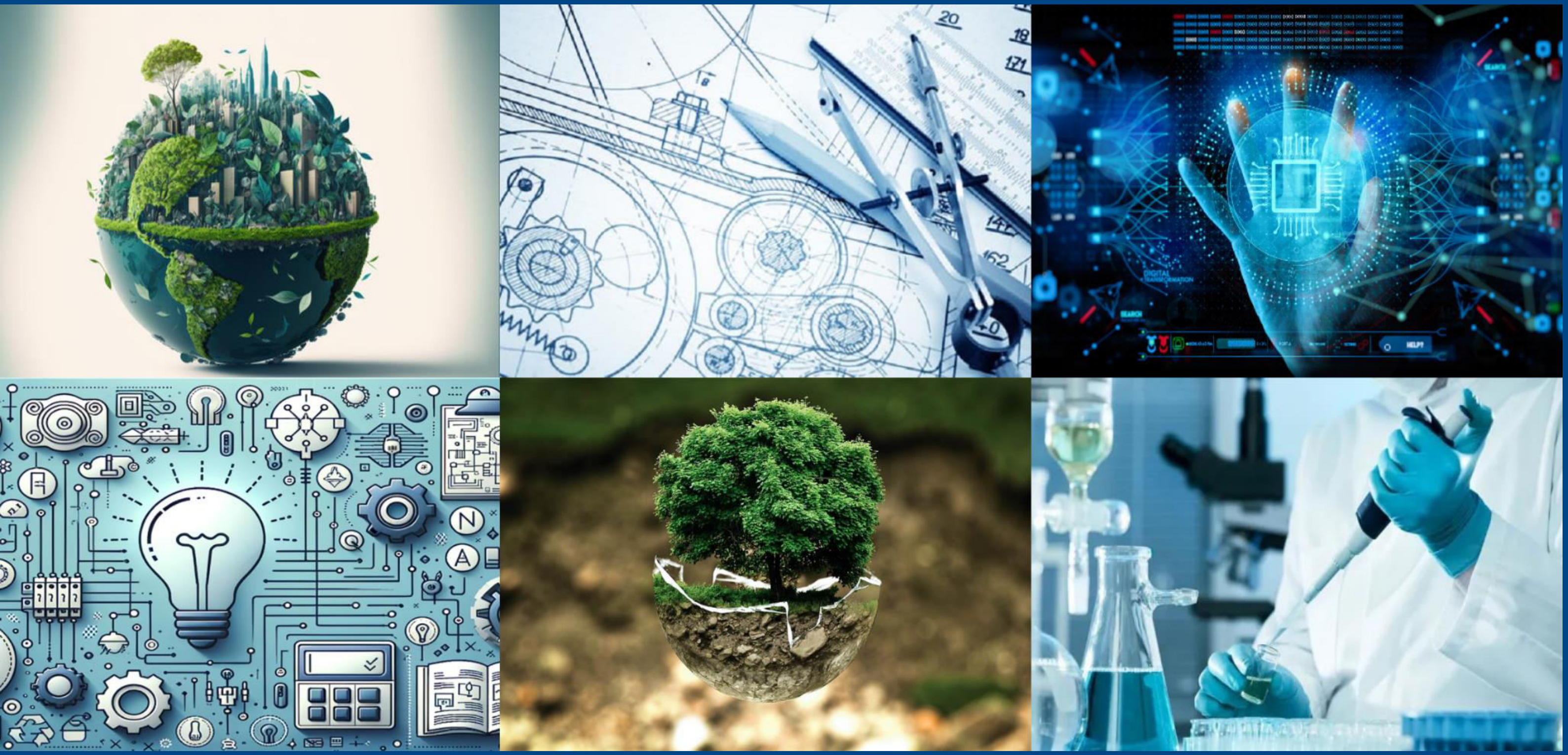
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Android Image Steganography with Least Significant Bit (LSB) Encoding

Dr.K.Baskar, Mrs.S.Ambigai Priya, M.Karthikeyan, T.Mohesh, R.Tamilarasan

Associate Professor, Dept. of AI&DS, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

Assistant Professor, Dept. of AI&DS, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

