Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 39, August 2023 – www.caeaccess.org

Implementing Image Steganography Techniques for Secure Data Hiding in the Development of an Android Application

Ayodeji Olusegun Akinwumi
Department of Computer Science,
Faculty of Science,
Adekunle Ajasin University,
Akungba Akoko, Ondo State,
Nigeria

Oluwatosin Lara Ogbeide
Department of Computer Science,
Faculty of Science,
Adekunle Ajasin University,
Akungba Akoko, Ondo State,
Nigeria

Deborah Feyisayo Folorunso
Department of Computer Science,
Faculty of Science,
Adekunle Ajasin University,
Akungba Akoko, Ondo State,
Nigeria

ABSTRACT
The rapid advancement of information and communication technology (ICT) has revolutionized communication and streamlined various tasks. With the widespread use of mobile phones by over 6 billion people globally, they have become the dominant means of communication and an essential personal tool. As mobile devices store sensitive personal data, ensuring data security has become paramount due to the rising incidence of digital crimes and the increasing reliance on these devices. While passwords and PINs have been employed as data security measures, research has indicated their vulnerability to attacks, highlighting the need for alternative techniques. In response to these challenges, this work introduces an Android application called 'The Hider', which uses the concept of image steganography for secure communication for Android phone users. The application is developed using Dart, a modern programming language, while the user interface (UI) is built with Flutter, a framework known for creating visually appealing and responsive interfaces. The proposed application utilizes cover images in formats like JPEG, PNG, or BMP to conceal both text and files, employing the AES encryption method. To enhance security, the application incorporates a secret key for encryption and decryption, along with a biometric feature that verifies the user's fingerprint. Considering these features, 'The Hider' application is recommended for all Android users seeking enhanced data security and privacy.

Keywords
Data security, steganography, cryptography, encryption, decryption, cover image, mobile devices, Android, The Hider.

1. INTRODUCTION
The rapid global growth of information and communication technology (ICT) has made communication between parties easier, greatly enhancing the efficiency of various operations. [1]. Without any doubt, ICT has greatly improved our way of life and streamlined the methods for carrying out tasks, primarily by enhancing communication channels and connectivity. The use of mobile phones has become an important component of communication in today's world. With over 6 billion people worldwide using mobile phones, they have become the most widely used and quickly expanding form of communication in human history [2].

Mobile phones are extensively utilized for various tasks such as phone calls, e-mailing, social networking, web browsing, online shopping, business and banking activities, among others [3]-[4]. Mobile device users consider them to be highly personal tools that not only assist in everyday activities but also store highly sensitive personal data [5]-[6]. With the continuous emergence of new tools and techniques and the growing reliance on mobile devices, ensuring data security for the information stored on these devices has become crucial in the face of the prevalence of digital crimes [7]. Information security, which plays a major role in any data transfer, has become increasingly important to protect sensitive data [8]-[9].

Data security is a mechanism for defending data against unwanted actions by unauthorized users. [10]. Data security involves measures taken to safeguard digital information from unauthorized access, manipulation, or theft. It encompasses various aspects, including the protection of hardware, storage systems, administrative controls, software, and the implementation of organizational policies and procedures [11]. In simpler terms, data security ensures that digital information is safe and secure from potential dangers such as hackers or unauthorized individuals who may attempt to access, edit, or steal sensitive data. Data security is very important for businesses, communicating parties and even all mobile phone users [12]. Data security operates under three triads, which are confidentiality, integrity, and availability [13], popularly known as the CIA. The confidentiality of data and information is manifested by limiting access to authorized individuals. Data integrity refers to the requirement that data be kept accurate and complete and not altered without permission, whether unintentionally or on purpose. The concept of availability in data security means making sure that authorized users always have easy access to the information they require. It implies that the data and resources must be consistently available, free from unwarranted disruptions or interruptions[14]-[15].

To counter the increasing number of attacks targeting mobile devices, a number of data security schemes have been employed, such as passwords and PINs [16]. However, these schemes are vulnerable to various types of attacks, including shoulder surfing, smearing, intersection attacks, and reflection attacks [17]. The study by [4] emphasized the shortcomings of passwords and PINs generated on mobile devices. According to the study, passwords and pins for mobile devices are harder to create and more prone to errors. Ultimately, the researchers discovered that passwords and PINs generated on mobile devices are significantly less secure against attacker and hackers. As a result, this suggests that conventional data protection techniques like passwords and PINs may not be

sufficient to prevent unwanted access. This necessitates the need to study other data security techniques that can be implemented for mobile device users, which will be more beneficial for phone users than the aforementioned security techniques. Steganography is a promising direction to explore. It is essential to develop a more secure and reliable method of data protection that can withstand these attacks and provide users with a safe platform for storing and transmitting sensitive information on their mobile devices.

