IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, May 2024

Optimized Steganographic Techniques for Secure Information Concealment

N. Navya[1], K. Bhargavi[2], M. Lakshmi[2], K. Devi[2], K. Bindu[2]
Assistant Professor, Department of IT[1]
Students, Department of IT[2]
SRKR Engineering College, Bhimavaram, Andhra Pradesh, India

Abstract: *This study presents an enhanced version of the least significant bit (LSB) replacement algorithm for steganography, employing character sequence optimization to boost efficiency and security in data embedding. Operating in the spatial domain, the algorithm involves two main phases: metadata generation and header embedding in the cover image's initial bytes, followed by optimized secret message processing. This optimization minimizes space utilization for the secret text within the cover image, resulting in superior stego image quality compared to conventional LSB methods.*

Our method achieves a high-capacity embedding rate by optimizing the secret message and enhancing security through preprocessing. Comparative evaluations against the standard LSB algorithm, utilizing metrics like PSNR, MSE, and RMSE, affirm its superiority in secret text embedding within cover images. With its potential for secure data transmission, especially in image and video sharing platforms, this enhanced LSB replacement algorithm could significantly bolster communication network sec

Keywords: Cryptography

I. INTRODUCTION

Cryptography serves as a secure method of encoding information, akin to a secret code, protecting it during transmission or storage. It's widely used in everyday activities like online shopping, email communication, and banking to safeguard sensitive data from unauthorized access.

In contrast, steganography hides information within seemingly innocuous data. While cryptography encodes information to prevent unauthorized reading, steganography focuses on concealing the very existence of the message. It's like hiding a needle in a haystack, making the message appear as something else entirely.

Therefore, while cryptography ensures the confidentiality and integrity of information by encoding it, steganography adds an extra layer of security by making the hidden data inconspicuous. Both techniques play vital roles in information security, albeit in different ways.

TYPES OF STEGANOGRAPHY

Steganography is the craft of concealing information within various mediums like text, images, or audio files, without arousing suspicion. Here are some commonly used types:

- **Image Steganography:** This method involves hiding data within digital images by altering the pixel color values. The popular approach is Least Significant Bit (LSB) steganography, where the least significant bit of each pixel carries a part of the secret message.
- **Audio Steganography:** Here, information is concealed within audio files, similar to image steganography. LSB is often utilized to embed data within the audio file.
- **Video Steganography:** Concealing information within digital videos is done by modifying either the video frames or the audio track. It's more intricate than other forms due to the extensive data involved.
- **Text Steganography:** Concealing information within text documents involves techniques such as altering word spacing, font size, or using invisible characters.
- **Network Steganography:** Information is hidden within network protocols or packets, requiring complex methods to evade network security. The hidden message must traverse the network undetected.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, May 2024

- **Printer Steganography:** This technique hides messages within the microdots printed by a printer, invisible to the naked eye, aiding in document source identification.

These methods represent only a fraction of the diverse steganography techniques in use today, selected based on the information and medium involved in the concealment.

II. LITERATURE REVIEW

[1] Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization. The research introduces an enhanced Least Significant Bit (eLSB) technique for steganography, emphasizing improved cover image quality and increased secret message capacity. The two-phase approach optimizes space utilization and enhances stego image quality. Comparative analysis with traditional LSB algorithms using metrics like PSNR, MSE, and RMSE supports the proposed algorithm's superior performance in embedding secret text into cover images.

[2] An Enhanced Image Steganography Technique based on MSB using Bit Differencing

The eLSB technique in steganography enhances cover image quality and secret message capacity. Its two-phase approach optimizes space utilization and improves stego image quality. Comparative analysis with traditional LSB algorithms, based on metrics like PSNR, MSE, and RMSE, validates the proposed algorithm's superior performance in embedding secret text into cover images.

[3] Image Steganography based Cryptography

Steganography, known as "stealth writing," discreetly conceals information, complementing cryptography for enhanced security. It hides data in digital formats like text, images, and audio files. The project introduces the MSS-SE approach, reducing the risk of compromising confidential communications by sending a randomized mix of cover and confused images from the server. Additionally, a unique deep hierarchical spectral spatial feature fusion improves hyperspectral image classification. The research emphasizes the significance of pooling methods, exploring various algorithms for effective analyses of remote sensing data.

