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: 7.67
Volume 5, Issue 2, March 2025

Secure Data Transfer using Image Steganography and Cryptography with Rail Fence

Prof. Shrikant S. Gurav, Sahil Kadam, Atharv Gurav, Saurabh Sawant, Aniket Shinde, Akash Kadam
Sant Gajanan Maharaj College of Engineering, Mahagaon, Kolhapur, Maharashtra, India

Abstract: *In today's world, secure data transfer is essential. This research paper introduces a simple and effective solution by combining Image Steganography and Rail Fence Cryptography to protect information. First, the hidden message is secured with Rail Fence Cipher encryption. Then messages are hidden inside images using the Least Significant Bit (LSB) technique, which makes changes invisible to the human eye. This double layer of protection keeps the information safe and hidden from attackers. The system, "Secure Data Transfer Using Image Steganography and Cryptography with Rail Fence" utilizes a hybrid approach combining cryptography with rail fence and image steganography with LSB method to safeguard data transfer. This hybrid method aims to enhance security and privacy in data transmission, particularly when sensitive or confidential information needs to be exchanged.*

Keywords: Secure Data Transfer, Image Steganography, Rail Fence Cryptography, Least Significant Bit (LSB).

I. INTRODUCTION

This project presents a web tool for secure data transfer of text messages using a security approach, combining cryptography and image steganography. The system, "Secure Data Transfer Using Image Steganography and Cryptography with Rail Fence," aims to improve the security of data transmission, especially when sensitive information is involved. It utilizes a dual-layer security method to ensure data confidentiality, integrity, and secure access through user authentication mechanisms. By leveraging technologies such as Django, Python, and sqlite3, the project aims to provide robust security solutions across various domains, including social security, detective agency, government sectors and corporate communication. The system will utilize encryption algorithms like Rail Fence and the LSB method for image steganography to ensure maximum accuracy in data transfer without errors or data loss. The Rail Fence Cipher, often referred to as the "Zigzag Cipher," derives its name from the way plaintext is arranged in a zigzag pattern within a rectangular grid before being read row-wise to produce the ciphertext.Image steganography hides the encrypted data within an image, making it less likely to be detected by potential attackers or third party. This technique embeds secret data by substituting the least significant bits of image pixels with the bits of the hidden information.

II. METHOD

1. Rail Fence

The Rail Fence Cipher is a type of transposition cipher where plaintext is written in a zigzag pattern across multiple rows (rails) and then read sequentially, row by row, to generate the ciphertext. It does not change the letters but alters their positions, making it harder to read directly. The number of rails determines the complexity of the encryption, with higher rails increasing the level of scrambling.

Decryption requires reconstructing the zigzag pattern to retrieve the original message. This cipher is simple to implement but is not very secure, as it can be easily broken using pattern analysis or anagramming techniques. It is primarily used for educational purposes to understand basic cryptographic principles.

Example:

The plaintext we have i.e. "defend the east wall" having a key size or the size of the row is 3, we get the encryption method below, and the cipher text became: "dnetleedheswlxftaax".

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: 7.67
Volume 5, Issue 2, March 2025

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Fig 1.1 Rail Fence Cipher

2. ASCII Code Encryption:

ASCII code encryption by shifting, also known as a Caesar cipher, is a substitution cipher where each letter in the plaintext is shifted a certain number of positions down or up the alphabet. In the context of ASCII code, each character is represented by a unique numerical value. The basic idea behind this encryption technique is to modify these numerical values by adding or subtracting a fixed number, known as the shift value, to each character's ASCII code.

Here's how it works step by step:

1. Convert Characters to ASCII: First, each character in the plaintext message is converted to its corresponding ASCII value, example the ASCII value of 'A' is 65, 'B' is 66, and it continues sequentially for other characters.

2. Shift the ASCII Values: The ASCII values of the characters are then shifted by a fixed number of positions. For example, if the shift

value is 3, 'A' (65) becomes 'D' (65 + 3 = 68), 'B' (66) becomes 'E' (66 + 3 = 69), and so forth. 17

3. Wraparound: In the case of the English alphabet, if the shift extends beyond 'Z' (90) for positive shifts or before 'A' (65) for negative shifts, the alphabet wraps around. For example, with a shift of 3, 'X' (88) would become 'A' (88 + 3 = 91, but due to wraparound, it becomes 65).

4. Convert Back to Characters: Finally, the modified ASCII values are converted back to characters. Each shifted ASCII value corresponds to a specific character, forming the encrypted message.