UG Student, Dept. of AI&DS, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

UG Student, Dept. of AI&DS, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

UG Student, Dept. of AI&DS, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

ABSTRACT: Steganography, the practice of concealing data within images, remains crucial for secure communications and data privacy. It has gained attention in governmental, corporate, and personal communications. With increasing privacy demands, steganographic techniques have evolved, integrating advanced algorithms to hide and retrieve data effectively. Using frequency domain methods, machine learning models, and Least Significant Bit (LSB) embedding, image steganography enhances security, resilience, and imperceptibility. Optimized algorithms now allow hiding larger data volumes without degrading image quality. User-friendly tools and mobile apps have expanded accessibility, driving further innovation. Researchers explore deep learning, reversible data hiding, and encryption-integrated steganography for stronger security. As digital privacy evolves, steganography remains vital for secure information sharing.

KEYWORDS: Steganography, Data Hiding, Cover Image, Encryption, Machine Learning, Least Significant Bit (LSB), Digital Privacy, Deep Learning, Secure Communication.

I. INTRODUCTION

The "Android Image Steganography the usage of Least Significant Bit (LSB) Encoding" assignment is all about locating a way to hold sensitive information safe with out every person realizing it. With hackers and cyberattacks going on all of the time now, it’s crucial to shield facts—whether it’s personal, commercial enterprise-related, or maybe authorities secrets. This venture does just that via the use of a method known as steganography, in which we hide facts inside virtual photographs. So, how does it work? Well, the center approach is called Least Significant Bit (LSB) encoding. Basically, it way we hide the facts in the least major components of the photograph, that are the smallest bits of facts that make up each pixel. The cool component is that you cannot tell something is hidden, because the image itself looks flawlessly ordinary. On top of that, we use encryption, so now not simplest is the records nicely hidden, but it’s also locked up tight. This guarantees that despite the fact that someone does figure obtainable hidden records, they received be capable of study it without the important thing What’s clearly exciting is this mission indicates how steganography is evolving. It’s no longer only a few old-school technique of hiding messages anymore—it’s something that can be utilized in actual-lifestyles conditions to maintain communication safe. Combining this approach with modern-day encryption methods manner we are able to create a strong strategy to stable facts and communications in a international in which digital threats are anywhere. A huge recognition of the assignment is making sure it’s easy for each person to apply. That’s why there’s a cellular app, so absolutely everyone with a telephone can use it to safely percentage their facts, irrespective of in which they may be. It's all about making these superior safety methods available to ordinary human beings, not simply tech professionals.

How does it work? Basic technology is known as the minimum important bit (LSB) coding. In short, this means that we hide information in the areas that at least appear, the smallest data points include each pixel. One of the most important demanding situations in virtual safety is making sure that the protection doesn’t intrude with the person experience. With this undertaking, the photo quality remains intact, which means that the person doesn’t should sacrifice whatever in phrases of appearance for superior protection. The hidden statistics blends seamlessly with the picture, supplying an answer that is both realistic and unobtrusive. Additionally, the use of mobile apps aligns with the fashion of cellular-first era. With extra people counting on smartphones for the entirety from banking to communication, ensuring privacy on cellular systems is crucial. The ease of use and comfort of a cell app facilitates make superior safety capabilities available to each person, that could encourage more people to prioritize virtual privacy. To ensure the facts stays greater secure, the assignment additionally makes use of encryption, meaning the message itself is included along with the fact that it's hidden. Android Image Steganography who uses the least important bit (LSB) that encodes "Project" provides a smart, practical way to protect sensitive data in today's rapid digital world. By using information in images and using encryption, this ensures that communication remains private and safe, when cyber is cyber, cyber threats are still relevant in modern security solutions.

