Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 9. No. 2, 2021

Article Citation Format
Sarumi, J.A. , Longe, O.B & Adelodun, F.O.(2021): An Android-Based Image Steganography System for Concealing Data and Information Transmission Using Adaptive Image Steganography. Journal of Digital Innovations & Contemp Res. In Science., Engineering & Technology. Vol. 9, No. 2. Pp 19-38
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V9N2P6

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 4th June, 2021
Review Type: Blind
Final Acceptance:: 19th August, 2021

An Android-Based Image Steganography System for Concealing Data and Information Transmission Using Adaptive Image Steganography

Sarumi, J.A. (PhD), Longe, O.B. (PhD) & Adelodun, F.O.
Department of Computer Science, Lagos State Polytechnic, Ikorodu, Lagos Nigeria
Faculty of Computational Sciences & Informatics, Academic City University College, Accra, Ghana
Department of Computer Science, The Polytechnic, Ibadan, Nigeria
E-mails: jerrytechnologies@yahoo.co.uk; olumide.longe@acity.edu.gh; adelodunfelicia@gmail.com
Phone: +2348023408122, +233595479930, +2348033815562

ABSTRACT

The growth in the volume of information transmission and transaction over the internet has necessitated the development and enhancement of measures and techniques required to ensure the safety of critical information during transmission. with developments in mobile technologies and the adoption and diffusion of android mobile devices, research must therefore continue to explore more secured media in which information can be hidden. One of such medium is the use of image carriers referred to as steganography. In tis paper, we provide insughts into the development of an android-based Image Steganography System for concealing data and information using adaptive image steganography. The Least Significant Bit (LSB) algorithm was employed as the algorithmic sequence for the development. Preliminary results from implementation and testing showed promising results

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

1. INTRODUCTION

Watermarking and fingerprinting are closely related technologies to steganography, which are primarily concerned with the protection of intellectual property rights. Watermarking marks all the instance of an object in the same way. Watermarking signature contains the information hidden in the watermark, created to suggest the originality or possession for the aim of copyright. Fingerprinting embeds different unique mask in distinct copies of the carrier object that are supplied to different customers. With this, the copyright owner identifies the consumer that breaks or violates their licensing agreement by supplying the property to third parties. Cryptography is a technique used in securing the secrecy of transmitted information. It is hard enough to keep the contents of a message secret. Various strategies are developed in encrypting and decrypting in order to keep the knowledge secret. It may even be necessary to keep the existence of information secret. Steganography is the technique employed to keep the knowledge of the existence of the user's information secret *(Kadam et al., 2012).*

Wit the need to communicate sensitive information or personal messages secretly to a particular target destination without the fear of the message being breached or intercepted by a malicious third-party, considering the security challenges posed to users over the internet and possible identity thefts, we are forced to take matters into our own hands and protect ourselves from malicious people. These means of protection need to be fast, very accessible and handy. Different steganography systems have been built on computer systems, (desktops, laptop) but there is also a need to have this system built on handheld devices, for ease of use. With the recent advancement in hardware and software capabilities of smart devices, we can use their speed and processing power to create a steganography system on such devices. This would enable information hiding to be faster and more accessible to users.

1.1 Research Thrust

The aim of this research is to develop an android based image steganography system. Incremental development software process model will be used to develop the systemt. Several versions of the application will be tested as it is being developed and continuous work will be done until the final version is ready. Layered System Architecture is the preferred system architecture to be used for the development of this project because the major goal is to develop a security tool, in which a layered structure is best used, with the most critical aspect of the system protected in the innermost layers, with a high level of security validation applied to that layer. The scope of the research is to implement steganography on an android device as a tool for hiding information in an image file, information to be hidden may include any form of files (text, media or data files) and also upon retrieval of the concealed file from the image, the user can determine where the retrieved file will be stored. It also tries to make information hiding simpler and user-friendly.

1.2 Research Justification

Steganography offers to help us hide information we hope to transfer over a medium, using the various algorithm, depending on how robust our host machine or how we design our system. Users information can be well hidden and protected from the malicious party.

Considering Cybersecurity and other related security challenges, this study, if adopted, could provide the security of data and information to the following;

a) Aid transmission of high-level or top-secret documents between governments and her agencies.
b) In identity management (identity card), details of personal information could be embedded in JPEG image as passport photography.
c) It can be implemented by INEC for election in an online voting system.
d) It can be used by the Military in their communication system.
e) It can be used in the medical field to communicate hidden details of patients' treatment as it could be embedded into images and send to authorized users so as to reduce time period of carrying files, cost and protection of the resulting information.

2. EVALUATION OF EXISTING TECHNIQUES

Existing algorithms with respect to image steganography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the steganographic system. (*Shaddad et al., 2008)* The fig below shows the relationship between the parameters

- LSB technique in the spatial domain is a practical way to conceal information but, at the same time, it is vulnerable to small changes resulting from image processing or lossy compression. Although LSB techniques can hide large quantities of information i.e., high payload capacity, they often compensate the

statistical properties of the image and thus indicate low robustness against statistical attacks as well as image manipulation. (*Hamid et al., 2012)*

- The promising techniques such as DCT, DWT and the adaptive steganography are not susceptible to attacks, especially when the hidden message is small. This can be justified in relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms. The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers' attention towards JPEG images. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival. (*Hamid et al., 2012)*
- Spread spectrum techniques are generally quite robust against statistical attacks since the hidden message is spread throughout the image. However, a determined attacker is capable of compromising the embedded data using some digital processing, such as noise reduction filters, which are similar to the ones used in the decoding process to estimate the original cover. Spread spectrum encoding is extensively used in military communications due to its robustness against detection. When a message is embedded, an attacker cannot be easily recognized and it will be difficult to extract it without knowing the suitable keys. SISS is very good for steganography because of the reasonable high capacity and high difficulty proposed in the process of detection and extraction. (*Hamid et al., 2012)*
- The statistical techniques in most cases are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. Defences could be considered to make the statistical techniques as robust as the watermarking scheme. The payload capacity and invisibility depend on the cover image selected. (*Hamid et al., 2012)*
- Unlike many LSB methods, distortion techniques do not upset any statistical properties of the image. In contrast, the need to send the cover image over a secure channel limits the worth of this technique. As in any steganographic technique, the cover image should never be used more than one time. If an attacker alters the stego-image by cropping, rotating, or scaling, the alteration can easily be perceived by the receiver and can fairly be reversed to the point where the message encoded with error correcting information can be fully recovered. Error correcting information also aids if the stego-image is filtered through a lossy compression scheme such as JPEG. Adopting this technique limits the hidden information capacity, since adding distortion to the cover image is the basis of the embedding algorithm. As a result, the distorted image will be more vulnerable to the HVS. (*Hamid et al., 2012)*

