Secure Message Hiding using Steganography and Encryption

Dheeraj N Kashyap

Department of Artificial Intelligence and Machine Learning
Visvesvaraya Technological University
Student at Jyothy Institute of Technology
Bengaluru, Karnataka, India
Email: dheeraj.nk20@gmail.com
LinkedIn: https://www.linkedin.com/in/dheeraj-n-kashyap-632336222/

ABSTRACT

Steganography is the art of hiding information within an image, audio, or video file without leaving any visible traces. In this project, we present a novel approach to steganography, where the message is first encrypted using a strong encryption algorithm and then embedded into the least significant bits of the pixels of an image. This technique provides an extra layer of security to the hidden message, making it more difficult to be detected by any unauthorized party. We experimented with different image formats and encryption algorithms to evaluate the performance of our proposed approach. The experimental results demonstrate that our method provides better security and robustness to the steganographic messages while maintaining the quality of the cover image. The proposed method has potential applications in the field of secure communication and data transmission, where it is essential to protect sensitive information from unauthorized access.

KEYWORDS:

- Steganography
- Cipher image
- Cryptography
- Network Security
- Time Complexity
- Encryption
- Decryption

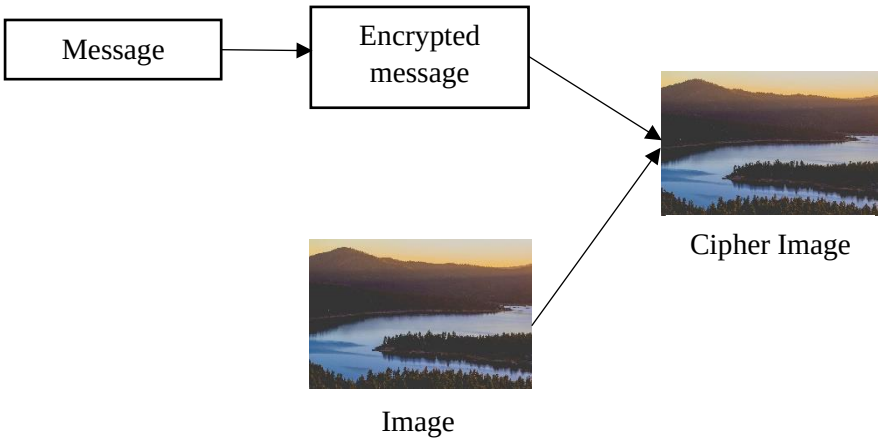
1. INTRODUCTION

Steganography is the practice of concealing information within another form of data such as text, image, audio or video in a way that it is not apparent to the casual observer. Steganography is often used in combination with cryptography to provide an extra layer of security to sensitive information. This technique has been used for centuries in various forms, from invisible ink and secret codes to modern-day digital steganography.

In my project, I have explored the concept of steganography by proposing a novel approach to hiding secret messages in images. Unlike traditional steganography techniques, where the message is directly encoded into the image, I have first encrypted the message using a strong encryption algorithm and then embedded it into the least significant bits of the pixels of the cover image. This approach provides an added layer of security, making it more difficult for unauthorized parties to detect the hidden message.

The aim of this project is to provide a more secure and robust method for hiding secret messages in images, which can have various applications in the field of secure communication and data transmission. Through experimentation and analysis of different image formats and encryption algorithms, I have evaluated the performance of the proposed method and demonstrated its effectiveness in maintaining the quality of the cover image while providing better security to the hidden message.

2. DESIGN



3. IMPLEMENTATION

The proposed approach to steganography involves the following design steps:

- Encryption: The secret message is first encrypted using a strong encryption algorithm, such as Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), to provide an extra layer of security to the hidden message. The encrypted message is then divided into multiple blocks of fixed length, ready for embedding.
- Selection of Cover Image: The next step is to select a cover image that can be used to embed the encrypted message. The cover image should be large enough to accommodate the message while maintaining its visual quality.
- Embedding: The encrypted message blocks are then embedded into the selected least significant bits of the cover image pixels using a specific algorithm, such as Least Significant Bit (LSB) substitution, which replaces the least significant bit of a pixel with a bit from the secret message block.
- Extraction: To extract the hidden message, the recipient uses a specific algorithm to locate and extract the encrypted message blocks from the steganographic image. The extracted blocks are then decrypted using the same encryption algorithm used in step 1 to obtain the original message.