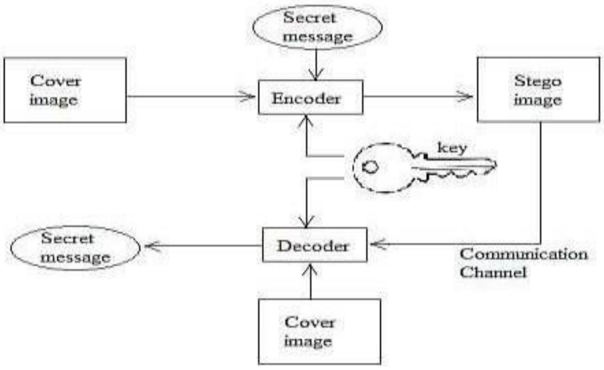


FIGURE 1. INTRODUCTION TO STEGANOGRAPHY

To summarize, the project thus presented allows for immovable image quality while providing a secure and smooth approach to data concealment. It brings together steganography and encryption in a way that ensures the confidentiality of the hidden message as well as security in the process of embedding it. The mobile-first approach caters to the increasing dependence on smartphones for communication and digital transactions by making the solution simpler for the user to access. This implementation does not only improve security, but also increases the awareness of digital privacy. The combination of encryption and LSB steganography provides the system with an efficient, practical, and applied solution for the protection of sensitive material amidst the problem of cyber threats.

II. LITERATURE SURVEY

Image steganography is a critical field in data security, aiming to conceal information within images to ensure secure communication. Various methodologies have been proposed, incorporating different cryptographic and steganographic techniques to enhance data confidentiality and robustness against attacks. The study by Esther Hannah et al. proposed an Android-based image steganography approach using the Least Significant Bit (LSB) method combined with password-based encryption. Their methodology involved encrypting the image using a symmetric encryption algorithm before embedding the encrypted secret key into a cover image through an asymmetric encryption technique. Similarly, Bharti Sahu et al. introduced a novel steganographic method that balances information concealment and visual quality, ensuring that hidden messages remain undetectable while preserving the original image quality. Another significant approach is found in the work of Richard Kofi Kyei et al., where RSA encryption was integrated with LSB insertion to enhance security. This method ensured that the encrypted message, embedded within the cover image, could only be decrypted using the recipient's private key, thus improving resistance against brute-force attacks .

In terms of accuracy, the study by Sahu et al. measured superior visual imperceptibility when compared to conventional LSB techniques, as measured by the Peak Signal-to-Noise Ratio (PSNR). In a similar vein, the suggested model that combined CNN-based steganography with Generative Adversarial Networks (GANs) showed improved security and resilience, successfully fending off steganalysis attacks. Recent advancements in image steganography integrate cryptographic encryption, LSB (Least Significant Bit) techniques, and deep learning to enhance data security. Esther

Hannah et al. (2023) proposed an Android-based steganographic system that encrypts messages using symmetric encryption, secures the encryption key with asymmetric encryption (e.g., RSA), and embeds the encrypted key into an image using LSB substitution, ensuring confidentiality and resistance to unauthorized access. adverse social effects of AI use, accountability, and transparency. We will also talk about ethical and social issues in an effort to identify long-term AI solutions.

In recent times, image steganography has advanced toward improving security, imperceptibility, and robustness. In this, RSA and AES cryptographic techniques were incorporated with LSB-based methods to prevent brute-force attacks and unauthorized access. Adaptive pixel selection and multi-layered encryption improved their resilience to steganalysis. Deep learning models-CNNs and GANs-have been developed to enhance data concealment by making stego images nearly undetectable. Innovative techniques like Knight's Tour-based embedding and bit-plane slicing further strengthened security. These advancements still promise modern digital communication efficient, secured, and adaptable steganographic systems while dealing with the ethical issues regarding AI-based security solutions.