Table 1 Comparing Image Steganography Techniques

Parameters	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques	File and Pallet embedding
Imperceptibility	High*	High	High	Medium*	Low	High*
Robustness	Low	High	Medium	Low	Low	Low
Payload Capacity	High	Low	High	Low*	Low	High

Table : Summary of Literature Survey on Steganography Encryption Techniques

Author(s)	Name	Description
D. Debnath et al.	"An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography"	These Authors proposed a new method in which both steganography and cryptography is used. Data is first encrypted using hill cyphers and then embedded into RGB cover image
D.E.M. Ahmed and O.O. Khalifa.	"Robust and Secure Image Steganography Based on Elliptic Curve Cryptography"	Their research work focuses on LSB image steganography along with elliptic curve cryptography (ECC). Secret information is first encrypted with the help of ECC and then ciphered information is embedded into cover image
N.A. Al-Otaibi, and A.A. Gutub	"Robust and Secure Image Steganography Based on Elliptic Curve Cryptography"	They designed a new system based on two layers of steganography and cryptography. Steganography layer use multiple LSB bit embedding and cryptography layer use AES algorithm for data encryption. Experimental results show that 1LSB and 2LSB embedding have good stego image quality than higher bit embedding
M. R. Islam et al.	"An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography"	These Authors proposed a new and improved version of LSB steganography based on efficient filtering using status bit. AES cryptography algorithm is applied to gain a higher level security to hidden secret data. Bitmap images are used as cover images. The proposed system has high PSNR and data hiding capacity
S. Krishnagopal et al.	"Image Encryption and Steganography Using Chaotic Maps with a Double Key Protection"	In this proposed work Chaos based cryptography is used with steganography. Chaotic logistic and cat maps are used as the base for their image encryption algorithm. Results demonstrate that proposed system has 0.981 SSIM index value and 47.71 dB PSNR
S. Song et al.	"A Novel Secure Communication Protocol Combining Steganography and Cryptography"	Authors proposed a very innovative method that combines the steganography and cryptography into one system. No separate computations will be done for these two. Hence the new system needs very few computations than existing techniques, while maintaining high-security level. Simulation results show that this system is safe from Steganalysis attacks

3. SYSTEM ANALYSIS AND DESIGN

3.1 Least Significant Bit Insertion.

This technique chosen the Least Significant Bit Insertion as the steganography technique I wish to implement in this project. In the LSB method, an image is used. An image is more than strings and string of bytes. Each byte in an image represents different colours. The last few bits in a colour byte do not hold much significance as the first few bits. Therefore, only two bits differ in the last few bits that represent a colour which is indistinguishable to human eyes. In the LSB method, least significant bits of a cover image is altered such that we can embed information. The example shows how letter A is hidden in the first 8 bits of 3 pixels in a 24-bit image. Since the 8-bit letter A requires only 8 bytes to hide it, the ninth byte of the 3 pixels used to hide the next character of the hidden message. *(U.K. Essays, 2018)*

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)

The five underlined bits are the 5 bits which were altered. With LSB insertion technique, on average half of the bits of an image are changed. 'A' is an 8-bit letter and requires 8 bits for hiding. The ninth byte of 3 pixels is used for hiding the next character of the secret message. *(Kaur et al., 2011).* The slight variations of this technique allow the messages to embed into two or more least significant bits per bytes and increases the information hidden capacity of the cover object, but the cover object is degraded and easily detectable. LSB insertion is easy to implement and is also easily attacked if the modifications are done wrong. Improper modifications in colour palette and simple image calculations will destroy the hidden message. Image resizing and image cropping are same examples of image manipulations. *(U.K. Essays, 2018).*

Systems analysis is a major part of the systems development life cycle in which helps us understand how the current system works, its shortcomings and what area can be improved on it, while system design, on the other hand, involves the process of defining the architecture, modules, interfaces, and data for a system to satisfy user-specified requirements. Systems design could be seen as the application of systems theory to system development. It also involves all forms of system modelling to depict in theory what the system should look like.

3.2 Description And Limitation Of Existing System

Existing systems are desktop application that uses the Least Significant Bit image steganography algorithms on desktops and personal computers. It required the user who needs to hide or encrypt his/her data in an instant, to turn on their personal computer and run the desktop app. In an era where some mobile phones are twice as fast as some computers system and information needs to travel at almost lightning speed. This is simply acceptable.
The following are some of the limitations deduced about the previous system;

a) The system was platform dependent. It runs on only a windows machine
b) The system was limited to personal computers alone as stated above.
c) The system wasn't robust; it only could handle images of limited size, and images from a single file format (.bmp)

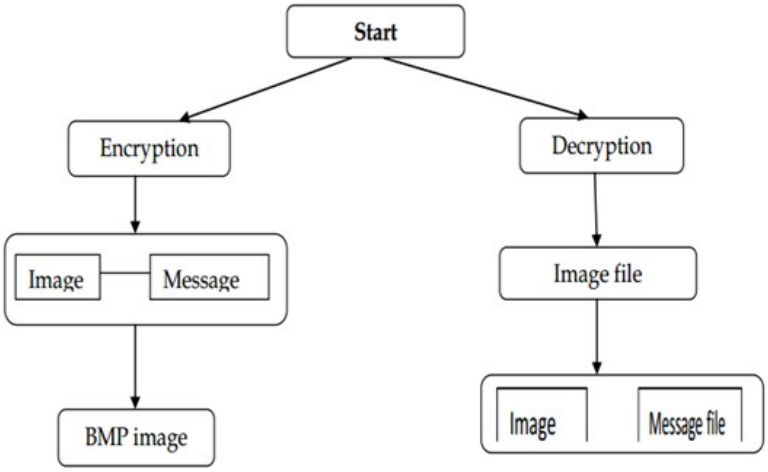

Figure 3.1 Flow of the existing system

3.3 The Proposed System

The proposed system is an android based image steganography system to be used as a security tool based on adaptive steganography techniques, which has an in-built steganography system to conceal user's private information, and also it reveals other user's information concealed by users of the Android application using the same steganography algorithms. It first encrypts the user data with the standard Advanced Encryption Standard (AES) algorithm before embedding them in the image to serve as a means of prevent from information tampering.