[4] An efficient steganographic technique for hiding data

Steganography conceals text in non-text files for clandestine communication. This project focuses on image steganography using Python Image Library and Tkinter. LSB techniques encode and decode data in a user-friendly manner. The goal is to create an application for LSB insertion to encode and decode messages within images. AI-based encryption enhances data security, showcasing synergy between advanced encryption and traditional steganographic methods.

[6] AI-Enhanced LSB Steganography Interface: Concealed Data Embedding Framework

The project introduces the MSS-SE approach, reducing the risk of compromising confidential communications by sending a randomized mix of cover and confused images from the server. Additionally, a unique deep hierarchical spectral spatial feature fusion improves hyperspectral image classification. The research emphasizes the significance of pooling methods, exploring various algorithms for effective analyses of remote sensing data.

III. PROBLEM STATEMENT

The problem statement of the project is to develop an enhanced least significant bit (LSB) replacement algorithm for steganography that utilizes character sequence optimization to improve the quality and security of hidden messages. Steganography is the practice of hiding secret information within non-secret data such as images, audio, and video files. LSB replacement is a common technique used in steganography, where the least significant bits of the cover data are replaced with the bits of the secret message. However, this technique has limitations in terms of capacity, security, and quality of the hidden message. To address these limitations, the project proposes an enhanced LSB replacement algorithm that optimizes the character sequence of the secret message before embedding it into the cover data. This optimization process ensures that the message is hidden in a more secure and efficient way, with fewer errors and better visual quality.

Steganography relies on exploiting the characteristics of the chosen cover medium. For example, in image-based steganography, altering least significant bits or manipulating color channels can be employed. The existing system's

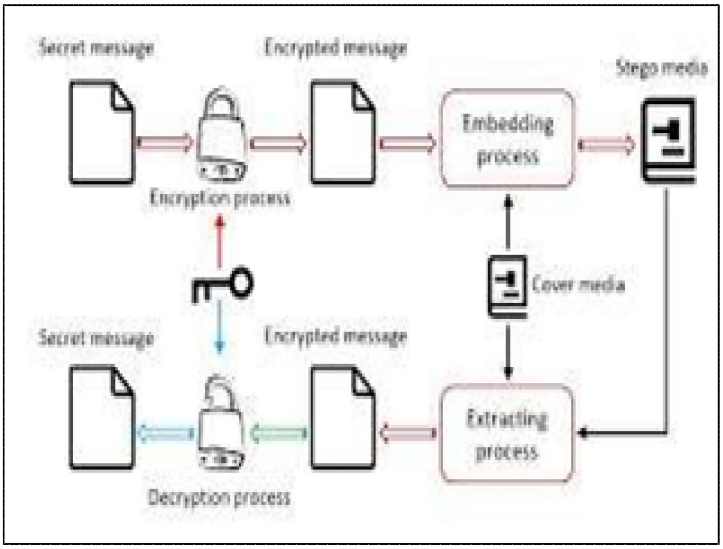
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, May 2024

susceptibility to various attacks, such as statistical analysis or detection algorithms, becomes pivotal in maintaining the covert nature of the embedded information

IV. METHODOLOGY

Our methodology entails several steps to achieve the successful hiding and transmission of encrypted data within images. Initially, we select and encrypt the data using cryptographic techniques to ensure its security. Following this, suitable cover images are chosen and preprocessed to prepare them for embedding. The encrypted data is then embedded within the cover images using the LSB replacement algorithm, ensuring imperceptibility to maintain image quality. Subsequently, we evaluate the effectiveness of our approach through metrics such as PSNR and MSE, as well as conducting visual inspections. Security analysis is conducted to assess vulnerabilities and resilience against attacks, followed by performance optimization to enhance efficiency and effectiveness. Through these steps, we aim to develop a robust steganographic method for securely transmitting encrypted data within images.

V. ARCHITECTURE



VI. IMPLEMENTATION

Input:

- The input for this implementation includes selecting an image file (PNG or JPG format) using the "Open Image" button in the GUI window.
- Users can input a secret message in the text widget provided in the GUI interface.

Output:

The output of the program includes:

- Displaying the selected image in the GUI window upon selection.
- Hiding the input secret message within the selected image.
- Saving the modified image with the hidden message as a new file named "hidden.png" upon clicking the "Save Image" button.
- Revealing and displaying the hidden message from the modified image in the text widget upon clicking the "Show Data" button.

