MULTI-IMAGE STEGANOGRAPHY USING ADVANCED ENCRYPTION STANDARD

Om H. Inagle[1], Anushka B. Kadam[2], Saily G. Patil[3], Sahil V. Shilimkar[4], Prof. Shilpa Tiwari[5]

[1,2,3,4,5]Computer Engineering, Zeal Polytechnic, Pune, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS36739

ABSTRACT

Steganography is the practice of hiding information within other non-secret data, making it difficult for unintended recipients to detect the presence of the hidden information. The primary goal of steganography is to ensure the confidentiality of the message by concealing its existence rather than encrypting it. This technique can be applied to various forms of images.

Keywords: Steganography, Hiding Information, Confidentiality, Concealment, Hidden Information, Detection, Encryption, Images.

1. INTRODUCTION

Steganography involves concealing messages within digital media, such as images, making it an essential tool for secure communication. Android, being a widely used mobile platform, offers an excellent medium for applying steganography. This survey aims to provide an overview of image steganography techniques used in Android-based applications and evaluate their effectiveness.

Android-Based Steganography Applications:

1.1 Android Application for Image Steganography Using Android Studio (IJRASET)

This paper presents an Android application for hiding messages in images using the LSB method. The application is designed for ease of use and provides moderate security but may not withstand sophisticated steganalysis attacks.

1.2 Steganography on Android-Based Smart Phones (Stanford)

The Stanford project focuses on implementing steganography on Android devices, utilizing more advanced methods like DCT. The app provides a more secure way to hide data but comes with increased processing time and complexity.

1.3 Comparative Study on Steganography Techniques for Android (IJCRT)

This paper compares several image steganography techniques applied to Android platforms. It highlights the advantages and disadvantages of LSB, DCT, and other frequency domain methods, focusing on performance, security, and practicality in real-world applications.

2. LITERATURE SURVEY

Steganography is a technique that conceals information within non-secret data, typically digital media like images, to protect the confidentiality of the message by hiding its existence rather than encrypting it alone. Steganography differs from cryptography, which focuses on encrypting information but makes it apparent that encryption has been used. Various steganographic techniques have evolved, especially in Android-based applications, which are popular due to the widespread use of Android devices in communication and data.

2.1 Least Significant Bit (LSB) Technique: A simple method of replacing the least significant bit in each pixel with hidden data. This method is prone to steganalysis, as even slight modifications in the image can reveal hidden data.

2.2 Discrete Cosine Transform (DCT) Method: A frequency-domain method typically used in JPEG images. It modifies frequency components rather than pixel values, offering more security, but it is computationally intensive.

2.3 Spread Spectrum Techniques: Data is spread across multiple frequencies, making the hidden information more robust against attacks. However, these techniques demand significant processing power.

2.4 Adaptive Steganography: Dynamically adjusts the data embedding based on the image's features, balancing security and imperceptibility.

Problem Statement:

As digital communication becomes increasingly prevalent, ensuring the security and confidentiality of transmitted information is a growing concern. While traditional encryption techniques protect the content of the message, they do not hide the fact that communication is taking place. This can attract attention from malicious actors, making the transmission vulnerable to interception. Steganography offers a potential solution by concealing the existence of the message, but current techniques face challenges in balancing security, performance, and usability, particularly in resource-constrained environments like smartphones.

The challenge lies in designing a steganographic method that is secure against detection (steganalysis), performs well on mobile devices with limited resources, and remains easy to implement. While more advanced methods like DCT provide greater security, they often come at the cost of increased computational requirements, which can negatively affect performance on Android-based devices.

Proposed Solution:

The proposed solution combines AES encryption with multi-image steganography to enhance data security by embedding encrypted information across multiple images. This dual-layer approach ensures that even if part of the hidden data is exposed, the encrypted content remains protected.

In this method, data is first encrypted using AES, then embedded in images using techniques like **DCT**, making detection more difficult. Adaptive methods adjust the embedding based on image features, enhancing security and imperceptibility.

Optimized for Android, this approach reduces computational demands, and integration with cloud technologies allows scalable, secure communication for messaging, file sharing, and disaster response scenarios.