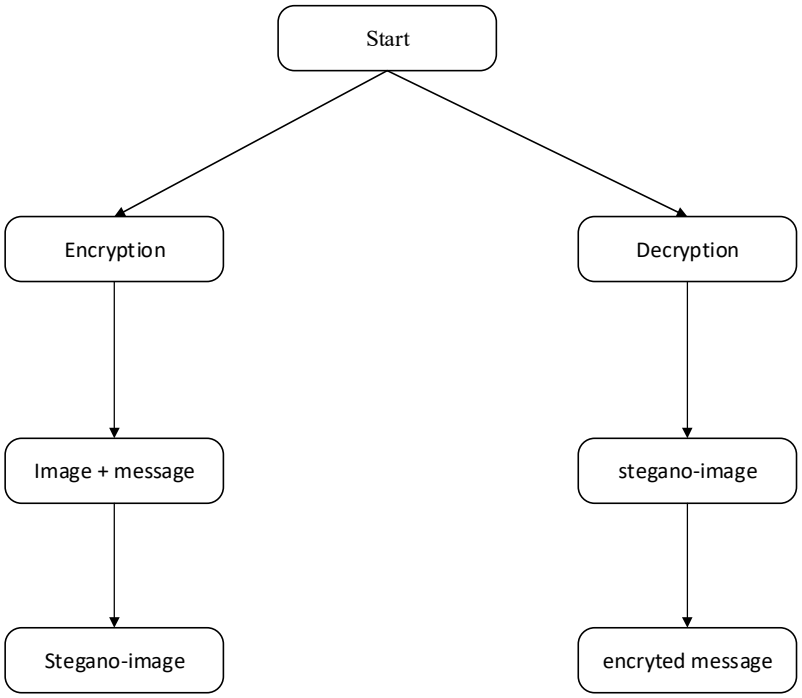

Figure 3.2 Flow of proposed system

3.4. Software Development Process Model

The proposed system would use incremental development as the software development process model. Several versions of the app will be tested as it is being developed and continuous work will be done until the final version is ready. The Layered architecture will be used for this System. It enables separation of concern and offers simplicity and consistency. Another major factor is because this system is developed as a security tool, a layered structure for the architecture is best used, with the most critical assets protected in the innermost layers, with a high level of security validation applied to these layers. The layered approach supports the incremental development of systems. As a layer is developed, some of the services provided by that layer may be made available to users. The architecture is also changeable and portable. So long as its interface is unchanged, a layer can be replaced by another, equivalent layer. Furthermore, when layer interfaces change or new facilities are added to a layer, only the adjacent layer is affected. As layered systems localize machine dependencies in inner layers, this makes it easier to provide multi-platform implementations of an application system. (Sommerville, 2011)

Architectural Diagram

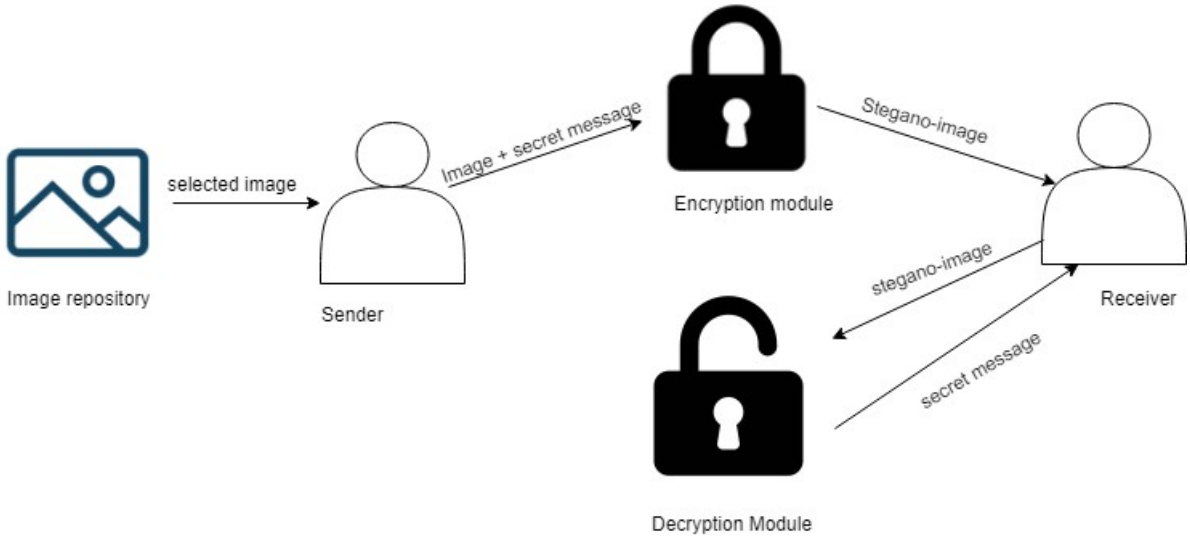

Figure 3.3 System Architecture diagram

Context Diagram

This models a high-level view of the system, it defines the boundary between the system, or part of a system, and its environment (external systems), showing the entities that interact with it. The context diagram of the system is shown below;

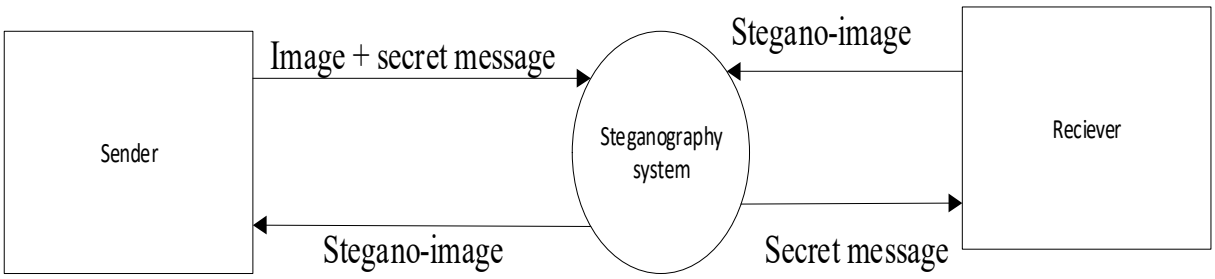

Figure 3.4 Context Diagram of the System

Use Case Diagram:
This is a graphical display of all the possible interactions in the system.

