WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Image Steganography

Swagatam Prasad[1], Sahil Dalve[2] and Asst. Prof. Gauri Mhatre[3]

[1,2,3]Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India
Email: swagatamprasad@gmail.com

ABSTRACT

The practice of hiding information within other data in order to protect the confidentiality of a secret message is known as steganography. The aim of image steganography is to include hidden data into a picture as little as possible without affecting the image's overall appearance. If successful, the modifications reflect the secret message but have no appreciable effect on the carrier. The information might not be related to the carrier sound or image, or it could contain carrier-specific information like the author, a digital watermark, or a fingerprint. Data and video transmissions, as well as image, audio, and text files, can all contain hidden information thanks to steganography. When message is hidden in the carrier a Steganography carrier is formed for example a Steganography -image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses.

INTRODUCTION

In an era dominated by the relentless surge of digital communication, the need for secure and confidential information exchange has become paramount. Image steganography, an ancient art of concealing messages within seemingly innocuous images, has reemerged as a pivotal technique in the realm of data security. Unlike encryption methods that focus on rendering information indecipherable, steganography operates on the principle of hiding the very existence of a message. This clandestine approach to communication holds promise in various fields, from secure data transfer to covert intelligence operations. This paper delves into the intricacies of image steganography, exploring its historical origins, fundamental principles, and contemporary applications. As we navigate through the complexities of this covert art, we aim to shed light on its significance in safeguarding sensitive information, its role in digital forensics, and the ethical considerations surrounding its use. In an age where information is both a valuable asset and a potential liability, understanding the nuances of image steganography becomes imperative for those seeking to navigate the intricate landscape of secure communication.

Related Work

The symmetric encryption technique is one of the oldest and most famous methods of maintaining data security; the secret key can be a text or several random characters. The secret key is implemented by a text message to change its content.When the sender and recipient are aware of each other's keys, the encryption mechanism employed in this technique encrypts each character into multiple alphabetic characters. The secret key is then used to both encrypt and decrypt the message. Block cyphers, or more precisely, encryption techniques, are used in blowfish. The term "cypher" is often used to describe it. Blowfish has a 64-bit block size and uses keys with a bit range of 3 to 2448. According to Bruce Schneier, who created it, it is royalty-free, open source, and free to use. AES is frequently used, even though Blowfish is included in a number of cypher suites and encryption techniques. Since no cryptanalysis attempt has been successful, blowfish is secure. The Steganography image was created by combining the encrypted payload image with the cover image. We assessed the Steganography image's performance using measures including PSNR, MSE, and entropy. The significance of creating a secure organisation in the face of substantial industry and regulatory expectations is emphasised in this essay.

The widespread use of Wi-Fi networks for remote access to various resources and devices makes them an essential component of modern organizations. Security measures must be taken to mitigate Wi-Fi risks and prevent hacking attempts. This article provides an overview of essential security measures for different organizational contexts to ensure a secure organizational environment. Image steganography is one of the top choices among experts in data hiding. The biggest challenge in designing a steganographic system is to balance measures such as the quality of the cover image, capacity, and robustness to various attacks [29]. This study aims to comprehensively review various existing image steganography techniques concerning their performance evaluation standards. The challenges faced and the future directions of this field are also discussed. A comprehensive performance evaluation of reversible image steganography techniques was conducted. Techniques from the past two decades were compared using standard test images, with PSNR and embedding capacity as the evaluation parameters. The results of each technique were tabulated, analyzed, and compared to provide a clear understanding of their performance. Descriptive statistics and an in-depth analysis were also performed to assess these past techniques of the standard test. Image steganography is a technique that involves hiding information within an image in such a way that it is difficult to detect. The technical specifications for

image steganography can vary based on the specific algorithm or method used. Below are some general considerations and components that are often part of image steganography systems:

Steganographic Algorithms:

Various algorithms can be used for hiding information within an image. Common ones include:

Least Significant Bit (LSB) insertion: Modifying the least significant bit of each pixel to encode information.

Frequency domain techniques: Altering the frequency components of an image, such as Discrete Cosine Transform (DCT) for JPEG images.

Spread Spectrum: Spreading the hidden data across the image using a pseudorandom sequence.

Security:

The security of a steganographic method is crucial. It should resist various attacks, including statistical analysis, visual inspection, and known steganalysis techniques.

Encryption:

Encrypting the data before hiding it can enhance security. This ensures that even if the steganographic content is discovered, it remains unreadable without the decryption key.

Payload Size:

The size of the payload (the hidden information) that can be embedded in an image depends on the chosen steganographic method. Balancing between a larger payload and maintaining a low impact on image quality is essential.

LSB Technique

This is the most basic and essential image Steganographic Technique embedding technique. Data can be buried in the least significant portions of the cover image using this technique, and the hidden image in the cover file remains undetectable to the naked eye. This method can be used to hide images that are 24-bit, 8-bit, or grayscale. Here, each pixel's two least significant bits are replaced with the secret message bit until the message end. For example, when using a 24-bit image, one can store six bits in each pixel by changing at least two bits of each red, green, and blue color component. For example, a twenty-four bit can be as follows: 11000110 00110101 11100011 11011011 01101110 11001110

Genetic Algorithm (GA)

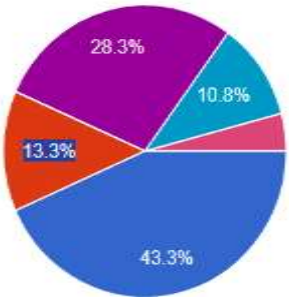
The genetic algorithm-based steganography method incorporates any image embedding technique to hide the data in an image with improved security. The genetic algorithm is a problem-solving method based on natural selection, the driving force behind biological evolution. The genetic algorithm repeatedly modifies a population of individual solutions. The genetic algorithm randomly selects parents from the current population at each phase and uses them to produce the following generation of children. Thus, over successive generations, the population evolves towards an optimal solution.

