WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Android Based Image Steganography

Arman Mohanty[1], Aman Kumar[1], Mohd. Hashir Umar Khan[1], Mukut Gupta[1] and Shalu Tyagi[2]

[1] Computer Science (Artificial Intelligence & Machine Learning) Department, Raj Kumar Goel Institute of Technology, Students, Ghaziabad, India {2000331530015, 2000331530010, 2000331530027, 2000331530028}@rkgit.edu.in

[2] Computer Science (Artificial Intelligence & Machine Learning) Department, Raj Kumar Goel Institute of Technology, Assistant Professor, Ghaziabad, India shalufai@rkgit.edu.in

ABSTRACT.

The paper discusses the creation of a system for hiding data within images on Android devices, known as steganography. As the internet and mobile technology usage grows, ensuring the security of transmitted information becomes crucial. The system employs the Least Significant Bit (LSB) algorithm, a popular method for embedding data within images. Initial tests of the system showed promising results. Further details about the implementation process, testing outcomes, and potential applications could enhance the paper's depth and usefulness.

Keyword: Android, image steganography, data, information, transmission, images, security

1. Introduction

Watermarking and fingerprinting are closely linked to steganography, all focusing on safeguarding intellectual property rights. Watermarking applies a consistent mark to all instances of an object, containing hidden information to signify originality or ownership for copyright purposes. Fingerprinting, on the other hand, embeds unique identifiers into individual copies of the object, allowing copyright owners to trace unauthorized distribution. Cryptography, another method for securing information, is primarily concerned with keeping the content of messages confidential. Various encryption and decryption techniques are employed to maintain secrecy. Additionally, cryptography may extend to concealing the mere existence of information. Steganography, therefore, plays a crucial role in concealing the presence of a user's information altogether.

Given the imperative to securely transmit sensitive or personal messages to specific recipients without risking interception by malicious entities, particularly in the face of internet security challenges and potential identity theft, individuals must proactively safeguard their communications. It is essential that these protective measures are not only swift but also easily accessible and convenient for users. While steganography systems have traditionally been developed for desktop and laptop computers, there is a growing necessity to extend these capabilities to handheld devices for enhanced usability. Leveraging the increasingly advanced hardware and software capabilities of smartphones and tablets, we can harness their processing power to create steganography systems tailored for these devices. This adaptation would facilitate faster and more accessible information concealment for users on the go.

1.1. Aim

The objective of this study is to create a steganography system specifically designed for Android devices. We plan to adopt an incremental development approach, where the system evolves through multiple versions, each subjected to rigorous testing until the final iteration is achieved. For the project's architecture, we favour a Layered System Architecture to ensure robust security. This structure entails placing the most critical system components in the inner layers, providing them with extensive security validation. Our research scope encompasses implementing steganography on Android devices to enable the concealment of various types of files within image files. Additionally, users will have the flexibility to choose the location for storing retrieved hidden files. Our aim is to streamline the process of information hiding, making it more intuitive and user-friendly.

1.2 Justification

Steganography provides a means to conceal information during transmission, utilizing various algorithms based on the strength of the host system or system design. This ensures that users' information remains safeguarded from potential threats. Embracing this study could address cybersecurity concerns and enhance data security in several domains:

- Facilitating the secure exchange of sensitive documents, including top-secret materials, among governments and their agencies.

- Enhancing identity management by embedding personal details, such as those found on identity cards, within JPEG images, such as passport photos.
- Enabling the implementation of steganography in online voting systems by organizations like the Independent National Electoral Commission (INEC).
- Supporting secure communication within military networks through the integration of steganography.
- Improving efficiency and confidentiality in the medical field by embedding hidden treatment details within images, thereby reducing the time, cost, and risk associated with traditional file transmission methods.

2. Evaluation of existing technologies

When it comes to image steganography algorithms, each has its strengths and weaknesses. Thus, it is crucial to carefully consider which approach is most appropriate for a given scenario. As previously discussed, there are various criteria for evaluating the performance of a steganographic system.