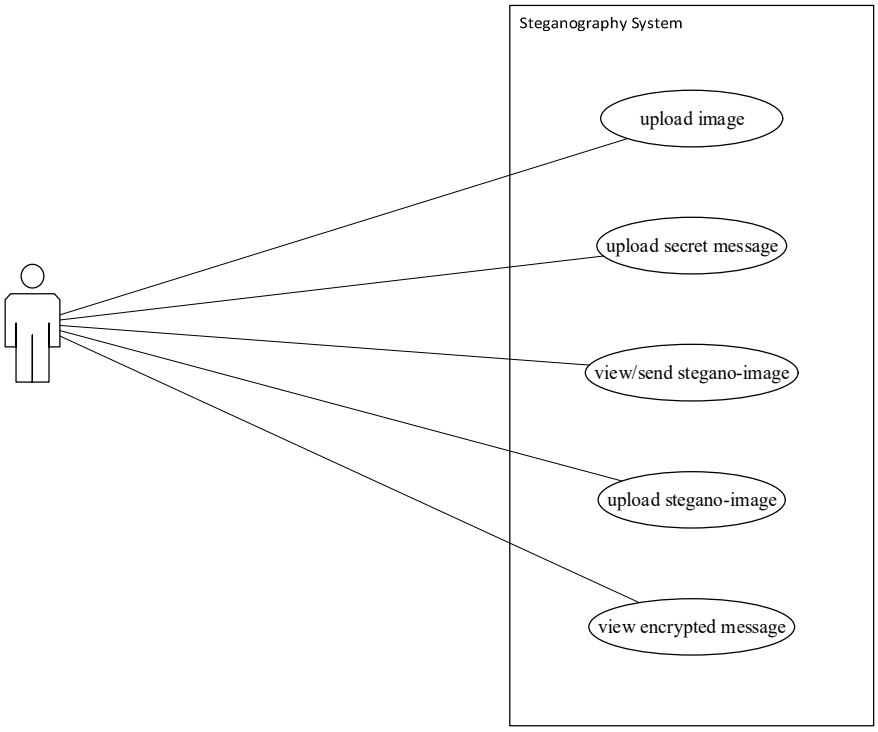

Figure 3.5 Use Case Diagram of The Proposed System

Sequence Diagram:
This model depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

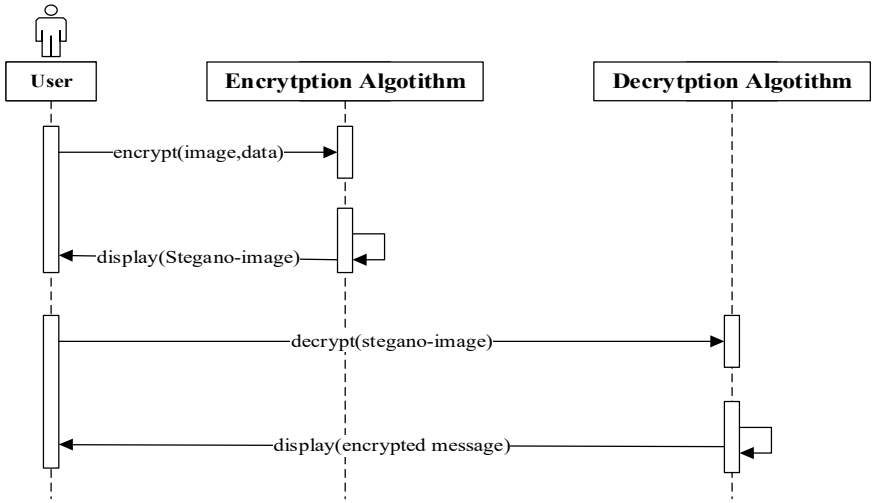

Figure 3.6 Sequence diagram of the proposed system

Process Model

Process modelling involves 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.

- **Data-flow Diagram:** This illustrates the movement of data between external entities and the processes and data stores within a system.