Steganography means to "to be hidden in plain sight" and comes from the Greek word "secured writing" [18]. Steganography is the art and science of encoding a secret message within a cover medium, that is, using the cover medium to conceal the hidden information [19]-[20]. The purpose of steganography is not only concealing data but also masking the act of transmitting secret information. By hiding the secret data within another file, steganography ensures that only the intended recipient is aware of the existence of the message, keeping others unaware of its presence [21]. The implication of steganography is that it allows for covert communication and secured data storage by hiding secret information within innocent-looking cover media. By concealing the presence of the message, steganography ensures that unauthorized individuals are unaware of the sensitive data. Steganography techniques enable discreet and secure communication between the sender and intended recipient, enhancing the confidentiality and privacy of the information being conveyed.

Methods of steganography can be broadly categorized into text steganography, image steganography, audio steganography, video steganography, and network steganography [18]-[19]. Text steganography involves modifying text formatting or altering certain characteristics of textual elements. Image steganography conceals a message within an image without visibly affecting its appearance by changing pixels with significant color variations. Audio steganography hides data within audio files, utilizing the imperceptible differences in the Human Auditory System (HAS) to conceal the embedded information. Video steganography involves modifying videos to exclude specific objects from the scene and then inserting the original frame into the modified video. Network steganography exploits network protocol fields to create hidden channels between secret senders and receivers, enabling data concealment [19], [22]-[23]. These methods allow for the covert transmission of information across different media types while maintaining the appearance or functionality of the cover media.

However, the focus of this research is to implement a robust encryption algorithm, which is advanced image steganography, in the development of a mobile application called 'The Hider'. The objective is to develop a robust and secured platform for storing and transmitting secret messages, thereby ensuring the protection of sensitive information from unauthorized access. The proposed application utilizes advanced security measures such as biometric authentication and will provide users with the capability to hide and secure various file formats, such as TXT, PDF, and Word documents, within images using a secret key. The research explores the integration of image steganography in Android devices, focusing on encrypting and sending secret messages discreetly as well as hiding documents by embedding them into images for enhanced security and privacy. Furthermore, this study aims to provide comprehensive insights into the practical implementation of image steganography techniques and the seamless integration of document encryption and decryption functionalities within the Android environment on mobile phones. This technique provides a promising solution to the problem of data security on mobile devices, and the findings will contribute valuable knowledge to the field of data security and facilitate the development of secure communication applications on mobile devices.

2. RELATED WORKS

There have been numerous studies done on the application of steganography methods specifically for Android phones. Some of these studies are presented below.

The work of [24] developed an Android application called MoBiSiS (Mobile Steganography Imaging System) for sending images through MMS. The developed application enhances the capabilities of steganography algorithms by implementing them in an Android-based application. The application allows users to send stego-images via the Multimedia Messaging Service (MMS) and retrieve them from the device's message inbox for extracting the hidden message embedded within the stego image. However, the developed application has a restriction in that the cover image size must be under 30 KB in order for the secret message to be encoded in it. Messages can only be sent through MMS and not through other means such as email, social media or other communication channels, which is another limitation. The researchers in [25] developed an Android-based application based on both steganography and cryptography techniques called SmartSteg. The developed app hides a variety of files and works on different Android versions with very good processing speed. As noted by [26], the concept of the SmartSteg application may not be widely embraced by many users or researchers in the field. StegoApp, proposed by [26], is an Android-based image steganography application that uses the Least Significant Bit (LSB) algorithm. The app can conceal lengthy text messages of up to 100 words in a cover image, which can later be recovered using the same software. The application can also hide an image inside another cover image.

In [27], a hospital database system was implemented using image steganography, which offers enhanced security for biomedical reports, patient privacy, and highly confidential patient information. This system allows digital storage of patient images and reports within databases, ensuring that unauthorized individuals cannot access the information directly. The patient bio-data details, ailments, and prescribed medications are transformed using a steganography technique before being stored in the database. However, the image used must be minimal in size, and the encrypted data must be kept minimal to avoid detection within the cover image. The researchers in [28] developed a mobile application that will allow users to use cover images of small sizes to embed text and files. This makes the execution of encoding and decoding take less time. However, the application allows for the optional use of a secret key for encryption. However, this choice significantly reduces the robustness of the app, making it more vulnerable to potential attacks. Additionally, a limitation of the developed application is that the size of the cover image must be below 4 KB in order to successfully encode the secret message within it.

Based on the review conducted, most of the applications developed for image steganography are primarily designed to conceal short text messages within small cover images. The maximum number of words that can be hidden in the cover image is typically limited to 100 or less. This implies that there

is a limited capability for the Android applications already available in the market. This is an area where the researcher seeks to make a significant contribution. Furthermore, these applications often convert the original image format into a different format, such as PNG, after embedding the text message. Therefore, this study proposes a new steganography application that improves upon work of previous researchers in this area. The proposed application will be able to hide lengthy text messages exceeding 100 words in cover images and can encrypt and decrypt PDFs, Word documents, and images. It will also include a secret key for secure encryption and decryption, as well as an enhanced fingerprint security feature for user privacy and preventing unauthorized access.

