HIDING DATA USING ASYMMETRIC CRYPTOGRAPHY AND STEGANOGRAPHY

Govind Yadav*1, Aniket Gupta*2, Sanjeev Kumar*3, Ankur Rai*4, Julie Bhayani*5, Prof. Monika Deshmukh*6

*1,2,3,4,5,6Dept. Of Computer Science & Engineering, Sandip University Nashik, India.

DOI: https://www.doi.org/10.56726/IRJMETS47359

ABSTRACT

Protecting information from unauthorized access has always been a priority during data transit. People have developed different solutions, one of them is steganography. This technique is highly effective in masking data by embedding it within another file, such as an audio or picture file. It creates a layer of security that makes it extremely challenging for unauthorized individuals to access or view the concealed data while it is in transit. To further enhance data security, asymmetric encryption can be integrated with steganography. This involves encrypting the data using asymmetric cryptography before embedding it with steganography. Combining these two methods, an extra layer of protection to the data. To avoid suspicion, it can be helpful to convey private information carefully during conversations on social media.

Keywords: Data Security, Steganography, Asymmetric Cryptography.

I. INTRODUCTION

In the landscape of ensuring secure data transmission, safeguarding information from unauthorized access has consistently been of utmost importance. Over time, diverse strategies have been devised to address this concern, with one notable approach being steganography. This innovative technique proves highly adept at concealing data by seamlessly embedding it within seemingly innocuous files, such as audio or image files. This process establishes a robust layer of security, making it exceedingly challenging for unauthorized entities to intercept or decipher the concealed information during its transit.

To further strengthen data security during transmission, the integration of asymmetric encryption emerges as an important component in confidentiality. By employing ECC asymmetric cryptography, the data undergoes encryption before its concealment through steganography. This collaborative approach not only introduces an additional layer of protection to the transmitted data but also ensures that intercepted information remains cryptic and inaccessible without the appropriate decryption key.

In the context of real-time communication needs, the fusion of LSB image and audio steganography with ECC asymmetric cryptography takes on a new dimension. This innovative combination lays the groundwork for the development of real-time chat software that operates seamlessly while providing enhanced security. By seamlessly integrating these techniques into the architecture of a chat application, conversations conducted on social media platforms can occur with an added layer of privacy and security. This approach aims to evade detection and provides users with increased confidence in the confidentiality of their exchanged information.

II. METHODOLOGY

The primary objective of implementing steganography encryption is to guarantee the secure transfer of data over the Internet. While there are various techniques such as frequency domain methods, spread spectrum techniques, and encryption algorithms like AES, DES, and ECC, this research exclusively focuses on LSB and ECC. Specifically, the steganography aspect employs the Least Significant Bit (LSB) technique, while Elliptic Curve Cryptography (ECC) is utilized for encryption.

Recent years have highlighted vulnerabilities in RSA public keys, notably showcased in the 2020 Keyfactor study, identifying practical vulnerabilities known as 'factoring' in 1 out of every 172 certificates using RSA keys[1]. ECC emerges as a more secure alternative to RSA, addressing the discrete logarithm problem, which is proven to be significantly more challenging than factoring large numbers—the foundation of RSA. ECC's key generation results in smaller keys than RSA adheres to standards, and permits increased data size encryption compared to RSA's limitation to 256 characters. For example, ECC achieves the same security level with a 224-bit key, whereas RSA requires a larger 2048-bit key.
The methodology commences with the generation of ECC keys, both public and private. The private key is employed for encryption, while the public key is shared for decryption, facilitating key exchange between sender and receiver. Subsequently, the message undergoes conversion into ciphertext using the private key. Post-encryption, the steganography method is chosen based on input length, with LSB employed for embedding. The cover medium, randomly chosen from images, audio, files, or videos, is instrumental in masking the alteration of the encrypted message. Adhering to a departure from traditional steganography practices, the file size is matched to the message length to minimize bandwidth usage.

For shorter messages, typically under 200 characters, emojis serve as the cover medium. This involves selecting a random list of emoticons converted into a byte array for processing. LSB is then applied to the emoticons using encrypted data, minimizing byte transfer and enhancing data security. This approach effectively conceals the transferred data behind emoticons, reducing suspicion for potential intercepting parties. The reverse process at the receiver's end involves decoding the encrypted message using LSB and decrypting it using the public key received from the sender. In cases where the input message length exceeds 200 characters, the same process is repeated, with the only difference being the use of other cover mediums. This comprehensive methodology ensures robust data security through the synergistic application of LSB steganography and ECC encryption in a real-time environment like chat application.

III. CONCLUSION

In conclusion, the integration of LSB steganography and ECC encryption in the context of secure data transfer over the Internet presents a sophisticated and effective approach. By selectively focusing on these techniques among the myriad available, we aimed to streamline the methodology, optimizing for both security and efficiency.

The vulnerabilities identified in RSA public keys, as evidenced by the 2020 Keyfactor study, underscore the necessity for robust alternatives. The adoption of ECC, with its emphasis on addressing the discrete logarithm problem, establishes a more secure foundation. The smaller key sizes, adherence to standards, and increased data size encryption capabilities of ECC provide tangible advantages over RSA, with ECC achieving comparable security levels using significantly smaller keys.

The methodology, starting with the generation of ECC keys for encryption and decryption purposes, sets the groundwork for secure communication. The subsequent conversion of messages into ciphertext using ECC ensures confidentiality. By incorporating LSB steganography based on input length, and choosing cover media strategically matched to the message length, our approach not only prioritizes security but also optimizes bandwidth usage, deviating from conventional steganography practices.

The innovative inclusion of emojis as a cover medium for shorter messages adds a layer of disguise, minimizing byte transfer and enhancing data security. This novel approach capitalizes on the commonplace use of emojis in digital communication, rendering intercepted data less conspicuous. The versatility of the methodology, seamlessly transitioning to Image LSB Steganography for longer messages, underscores its adaptability and practicality in real-world scenarios.

The synthesized combination of LSB steganography and ECC encryption, as outlined in the research, lays the groundwork for a real-time chat software environment that upholds a high standard of data security. Through the careful selection and integration of these techniques, we have not only addressed the vulnerabilities associated with traditional methods but have also introduced an innovative, efficient, and secure framework for digital communication. This comprehensive methodology contributes significantly to the ongoing discourse on data security, providing a practical solution for safeguarding sensitive information in the digital age.

IV. REFERENCES


