Steganographic Messaging App

Basel Kelziye, Mevlana Halit Kaya
Bilgisayar Mühendisligi Bölümü˘ Yıldız Teknik
Üniversitesi, 34220 Istanbul, Türkiye

***Özetçe* —Bu projenin amacı iki ki¸sinin internet üzerinden güvenli bir ¸sekilde ileti¸sim kurabilmesidir. Gönderilecek olan mesaj önce son yıllarda sıkça kullanılan ¸sifreleme metodlarından biri ile ¸sifrelenir. S¸ifrelenmi¸s metini bit seviyesinde her pikseli manipüle edilerek fotografa gömülür ardından foto˘ graf˘ internet üzerinden yollanır.**

Anahtar Kelimeler—En dü¸sük anlamlı bit (LSB), anahtarlı karma mesaj dog˘rulama kodu(HMAC),

***Abstract*—The purpose of this project is to secure a safe communication between 2 peers over the internet.The message that is willing to be transferred first gets encrypted and then this encrypted text gets embedded inside an image in a bitlevel by manipulating each pixel, and then transmitting this manipulated image over the internet.**

Keywords—Lease significant bit (LSB), Hashed-based Message Authentication Code (HMAC).

I. Introduction

Communication between humans is essential for the functioning of society. It allows us to share ideas, express emotions, and build relationships. The advancement of technology has greatly impacted the way we communicate, making it faster and more convenient than ever before. The internet has made it possible for people to communicate with others across the globe in real-time, and the development of smartphones and other mobile devices has made it possible to stay connected at all times.

However, with the convenience and ease of communication, comes the need for security. Cryptography is the practice of secure communication, it is used to protect information from unauthorized access or manipulation. It is particularly important when communicating over the internet, as the information sent may pass through multiple networks and devices before reaching its destination. As a result, the use of cryptography is essential to ensure that the information remains confidential and is not tampered with during transmission. It's also important to protect the integrity of the information, to make sure that the information is not modified or replaced during the transmission. Without cryptography, sensitive information such as personal data, financial transactions, and confidential communications would be vulnerable to cyber-attacks and malicious actors.

In this project, our primary objective is to establish a secure and private mode of communication between users by utilizing Cryptography and Steganography techniques.

II. Methods

In our application, when a user initiates the transmission of a message, it undergoes encryption through the RSA encryption scheme. Subsequently, the encrypted message is embedded within an image utilizing the Least Significant Bit steganography technique. The resulting image, containing the embedded message, is then transmitted over the internet.

A. Steganography

Steganography is the practice of hiding information within other data in a way that makes it difficult or impossible to detect. This can be done by embedding messages within an image, audio, or video file, or by hiding data in a seemingly innocent file or message. The goal of steganography is to conceal the existence of the message from unauthorized parties, making it a useful technique for sending sensitive information without detection. For example, a message could be hidden within an image and sent over the internet, and the only way to reveal the message would be to know the specific technique and parameters used to hide it. This technique can be used for legitimate or malicious purposes, it is important to be aware of the potential for steganography to be used for illegal activities such as sharing secret information or spreading malicious software.

Consider the two images in Figure 1, with a human bare eye it is impossible to detect the difference between the images, but the truth is that one image is manipulated and contains the message "Attack at midnight" and the other one is not manipulated.

Figure 1 S¸ekil örnegi˘

There are various steganographic techniques a few are mentioned bellow:

- Least Significant Bit (LSB) insertion: This technique involves replacing the least significant bits of the cover image with the bits of the secret message.
- Masking and filtering: This technique involves using a mask to hide the secret message within the cover image by manipulating the image's color or frequency components.
- Transform domain techniques: These techniques involve transforming the image into a different domain (such as the frequency domain) and then hiding the secret message within the transform coefficients.

- Algorithms based on chaos: These techniques involve using chaotic systems to encrypt the secret message and then hide it within the cover image.
- Audio Steganography: This technique involves hiding information within audio files by slightly altering the amplitude of certain audio samples.
- Video Steganography: This technique involves hiding information within video files by slightly altering the color of certain video frames. • Text Steganography: This technique involves hiding information within text files by slightly altering the spaces or line breaks.
- Network Steganography: This technique involves hiding information within network packets by slightly altering the header information.