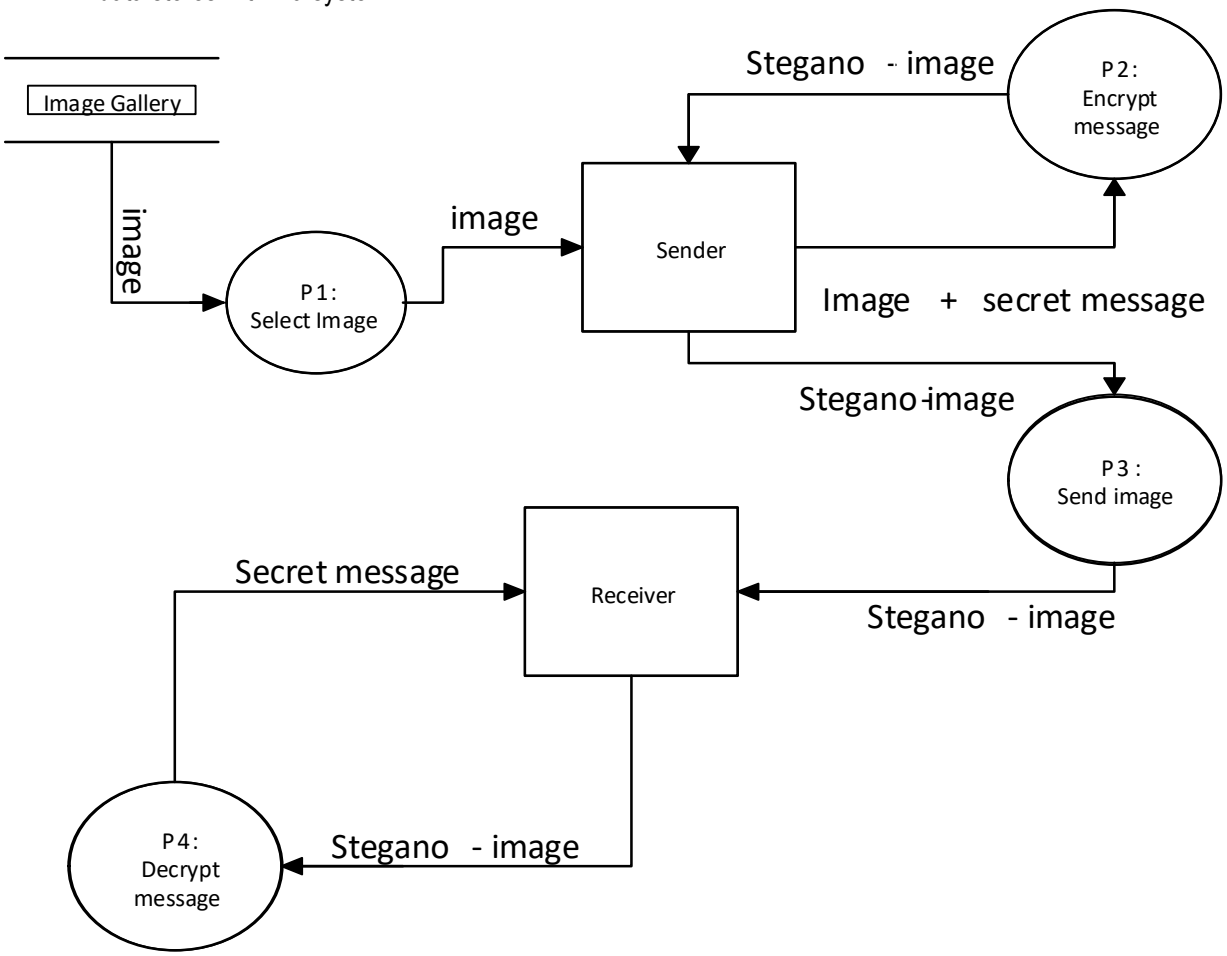

Figure 3.7 Dataflow diagram (Level-0 Diagram)

Activity Diagram.

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. It is used to describe the dynamic aspects of the system. An activity diagram is basically a flowchart to represent the flow from one activity to another activity.

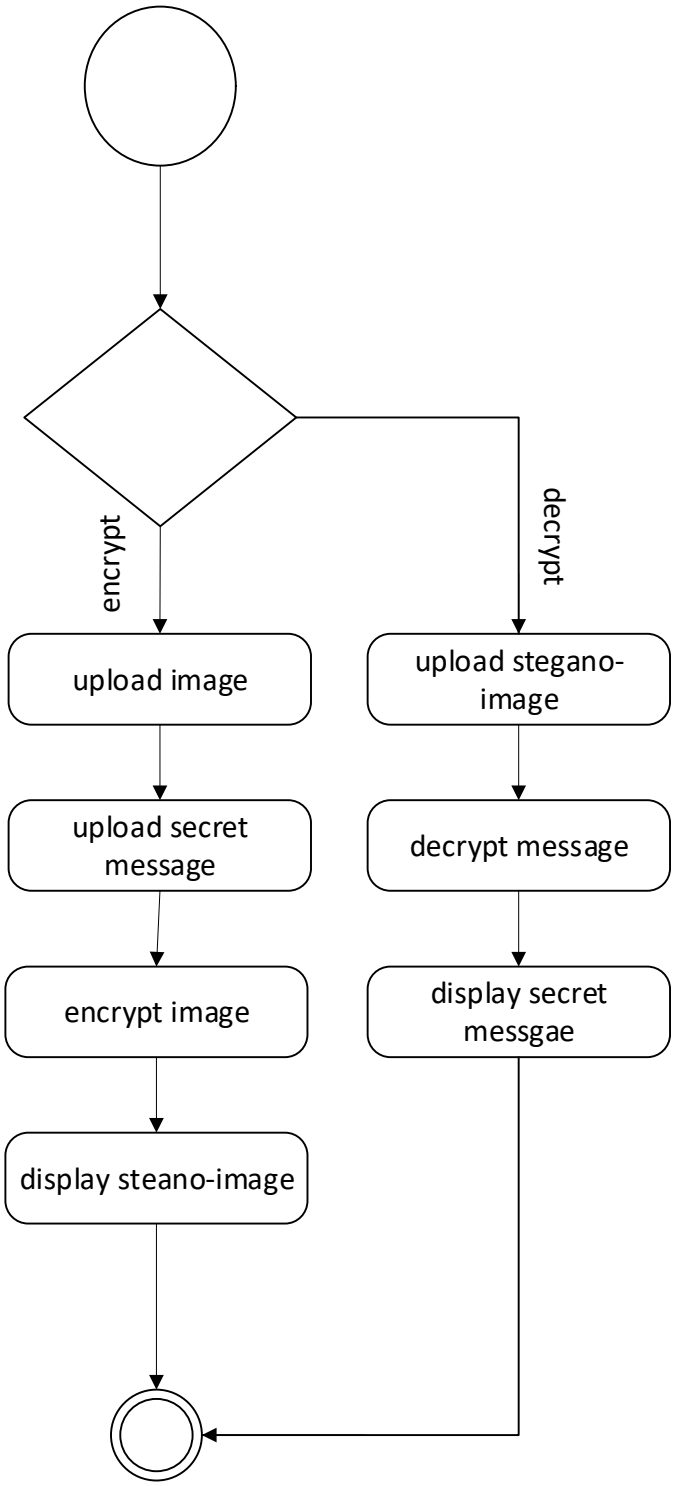

Figure 3.8 Activity diagram of the proposed system.

4. SYSTEM IMPLEMENTATION

In this section we introduce tools employed for the system development. Gradle, an open-source build automation system that builds upon the concepts of Apache Ant and Apache Maven and introduces a Groovy-based domain-specific language (DSL) instead of the XML form used by Apache Maven for declaring the project configuration. Gradle uses a directed acyclic graph ("DAG") to determine the order in which tasks can be run. Gradle was designed for multi-project builds, which can grow to be quite large. It supports incremental builds by intelligently determining which parts of the build tree are up to date; any task dependent only on those parts does not need to be re-executed. GitHub is a web-based hosting service for version control. It is used by several developers around the world to collaborate together on projects and make contributions. GitHub provides support for bug tracking, access control and task management. Developers can do code review and refactoring, contribute to other projects as well as manage different versions of their projects.

Android Studio is the officially integrated development environment for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It provides the fastest tools for building apps on every type of Android so it is most appropriate for this project. Git is a distributed version control system for tracking changes in source code during software development. It is designed for coordinating work among programmers, but it can be used to track changes in any set of files. Its goals include speed, data integrity, and support for distributed, non-linear workflows. LSB method is chosen as the Steganographic mechanism. Java is a general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. The platform for app development in Android is Java. This means that you use the **Java** library and code the applications in Java programming language. The most widely used programming language for android application development is Java.

The Android framework is the set of APIs' that allow developers to quickly and easily write apps for android phones. It consists of tools for designing UIs like buttons, text fields, image panes, and system tools like intents (for starting other apps/activities or opening files), phone controls, media players, etc. It makes it easier to write codes in the android studio and develop scalable android applications.

4.1 System Interface

App Landing Screen Page
A screen is a form of the landing page for the application. It has a simple and easy to use interface. This screen contains the basic menu items of the functionalities of the app.