For example, let's say we want to encrypt the message "DEFENDTHEWALL" with a shift value of 3:

'D' (68) + 3 = 71, which corresponds to 'G'
'E' (69) + 3 = 72, which corresponds to 'H'
'F' (70) + 3 = 73, which corresponds to 'I'
'E' (69) + 3 = 72, which corresponds to 'H'
'N' (78) + 3 = 81, which corresponds to 'Q'
'D' (68) + 3 = 71, which corresponds to 'G'
'T' (84) + 3 = 87, which corresponds to 'W'
'H' (72) + 3 = 75, which corresponds to 'K'
'E' (69) + 3 = 72, which corresponds to 'H'
'W' (87) + 3 = 90, which corresponds to 'Z'
'A' (65) + 3 = 68, which corresponds to 'D'
'L' (76) + 3 = 79, which corresponds to 'O'
'L' (76) + 3 = 79, which corresponds to 'O'

So, the encrypted message for "DEFENDTHEWALL" with a shift of 3 would be "GHIHQGWKHZDOO".

The text "GHIHQGWKHZDOO" is converted into binary by first determining the ASCII values of each character and then representing them in 8-bit binary form. The ASCII values are: G (71), H (72), I (73), H (72), Q (81), G (71), W (87), K (75), H (72), Z (90), D (68), O (79), O (79). Converting these to binary,

We get: 01000111 01001000 01001001 01001000 01010001 01000111 01010111 01001011 01001000 0101101001000100 0100111101001111. This binary representation is crucial in computer systems as it allows text data to be stored, processed, and transmitted efficiently. It is widely used in cryptography, networking, and digital communication to encode messages securely. Understanding binary conversions is fundamental in fields like programming, encryption, and data transmission.

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: 7.67
Volume 5, Issue 2, March 2025

3. Image Steganography using LSB:

Images consist of pixels, where each pixel represents a specific colour value. In grayscale (black and white) images, pixel values range from 0 to 255, with 0 indicating black and 255 representing white. One method of embedding secret data involves modifying the least significant bits of the image pixels to store the hidden information. The image obtained after embedding is almost similar to the original image because the change in the LSB of the image pixel does not bring too many differences in the image. For example, 0 is black. Modifying the value to 1 will have minimal impact, as it remains black but appears as a slightly lighter shade.

In a 24-bit image, each colour component—red, green, and blue—is represented by a byte. This allows for the storage of one bit in each colour channel, meaning a total of 3 bits can be embedded per pixel. Consequently, an image with a resolution of 800 × 600 pixels can accommodate up to 1,440,000 bits or 180,000 bytes of hidden data. For example, a grid for 3 pixels of a 24-bit image can be as follows: (00101101 00011100 11011100) (10100110 11000100 00001100) (11010010 10101101 01100011).

When the number 200, whose binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows: (0010110**1** 0001110**1** 1101110**0**)
(1010011**0** 1100010**1** 0000110**0**)
(1101001**0** 1010110**0** 01100011)

4. Flow Chart:

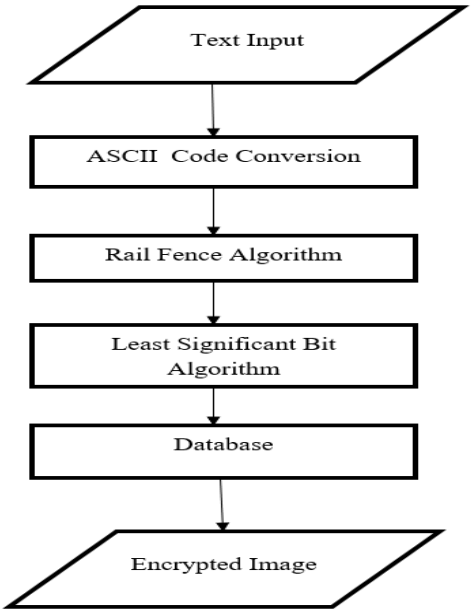

Fig 4.1 Module Design

Here is a brief explanation of each step in the flowchart:

1. Text Input:

The user provides the plain text that needs to be encrypted.

2. ASCII Code Conversion:

The input text is converted into its corresponding ASCII values to facilitate further encryption.

3. Rail Fence Algorithm:

A transposition cipher technique that rearranges characters in a zigzag pattern across multiple rails to enhance security.

4. Least Significant Bit (LSB) Algorithm:

A steganography technique where encrypted data is hidden within the least significant bits of an image.