Acknowledgment

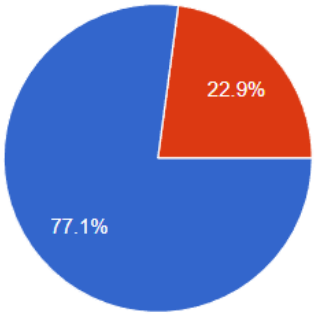
Population Embed Acknowledgment discreetly within an image using steganography techniques. Conceal textual information by subtly altering pixel values without noticeable visual impact. Utilize metadata fields, like EXIF data, to store acknowledgment details in the image file. Apply watermarks containing acknowledgment information to subtly mark the image. Incorporate cryptographic signatures or hashes for integrity verification of acknowledgment data. Document and communicate the presence of embedded acknowledgments to intended recipients

Figures and survey result

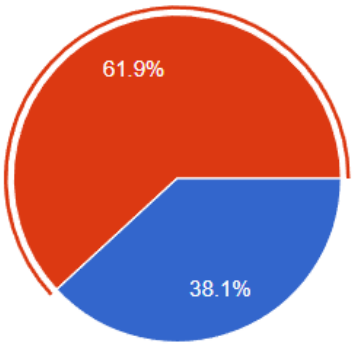
1.Select your age group



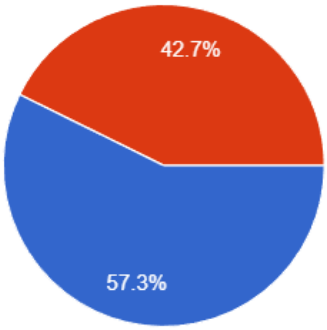
2. Is it important to communicate the presence of embedded information to intended recipients in steganography?



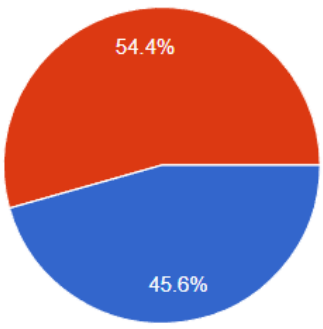
3. Is image steganography a technique used for hiding information within images?



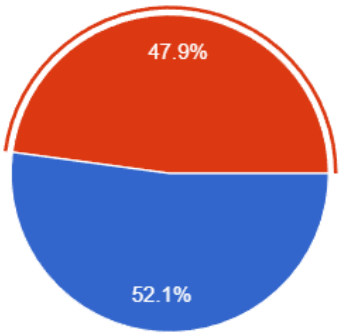
4. Can steganography be applied to conceal messages in audio filea?



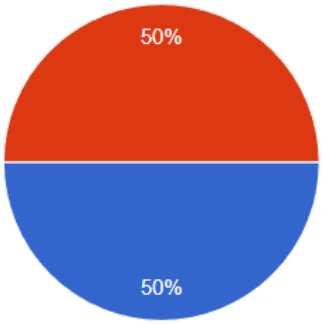
5. Does Steganography focus on hiding the existence of information rather than encrypting it?



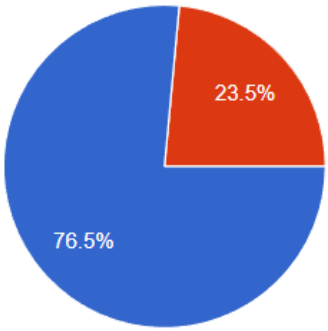
6. Is text embedding a common method in image steganography?



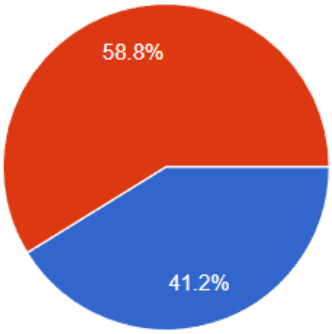
7. Can metadata fields, such as EXIF data, be manipulated for steganographic purpose?



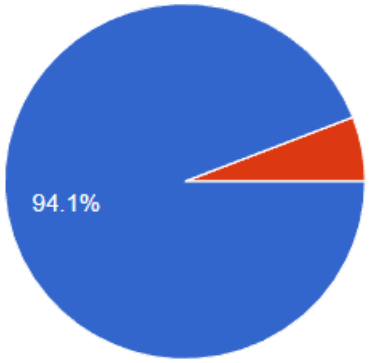
Is watermarking a technique employed in image steganography for subtle information embedding?



Are crytographic signature used in steganography to ensure data integrity?



Does the effectiveness of steganography depend on concealing information with arousing suspicion?



CONCLUSION

In conclusion, image steganography is a powerful and evolving technique that plays a crucial role in secure communication and data protection. By embedding secret information within the pixels of an image, steganography provides a covert channel for transmitting sensitive data without arousing suspicion. This method has proven effective in various applications, including digital watermarking, copyright protection, and confidential communication.

REFERENCES

1See Alattar's "Digital Image Steganography: Survey and Analysis of Current Methods" for information on the most current advancements in this field.

[2Tirkel and Morkel's "Steganography and Steganalysis: Concepts and Practice" is an invaluable tool for comprehending the two aspects of the steganographic procedure.

3] Li and Liang's "Steganography in Digital Media: Principles, Algorithms, and Applications" provides practical insights through real-world viewpoints and examples. Memon and Wong's "Introduction to Digital Watermarking" addresses overlaps.