Mini Project Report on

IMAGE STEGANOGRAPHY

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

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted by:

Aish Goyal **GE-202016596**

Under the Mentorship of

Ashwini Kumar

Designation

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

July-2023

Graphic Era
Deemed to be
University
DEHRADUN

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the project report entitled **"Image Steganography"** in partial fulfilment 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 **Mr. Ashwini Kumar, Professor**, Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun.

Aish Goyal GE-202016596

Table of Contents

Chapter 1

Introduction

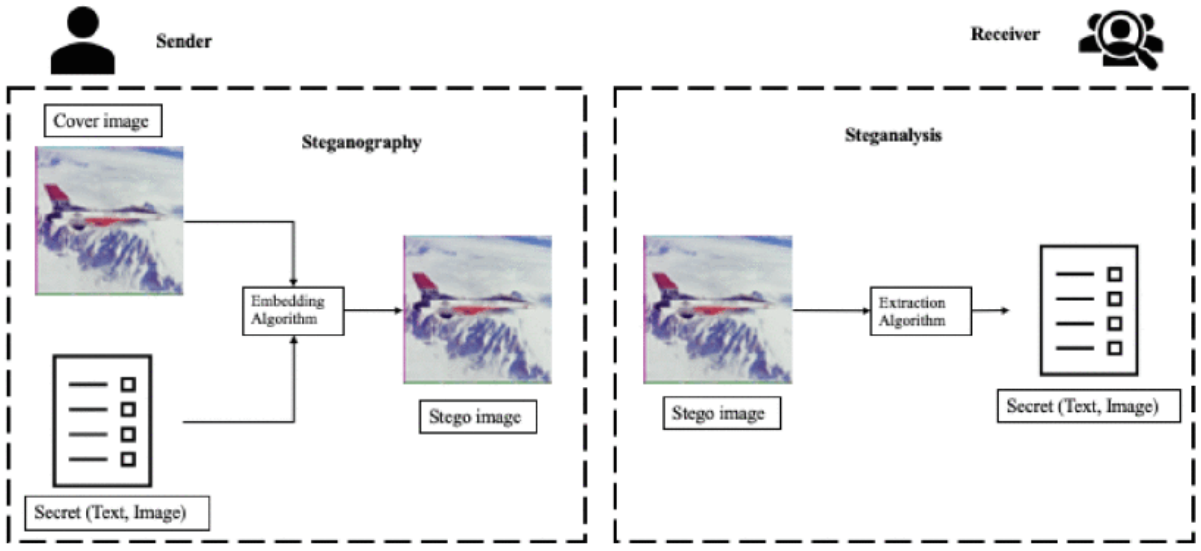
Image steganography is a way to cover mystery statistics/messages inside a photo without changing its visible look significantly. It is a shape of statistics hiding, wherein the hidden statistics are embedded in the photo's pixel values or its metadata. The intention is to make the hidden statistics undetectable to an observer who's blind to its existence.

1.1 Introduction

Image steganography is a method to hide data within the pixels of an image. It leverages the human perception limitations to conceal data in a way that it is difficult to detect. It can be used to hide sensitive or confidential data within an image file. By embedding the data in the image, steganography provides a covert communication channel, as the casual observer is typically unaware of the existence of the hidden message.

Every steganography consists of three components:

1. Cover object
2. Message object
3. Resulting Steganographic object



Conventionally, Least Significant Bits (LSB) substitution method is employed to perform image steganography where the input image is called the cover image and the output image

containing the secret data is called the stegno image. Cover images are usually of higher pixel quality, out of which not all the pixels are used. LSB methods work under the assumption that modifying a few pixel values would not show any human eye detectable changes. The secret information is in binary form. The cover image is scanned to determine the least significant bits in the noisy area which are used in the process of steganography. The binary bits from the secret image are then substituted in the LSBs of the cover image to finally create a stegno image containing the secret message which is undetectable by the human eye.

