An Android Application For Digital Image Steganography Techniques

Prof.Yogesh.B.Jadhao[1], Mr.Pavan.V.Kalamkar[2], Ms.Kanchan.S.Wadode[3], Ms.Shital.R.Ganbas[4], Ms.Swati.V.Borle[5]

Department of Computer Science And Engineering, Padm.Dr.V.B.Kolte College Of Engineering, Malkapur

Abstract: The word Steganography is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing' ,or 'hidden writing'. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks. As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover image and the image obtained after steganography is called the stego image. This System encodes and decodes secret text messages and images into and from the cover image. To encode text messages and images into the cover image, users need to first load the cover images into the application.

Keywords: *Text Hiding in images, Image Hiding in images, Image Steganography, Encryption, Decryption, Secret Communication*

I. INTRODUCTION

In the rapidly evolving digital era, the need for secure data transmission has become increasingly significant. Digital image steganography, a technique of concealing secret information within digital images, offers a robust solution to protect sensitive data from unauthorized access. Unlike traditional encryption methods that make data transmission noticeable, steganography ensures data confidentiality by embedding information in a way that is imperceptible to the human eye. This technique leverages various algorithms and methods to embed data without compromising the visual quality of the cover image. The development of an Android application for digital image steganography provides a portable and user-friendly platform for secure communication, making data protection more accessible to a wider range of users. This paper explores the implementation of digital image steganography techniques within an Android application, focusing on their effectiveness, security measures, and overall performance.

II. METHODOLOGY

The methodology for this project, "An Android Application For Digital Image Steganography Techniques" involves the design and development of an Android-based application that implements various image steganography techniques for secure data embedding and retrieval. The project utilizes Java and Android Studio for application development, incorporating established steganographic algorithms such as LSB (Least Significant Bit), DCT (Discrete Cosine Transform), and others to hide and extract messages within digital images. The process begins with the user selecting an image file through the app interface, after which a secret message (text or binary data) is encoded into the image using one of the chosen steganographic techniques. The application then saves the image with the embedded message in a manner that does not visibly alter the image to the human eye. For the extraction phase, the user inputs the stego-image, and the app decodes the hidden data using the reverse process of the encoding technique. The performance of these methods is evaluated based on the image quality (PSNR – Peak Signal-to-Noise Ratio), the capacity of hidden data, and the computational efficiency of encoding/decoding. Additionally, the app's usability and interface design are tested for intuitiveness and ease of use, ensuring that both novice and experienced users can perform secure data hiding and retrieval without difficulties. The final evaluation of the application's effectiveness will involve comparing the stegoimages with their original versions to assess visual quality and the success of data extraction.

III. ARCHITECTURE

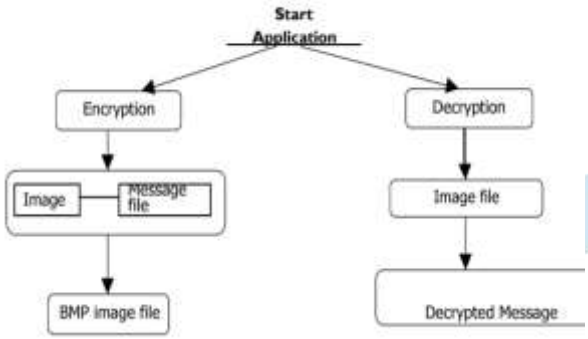

Fig. 1 Architecture

The given architecture diagram represents an image steganography system that embeds a secret message within an image using encryption and later extracts it through decryption. The process begins with the application, which provides two main functionalities: encryption and decryption. In the encryption phase, an input image and a message file are combined using a steganographic algorithm, producing a BMP image file with the hidden message embedded inside it. The decryption phase involves extracting the concealed message from the encoded image file, revealing the original secret message.Image steganography techniques generally fall into spatial domain and frequency domain methods. Spatial domain techniques, such as Least Significant Bit (LSB) substitution, modify pixel values directly to encode data, making them easy to implement and computationally efficient. Frequency domain methods, like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), embed messages within transformed coefficients of an image, enhancing security and robustness against attacks such as compression and noise.In this architecture, the encryption process likely uses LSB-based steganography due to the choice of BMP format, which preserves pixel integrity without compression artifacts. The decryption process simply retrieves the hidden bits and reconstructs the original message. Such a system is useful for secure data transmission, watermarking, and covert communication.

IV. APPLICATIONS

The applications of an Android application for digital image steganography techniques are diverse, spanning various sectors where secure and covert communication is essential.