1. **ENCODE** this button when clicked accepts an image, requests for encoded text and encode the text into the image.
2. **DECODE:** this button when clicked accepts an image, decodes the image and reveals the encoded text.
3. **SEND IMAGE:** this button when clicked shows a popup menu that allows you send the encoded image from the phone gallery via any platform. i.e. WhatsApp, twitter, email etc.

Figure 4.1 Application landing screen

Encode Page

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.

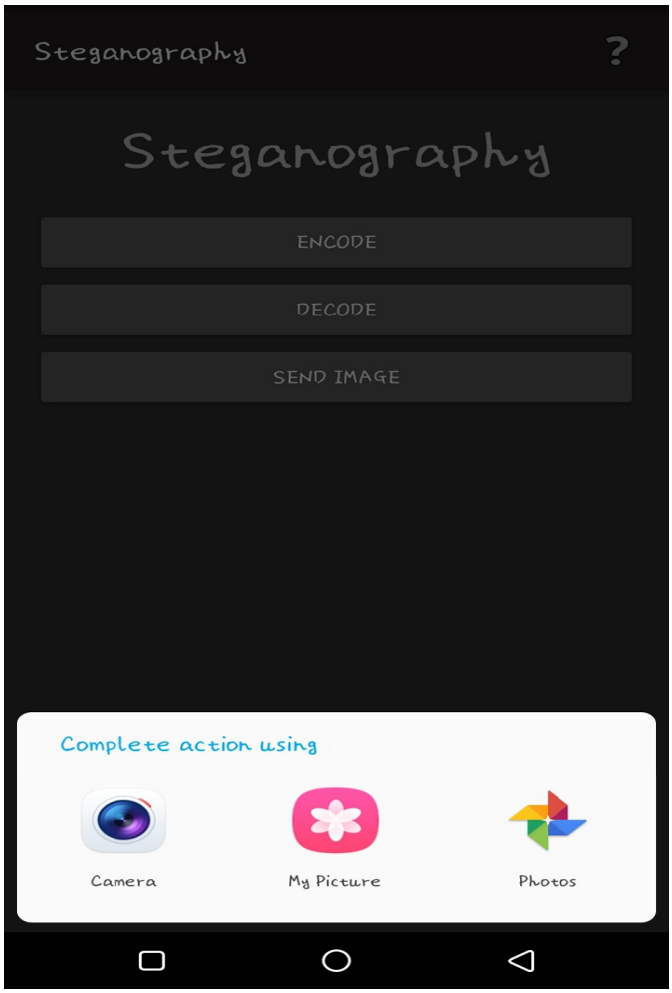

Figure 4.2 Encode screen, image selection pop-menu

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.

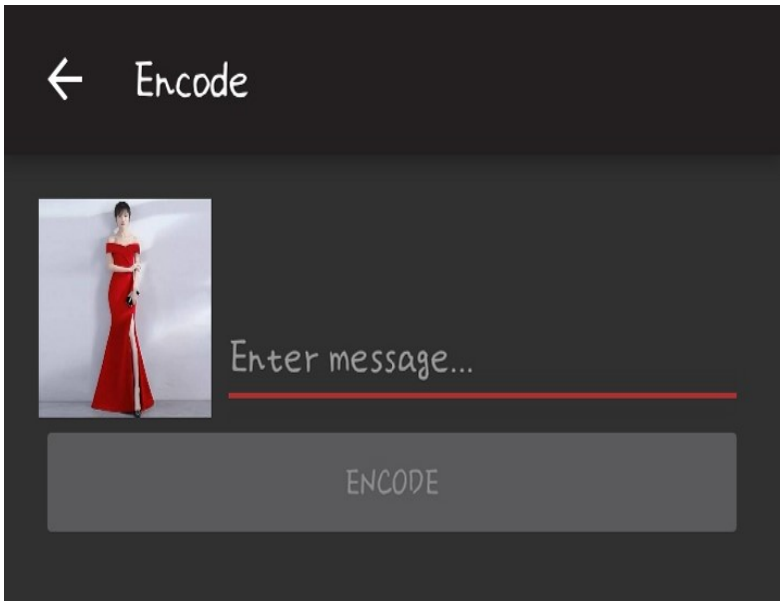

Figure 4.3 Enter message to be encoded screen

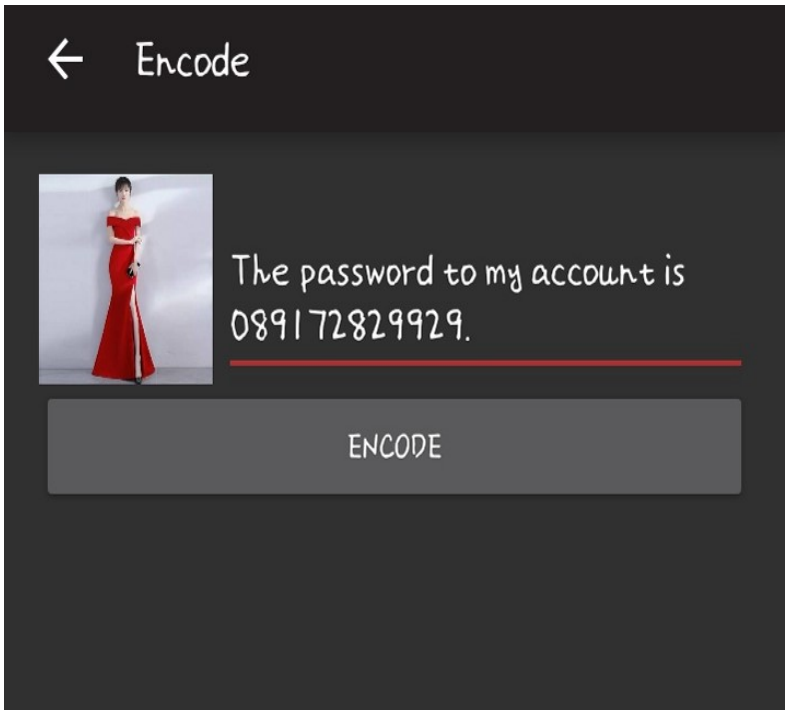

Figure 4.4 Enter message screen, with user secret message

Encoded Image page
After encoding the image, the image is displayed on a new page where it can be saved in a gallery or sent via different social platforms.