1.2 Uses

Security and privacy: Steganography may be used as an extra layer of protection to defend touchy data. By mixing the name of the game information with an innocent-searching image, it provides a further stage of obfuscation, making it tougher for unauthorised people to locate or get admission to the hidden data. It is especially beneficial while transmitting information over insecure channels or while storing touchy information in public repositories.

Digital watermarking: Steganography strategies are typically hired in virtual watermarking, that is the manner of embedding imperceptible data into virtual media, including pictures or videos. Watermarks are regularly used for copyright protection, authentication, and monitoring purposes. By hiding particular identifiers inside the image, possession may be installed or unauthorised use may be detected

Covert communique: Steganography has been used traditionally for covert communique in diverse scenarios. For example, it's been hired with the aid of using journalists, activists, or people residing beneath neath oppressive regimes to transmit touchy data discreetly. By concealing messages inside innocent-searching pictures, they are able to pass censorship or surveillance measures.

Data hiding in virtual forensics: In virtual forensics, steganography performs a position in hiding or embedding information inside pictures for investigative purposes. This approach allows investigators in concealing touchy data in the course of information extraction or transporting proof without elevating suspicion.

Research and improvement: Steganography serves as a subject of studies and improvement in data protection. Scientists and specialists constantly discover new strategies and algorithms to enhance the effectiveness and robustness of steganographic methods. This ongoing painting is critical in each advancing the sector and improving the countermeasures to locate and save you malicious makes use of steganography.

Chapter 2

Literature Survey

Steganography, the art of concealing information within various media, has been a subject of interest for researchers in the field of information security. In particular, image steganography has attracted significant attention due to the widespread use of digital images and the potential for easy and secret communication.

Steganography Fundamentals:

Steganography involves hiding secret information within cover media while maintaining its original appearance. It aims to achieve imperceptibility, robustness, and capacity, ensuring that the hidden message remains undetectable and resistant to attacks. The field of steganography encompasses various media types, including text, audio, video, and images. However, image steganography is of particular interest due to the abundance of digital images and their ease of dissemination.

Image Steganography Techniques:

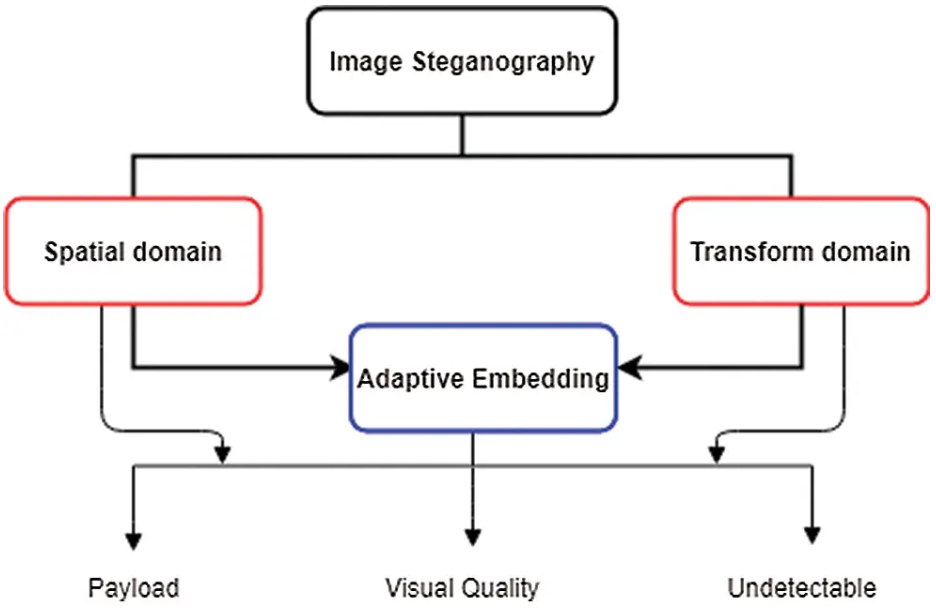
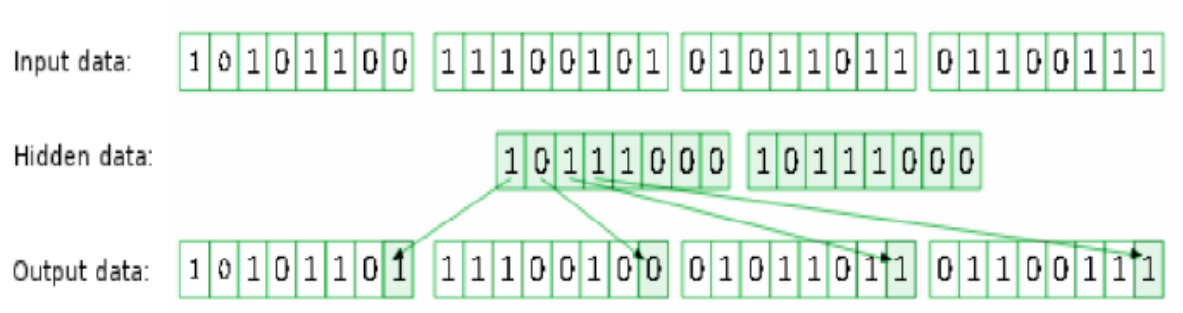