- The Least Significant Bit (LSB) technique in the spatial domain provides a practical means of hiding information. However, it is susceptible to minor alterations caused by image processing or lossy compression. While LSB techniques can accommodate large amounts of data (high payload capacity), they tend to distort the statistical properties of the image, resulting in reduced resilience against statistical attacks and image manipulation.
- Advanced techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and adaptive steganography show promise in terms of resistance to attacks, particularly when concealing small messages. This resilience stems from their ability to modify coefficients in the transform domain while minimizing image distortion. However, these techniques typically have a lower data payload compared to spatial domain algorithms. Experiments focusing on DCT coefficients have yielded encouraging results, prompting further investigation into JPEG images. Working within the DCT framework enhances steganography's effectiveness and reduces vulnerability to statistical attacks. Additionally, embedding in the DWT domain demonstrates constructive outcomes, surpassing DCT embedding, particularly in terms of surviving compression processes.
- Spread spectrum techniques offer robust resistance against statistical attacks because the hidden message is dispersed across the entire image. However, determined attackers can potentially compromise embedded data through digital processing, such as noise reduction filters, similar to those used in decoding to estimate the original cover. Spread spectrum encoding finds extensive use in military communications due to its ability to evade detection. Once a message is embedded, it becomes challenging for an attacker to identify it without the appropriate keys. Steganographic Image Selection Scheme (SISS) is particularly effective in steganography due to its significant data capacity and the considerable difficulty it poses for detection and extraction processes.
- Statistical techniques are often susceptible to various attacks, including cropping, rotating, and scaling, as well as those targeting watermarking methods. To enhance their robustness, defences should be explored to bring statistical techniques on par with watermarking schemes. The payload capacity and invisibility of these techniques are contingent upon the choice of the cover image.
- Distortion techniques, unlike many Least Significant Bit (LSB) methods, do not disrupt the statistical properties of the image. However, the necessity of transmitting the cover image through a secure channel diminishes the practicality of this approach. As with any steganographic method, reusing the cover image is strongly discouraged to maintain security. If an attacker manipulates the stego-image by cropping, rotating, or scaling, these alterations can be easily detected by the recipient and potentially reversed, especially when error correcting information is employed. This additional information also helps in scenarios where the stego-image undergoes lossy compression, such as JPEG. Nevertheless, implementing distortion techniques inherently reduces the capacity for hidden information since the embedding process relies on adding distortion to the cover image. Consequently, the distorted image becomes more susceptible to detection by the Human Visual System (HVS).

3. System analysis and design

3.1 Least significant bit insertion

The chosen technique for this project is Least Significant Bit (LSB) Insertion, a form of steganography. In LSB, information is hidden within an image. An image, composed of bytes representing different colours, offers a canvas for concealment. The least significant bits of these colour bytes, which hold less visual significance, are altered to embed information. This method ensures that the changes are imperceptible to the human eye. For instance, in a 24-bit image, the first 8 bits of 3 pixels can be manipulated to conceal a character like 'A'. Since the 'A' requires only 8 bytes, the ninth byte of the 3 pixels can be utilized to hide the next character in the message.

The example shows that in a 24-bit image, letter A can be hidden in the first 8 bits of 3 pixels.

Pixels: (00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

A: 01000010

Result: (00100110 11101001 11001000)

(00100110 11001000 11101000)

(11001001 00100110 11101001)

In the LSB insertion technique, the five bits indicated were altered to conceal information. Typically, around half of an image's bits are modified using this method. Since 'A' is an 8-bit letter requiring 8 bits for concealment, the ninth byte of 3 pixels is utilized to hide the next character of the secret message. Variations of this technique enable messages to be embedded into two or more least significant bits per byte, thus expanding the capacity for hidden information within the cover object. However, this approach often leads to degradation of the cover object, making it more detectable. While LSB insertion is straightforward to implement, it is also vulnerable to attacks if modifications are improperly executed. Mistakes in colour palette adjustments or basic image calculations can inadvertently destroy the hidden message. Examples of such destructive image manipulations include resizing and cropping.