3. METHODOLOGY

3.1 System Design

The proposed application is designed using Dart, a modern programming language known for its flexibility and ease of use. Dart is an object-oriented language with built-in support for asynchronous programming, making it well suited for applications that need non-blocking input and output operations. Its support for classes and interfaces makes it simple to construct straightforward, reusable code. Dart's popularity among programmers is on the rise because of the language's flexibility and power, both of which makes it ideal for creating web and mobile applications [29]. The user interface (UI) of the app is built with Flutter, a powerful framework for creating visually appealing and responsive user interfaces. Flutter is an open-source framework developed by Google for building mobile apps. It paves the way for the development of high-performance, visually attractive mobile apps that can run on both iOS and Android platforms from a single codebase [30].

By utilizing these technologies, the app has a robust system design with an intuitive and user-friendly interface. The integration of Dart and Flutter will also enable the app to perform efficiently and seamlessly on Android devices, providing users with a high-quality and enjoyable experience.

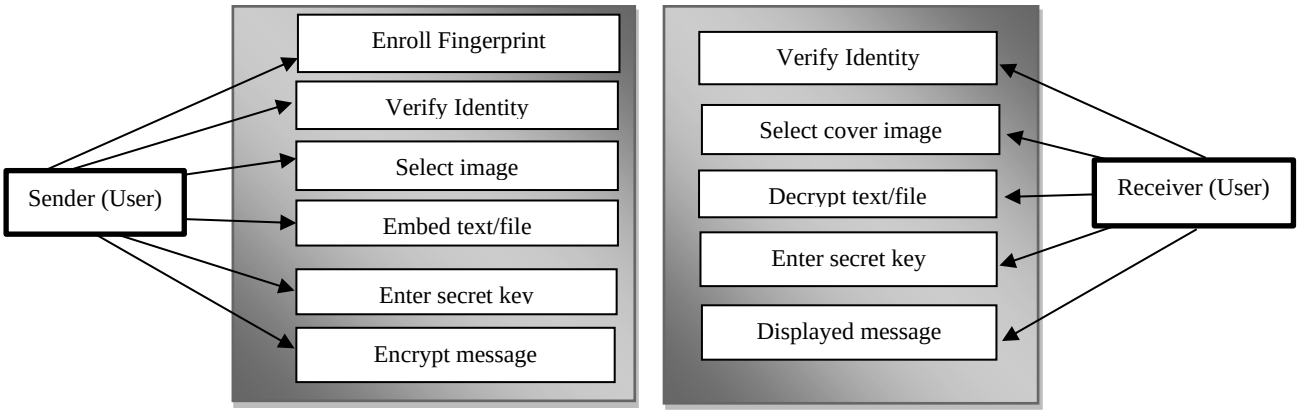

Figure 1: Use-Case Model of the Proposed Application

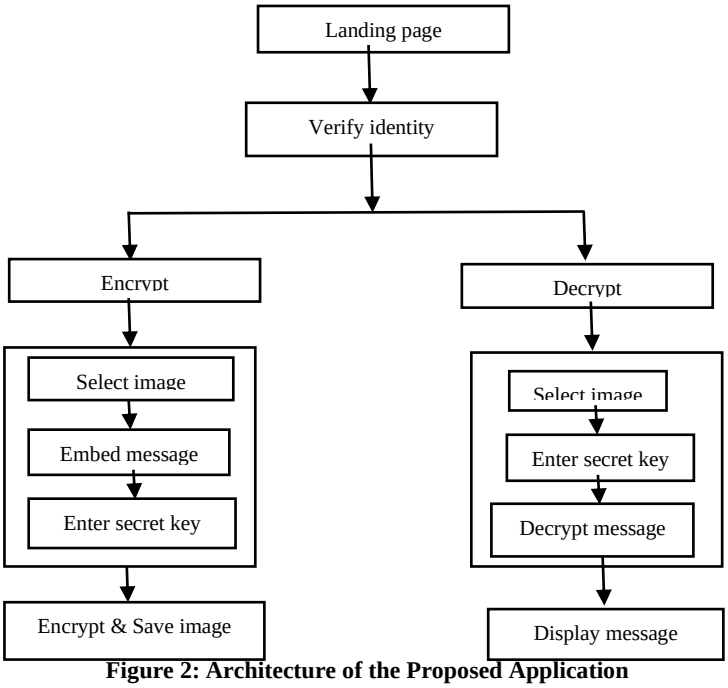

Figure 2: Architecture of the Proposed Application

3.2 Algorithm

The algorithm that will be adopted for the encryption and decryption processes is the Advanced Encryption Standard (AES) algorithm. The AES algorithm is a widely used symmetric encryption algorithm that is used to securely encrypt and decrypt digital data. By using the AES method for encryption, it is exceedingly difficult for hackers to decipher the original data. AES is widely regarded as resistant to all known attacks, making it highly trusted and recognized as the standard encryption algorithm by the United States Government and other various organizations [31]. The AES algorithm consists of four phases, executed sequentially, forming rounds. It encrypts plaintext through an initial round, nine equal rounds, and a final round, operating on a 4x4 state array [32].