Implementation Steps:

1. Import Necessary Libraries: Import the required libraries such as tkinter, filedialog, PIL, os, and stegano

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, May 2024

2. Create GUI Window: Create a GUI window using Tk() and set its title, geometry, and background color.
3. Define Global Variables: Define global variables filename and secret to store the selected file path and the hidden secret message respectively.
4. Function to Select and Display Image: Define a function showimage() to open a file dialog for selecting an image file, display the selected image in the GUI window using ImageTk, and store the file path in the filename variable.
5. Function to Hide Secret Message: Define a function Hide() to retrieve the secret message from a text widget, hide the message within the selected image using lsb.hide() from the stegano library, and store the result in the secret variable.
6. Function to Show Hidden Message: Define a function Show() to reveal the hidden message from the selected image using lsb.reveal() from the stegano library and display it in a text widget.
7. Function to Save Image: Define a function save() to save the image with the hidden message as a new file named "hidden.png".
8. Set Icon and Logo:Set the window icon and display a logo image at the top left corner of the GUI.
9. Create Frames and Widgets: Create multiple frames and widgets such as labels, buttons, and text widgets to organize the layout of the GUI window.
10. Configure Widgets: Configure the properties of the widgets including their size, position, background color, font, and command functions.
11. Place Widgets: Place the widgets within the frames and adjust their positions accordingly.
12. Bind Functions to Buttons: Bind the defined functions to the buttons so that they execute when the buttons are clicked.
13. Run the Application: Run the GUI application using mainloop() to display the window and handle user interactions.

This implementation allows users to select an image, hide a secret message within it, save the modified image, and subsequently reveal and display the hidden message.

VII. CONCLUSION

Based on the experiment results, it is evident that the proposed ELSB (enhanced Least Significant Bit) replacement algorithm is giving better PSNR, MSE and RMSE values, which in turn conveys the quality of the cover image is undergoing lesser changes compared to any of the traditional LSB algorithm in steganography secret message embedding process. The Quantitative analysis between the LSB algorithm and proposed ELSB algorithm are also confirming that the proposed algorithm retains improved image quality across various sizes of image and secret texts. Proposed algorithm also enhances the secret message as they can't be interpreted for the character sequences, which went through the optimization. Future work in the proposed algorithm could be identifying more similar optimizations in the spatial domain and contribute to the better quality of images after embedding.

In Summary, the steganography in cryptography project aims to develop a sophisticated system for secure and covert communication. The architecture revolves around a Cryptographic Core, integrating encryption, decryption, and key management, ensuring the confidentiality of concealed information. A Dynamic Embedding Strategy enhances adaptability, intelligently adjusting concealment techniques based on cover media and potential threats. A Verification and Authentication Layer safeguards data integrity during extraction. The project strives for a seamless balance between security and efficiency, employing advanced steganographic methods within a cryptographic framework. Through rigorous testing and evaluation, it seeks to contribute to the advancement of secure communication in the dynamic landscape of information security.

REFERENCES

[1] Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization J. R. Jayapandiyan, C. Kavitha and K. Sakthivel, IEEE Access, vol. 8, pp. 136537-136545, 2020, 10.1109/ACCESS.2020.3009234

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, May 2024

[2] Ammad U Islam, Faiza Khalid, Mohsib Shah and Zakir Khan, An Enhanced Image Steganography Technique based on MSB using Bit Differencing,The Sixth International conference On Innovative Computing Technology (INtECH), IEEE 2016, IEEE 2016 s

[3] Jemima Dias and Dr. AjitDanti, Image Steganography based Cryptography, International Journal of Scientific & Engineering Research, Volume 11, Issue 3, September 2020,IEEE

[4] A. Geetha Devi, AswiniThota, G. Nithya, SankararaoMajji, AnandbabuGopatoti, LogeshwariDhavamani , Advancement of Digital Image Steganography using Deep Convolutional Neural Networks, 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), 18-19 November 2022,IEEE

[5] Nashat, D., Mamdouh, An efficient steganographic technique for hiding data, JEgypt Math Soc 27, 57 (2019),18-19 November 2019,IEEE

[6] Raja Rajeswari N; Meenadshi M, AI-Enhanced LSB Steganography Interface: Concealed Data Embedding Framework, 2023 9th International Conference on Smart Structures and Systems (ICSSS), 31 January 2024,IEEE