III. PROPOSED METHODOLOGY

Steganography is a field concerned with concealing messages, but the visible presence of anomalies in statistical domains indicates the challenges it faces regarding detection. Detection probabilities and false alarm rates show that there is an urgent need for embedding to be of an adaptive nature and encryption that is sufficiently resilient to ensure steganography inter a non-detection process. The Probability of Detection, P_D, describes the efficiency with which a system can aid in the identification of suspect images showing signs of hidden messages, which becomes stronger with increasing data volumes. P_F, or Probability of False Alarm, relates to the likelihood of wrongly assuming that a clean image is steganographic. An active coupling between both these probabilities is imperative to upholding their security while mitigating false positives. Steganographic capacity is more about the maximum quantity of information that can be inscribed invisibly in an image so that it will not be detected by visible changes of images. When utilizing hidden information, it should not create distortion in images since these changes can be marked by statistical analyses. It is crucial that secret steganographic methods have both considerable capacity and invisible changes. In contrast to the fixed approaches, adaptive techniques make adjustments within the data embedding in correspondence with the attributes of the image. These may involve using the position of embedding, considering bit selection, or changes made to the pixel changes that are going to evade detection. Adaptive techniques enhance protection in view of the dynamism with which their execution exploits natural features of images, including textures and distributions based on colors. Enhanced encryption algorithms Support Steganography by changing hidden messages into the unintelligible fashion before being embedded within. Most types of traditional hidden information are defenseless once they are detected, but this can be dealt with by employing encryption: it adds security in one further step. In at least some cases, the combination of cryptography involving AES, RSA, and so on with steganography lends to ever-greater resilience against attacks. Putting together all efforts made towards optimizing detection probabilities, contextual embedding, and encrypting drives up the efforts towards strengthening steganographic security, ensuring that hidden messages remain undetectable even with the most advanced analysis.

IV. TECHNOLOGIES USED

1. LEAST SIGNIFICANT BIT (LSB):

One of the most straightforward and popular methods in spatial domain steganography is this one. It functions by substituting bits from the hidden message for the least significant bit of each pixel's color value. Since the least significant bits have minimal impact on the overall image, the alterations remain visually imperceptible.

2. SOFTWARE TOOLS & MOBILE APPLICATIONS:

Tools like StegHide, OpenStego, and SteganoGAN provide user-friendly interfaces for embedding and retrieving hidden messages. StegSolve aids in analyzing stego-images, while Hide and Seek offers secure LSB-based steganography. Mobile apps such as PixelKnot and Steganography Master enable steganographic communication on smartphones.

3. MACHINE LEARNING-BASED STEGANOGRAPHY:

Image steganography project leverages machine learning-based models to enhance security, imperceptibility, and robustness. Convolutional Neural Networks (CNNs) optimize the embedding process by identifying ideal regions for data hiding. Generative Adversarial Networks (GANs) improve detection resistance by generating stego-images that closely resemble original ones. Autoencoders are used for encoding and decoding hidden messages efficiently while preserving image quality.

4. ENCRYPTION-INTEGRATED STEGANOGRAPHY:

Image steganography project incorporates encryption-integrated steganography to enhance the security of hidden messages. By encrypting the data before embedding it into the image, techniques like AES (Advanced Encryption Standard) and RSA encryption ensure because without the decryption key, the secret message cannot be read, even if it is discovered. For mobile apps, ChaCha20 offers a portable encryption substitute.

5. REVERSIBLE DATA HIDING (RDH):

Methods for Reversible Data Hiding (RDH) to guarantee that, following data extraction, the original image can be entirely restored. Methods like Histogram Shifting and Difference Expansion create space within the image for embedding data without permanently altering the cover image.

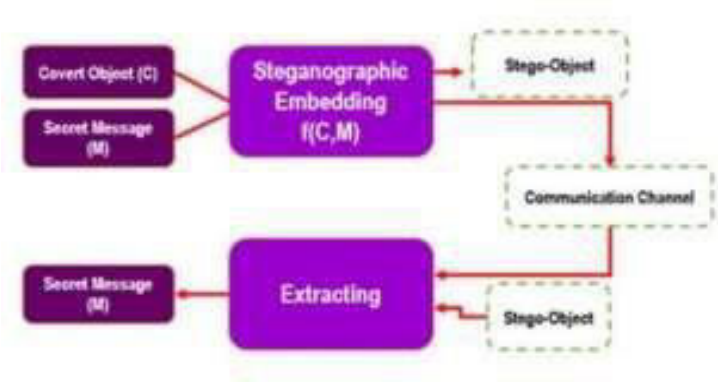


FIGURE 2. TECHNOLOGICAL ARCHITECTURE WHY LEAST SIGNIFICANT BIT?