3.3 Architecture and System Flow

The use case model for the proposed 'Hider App' is visually represented in Figure 1, illustrating the interactions and functionalities within the application from a user's perspective. The use case diagram outlines the essential user actions and system responses that define the app's operation. The architecture of the Android application is illustrated in Figure 2, while Figure 3 depicts the flowchart, which shows the interaction and sequence of steps involved in the proposed application.

3.3.1 Hardware Requirements

(i) **Processor Speed:** 1.5 GHz processor or more
(ii) **RAM:** 2GB RAM or more
(iii) **Storage:** 2GB of storage or higher
(iv) **Network connectivity:** It is an offline application; hence, it does not require an internet connection.

3.3.2 Cover Image Requirements

(i) **Format:** JPEG/PNG/GIF/BMP.
(ii) **File size:** Less than 3mb

3.3.3 Application Specifications

Below is the specification of the proposed application requirements and its file size before installation.

(i) **Operating system:** Android
(ii) **Total File Size:** 41.08 Megabytes
(iii) **Minimum Software Development Kit (SDK):** Android 4.4 (API 16)

4. RESULTS AND DISCUSSION

When the developed 'Hider' application is launched, it displays the landing page featuring the application logo, as shown in Figure 4. After a 5-second animation, the user is directed to the fingerprint authentication page, as revealed in Figure 5. The user is required to verify their identity using the fingerprint mechanism before they can be granted access to use the application. Successful verification of the fingerprint grants access to the home page, which contains encryption and decryption buttons (Figure 6). Each button leads to a distinct interface for encryption and decryption operations. If the user clicks the encrypt button, the mobile application will open the image selection page for encryption. Here, the user has the option to either select a cover image from their device's gallery or capture a new image using the device's camera. Once the image is selected, the application prompts the user to embed either text or a file into the chosen cover image, as shown in Figure 7.

The user can choose to encrypt files from their device or simply encrypt text, which will be embedded into the previously selected cover image. After this is done, Figure 8 shows the redirection page where the user is expected to input the secret key to use for the encryption process, as shown in Figure 8.