Image steganography techniques can be broadly classified into spatial domain and frequency domain methods. Spatial domain techniques, such as LSB (Least Significant Bit) substitution and pixel-value differencing, operate directly on the pixel values of the cover image. Frequency domain techniques, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), transform the image into a frequency representation before embedding the secret data.

LSB Substitution:

LSB substitution is one of the simplest and most commonly used techniques in image steganography. It involves replacing the least significant bit of the pixel values in the cover image with the bits of the secret message. The alteration of the LSB has minimal impact on the visual quality of the image, making it suitable for hiding information imperceptibly.



Current Research and Techniques:

Recent advancements in image steganography have focused on enhancing the capacity, security, and robustness of steganographic systems. Researchers have explored sophisticated algorithms that utilise more significant bits for data hiding, adaptive methods for dynamic embedding, and advanced encryption techniques to protect the hidden information. Additionally, the utilisation of machine learning algorithms and deep neural networks has gained attention to improve the hiding capacity and resistance against detection.

Evaluation Metrics:

Evaluating the performance of image steganography techniques requires the use of appropriate metrics. Commonly used metrics include Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Bit Error Rate (BER), and Visual Information Fidelity

(VIF). These metrics provide quantitative measures of the distortion introduced by the steganographic process and the similarity between the original and stego images.

Applications and Challenges:

Image steganography finds applications in various domains, including secure communication, copyright protection, covert messaging, and digital forensics. However, the technology also poses challenges, such as the detection and extraction of hidden information, attacks by adversaries attempting to remove or alter the embedded data, and the trade-off between hiding capacity and visual quality.

Conclusion:

The literature on image steganography demonstrates the significance and potential of concealing information within digital images. Various techniques and algorithms have been developed, with ongoing research focusing on improving capacity, security, and robustness. The practical applications of image steganography continue to evolve, and advancements in machine learning and deep neural networks open new avenues for future exploration in the field.

Chapter 3

Methodology

1. Import the necessary libraries and load the cover image and the secret message.

2. Convert the cover image and the secret message into matrices of pixel values.

3. Ensure that the size of the secret message does not exceed the available space in the cover image.

4. Choose the LSB plane(s) to modify. The LSB of each pixel is typically used for embedding.

5. Encode the length of the secret message into the cover image. This will be used during extraction.

6. Iterate over the pixels of the cover image and modify the LSBs according to the secret message.

   - Extract a pixel from the cover image.

   - Extract the next bit of the secret message.

   - Modify the LSB of the pixel with the secret bit.

   - Replace the pixel in the cover image with the modified pixel.

7. Save the stego image (cover image with embedded secret message) to a file.

8. To extract the secret message from the stego image:

   - Load the stego image.

   - Retrieve the length of the secret message from the LSBs of the pixels.

   - Extract the LSBs of the pixels to reconstruct the secret message.