Here are some key areas:

1. Confidential Communication: a. Individuals seeking private communication can use it to exchange sensitive information without raising suspicion. b. Journalists and activists can protect their sources and transmit information securely in restrictive environments.

2. Data Protection and Security: a. Embedding digital watermarks for copyright protection and intellectual property rights. b. Concealing sensitive data within images for secure storage and transmission. c. Cybersecurity professionals can hide encryption keys or other critical data to enhance security measures.

3. Law Enforcement and Intelligence: a. Covertly transmitting information during investigations. b. Embedding forensic markers within images for tracking and identification.

4. Healthcare: a. Securely storing and transmitting patient data within medical images. b. Protecting the privacy of sensitive medical information.

5. Military and Defense: a. Securely transmitting confidential information in military operations. b. Hiding mission-critical data within seemingly innocuous images. Essentially, any scenario where the need to hide information exists can benefit from digital image steganography.

V. LITERATURE REVIEW

Digital image steganography has been widely explored as a technique for secure data transmission by embedding secret information within images while maintaining their perceptual quality. Various steganographic methods, such as Least Significant Bit (LSB) substitution, Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), have been proposed to enhance security and imperceptibility (Kharrazi et al., 2004; Cheddad et al., 2010). Android-based implementations of image steganography have gained traction due to the widespread use of mobile devices for secure communication (Patel & Bhalodi, 2013). Recent studies have introduced hybrid techniques that combine cryptography and steganography to strengthen data protection on mobile platforms (Singh et al., 2020). Moreover, research has focused on improving robustness against steganalysis attacks, ensuring that embedded data remains undetectable by adversarial models (Hussain et al., 2018). Despite advancements, challenges persist in optimizing computational efficiency

and storage constraints for real-time mobile applications. (Gupta & Sharma, 2021). The integration of steganography into Android applications presents opportunities for secure messaging, watermarking, and authentication in mobile environments. However, further research is needed to enhance performance, security, and usability in practical implementations.

1. Summary of past research - Past research on steganography techniques utilizing digital images has significantly advanced the field, focusing on various methods for concealing information, within image files. Early techniques primarily relied on the Least Significant Bit (LSB) method, where bits pixel values are altered to embed secret messages. Subsequent studies introduced more sophisticated approaches, such as transform domain techniques, which embed data in the frequency domain of images to enhance security and imperceptibility. Researchers have also explored adaptive steganography, which adjusts embedding strategies based on the characteristics of the host image to improve robustness against detection. Additionally, advancements in machine learning have paved the way for intelligent algorithms that optimize the steganographic process. Overall, the lite image quality, and the efficiency of extraction processes, highlighting the need for continued innovation in mobile applications to make these techniques more accessible to users.

2. Key study and Findings - A key study in the realm of image steganography is the work conducted by Cox et al. (2008), which explored the use of Least Significant Bit (LSB) substitution combined with frequency domain techniques for enhanced security. This research demonstrated that embedding information in the frequency domain significantly reduces the likelihood of detection compared to traditional LSB methods, which are more susceptible to image manipulation. The findings indicated that while LSB is simple and effective for basic applications, its vulnerabilities necessitate the integration of more complex techniques to improve robustness against steganalysis. Additionally, the study highlighted the importance of employing adaptive methods that consider the perceptual characteristics of images, leading to better data concealment and preservation of image quality. This research underlines the critical need for continuous development in steganography techniques, particularly in mobile applications, to cater to growing security demands in digital communications. Digital image steganography involves embedding secret data within an image in such a way that it remains undetectable to an observer. With the proliferation of mobile devices, Android applications have become a popular platform for implementing steganography techniques, offering portability and ease of access. Recent studies have explored various methods for embedding hidden information into digital images, such as Least Significant Bit (LSB) substitution, Discrete Cosine Transform (DCT), and histogram-based techniques. Android applications leverage these methods, often incorporating additional security measures like encryption and compression to enhance both the confidentiality and efficiency of the embedded data. Researchers have highlighted the growing importance of developing user-friendly interfaces within these applications, as well as ensuring minimal distortion in image quality and high data capacity. Furthermore, the performance of Androidbased steganography apps has been analysed in terms of robustness against attacks, embedding capacity, and computational efficiency. Despite significant advancements, challenges remain in optimizing these applications for resource constrained mobile devices, requiring novel algorithms that balance security, performance, and usability. Studies also emphasize the need for cross-disciplinary approaches, combining cryptography, image processing, and Android development techniques to improve the reliability and practical utility of steganography in mobile environments.