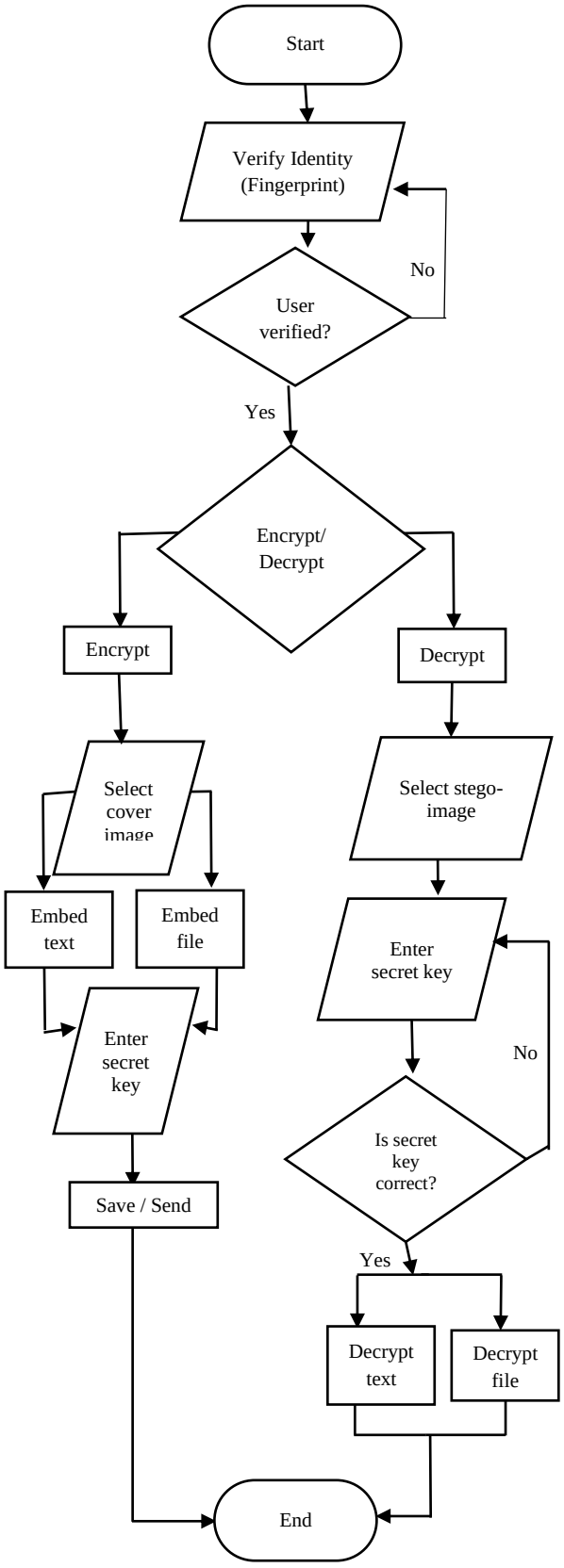

Figure 3: The Flowchart Diagram of the Proposed Application

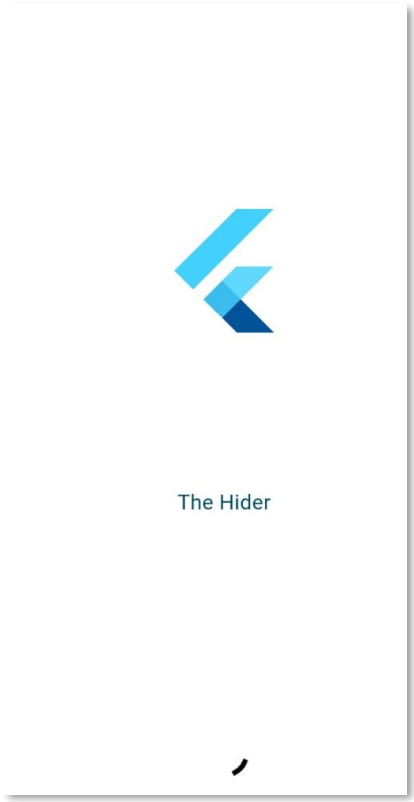

Figure 4: Landing Page

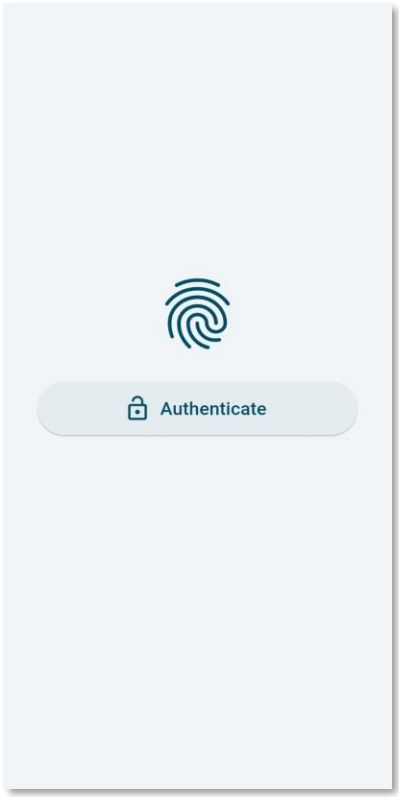

Figure 5: Authentication Page

Figure 6: Home Page/Encrypt/Decrypt Page

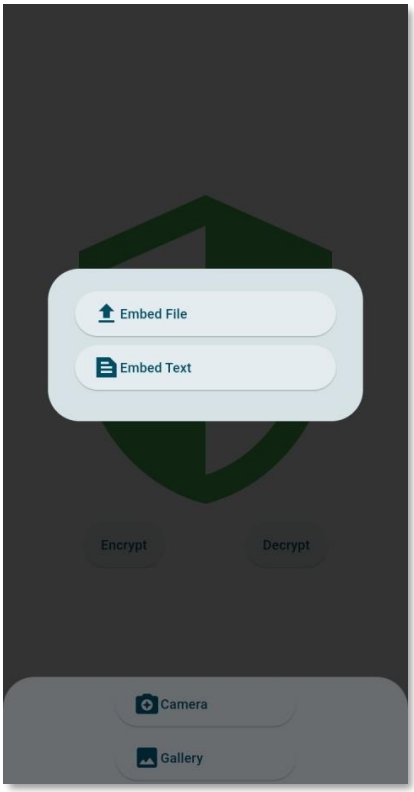

Figure 7: File and Text Encryption Interface

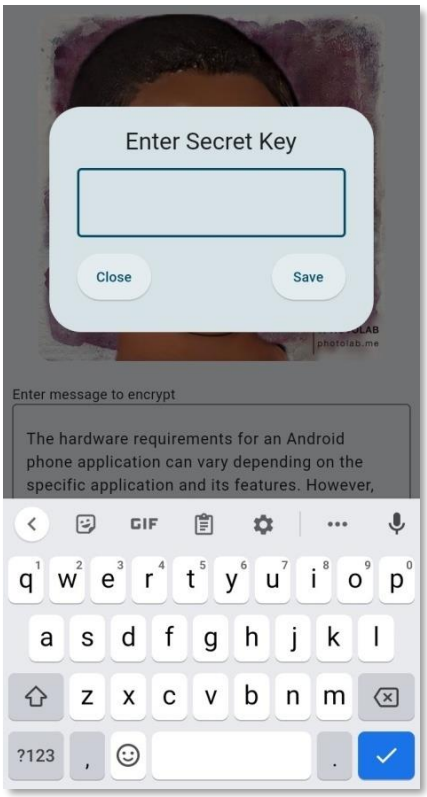

Figure 8: Secret Key Page

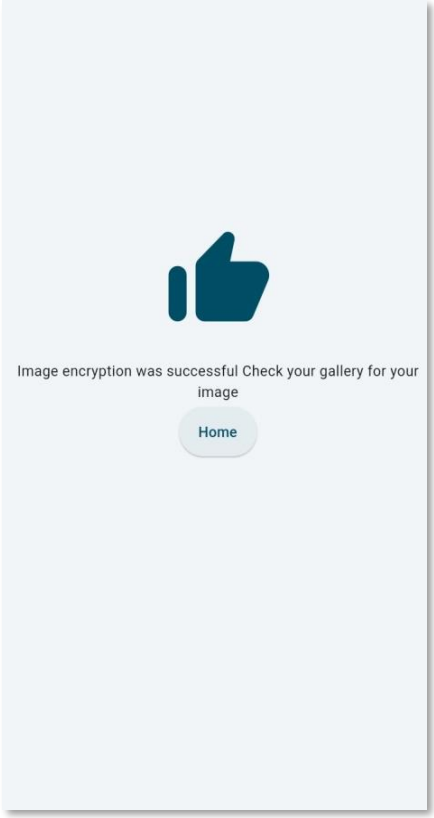

Figure 9: Successful Encryption Message

Figure 10: File and Text Decryption Interface

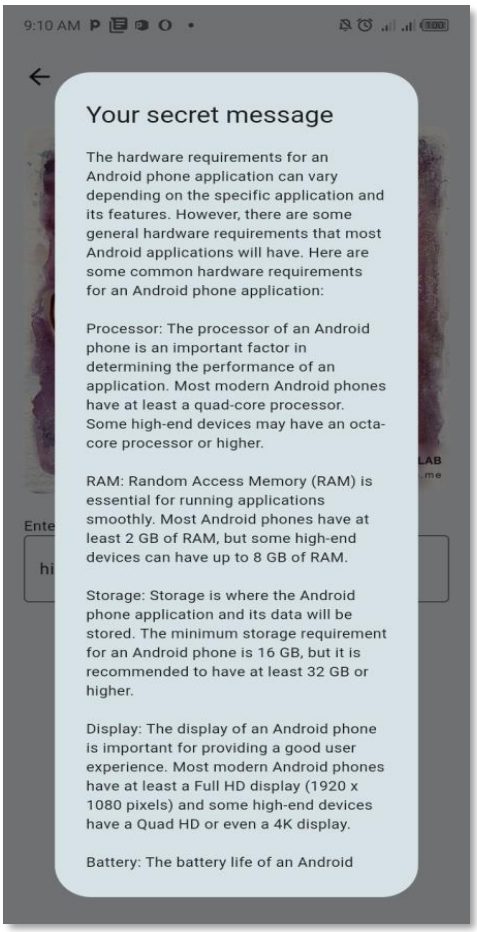

Figure 11: Secret Message for Embedded Text.

The secret key is intended exclusively for the sender and receiver of the stego-image. If obtained by a third party, it could potentially result in message intrusion. However, the inclusion of biometric authentication provides an additional layer of security, making it difficult for an intruder to gain access.

Once the secret key has been generated, the application will present the next interface (refer to Figure 9), confirming the successful encryption process. Additionally, the app provides a description of the location where the stego-image is stored on the user's device. The sender can then decide to use any means of transmission to convey the stego-image according to their preference.

To begin the decryption process of the stego-image, the user launches the application and undergoes fingerprint verification. Once successfully verified, the home page is displayed, featuring encryption and decryption buttons. Upon selecting the decrypt button (see Figure 6), the image selection interface where the user selects the appropriate stego-image for decryption will be displayed. After the stego-image has been selected, the interface to decrypt text or a