithms:</u>

1. Input:

- Original Content (e.g. image, audio, video)
- Watermark (e.g. logo, copyright information)

2. Select Embedding Method:

Choose a technique to embed the watermark into the original content:

- Spatial domain techniques (altering pixel values directly).
- Frequency domain techniques (modifying frequency components).
- Spread Spectrum techniques (spreading watermark across the content).

3. Embed the Watermark:

- Modify the original content according to the chosen embedding method to incorporate the watermark.
- Ensure the modifications are robust against common attacks (e.g. cropping, compression).

4. Output:

- Obtain the watermarked content.

5. Optional:

- Encrypt the watermark for added security.

6. Transmission or Storage:

- Transmit or store the watermarked content.

7. Detection (for verification):

- Use a detection algorithm to locate and extract the watermark from the watermarked content.

8. Verification:

- Verify the extracted watermark to confirm authenticity or ownership.

9. Optional:

- Assess the quality of the watermarked content (e.g. perceptual quality, robustness against attacks).

3. Experimental Setup :-

Hardware:
Computers: Any modern computer can be used for steganography and watermarking tasks.

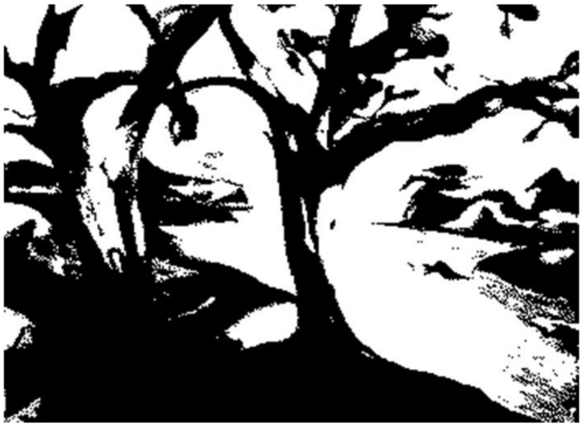
Software:
-Python libraries for image processing.
-Image for encryption.

RESULTS

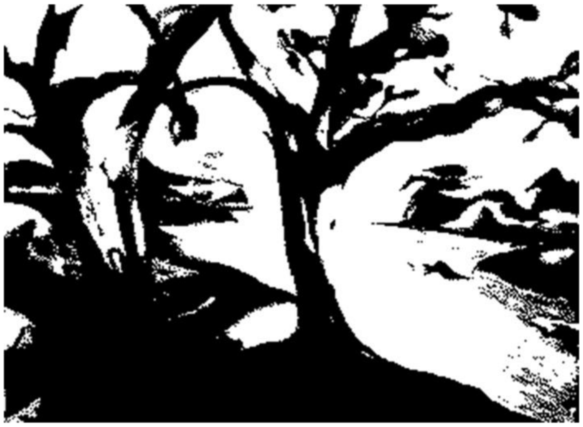
STEGANOGRAPHY RESULTS :-

1]

- Input :-



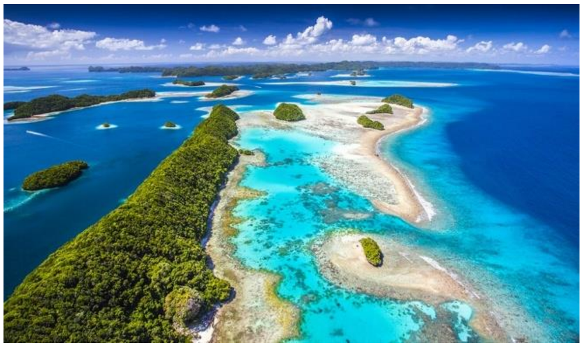
- Output :-



2]