VI. CONCLUSION

In conclusion, this project on image steganography successfully demonstrates the effectiveness of embedding and extracting hidden data within digital images, offering a secure method for covert communication. The implementation of steganographic techniques ensures that sensitive information can be transmitted discreetly, with minimal impact on image quality and resilience against common threats. The project highlights the potential of steganography in enhancing data security in various fields and lays the foundation for further research and refinement of these techniques to meet evolving cyber security demands.

VII. REFERENCES

[1] S. Dhawan and R. Gupta, ‘‘Analysis of various data security techniques of steganography: A survey,’’ Inf. Secur. J. Global Perspective, vol. 30, no. 2, pp. 1–25, 2020, doi: 10.1080/19393555.2020.1801911.

[2] N. Rashmi and K. Jyothi, ‘‘An improved method for reversible data hiding steganography combined with cryptography,’’ in Proc. 2nd Int. Conf. Inventive Syst.

Control (ICISC), Jan. 2018, pp. 81–84, doi: 10.1109/ICISC.2018.8398946.

[3] C.-T. Huang, N. S. Shongwe, and C.-Y. Weng, ‘‘Enhanced embedding capacity for data hiding approach based on pixel value differencing and pixel shifting technology,’’ Electronics, vol. 12, no. 5, p. 1200, Mar. 2023, doi: 10.3390/electronics12051200.

[4] G. Peter, A. Sherine, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, ‘‘Histogram shifting-based quick response steganography method for secure communication,’’ Wireless Commun. Mobile Comput., vol. 2022, pp. 1–11, Mar. 2022, doi: 10.1155/2022/1505133.

[5] J. Yang, D. Ruan, J. Huang, X. Kang, and Y.-Q. Shi, ‘‘An embedding cost learning framework using GAN,’’ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 839–851, 2020, doi: 10.1109/TIFS.2019.2922229.

[6] A. Khalifa and A. Guzman, ‘‘Imperceptible image steganography using symmetryadapted deep learning techniques,’’ Symmetry, vol. 14, no. 7, p. 1325, Jun. 2022, doi: 10.3390/sym14071325.

[7] D. Volkhonskiy, I. Nazarov, and E. Burnaev, ‘‘Steganographic generative adversarial networks,’’ 2017, arXiv:1703.05502.

[8] J. Zeng, S. Tan, B. Li, and J. Huang, ‘‘Large-scale JPEG image steganalysis using hybrid deep-learning framework,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 12001214, May 2018, doi: 10.1109/TIFS.2017.2779446.

[9] D. Hu, Q. Shen, S. Zhou, X. Liu, Y. Fan, and L. Wang, ‘‘Adaptive steganalysis based on selection region and combined convolutional neural networks,’’ Secur. Commun. Netw., vol. 2017, pp. 1–9, Jan. 2017, doi 10.1155/2017/2314860.

[10] G. Xu, H.-Z.Wu, and Y.-Q. Shi, ‘‘Structural design of convolutional neural networks for steganalysis,’’ IEEE Signal Process. Lett., vol. 23, no. 5, pp. 708–712, May 2016, doi: 10.1109/LSP.2016.2548421 adversarial

[11] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, ‘‘A novel image steganography method via deep convolutional generative networks,’’ 10.1109/ACCESS.2018.2852771. IEEE Access, vol. 6, pp. 3830338314, 2018, doi:

[12] Y. Sun, Y. Lu, X. Yan, L. Liu, and L. Li, ‘‘Robust secret image sharing scheme against noise in shadow images,’’ IEEE Access, vol. 9, pp. 23284–23300, 2021, doi: 10.1109/ACCESS.2021.3056893.

[13] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, ‘‘A machine learning model for improving healthcare services on cloud computing environment,’’ Measurement, vol. 119, pp. 117–128, Apr. 2018, doi: 10.1016/j.measurement.2018.01.022.

[14] Z. F. Yaseen and A. A. Kareem, ‘‘Image steganography based on hybrid edge detector to hide encrypted image using Vernam algorithm,’’ in Proc. 2nd Sci. Conf. Comput. Sci. (SCCS), Mar. 2019, pp. 75–80, doi:10.1109/SCCS.2019.8852625.

[15] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, S. Nidhal, N. S. Jalood, A. N. Jasim, and A. H. Shareef, ‘‘New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity,’’ IEEE Access, vol. 7, pp. 168994–169010, 2019, doi: 10.1109/ACCESS.2019.2949622.