WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Multi-Layered Security for Confidential Data Transmission

Archana Gopnaryana, Granthik Bhor, Pritesh Barik, Soham Kambli, Aryan Mahadeshwar, Arya Gabhane

Information Technology, Vidyalankar Polytechnic, Wadala(E), Mumbai-400037

ABSTRACT

The project " Multi-Layered Security for Confidential Data Transmission" focuses on safeguarding your messages during transmission. The Project "Multi-Layered Security for Confidential Data Transmission" devised a method to conceal user's message within an image ensuring it remains highly secure from interception or unauthorized access. Prior to embedding the message it implements layers of protection including compression, password encryption setting expiration dates personalizing it for users and employing advanced encryption algorithms such, as RSA LSB Modulus 4 steganography and the MD5 hash algorithm. Once these security protocols are implemented the message is covertly integrated into the image using steganography techniques. Consequently, even if someone attempts to inspect the image, they will be unable to decipher the concealed message without utilizing decryption tools.

Keywords: Security, RSA-LSB, Encryption, Steganography.

Introduction

In an era defined by the relentless pace of digital communication and the ever-present threat of data breaches, the imperative to safeguard sensitive information during transmission has become more critical than ever before. Recognizing this pressing need, "Multi-Layered Security for Confidential Data Transmission" emerges as a pioneering project at the forefront of ensuring the utmost protection for data in transit. The "Multi-Layered Security for Confidential Data Transmission" project aims to enhance security in message transmission by employing RSA-LSB-Modulus 4 steganography and MD5 hash for data integrity. It prioritizes privacy protection and authenticates receivers via registration details, addressing the need for convenient yet robust security measures. The paper encompasses the methodologies, algorithms, and contributions of the "Multi-Layered Security for Confidential Data Transmission" project, providing insights into its innovative approach to data security.

Image steganography is a technique used to hide secret data within digital images without perceptibly altering their appearance. This covert communication method involves embedding encrypted information into the least significant bits (LSBs) of pixel values in the cover image. The choice of cover image is crucial, as it should possess complex patterns to deter detection. Common encoding techniques include LSB substitution and LSB matching. Optionally, encryption can be applied to enhance security before embedding the data. Stego images, generated after embedding, appear visually like the original images but contain hidden data. Extraction methods analyse the LSBs of stego images to retrieve the embedded information. While offering covert communication and enhanced security, image steganography faces limitations in capacity and vulnerability to detection through steganalysis techniques. Despite these challenges, it remains a valuable tool for secure data transmission, offering an additional layer of protection in digital communication. [1]

The RSA-LSB-Modulus 4 steganography method revolutionizes covert communication techniques by intricately embedding encrypted message bits within specific LSB (Least Significant Bit) positions of image pixels using the RSA encryption algorithm. Unlike conventional LSB steganography approaches, this method introduces a heightened level of sophistication and intricacy, significantly enhancing resistance against detection and removal of hidden messages.

At its core, RSA-LSB-Modulus 4 steganography combines the robust principles of RSA encryption with LSB embedding, forming a formidable layer of security for covert communication. By leveraging RSA encryption's strong cryptographic properties, the method ensures that the embedded message bits remain highly secure and resistant to unauthorized access or decryption attempts. The process involves strategically embedding encrypted message bits into LSB positions, adding complexity, and making detection and removal of hidden messages considerably more challenging. This complexity not only fortifies data security but also raises the bar for conventional LSB steganography detection techniques, rendering them less effective against the sophisticated encryption methods employed.

Furthermore, the RSA-LSB-Modulus 4 steganography method enhances data security standards by offering robust protection for sensitive information during transmission. Its integration of RSA encryption and LSB embedding creates a multifaceted approach that significantly strengthens the security of covert communication channels. In summary, the RSA-LSB-Modulus 4 steganography method represents a significant advancement in covert

communication security, combining the strengths of RSA encryption and LSB embedding to ensure the utmost protection of sensitive information. Its complexity and sophistication set new standards for data security, thwarting conventional detection techniques and ensuring the integrity and confidentiality of transmitted data.[2]

The inclusion of the MD5 hash algorithm enhances the security of the steganographic embedding process by ensuring the integrity of transmitted data. MD5 generates a fixed-size hash value (128-bit) based on the message contents, serving as a powerful deterrent against tampering and unauthorized alterations. Despite vulnerabilities to collision attacks, MD5 remains effective for verifying data integrity in various contexts such as file integrity checks and digital forensics due to its fixed output size and efficiency.

In addition to encryption and integrity checks, the project employs a multifaceted approach to authenticate message recipients. This involves verifying the identity of recipients through unique registration details, monitoring session duration metrics, and compression. By leveraging these factors, the system constructs a robust authentication framework that safeguards against unauthorized access attempts and malicious intrusions. This meticulous verification process ensures the legitimacy of each recipient, thereby upholding the confidentiality of communications and bolstering user confidence in the security of their data exchanges. [3]

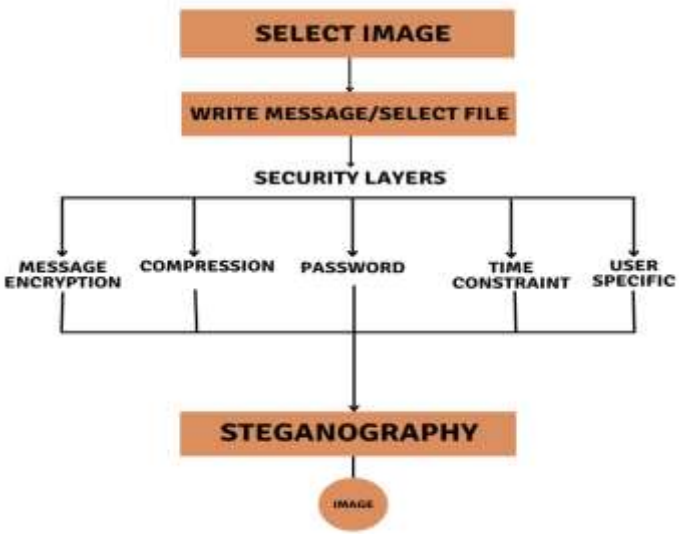
Problem Statement:

