**Pixel Cloak: Image Steganography for Secure Communication**

**Submitted for**

**IMAGE AND VIDEO PROCESSING**

Submitted by:

**(E23MCAG0083) Yash Kanani**

**(E23MCAG0006) Vijay Bhargav Bhamidi**

Submitted to

**DR. DINESH KUMAR**

**Jan-May 2024**

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

A close-up of a logo

Description automatically generated

**INDEX**

|  |  |  |
| --- | --- | --- |
| Sr.No | Content | Page No |
| 1 | **ABSTRACT** | 3 |
| 2 | **INTRODUCTION** | 3 |
| 3 | **RELATED WORK** | 3 |
| 4 | **METHODOLOGY** | 4 |
| 5 | **EXPERIMENTAL RESULT AND DISCUSSION** | 5 |
| 6 | **FUTURE SCOPE** | 6 |
| 7 | **REFERENCES** | 6 |
| 8 | **GitHub Link** | 6 |

1. **ABSTRACT**

Steganography, the art of hidden communication, has evolved from ancient practices to modern digital techniques. This review chronicles the progression of steganography, emphasizing its historical roots and its significance in the digital age. It explores the nuanced art of concealing information, balancing secrecy with the necessity of revelation. The study integrates diverse disciplines to unveil the sophisticated methods and applications of steganography, highlighting its role in securing confidential data and facilitating discreet exchanges. It portrays steganography as a confluence of historical knowledge and technological advancement, adept at masking messages in both tangible and intangible realms. In an era marked by heightened privacy concerns, steganography stands out as a critical tool for safeguarding information against the backdrop of pervasive digital communication.

1. **INTRODUCTION**

Steganography, derived from the Greek words for “covered” and “writing,” is a time-honoured method of secret communication that has persisted throughout history. From hidden inscriptions in wax tablets to modern techniques of embedding data within digital media, steganography has evolved significantly, becoming a complex fusion of art and technological science.

This review takes you through the intricate history and modern relevance of steganography in our digital era. It examines its beginnings, uses, and progress, highlighting the delicate balance between hiding and exposing information. This practice not only protects information from unwanted detection but also integrates it seamlessly into ordinary communication channels.

Incorporating knowledge from various fields such as mathematics, computer science, cybersecurity, and signal processing, this study explores the depths of steganographic methods and applications. It sheds light on the secret methods and strategies used to secure confidential information and enable discreet communication.

This investigation reveals that steganography is more than just a means of hiding; it represents a blend of historical insight and contemporary technological progress, where messages are concealed within both the physical and the digital worlds, seen and unseen. In today’s world, where constant connection brings increased privacy and security risks, the study of steganography becomes crucial, providing a hidden haven for information protection in the midst of overwhelming digital chatter.

1. **RELATED WORK**

Steganography, derived from the Greek words "steganos" (covered) and "graphein" (to write), is the art and science of concealing information within non-secret mediums to evade detection by unintended recipients. Dating back to ancient civilizations, steganography has evolved from physical methods like invisible ink and microdots to sophisticated digital techniques in the modern era.

In contemporary literature, steganography has garnered significant attention due to its applications in various domains, including cybersecurity, data transmission, and covert communication. Researchers have explored both theoretical frameworks and practical implementations of steganographic algorithms to enhance data security and privacy.

Theoretical studies delve into the mathematical principles underlying steganography, analyzing factors such as capacity, imperceptibility, and robustness of hidden data. These investigations often employ mathematical models like information theory and signal processing to optimize steganographic algorithms for efficient data embedding and extraction while maintaining covert communication.

On the practical front, researchers focus on developing steganographic techniques compatible with digital media formats such as images, audio, and video. Advances in machine learning and deep neural networks have enabled the creation of sophisticated steganalysis tools capable of detecting hidden information, prompting the development of more robust steganographic algorithms to counter detection efforts.

Moreover, the integration of steganography with encryption techniques, known as steganography encryption, provides an additional layer of security by encrypting the hidden data before embedding, further enhancing confidentiality.

Overall, the literature on steganography reflects its growing significance in safeguarding sensitive information and facilitating covert communication in an increasingly digitized world. As the field continues to evolve, interdisciplinary collaboration between mathematicians, computer scientists, and cybersecurity experts will be pivotal in advancing steganographic techniques and addressing emerging challenges.

1. **METHODOLOGY**

In this section we will discuss on the working of our proposed method.