Systems analysis plays a crucial role in the systems development life cycle by facilitating an understanding of the current system's functionality, identifying its weaknesses, and pinpointing areas for improvement. Conversely, system design encompasses defining the system's architecture, modules, interfaces, and data in order to meet the specified user requirements. It can be viewed as the application of systems theory to the development process, encompassing various forms of system modelling to conceptualize the desired system structure.

3.2 Description of existing system

Current systems, as shown in fig. 1, utilizes desktop applications employing Least Significant Bit (LSB) image steganography algorithms on desktop and personal computers. Users seeking to hide or encrypt their data instantly are required to power on their personal computers and launch the desktop application. However, in an age where certain mobile phones boast processing speeds twice as fast as some computer systems, and where information demands almost instant transmission, this approach is becoming increasingly impractical.

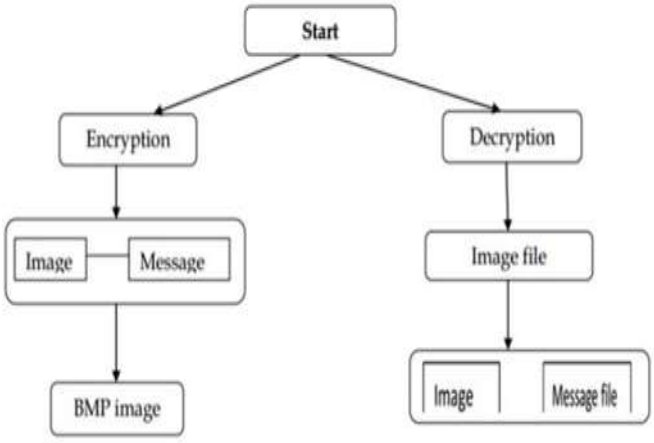

Fig. 1 Flow of the existing System

The proposed system (fig. 2) is an Android-based image steganography tool designed for security purposes, employing adaptive steganography techniques. It features an embedded steganography system to hide users' private information and also allows for the extraction of concealed information from other users of the Android application utilizing the same steganography algorithms. Prior to embedding, the user data undergoes encryption using the Advanced Encryption Standard (AES) algorithm, ensuring protection against information tampering.

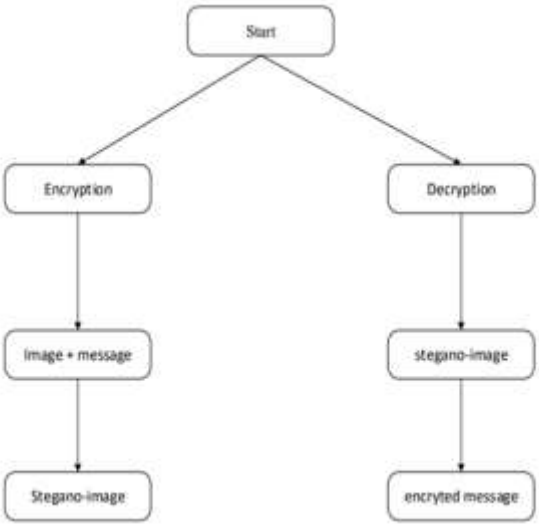

Fig. 2 Flow of the proposed system

This model provides, as shown in fig. 3, an overarching perspective of the system, delineating the boundary between the system or its components and its external environment, which includes other systems. It illustrates the entities that engage with the system. Below is the context diagram depicting the system.