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: 7.67
Volume 5, Issue 2, March 2025

5. Database:
The modified image containing the hidden encrypted text is stored in a database for retrieval.
6. Encrypted Image:
The final output is an image containing the encrypted message, which can only be retrieved using the decryption process

5. Architecture Diagram

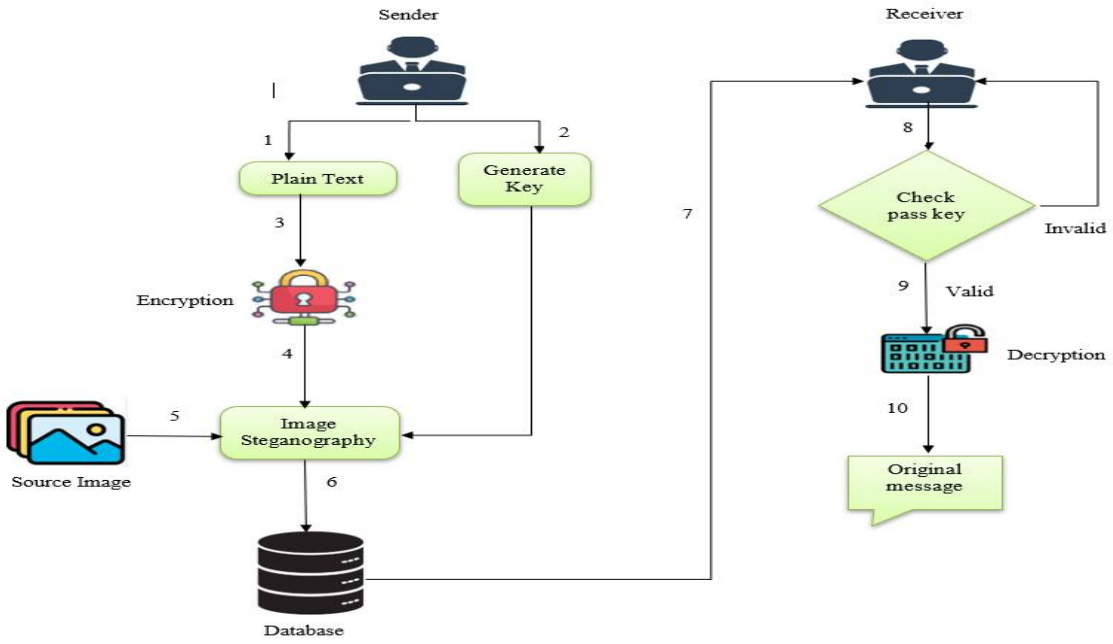

Fig 5.1 Architecture Diagram

Steps involved in Architecture Diagram:

Sender Side:

1. Plain Text Input: The sender starts with the original message.
2. Generate Key: A secret key is generated for encryption.
3. Encryption: The plain text message is encrypted using the generated key.
4. Apply Encryption: The encrypted message is now ready for embedding.
5. Image Steganography: The encrypted message is embedded into a source image.
6. Store in Database: The steganographic image is stored in a database for secure transmission.

Receiver Side:

7. Retrieve Stego Image: The receiver fetches the image from the database.
8. Check Pass Key: The receiver enters the decryption key.
9. Validation: If the key is valid, the system proceeds; otherwise, access is denied.
10. Decryption: The encrypted message is extracted and decrypted using the key.
11. Original Message: The receiver retrieves the original plaintext message.

III. CONCLUSION

The system, "Secure Data Transfer Using Image Steganography and Cryptography with Rail Fence," presents an advanced hybrid framework that synergizes cryptographic encryption with image steganography to fortify data security during transmission. By employing the Rail Fence cipher for encryption and the Least Significant Bit (LSB) technique

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: 7.67
Volume 5, Issue 2, March 2025

for steganographic embedding, the system establishes a multi-layered security paradigm that ensures data remains both concealed and cryptographically protected, thereby mitigating the risk of unauthorized access. Furthermore, the integration of user authentication mechanisms reinforces identity verification, ensuring that only authorized entities can retrieve the embedded information. This approach significantly enhances the confidentiality, integrity, and resilience of data transmission, addressing contemporary cybersecurity challenges. Its adaptability across diverse domains, including healthcare, finance, defence, and business communications, underscores its efficacy as a versatile and scalable solution for securing sensitive information in an increasingly digitalized and security-conscious landscape.

REFERENCES

[1]. Krishna Chaitanya Nunna, Ramakalavathi Marapareddy "Secure Data Transfer Through Internet Using Cryptography and Image Steganography ", IEEE SoutheastCon 2020

[2]. Mohak Kataria, Kurunandan Jain, Narayanan Subramanian, "Exploring Advanced Encryption and Steganography Techniques for Image Security" 2023 11th International Symposium on Digital Forensics and Security (ISDF)

[3]. Suraj Kumar , Santosh Kumar, Neeraj Kumar Singh , Anandaprova Majumder, SuvamoyChangder "A Novel Approach to Hide Text Data in Colour Image", 2018

[4]. Navjot Rathour , Poonam Rawat "Research on Image Stegnography using based on Suduko matrix and LSB Value with multi-level encryption", 2022 IEEE 2nd Mysore Sub Section International Conference (Mysuru).

[5]. M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. Srikanth, and M. Reddy, ''Digital video steganography using LSB technique,'' Red, vol. 100111, Apr. 2020, Art. no. 11001001.