file will be displayed, as illustrated in Figure 10. The decrypt text can be chosen if the message to be extracted is text, and if the message to be extracted is a document, the decrypt file can be selected. The next interface to be displayed is the secret key validation page. The application prompts the user to input the secret key used during encryption. The secret key validation is case-sensitive; if the secret key entered does not exactly match the key used for encryption, it will prompt an error message. However, if the secret key is an exact match, the application will display the secret text message embedded within the stego-image (as depicted in Figure 11). Alternatively, if a file is embedded, it will be successfully decrypted from the stego-image, ensuring user access to the content. This process confirms the successful decryption of the stego-image.

5. PERFORMANCE EVALUATION

The security of the transmitted data is assured in the application, ensuring that access to the encrypted message is exclusively granted to authorized individuals by means of biometric security and a secret key.

The Android application was tested on a Samsung A53 smartphone running Android 13, with a processor speed of 2.4GHz, a RAM size of 6GB, and a storage capacity of 128GB. A noteworthy advantage of this application is its ability to maintain the originality of the image transmitted. This feature thwarts any attempt by third parties to detect changes between the stego or original images. The detection of changes by unauthorized entities would compromise the fundamental purpose of employing image steganography. The analysis of results reveals a significant degree of similarity between the image before transmission and after reception, affirming the application's capability to reproduce the transmitted image.