Advantages (Simplified):

- **High Security**: By combining AES encryption with multi-image steganography, the system provides strong protection. Even if some hidden data is discovered, the encryption keeps it safe.
- **Resistant to Detection**: Techniques like DCT and adaptive methods make it harder for attackers to find the hidden data, even with advanced tools. This makes the system more robust when combined with encryption.
- **Scalable**: The solution can handle large amounts of hidden data and complex communication systems by using cloud technology, making it suitable for various secure applications.
- **Hard to Detect**: Adaptive methods ensure the hidden data does not affect image quality, making it nearly impossible to notice, which helps avoid suspicion.

1. **Disadvantages (Simplified):**

- **High Complexity**: Advanced techniques like DCT and multi-image embedding require a lot of processing power, especially on smartphones, which can slow down performance and drain battery life.
- **Slower Processing**: Combining AES encryption with multi-image steganography takes more time to encrypt and hide data, which might not be ideal for applications needing quick or real-time communication.
- **Vulnerability of Simple Methods**: Basic techniques like LSB are easier to detect by attackers if not paired with stronger methods, which makes using robust techniques essential to keep data safe.
- **Mobile Device Limitations**: Smartphones may struggle with these methods because they have limited memory and processing power. Balancing security and performance on these devices can be challenging.

2. **Evaluation and Analysis:**

   The evaluation focuses on key performance metrics such as computational speed, memory usage, and battery consumption on Android devices. Security is evaluated based on how resistant the techniques are to steganalysis attacks, while image quality is assessed using metrics like PSNR (Peak Signal-to-Noise Ratio).

3. **Trends and Challenges:**

Trends: Recent advancements in steganography have introduced machine learning and artificial intelligence to enhance the security of hidden data. Additionally, blockchain is being explored to provide immutable proof of message integrity.

Challenges: Developers face challenges in balancing security with performance, especially on resource-constrained devices like smartphones. Moreover, with evolving steganalysis tools, maintaining imperceptibility remains a key hurdle.

Future Directions:

Enhanced Security Algorithms: Future developments will likely focus on improving the robustness of steganographic methods by integrating AI and deep learning techniques to make hidden data more secure against detection.

Optimization for Mobile Platforms: the continued growth of Android devices, optimizing steganographic techniques for mobile platforms is essential. Researchers are working on reducing computational complexity while maintaining security.

Integration with Cloud Technologies: Combining mobile-based steganography with cloud services could offer a more scalable solution for secure communication, particularly in applications that require large amounts of data to be hidden.

3. CONCLUSION

The proposed multi-image steganography method, combined with AES encryption, presents a significant advancement in secure communication. By embedding encrypted data across multiple images, the method ensures that both the existence and the content of the hidden message remain protected. While challenges remain in balancing performance and security on mobile platforms, ongoing research in AI, machine learning, and cloud integration could provide solutions to these issues. This approach holds promise for applications where both confidentiality and imperceptibility are paramount, such as in secure messaging, digital rights management, and disaster recovery scenarios

4. REFERENCES

[1] IJRASET. (n.d.). Android application for image Steganography using android studio. Ijraset.com. Retrieved October 25, 2024, from https://www.ijraset.com/research-paper/android-application-for-image-steganography-using-android-studio

[2] Anjana, M. R. (n.d.). Android Image Steganography. Ijiird.com. Retrieved October 25, 2024, from http://ijiird.com/wp-content/uploads/050110.pdf

[3] Anjana, M. R. (n.d.). Android Image Steganography. Ijiird.com. Retrieved October 25, 2024, from http://ijiird.com/wp-content/uploads/050110.pdf

[4] Anjana, M. R. (n.d.). Android Image Steganography. Ijiird.com. Retrieved October 25, 2024, from http://ijiird.com/wp-content/uploads/050110.pdf

[5] Anjana, M. R. (n.d.). Android Image Steganography. Ijiird.com. Retrieved October 25, 2024, from http://ijiird.com/wp-content/uploads/050110.pdf