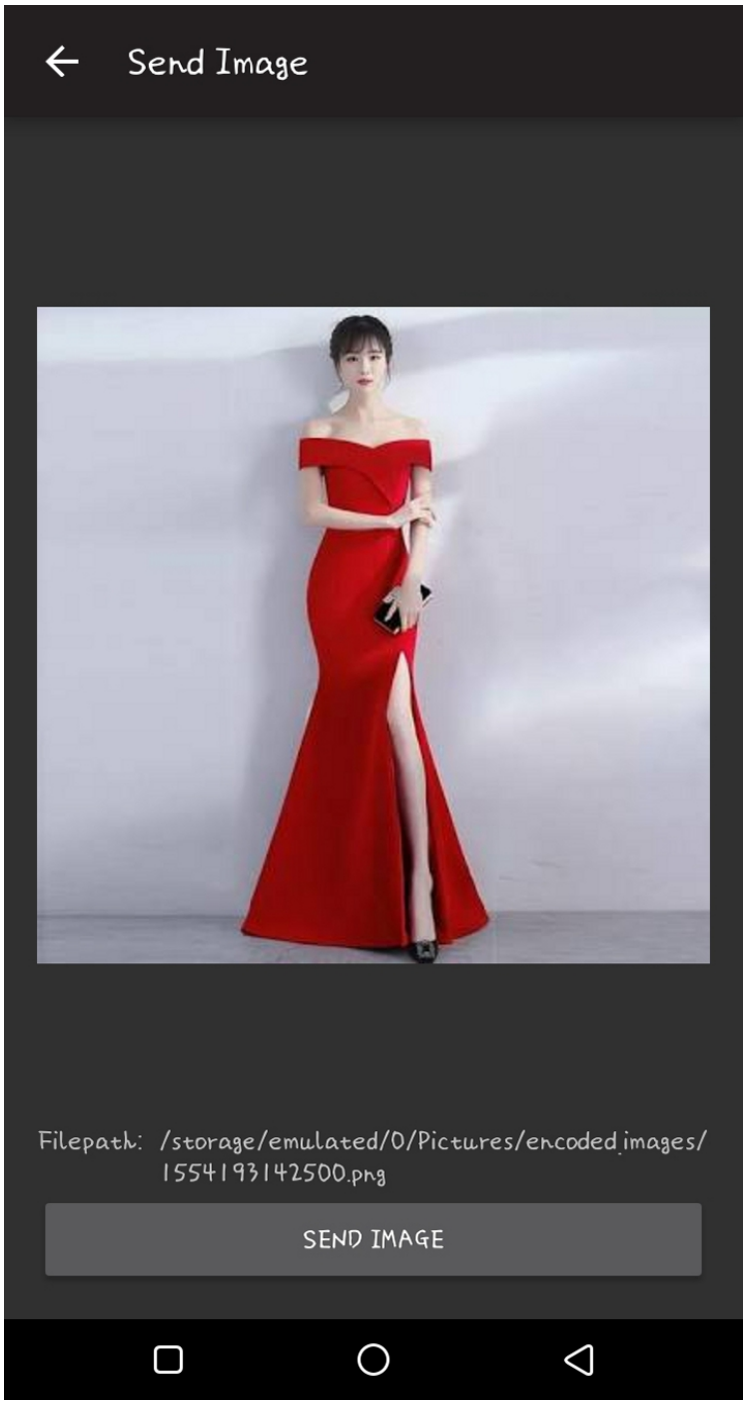

Figure 4.5 Stegano-image, also showing the send button

Decode Page

From this page, 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.