Performance analysis of the ‘Hider’ application was done using key performance metrics, namely, SSIM (Structural Similarity Index), PSNR (Peak Signal-to-Noise Ratio), and MSE (Mean Squared Error). These are widely used metrics that measure the performance of image encryption schemes. An SSIM value closer to 1 indicates a very high quality of the transmitted image. A higher PSNR value corresponds to superior image quality, and values closer to zero for MSE indicate good image quality [33].

Table 1: Comparison of the proposed application with existing works.

WORK	SSIM	PNSR (dB)	MSE
Poojarani et al. (2015)	0.759	30.65	0.965
Manikandan et al. (2021)	0.958	48.94	0.352
Proposed Application (The Hider)	**0.962**	**48.97**	**0.31**

Furthermore, a comprehensive comparison of the application's performance was conducted against some existing works, as shown in Table 1. It is evident from Table 1 that the 'The Hider' application outperforms the previously studied works in terms of PSNR, MSE, and SSIM values. The proposed app attains an SSIM of 0.962, a PSNR of 48.97, and an MSE of 0.31, respectively. These metrics outperform the values reported by the work of Poojarani et al. [34] and Manikandan et al. [35], signifying the developed app's superior image preservation capabilities. This suggests that the 'The Hider' application offers enhanced image quality and performance compared to its counterparts.

6. CONCLUSION & RECOMMENDATION

This work successfully developed an Android-based application called 'The Hider', utilizing image-steganography techniques. The primary focus of the developed mobile application is to ensure privacy, confidentiality, and data accuracy on mobile devices. The integration of the AES algorithm contributes to the efficiency and effectiveness of the developed application. This research work significantly contributes to the fields of data hiding, data protection, and secure communication by employing image steganography for the secure transfer of data and vital information. The development of 'The Hider' application enhances the existing body of knowledge in the realm of data security and provides a reliable solution for secure data communication.

However, the research also lays the foundation for further future work to enhance the steganography application developed in this work. Specifically, a new application can be developed to allow encryption and decryption of video files. Additionally, incorporating facial identification would also enhance the overall security of the application. Additionally, expanding compatibility to include mobile devices other than Android would broaden its accessibility and potential user base.

7. REFERENCES

[1] A. O. Akinwumi, A. O. Akingbesote, O. O. Ajayi, and F. O. Aranuwa, "Detection of Distributed Denial of Service (DDoS) attacks using convolutional neural networks," *Niger. J. Technol.*, vol. 41, no. 6, pp. 1017–1024, 2022, doi: 10.4314/njt.v41i6.12.

[2] M. Kuyucu, "Mobile Media as A Digital Communication Tool," in *New Searches and Studies in Social and Humanities Sciences*, 2021, pp. 33–52.

[3] E. Kadëna and L. Ruiz, "Adoption of biometrics in mobile devices," in *Symposium for Young Researchers*, Budapest, 2017, pp. 140–148.

[4] W. Melicher *et al.*, "Usability and Security of Text Passwords on Mobile Devices," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 527–539. doi: 10.1145/2858036.2858384.

[5] O. O. Ajayi, A. A. Omotayo, A. O. Orogun, T. G. Omomule, and S. M. Orimoloye, "Performance Evaluation Of Native and Hybrid Applications," *Commun. Appl. Electron.*, vol. 7, no. 16, pp. 1–9, 2018, [Online]. Available: www.caeaccess.org

[6] P. Weichbroth and Ł. Łysik, "Mobile Security: Threats and Best Practices," *Mob. Inf. Syst.*, vol. 2020, pp. 1–15, 2020, doi: 10.1155/2020/8828078.

[7] T. Krishnappa, "Mobile Security Threats and a Short Survey on Mobile Awareness: a Review," *Int. J. Eng. Appl. Sci. Technol.*, vol. 7, no. 8, pp. 83–88, 2022, doi: 10.33564/ijeast.2022.v07i08.007.

[8] G. Ramya, "Steganography Based Data Hiding for Security Applications," in *Proceedings of the International Conference on Intelligent Computing and Communication for Smart World*, IEEE, 2018, pp. 131–135. doi: 10.1109/i2c2sw45816.2018.8997153.

[9] Z. Lu and H. Mohamed, "A Complex Encryption System Design Implemented by AES," *J. Inf. Secur.*, vol. 12, no. 02, pp. 177–187, 2021, doi: 10.4236/jis.2021.122009.

[10] I. Mary and C. Prince, "Data Security : Threats , Challenges and Protection Data Security : Threats , Challenges and Protection," no. May, 2021.

[11] IBM, "What is Data Security?" https://www.ibm.com/topics/data-security (accessed Jul. 11, 2023).

[12] H. Rout and B. K. Mishra, "Pros and Cons of Cryptography , Steganography and Perturbation techniques," no. December 2014, 2015.