* 1. Importing Essential Libraries:

The libraries used in the process are Python Imaging Library (PIL), Image module, NumPy, and Matplotlib libraries

* 1. Creating Encryptor and De-cryptor:

Function: fill\_lsb(pixels)

This function facilitates the manipulation of pixel values within an image. It accepts an array of pixel values as input and is designed to flip the least significant bit (LSB) of the last pixel value in the array. The LSB manipulation serves as a fundamental operation for encoding and decoding information within the image.

Function: decrypt\_pixels(image)

The decrypt\_pixels() function forms a pivotal component of the decryption process. It operates on the entire image array, employing a systematic approach to deciphering encoded information. By examining the LSBs of seven consecutive pixels, the function discerns ASCII characters concealed within the image. This iterative process ensures comprehensive extraction of the hidden message embedded within the image.

Function: encrypt\_text\_in\_image(image, text)

In the encryption process, the encrypt\_text\_in\_image() function amalgamates text data into the image while ensuring seamless concealment. Initially, the image is flattened to facilitate efficient data manipulation. Special escape characters are strategically inserted within the image to demarcate the boundaries of the hidden message. For each character in the input text, the function dynamically adjusts the LSBs of the image pixels, thereby encoding the text imperceptibly into the image data.

Function: save\_image(image, path)

The save\_image() function orchestrates the preservation of the encrypted image onto a specified file path. Leveraging the capabilities of the Python Imaging Library (PIL), the flattened image data is reshaped and reconstructed into a coherent visual representation. Subsequently, the finalized image is stored in the designated location, ensuring accessibility and persistence of the encrypted content.

Function: decrypt\_image(path)

Integral to the decryption process, the decrypt\_image() function endeavors to retrieve concealed information from the encrypted image. Upon opening the image file, the function flattens the image data, thereby preparing it for systematic analysis. Iteratively, the function inspects the flattened array, decoding ASCII characters by examining the LSBs of pixel clusters. Notably, the function incorporates a mechanism to detect and halt decoding upon encountering designated escape characters, ensuring precise extraction of the concealed message.

1. **EXPERIMENTAL RESULT AND DISCUSSION**

Using this methodology, we achieved remarkable success in concealing binary data within images without altering their visible characteristics. This was made possible by leveraging the inherent psychovisual redundancy present in images, allowing us to manipulate bits with minimal impact on the actual pixel values.

Subsequently, encrypted images can be decrypted using the designated function, enabling the extraction of hidden messages. Notably, the encryption and decryption process is highly efficient, with modern-day machines capable of executing it in real-time without imposing a significant burden on computational resources.

The foloowing are some examples and results

|  |  |  |  |
| --- | --- | --- | --- |
| Original image | Message to be encypted | Resultant image  Creative representation of hidden message 01010111 | Decypted message |
|  | Yash Kanani Message |  | Yash Kanani Message <-END-> |
|  | There is a hidden message | Creative representation of hidden message 0101010110011 | There is a hidden message <-END-> |

1. **FUTURE SCOPE**

Presently, the embedded message appears only once in the encrypted image. Consequently, if that specific portion of the image is corrupted or inadvertently cropped by an application, the message would be irretrievably lost. To address this vulnerability, we are endeavoring to devise a method wherein the message will be embedded multiple times throughout the image, spanning from its corners to its center and surrounding areas.

This approach eliminates the need to conceal bits within every individual pixel, albeit at the cost of increased processing time. By strategically selecting key locations and preserving copies of the embedded messages, we aim to ensure sufficient redundancy and accuracy to mitigate any potential corruption or cropping issues effectively.

Furthermore, we are also developing an algorithm that diverges from the conventional method of simply encoding bits into the least significant bit (LSB) of an image. Instead, our algorithm strategically selects pixels at intervals of (n\*n + 1) to embed the message. This approach ensures that even if an adversarial user attempts to scrutinize all the bits, they won't discern the message easily, except for a few bits. We incorporate escape characters strategically placed in the gaps that deviate from the formula. As a result, only the initial few characters of the message can be deciphered from the image.

1. **REFERENCES**
2. Zhang, Q., Guo, Z., Zhu, Y., Vijayakumar, P., Castiglione, A., & Gupta, B. B. (2023). A deep learning-based fast fake news detection model for cyber-physical social services. Pattern Recognition Letters, 168, 31-38.
3. Chen, M. Y., Lai, Y. W., & Lian, J. W. (2023). Using deep learning models to detect fake news about COVID-19. ACM Transactions on Internet Technology, 23(2), 1-23.
4. Kishwar, A., & Zafar, A. (2023). Fake news detection on Pakistani news using machine learning and deep learning. Expert Systems with Applications, 211, 118558.
5. **GitHub Link**

[GitHub - YashKanani11/SecureIMG-stegnography](https://github.com/YashKanani11/SecureIMG-stegnography)