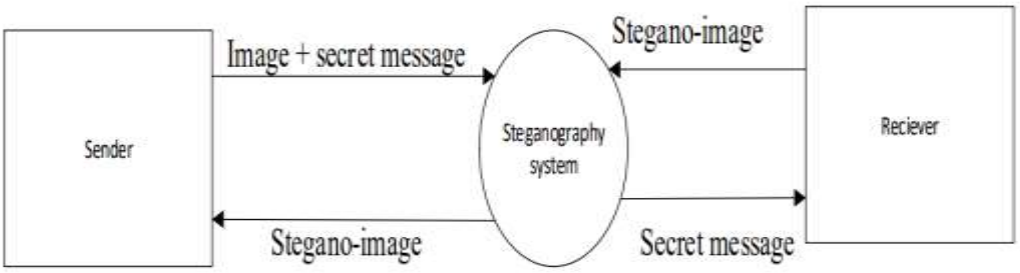

Fig. 3 Context diagram of the System

Process modelling involves, as shown in fig. 4, graphically representing the processes, or actions, that capture, manipulate, store, and distribute data between a system and its environment and among components within a system

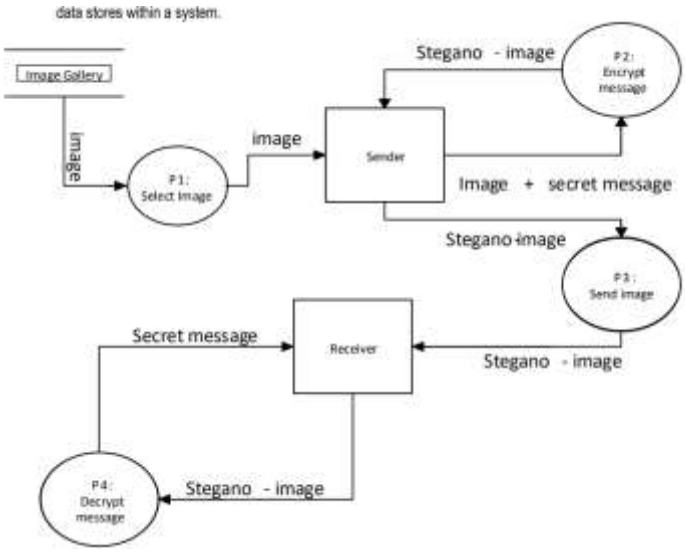

Fig. 4 Dataflow diagram (Level-0 diagram)

Activity diagrams, as shown in fig. 5, serve as visual depictions of step-by-step workflows, showcasing activities and actions while accommodating choice, iteration, and concurrency. They are employed to articulate the dynamic functionalities of the system. Essentially, an activity diagram functions as a flowchart, illustrating the progression from one activity to another.

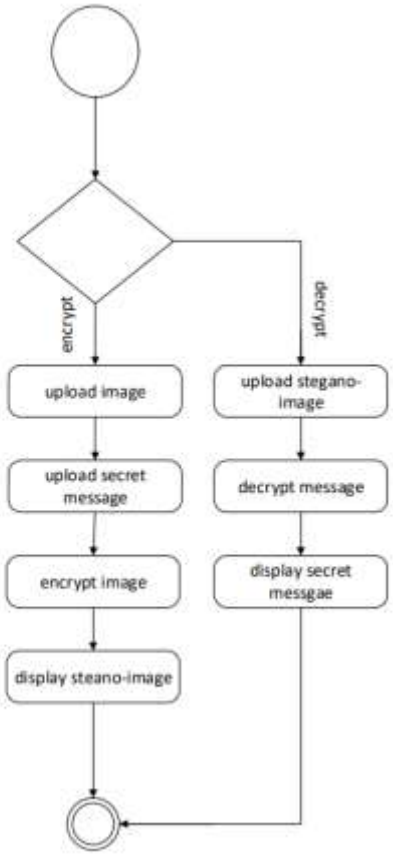

Fig. 5 Activity diagram of the proposed system

Encode Page, as shown in fig. 6, Clicking on the encode menu brings a pop up to select a picture folder for the encoded image. Users can choose to take pictures directly from the camera or select from the phone's picture folder. After selecting a picture option and selecting the image to encode, users can input the text to be encoded in the image and then encode the text into the image.

Fig. 6 Message after it is encoded in picture

From the page, as shown in fig. 7, Users can select the decode menu and a menu pops up with options to select an image to be decoded. After selecting the image, the text encoded in the image is decoded and displayed.