Because it is easy to apply, effective, and has little effect on image quality, LSB (Least Significant Bit) steganography is extensively utilized. The hidden data is hard for the human eye to see since it just slightly alters the image by substituting bits from the secret message for the least important pixel values. LSB allows for the efficient storage of significant amounts of data while maintaining fast embedding and extraction processes. It works well with various image formats, especially uncompressed ones, and can be enhanced with encryption or other techniques to improve security.

SECURE COMMUNICATION SYSTEM

• The Steganography-based system enables secure data concealment within digital images, ensuring confidentiality and privacy in communication. This system utilizes advanced steganographic techniques to embed and retrieve sensitive information while preserving image quality and imperceptibility.

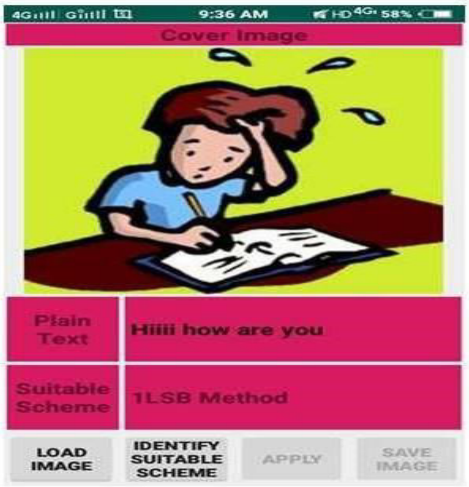
• Users interact with the system by entering a secret message into a dedicated textbox and selecting a cover image. The main function, main_func, orchestrates the core logic, embedding the message securely within the image while maintaining the integrity of the cover medium.

• The persistence setting (PERSIST) determines whether the system retrieves previously embedded messages or encodes new ones within the cover image, enabling efficient data storage and extraction. The Secure Data Buffer ensures the continuity of hidden information and protects against unauthorized access.

• The most critical part of the system lies in the Steganographic Processing Chain, which integrates data embedding algorithms, encryption techniques, and retrieval mechanisms. This ensures that the concealed message remains undetectable while allowing accurate extraction when needed. The User Interface simplifies the process, allowing users to input messages, upload images, and retrieve hidden data efficiently.

V. RESULT AND DISCUSSION

In Figure. 3, the image represents secure data embedding using LSB, ensuring minimal distortion but vulnerable to steganalysis. AES and RSA encryption enhance security, making hidden data harder to detect.

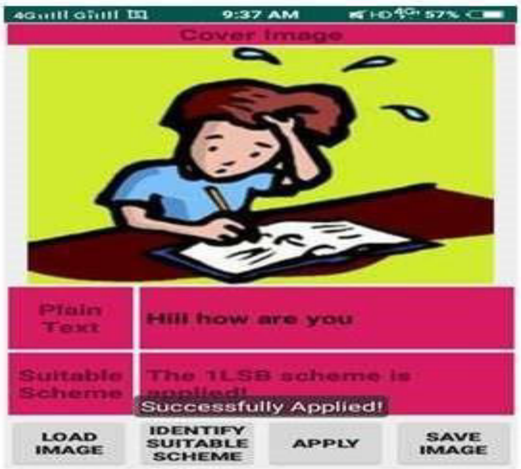


Plain Text: Hiiii how are you

Suitable Scheme: 1LSB Method

FIGURE. 3 SECRET MESSAGE

In Figure. 4, the image shows how GANs and DCT/DWT techniques optimize data embedding, improving resistance to compression and noise. This ensures the hidden data remains imperceptible.



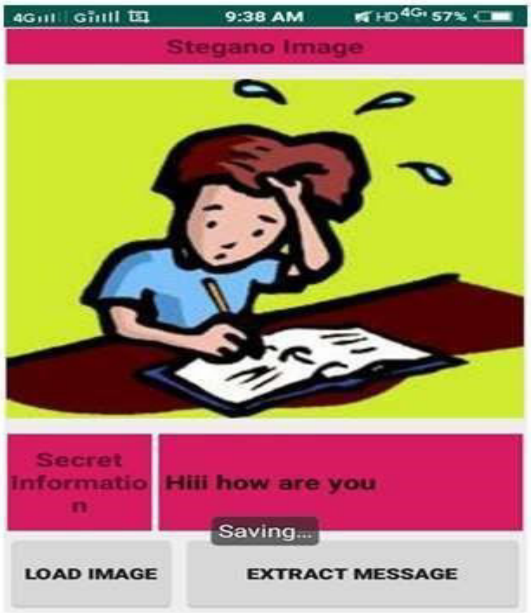
Plain Text: Hiii how are you

Suitable Scheme: The 1LSB scheme is applied!