In today's digital age, the transmission of sensitive information faces escalating risks of data breaches and unauthorized access. Existing encryption methods and security protocols often prove insufficient against sophisticated cyber threats and covert data interception techniques. There is a pressing need for a comprehensive, multi-layered approach to data transmission security that combines cryptographic strength, integrity verification, and robust authentication mechanisms.

Solution:

Addressing the escalating risks of data breaches and unauthorized access in today's digital age requires a comprehensive, multi-layered approach to data transmission security. The "Multi-Layered Security for Confidential Data Transmission" project offers a robust solution by integrating advanced encryption methods, steganography techniques, and authentication mechanisms. By employing RSA-LSB-Modulus 4 steganography and MD5 hash for data integrity, the project enhances security during message transmission. Leveraging RSA encryption and LSB embedding adds complexity to thwart sophisticated cyber threats, while MD5 hash algorithms ensure the integrity of transmitted data. Additionally, the project adopts a multifaceted approach to authenticate message recipients through registration details, session durations, and GPS tracking, mitigating unauthorized access attempts. Integration with social media APIs facilitates secure online transmission without compromising stringent security protocols. Through its innovative methodologies and algorithms, the project sets new standards for safeguarding sensitive information and establishing trust in digital communication channels.

Working of Systems



Select Image: The user chooses an image file in which they wish to hide the message or file. This image serves as the carrier for the hidden data. It could be any common image format like JPEG, PNG, or BMP.

Write Message/Select File: The user either writes the message they want to send or selects a file they want to embed within the image. This could include sensitive information like classified data, passwords, documents, or any other type of file.

Security Layer: Various security measures are implemented to enhance the reliability of the process. This could involve techniques such as data encryption, access control, error detection, and correction mechanisms to protect the integrity and confidentiality of the embedded data.

Message Encryption: The user's message or file is encrypted using a hash algorithm or any other encryption technique. This ensures that the embedded data remains secure and unreadable without the decryption key.

Compression: Optionally, the user may choose to compress the image to reduce its size before embedding the encrypted data. This can help optimize the file size for transmission and storage. The user can select the compression level based on their preferences.

Password: The user sets a password for the image file. This password adds an additional layer of security to the embedded data, ensuring that only authorized recipients with the correct password can access and decrypt the hidden message or file.

Time Constraint: The user can set a time slot during which the recipient can receive the image. This adds a temporal constraint to the delivery of the embedded message, enhancing security by limiting the exposure of sensitive information.

User Specific: If specified by the user, only the designated recipient mentioned by the user can receive the embedded message. This ensures that the message is delivered securely to the intended recipient and not accessible to unauthorized users.

Steganography: Using steganography techniques, the message or file is embedded within the pixels of the image in a way that is imperceptible to the human eye. This ensures that the hidden data remains covert and undetectable to anyone who might intercept the image.

By incorporating these steps, the process of embedding a message or file within an image becomes more secure, ensuring the confidentiality, integrity, and authenticity of the transmitted data.

Comparison between “Multi-Layered Security for Confidential Data Transmission” and existing technology.

The "Multi-Layered Security for Confidential Data Transmission" project introduces an innovative approach to data transmission security in today's digital era, aiming to address escalating risks of data breaches and unauthorized access. By employing RSA-LSB-Modulus 4 steganography, RSA encryption, MD5 hash algorithms, and authentication mechanisms, the project enhances message and data transmission security while minimizing information exposure risks. Unlike traditional steganography methods, the RSA-LSB-Modulus 4 technique embeds encrypted message bits within specific LSB positions using RSA encryption, adding complexity and sophistication to thwart detection and removal of hidden messages. Additionally, the inclusion of the MD5 hash algorithm ensures data integrity, safeguarding against tampering and unauthorized alterations during transmission. The project's authentication mechanisms, such as receiver validation via registration details and session periods, coupled with integration with social media APIs, offer robust protection against unauthorized access attempts. This multi-layered security approach sets the project apart from existing steganography technologies, emphasizing comprehensive protection and user convenience. Overall, the "Multi-Layered Security for Confidential Data Transmission" project represents a significant advancement in data transmission security, providing a comprehensive solution to safeguard sensitive information in an increasingly interconnected and digitized world.

Conclusion

In conclusion, the "Multi-Layered Security for Confidential Data Transmission" project represents a pioneering effort in safeguarding sensitive information during digital communication. By integrating advanced encryption techniques such as RSA-LSB-Modulus 4 steganography and MD5 hash for data integrity, the project ensures robust protection against unauthorized access and tampering. Through meticulous authentication mechanisms the project not only prioritizes privacy protection but also enhances user experience and accessibility. By setting new standards in covert communication security, this project paves the way for secure and seamless data transmission in an era defined by evolving cyber threats.

References

Research Papers:

1. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9335027
2. https://www.ijert.org/research/rsa-algorithm-and-lsb-steganography-IJERTV2IS100788.pdf
3. https://www.geeksforgeeks.org/what-is-the-md5-algorithm/