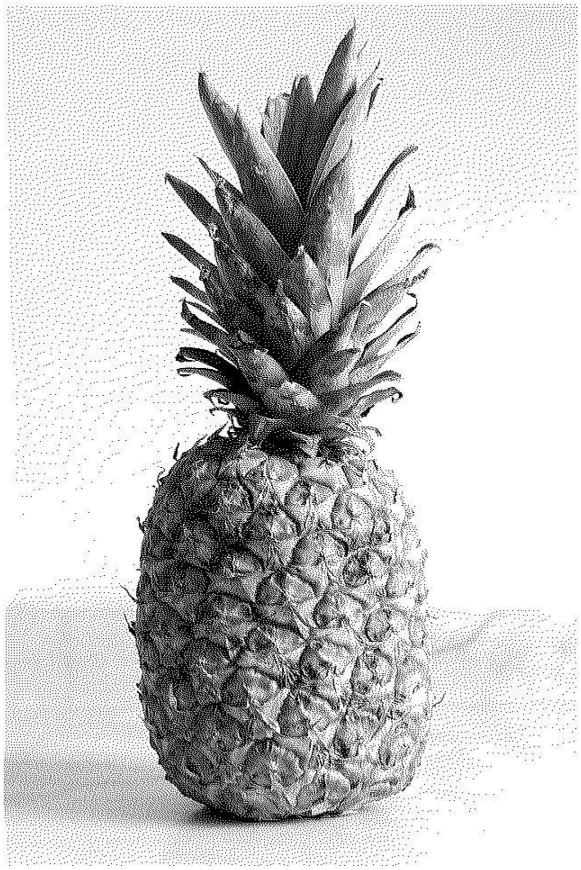
- Input :-

- Output :-

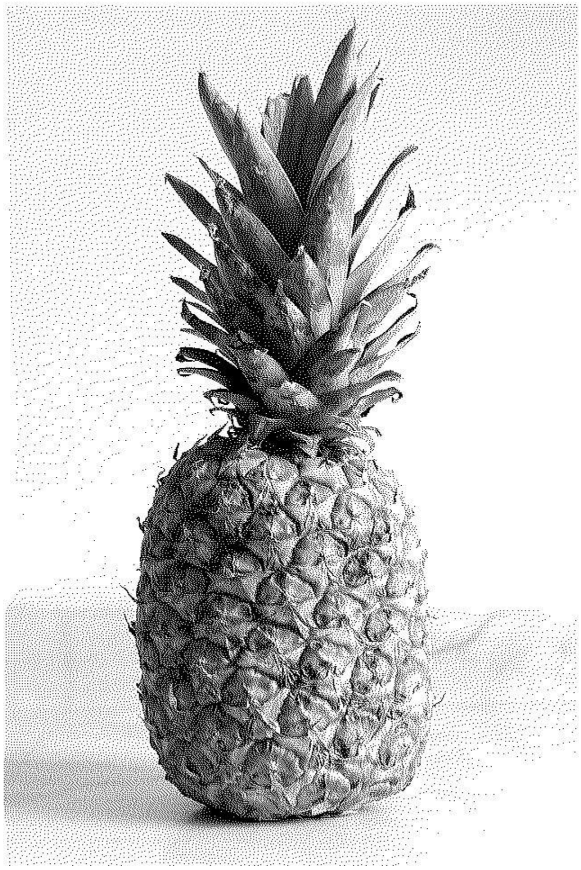


3]

- Input :-



- Output :-



WATERMARKING RESULTS :-

1]

- Original Image :-

- Hide Image :-

- Output Image :-

CONCLUSION

Currently, methods of steganography and digital watermarking are actively developing, and many researchers from different countries offer many new algorithms that differ in different quality characteristics. Despite the variety of developed algorithms, in the field of information embedding in digital images, there are still a number of unsolved problems. The overwhelming majority of modern embedding algorithms provide high imperceptibility of embedding, therefore, the attention of researchers working in this field should be aimed at achieving other embedding efficiency indicators: reversibility, robustness, and resistance to steganalysis. The review showed that work in these areas is underway, but there are still a lot of problems that require new original solutions.

In the nut shell, it is concluded that Steganography and watermarking issued to hide important data in another data so that hidden important data is only known to that person who is belonging to that data and not known by any attacker .This paper gives prescribed description of basics of Steganography and watermarking.

REFERENCES

1. Jaspreet Kaur, Navneet Kaur and Narwant S.Grewal on Digital Watermarking and its Techniques,Guru Nanak Dev Engineering College, ECE Department, GNDEC, Ludhiana, India.
2. Prajakta Hatwar, Ankita Balbudhe ,Pratik Gahlod, Prasanna Kshirsagar, Rasika Manapure Student,UG Research Guide on data hiding using watermarking aand steganography using image prrocessing, Department of Electronics & Telecommunication, Suroydaya College Of Engineering & Technology, Nagpur, Maharashtra, India . (Journal of Telecommunication Study).
3. 1OLEG EVSUTIN ,2ANNA MELMAN *,AND 3ROMAN MESHCHERYAKOV*, (Senior Member, IEEE) on digital steganography and watermarking for digital images. This work was supported by the Russian Science Foundation under Grant 19-71-00106.
4. Jasleen kour, Deepankar Verma on steganography techniques

.International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5).

5. Fatih Şahin, Taner Çevik, Mustafa Takaoğlu on the steganography concept. Article in International Journal of Computer Applications · May 2021.