Successfully Applied!

FIGURE. 4 INFORMATION HIDING

In Figure. 5, the image shows how GANs and DCT/DWT techniques optimize data embedding, improving resistance to compression and noise. This ensures the hidden data remains imperceptible.



Stegano Image

Secret Informatio n

Hiii how are you

Saving...

FIGURE.5 INFORMATION EXTRACTION

VI. CONCLUSION

Image steganography ensures secure, efficient, and imperceptible data hiding. Least Significant Bit (LSB) embedding hides small data but is vulnerable to detection. Frequency domain methods like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) enhance robustness against compression and resizing. Machine learning models such as Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs) improve adaptive embedding. Reversible Data Hiding (RDH) allows full image recovery. Encryption-integrated techniques using AES and RSA add security, ensuring data remains protected. This system supports secure communication, data privacy, and medical imaging while maintaining image integrity.

REFERENCES

[1] K. Baskar, G. K. D. Prasanna Venkatesan, S. Sangeetha, P. Preethi, "Privacy-Preserving Cost-Optimization for Dynamic Replication in Cloud Data Centers," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 927-932, DOI: 10.1109/ICACITE51222.2021.9404573.

[2] Amrutha C. V., Jyotsna C, “A Robust System for Video Classification: Identification and Tracking of suspicious Individuals from Surveillance Videos”, International Conference On Soft Computing & Signal Processing, 2020.

[3] N. Krishnnan, S. Ahmed, T. Ganta and G. Jeyakumar," A Video Analytics Based Solution for Detecting the Attention Level of the Students in Class Rooms,"2020 10th International Conference on Cloud Computing, Data Science & Engineering, Noida, India, 2020.

[4] M. Awais et al., "Real-Time Surveillance Through Face Recognition Using HOG and Feedforward Neural Networks," in IEEE Access, vol. 7,2019

[5] 5. K Baskar, GKD Venkatesan, R Jagatheswar, S Parthiban, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," Grenze International Journal of Engineering & Technology (GIJET), 2019.

[6] R Pavithra, Dr R Asokan, K Baskar, "Improving Privacy And Dynamic Updation Using Ranked Search Over Outsourced Cloud Data," International Research Journal of Engineering and Technology (IRJET), 2016.

[7] M Thangadurai, K Baskar, "Secure Outsourced Data Stream under Multiple Keys Using Random Algorithm in Cloud Computing," International Journal of Science, Engineering and Computer Technology, 2016.

[8] Steganography Algorithms in Color and Gray Scale Images," Proceedings of 2014 RAECS UIET Panjab University Chandigarh,06- 08, March 2014.

[9] Padmini.K, Champakamala .B.S, Radhika .D. K Asst Professors, Department of TCE, Don Bosco Inst-itute of Technology, Bangalore, "Least Significant Bit algorithm for image steganography"India International Journal of Advanced Computer Technology(IJACT), Volume 3,Number 4.

[10] Richard Apau, Michael Asante, Francis Twum, James Ben Hayfron-Acquah, Kwame Osei Peasah, "Image Steganography Techniques for Resisting Statistical Steganalysis Attacks: A Systematic Literature Review," PLOS ONE, vol. 19, no. 9, pp. 1-18, 2024.

[11] Richard Kofi Kyei, Joseph Kobina Panford, James Ben Hayfron-Acquah, "Enhancing Data Security in Android Smartphones Using Image Steganography, RSA Encryption with LSB Insertion," International Journal of Computer Applications, vol. 13, no. 8, pp. 45-53, 2024.

[12] Mohammed Abod Hussein, Younis Mohammed Younis, Ramadhan J. Mstafa, Haval I. Hussein, Ahmed L. Alyousify, "Android Image Steganography," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 11, no. 3, pp. 235-245, 2023

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com