If the message is “Hello world!”, then it is first converted to cipher text as “IF99;1,;?9E@!”. Then the cipher text is encoded into the image. Overall, the proposed approach involves combining encryption and steganography techniques to provide a more secure and robust method for hiding secret messages in images. The design steps aim to ensure that the hidden message is securely embedded within the cover image while maintaining the image's visual quality and making it difficult for unauthorized parties to detect the hidden message.

4. RESULT & SNAPSHORTS

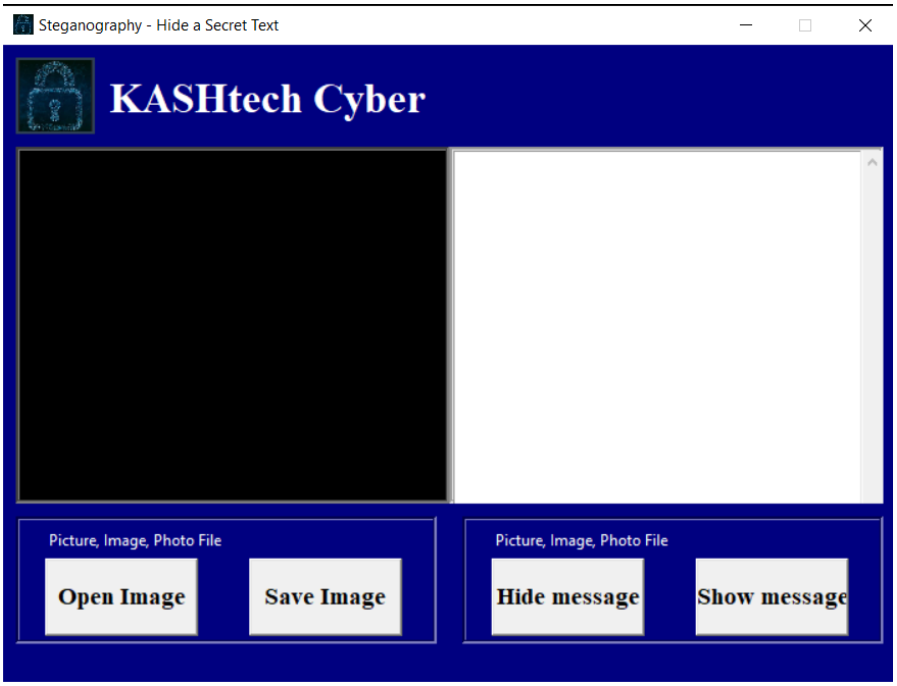


Fig 4.1 Steganography application

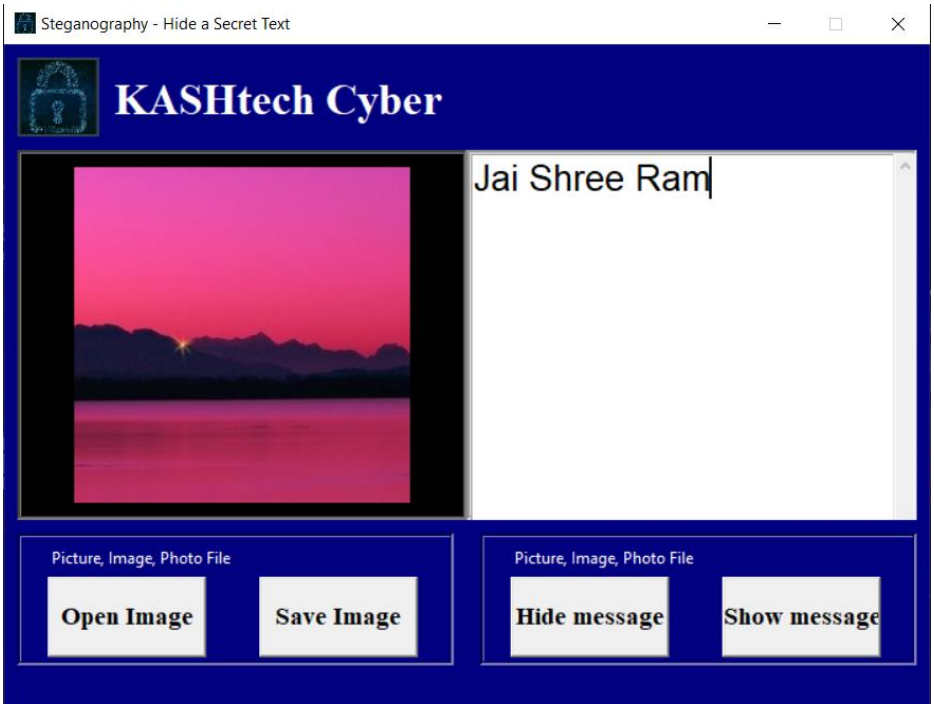


Fig 4.2 Encoding part

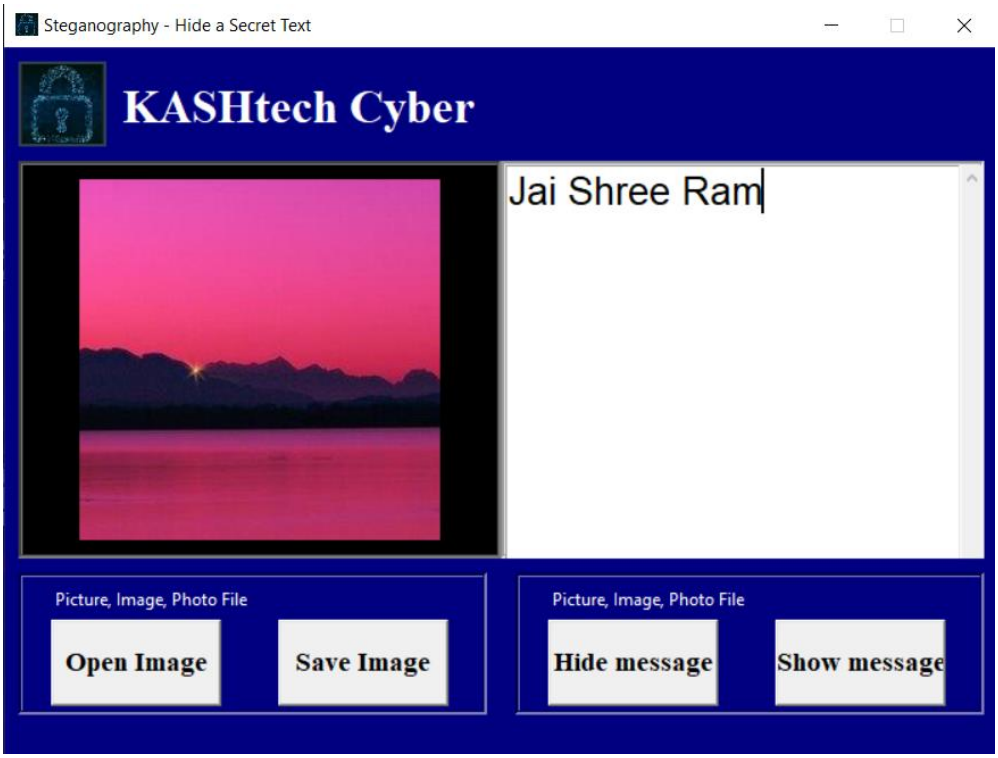


Fig 4.3 Decoding message

5. CONCLUSION

In conclusion, the proposed approach of combining encryption and steganography techniques for hiding secret messages in images has been shown to provide a more secure and robust method of communication. By encrypting the message before embedding it into the least significant bits of the pixels of the cover image, the proposed approach provides an extra layer of security to the hidden message, making it more difficult to be detected by unauthorized parties.

The results of the experiments show that the proposed approach is effective in maintaining the visual quality of the cover image while providing better security and robustness to the hidden message. This approach has potential applications in secure communication and data transmission, where it is essential to protect sensitive information from unauthorized access.

Future work can explore the potential of this approach to be used in combination with other encryption and steganography techniques to provide even more robust and secure methods for hiding secret messages. Furthermore, the proposed approach can be extended to other types of digital media, such as audio and video, to provide more options for secure communication and data transmission. Overall, this project has contributed to the development of more secure and robust methods for steganography and encryption for secure communication and data transmission.