9. Display or output the extracted secret message.

Extensions and Improvements:

- Explore different LSB planes for embedding to achieve a trade-off between imperceptibility and robustness.
- Implement other steganographic techniques like Huffman encoding or frequency domain-based methods.
- Apply encryption to the secret message before embedding it for added security.
- Experiment with different cover images and secret messages to observe the impact on the steganographic process.
- Develop a graphical user interface (GUI) for a user-friendly experience.

Chapter 4

Result and Discussion

Picture steganography has been utilised covertly in fact transmission with the aim that facts may be transmitted in a stable and thriller way. Based on the photograph steganography technique thriller facts has been transformed into parallel association and that has been set up with pixels bits of the duvet photograph. Various tactics were produced which have been utilised for method of facts masking up. In this paper an audit has been accomplished at the methodologies that may be utilised for facts concealing methods. Security from interruption or malevolent attacks may be executed thru man-made brainpower bureaucracy and thru encryption primarily based totally methodologies. On the basis of auditing unique photograph steganography tactics we are able to presume that LSB primarily based totally and AI primarily based totally methodologies supply higher steganography as assessment with current methodologies. These methodologies have a great beneficial role that those do now no longer impact the character of the photograph.

Chapter 5

Conclusion and Future Work

For future work on the steganography project, following possibilities can be considered:

1. **Enhanced Security**: Explore and implement advanced encryption techniques to further strengthen the security of the hidden data. You can research and integrate cryptographic algorithms like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) for encrypting the secret information before embedding it in the image.
2. **Multiple File Formats:** Extend your project to support embedding and extraction of hidden data in various image file formats, such as JPEG, PNG, GIF, or BMP. Each file format has its own specifications and challenges, so implementing support for multiple formats can enhance the versatility of your steganography tool.
3. **Audio and Video Steganography:** Extend the capabilities of your project to include hiding data within audio files (audio steganography) and video files (video steganography). This expansion allows for hiding information in different types of multimedia, providing a more comprehensive steganography solution.
4. **Error Correction Techniques:** Investigate and implement error correction techniques to make the steganography process more robust against noise or intentional attacks. Error correction codes like Reed-Solomon or Hamming codes can help ensure the accuracy of the hidden data during extraction, even in the presence of disturbances.
5. **Steganalysis Techniques:** Research steganalysis techniques that aim to detect the presence of hidden data in images. By understanding the vulnerabilities and

weaknesses of steganography methods, you can develop countermeasures and improve the effectiveness of your steganographic algorithms.

6. **Cross-Platform Support:** Extend your project to support multiple platforms, such as Windows, macOS, and Linux. This allows users to utilise your steganography tool regardless of their operating system preference.
7. **Performance Optimization:** Analyse and optimise the performance of your steganography algorithms to enhance speed and efficiency. Explore techniques such as parallel processing or optimization of memory usage to improve the overall performance of your project.
8. **User Interface Enhancements:** Continuously improve the user interface of your steganography tool to enhance user experience. Consider adding features such as drag-and-drop functionality, real-time preview of modified images, or progress indicators for long operations.
9. **Integration with Cloud Services:** Explore integrating your steganography project with cloud storage services to provide users with the option to store and retrieve their hidden data securely. This integration can offer convenient access to hidden information from multiple devices while ensuring data privacy.
10. **Research and Innovate:** Stay up to date with the latest advancements in steganography and related fields, such as machine learning and deep learning. Investigate innovative approaches and techniques that can push the boundaries of steganography, such as using neural networks for improved embedding and extraction.

References

[1] Image Steganography: A Review of the Recent Advances, Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane.**(Research Paper)**

[2] Image Steganography, Savitha Bhallamudi. **(Journal paper)**

[3] "Various Techniques of Image Steganography and its Future Scope : A Review", Alka Chauhan*, in Journal of Advances and Scholarly Researches in Allied Education | Multidisciplinary Academic Research. **(Journal paper)**

[4] "Image Steganography in Spatial Domain: Current Status, Techniques, and Trends", Adeeb M. ALhomoud, Intelligent Automation & Soft Computing **(Article)**

[5] "Image Steganography in Cryptography", https://www.geeksforgeeks.org/image-steganography-in-cryptography/ **(Online)**