B. Least Bit Steganography

In LSB steganography, the least significant bits of the pixels in an image are replaced with bits from the secret message. Because the least significant bits of an image's pixels have a minimal impact on the overall appearance of the image, and the bare human eye will not notice the
difference

The process of LSB steganography involves two steps: embedding the message into the image and extracting the message from the image. In the embedding process, the message is broken down into bits, and then the least significant bits of the image's pixels are replaced with the bits of the message. In the extraction process, the message is recovered by extracting the least significant bits of the image's pixels and reassembling them into the original message.

LSB steganography is a simple and efficient technique, but it has some limitations. One major drawback is its sensitivity to image compression and image processing operations, which can significantly alter the least significant bits of the image and make it difficult to extract the hidden message. Furthermore, LSB steganography is vulnerable to steganalysis, which is the process of detecting the presence of hidden information.

C. Cryptography

Cryptography is best described as "The communication in the Presence of an adversary". Means its a way to keep information secret and secure. It uses special codes or mathematical formulas to scramble the information in a way that makes it unreadable to anyone who doesn't have the key to unlock it. Think of it like a secret code that only you and the person you're sending the message to can read. This is important when sending sensitive information over the internet, like credit card numbers or personal information, to make sure that it doesn't fall into the wrong hands. Cryptography is also used to check that the information hasn't been tampered with, which ensures the integrity of the data.

Cryptographic techniques used in our projects are:

• RSA: its a widely-used public key encryption scheme. It is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described it in 1977.

In the RSA scheme, a public key is used to encrypt a message, and a private key is used to decrypt it. The public key, which is available to anyone, is used to encrypt a message, and the private key, which is kept secret, is used to decrypt it. In our application it is used to encrypt and decrypt the messages • HMAC: its a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.

III. Results & Discussion

The main objective of this project was to develop a secure texting application utilizing LSB steganography and RSA encryption. The study was conducted through a series of experiments in which plain text messages were encrypted using the RSA encryption scheme and then embedded within images using the LSB steganography technique. The resulting images were then transmitted through the developed application and the process was repeated to decrypt the message.

- Experiment 1: Message Concealment The first experiment aimed to evaluate the effectiveness of message concealment using LSB steganography. The plain text message was embedded within an image and the resulting image was analyzed for changes in visual quality and file size. The results showed that the changes in the image were minimal and not detectable to the human eye. Additionally, the file size of the image increased by less than 1%. • Experiment 2: RSA Encryption The second experiment aimed to evaluate the effectiveness of the RSA encryption scheme in securing the message. The plain text message was encrypted using RSA encryption with a key size of 2048 bits. The encrypted message was then decrypted using the corresponding private key. The results showed that the decryption process was successful and that the original message was recovered without any errors.
- Experiment 3: Functionality of the developed application

The third experiment aimed to evaluate the functionality of the developed application. The plain text message was encrypted using RSA encryption and then embedded within an image using LSB steganography. The resulting image was transmitted through the developed application and then decrypted using the corresponding private key. The results showed that the original message was successfully recovered and that the application provided a secure and private mode of communication. • Experiment 4: Safety of private keys The fourth experiment aimed to evaluate the possibility of an buffer overflow attack during the lifetime of the application,

using the "secure flutter storage" flutter library which uses the operating system's key store (in android) and key chain (in IOS) we hand over the responsibility of the keys protection to the device's operating system.

Overall, the results of the study indicate that utilizing LSB steganography and RSA encryption in combination provides an effective method for secure communication through a mobile application. The LSB steganography technique was found to be effective in concealing the message within an image without causing any significant changes in visual quality or file size. Additionally, the RSA encryption scheme was found to be effective in securing the message and ensuring that it can only be read by the intended recipient. The developed application was functional and user-friendly, providing a secure communication platform for users.

IV. Conclusion

In conclusion, the use of LSB steganography and RSA encryption in a texting application provides a secure method for transmitting images over the internet. LSB steganography allows for the covert insertion of data into an image, while RSA encryption ensures that the data is protected from unauthorized access. Together, these techniques provide a high level of security for sensitive information transmitted through the application. However, it is important to note that no method of encryption or steganography is completely foolproof and it's always a good idea to keep the system updated and monitor for any suspicious activity. Additionally, users should be aware of the legal implications of using such a system for nefarious purposes.

References