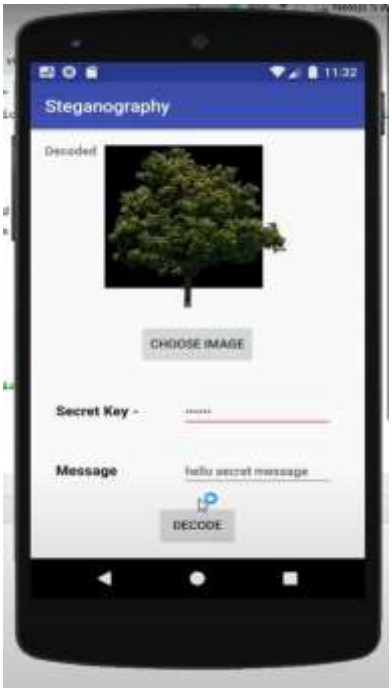

Fig. 7 Message after it is decoded from the picture

4. Summary

The rapid evolution of information technology and the widespread integration of social media into mainstream culture have resulted in an abundance of user data on these platforms. This data is constantly accessible and predominantly transmitted through smartphones. Despite assurances and the implementation of two-way end-to-end encryption, users' sensitive information remains vulnerable to exposure. This system allows users to conceal or disguise information within digital media, particularly images, before transmitting it via any desired platform or means.

5. Conclusion

In summary, following meticulous selection of the most suitable steganography algorithm and thorough analysis and evaluation of the system's design, the steganography system for Android devices has been effectively developed. Demonstrating robustness, it can manage a significant volume of data while guaranteeing the security of user information. The stegano-image remains imperceptible to observers, ensuring privacy. Moreover, the application encrypts user data with a key, adding an additional layer of security to prevent interception of messages.

6. Recommendation

This system is highly recommended for individuals seeking to address security challenges and mitigate data breaches. It encourages further exploration of steganography techniques and algorithms to enhance their effectiveness. Users concerned about information security are encouraged to utilize the application for storing and transmitting private information, thereby ensuring its protection.

References

1. A. Shaddad, J. C. (2022). Biometric inspired digital image steganography. 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (pp. 159-168). IEEE.

2. Arbind Tiwary, A. G. (2019). Different Image Steganography Techniques. International Journal for Computer Engineering and Applications, 13.

3. Essays, U. (2018). Steganography Using LSB Insertion Technique Computer Science Essay. London: UK Essays.

4. Essays, U. (2018). The Types and Techniques of Steganography Computer Science Essay. London: UK Essays.

5. Hamid, N. &.-q. (2016). Image Steganography Techniques: An Overview. International Journal of Computer Science and Security.

6. Jagvinder Kaur, s. K. (2016). Study Of Various Image Steganography Techniques. Amritsar: Amritsar College of Engineering and Technology, Amritsar, India.

7. Kashyap, N. (2016). Image Steganography Using Enhanced LSB Technique. International Journal of Scientific & Engineering Research, 6.

8. Katzenbeisser, S. (2011). Principles of Steganography.” in Information Hiding Techniques for Steganography and Digital Watermarking. London: Artech House.

9. Kavita Kavitha, A. K. (2009). Steganography Using Least Signicant Bit Algorithm. International Journal of Engineering Research and Applications , 338-341.

10. Laskar, S. A. (2008). High capacity data hiding using LSB steganography and encryption. International Journal of Database Management System. 57.

11. M. Kharazi, H. S. (2004). Image steganography: Concepts and practice.

12. Nagham Hamid, A. Y.-Q. (2003). Image Steganography Techniques. Perlis: University of Malaysia Perlis School of Communication and Computer Engineering, .

13. P. Kruus, C. S. (2003). A survey of steganography techniques for image files. Advanced Security Research Journal, 41-52.

14. Paulson, L. (2001). New system fights steganography. IEEE, 25-27.

15. S. Areepongsa, N. K. (2000). Exploring on steganography for low bit rate Wavelet based coder in image retrieval system. IEEE.