[13] Y. Shi, "Data Security and Privacy Protection," in *2018 IEEE International Conference on Big Data*, IEEE, 2018, pp. 4812–4819. doi: 10.1109/BigData.2018.8622531.

[14] D. Popescul, U. Alexandru, I. Cuza, and C. E. Intercultural, "The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security . A Reassessment from the Point of View of the Knowledge Contribution to Innovation The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security . A Rea," no. June 2011, 2018.

[15] C. K. Yee and M. F. Zolkipli, "Review on Confidentiality , Integrity and Availability in Information Security," *J. ICT Educ.*, vol. 8, no. 2, pp. 34–42, 2021.

[16] M. Sreelatha, M. Shashi, M. Anirudh, M. Kumar, and M. S. Ahamerv, "Authentication Schemes for Session Passwords using Color and Images," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 3, pp. 111–119, 2011.

[17] S. Y. Ameen, "Smart Android Graphical Password Strategy : A Review Smart Android Graphical Password Strategy : A Review," no. June, 2021, doi: 10.9734/ajrcos/2021/v9i230220.

[18] S. Mishra and M. D. S. Dominic, "Steganography Data Hiding Technique," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 8, no. June, p. 6, 2020.

[19] P. Bedi and A. Dua, "Network Steganography using the

Overflow Field of Timestamp Third International Option in an IPv4 Packet," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1810–1818, 2020, doi: 10.1016/j.procs.2020.04.194.

[20] S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques.," in *Proceedings of the International Conference on Computing for Sustainable Global Development*, 2014, pp. 870–875.

[21] J. Kour and D. Verma, "Steganography Techniques – A Review Paper," *Int. J. Emerg. Res. Manag. &Technology*, vol. 9359, no. 5, pp. 132–135, 2014.

[22] F. S. Mohamad, N. Sahira, and M. Yasin, "Information Hiding Based on Audio Steganography using Least Significant Bit," *Int. J. Eng. Technol.*, vol. 7, no. 4.15, pp. 536–538, 2018.

[23] A. K. Nawar, "Hiding Information in Digital Images Using LSB Steganography Technique," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 7, pp. 167–178, 2023, doi: 10.3991/ijim.v17i07.38737.

[24] R. Ibrahim and L. C. Kee, "MoBiSiS : An Android-based Application for Sending Stego Image through MMS," in *The Seventh International Multi-Conference on Computing in the Global Information Technology*, 2012, pp. 115–120.

[25] Dominic Bucerzan, C. Ratiu, and M.-J. Manolescu, "SmartSteg : A New Android Based Steganography Application SmartSteg : A New Android Based Steganography Application Introduction," *Int. J. Comput. Commun. Control*, vol. 8, no. 5, pp. 681–688, 2013, doi: 10.15837/ijccc.2013.5.642.

[26] A. Ullah and M. Ijaz, "Stego App : Android based image steganography application using LSB algorithm," *Int. Res. J. Eng. Technol.*, vol. 5, no. 9, pp. 862–865, 2018.

[27] P. D. Bhave, S. S. Desai, R. N. Mahale, and R. L. Mhatre, "Hospital Database System Using Image Steganography," *Int. J. Creat. Res. Thoughts*, vol. 9, no. 5, pp. 97–101, 2021.

[28] J. Shilwar, A. Kalsa, A. Ahire, and D. D. Pawar, "An Android Application For Image Steganography And Editing App," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 11, no. 4, pp. 517–519, 2022, doi: 10.17148/IJARCCE.2022.11491.

[29] A. M. Hassan, "JAVA and DART programming languages : Conceptual comparison," vol. 17, no. 2, pp. 845–849, 2020, doi: 10.11591/ijeecs.v17.i2.pp845-849.

[30] L. Dagne, "Flutter for Cross-Platform App and SDK Development," *Metrop. Univ. Appl. Sci.*, no. May, pp. 1–28, 2019.

[31] arcserve, "5 Common Encryption Algorithms and the Unbreakables of the Future," *Cybersecurity*, 2023. https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future (accessed Jul. 12, 2023).

[32] P. Telagarapu, B. Biswal, and V. S. Guntuku, "Design and Analysis of Multimedia Communication System," in *Proceedings of the Third International Conference on Advanced Computing*, Chennai: IEEE, 2011, pp. 193–197. doi: 10.1109/ICoAC.2011.6165174.

[33] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM , SSIM , MSE and PSNR — A Comparative Study," *J. Comput. Commun.*, vol. 7, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[34] P. Rani and A. Arora, "Image Security System using Encryption and Steganography," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 4, no. 6, pp. 3860–3869, 2015.

[35] T. Manikandan, A. Muruganandham, R. Babuji, V. Nandalal, and I. J. Mazher, "Secure E-Health using Images Steganography," *J. Phys. Conf. Ser.*, vol. 1917, pp. 1–7, 2021, doi: 10.1088/1742-6596/1917/1/012016.