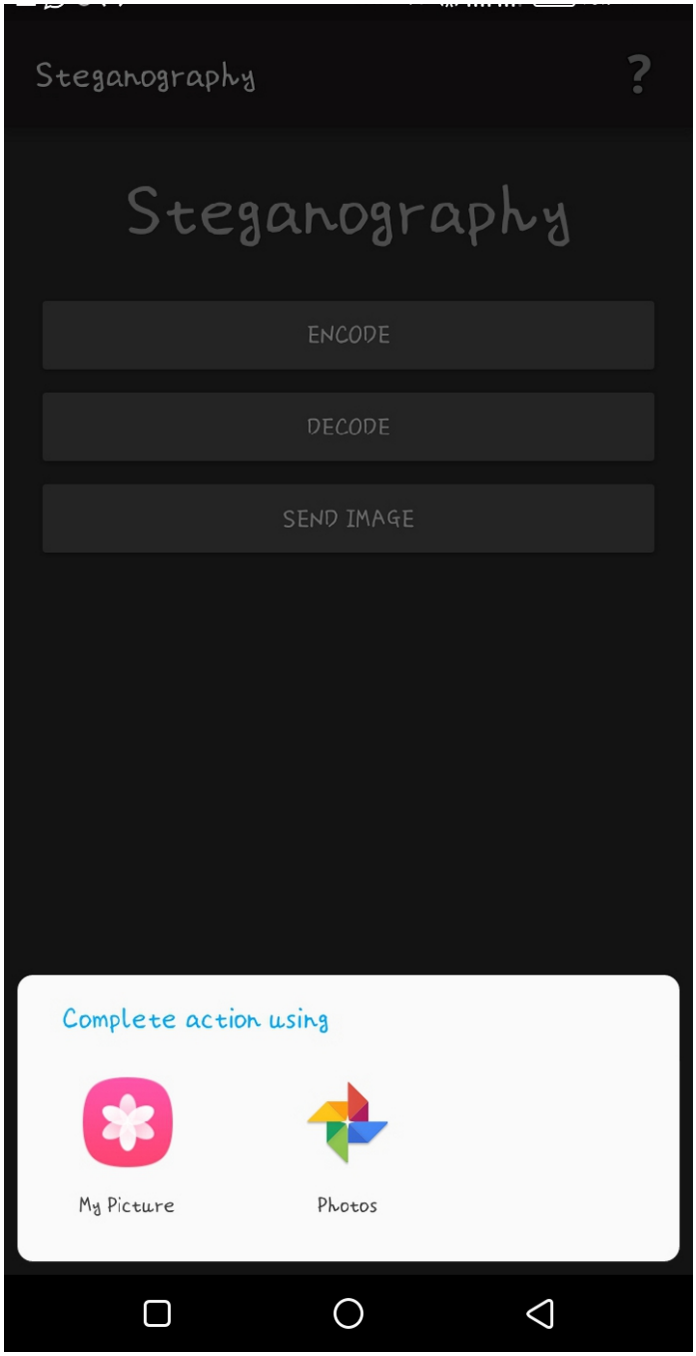

Figure 4.6 Select image pop-menu to decode a message

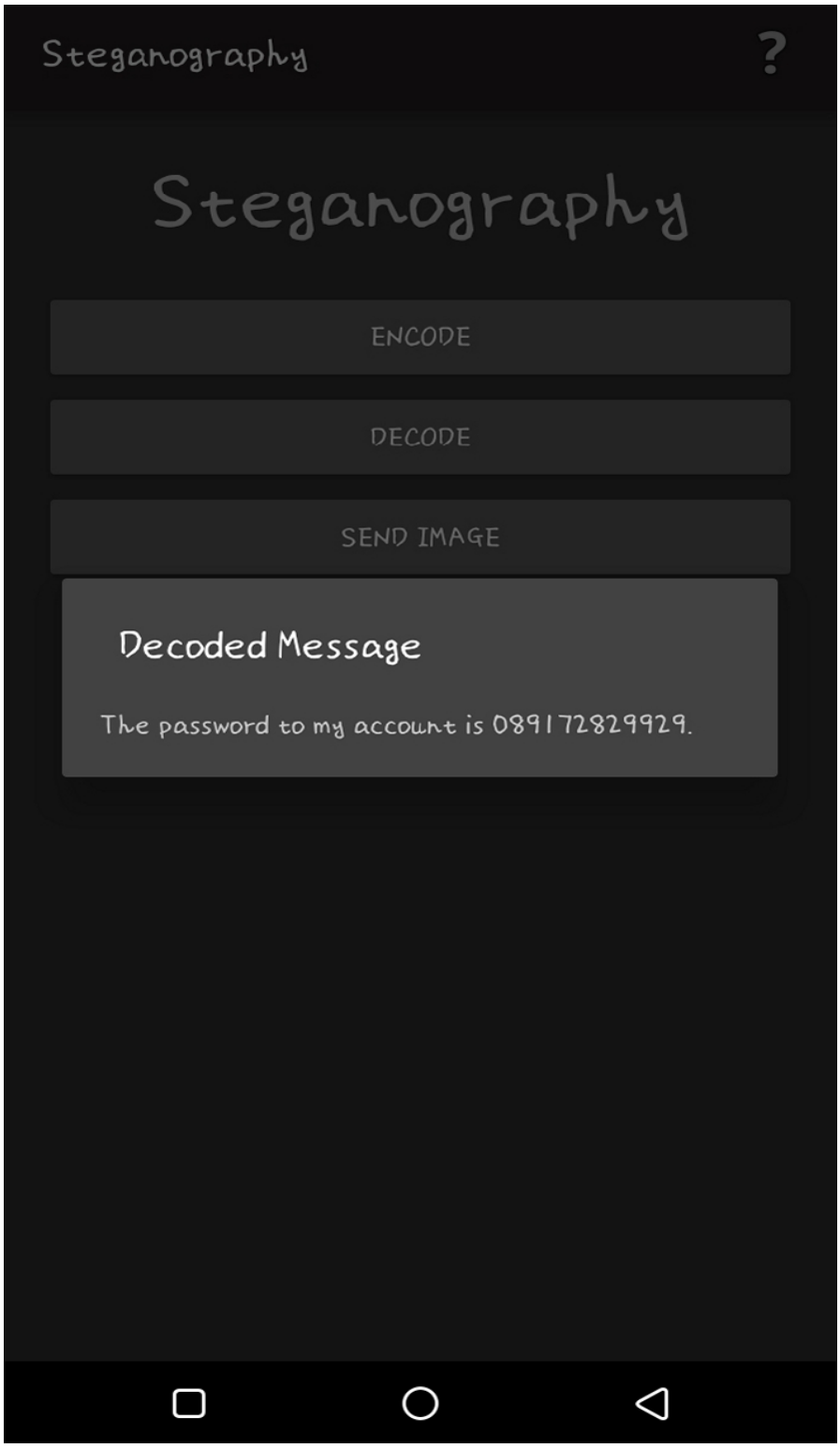

Figure 4.7 A display of the decoded message

4.2 System Testing

The system was tested in two phases, in order to check that it conforms to requirements and it performs all functionalities. The testing done includes Unit and Integration testing. Unit testing also is known as testing in small is the testing of individual components and modules in the system. This is done to ensure that the modules can function independently and without error. For this system, the Encode and the decode components were individually tested for errors and bugs. Different pictures and texts were inputted as test cases in order to detect error or bugs in the system. Integration testing involves testing all the modules together and integrating the components, also called testing as a whole. It checks how the components work and interact with each other. Integration testing tries to find an error in the communication and interaction between modules. For this system, the encoded and decoded modules were tested as a whole system using various test cases.

5. SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

Advancement in information technology and the explosion of social media into mainstream pop culture has led to the overflow of user information on social media, this information is always readily available and transmitted mostly through smartphone devices. People also store and transmit sensitive information through social media, even after the promises and application of a 2-way end to end encryption, user's information are still at risk of being exposed. This system enables users to disguise or mask the presence of information in digital media i.e. images in the context. This information is then transmitted via any means or platform the user wants.

5.2 Conclusion

In conclusion, after careful selection of the best steganography algorithm and proper analysis and assessment of the designed system, the steganography system for android devices was successfully built. It is very robust and could handle a fair amount of data. It also ensures the security of the user's information by making the stegano-image imperceptible to any onlooker. User's information can only be decoded using the application because aside hiding the data, user's data are also encrypted with a key which ensures the message cannot be easily intercepted.

5.3 Recommendation

This system is recommended to anyone that wishes to take up the security challenges and tackle data breaches, to carry out further studies on steganography techniques and algorithms, in order to further develop better algorithms. Users, who are information conscious are implored to use the application to store and transmit information they deem private to them and ensure the security

REFERENCES

1. A. Shaddad, J. C. (2008). 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. (2015). 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. (2012). *Image Steganography Techniques: An Overview.* International Journal of Computer Science and Security.
6. Jagvinder Kaur, s. K. (2011). *Study Of Various Image Stagnography 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. (2000). *Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking.* London: Artech House.
9. Kavita Kavitha, A. K. (2012). Steganography Using Least Signicant Bit Algorithm. *International Journal of Engineering Research and Applications* , 338-341.
10. Laskar, S. A. (2012). 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. (2012). *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. (2006). 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.
16. S. Areepongsa, N. K. (2000). Steganography for low bitrate Wavelet based image coder. *IEEE*, 597-600.
17. Sahoo, R. K. (2012). Some New Methodologies for Image Hiding using Steganographic Techniques. *International Journal of Computer Engineering and Applications*, 7.
18. Samir K Bandyopadhyay, D. B. (2008). *A Review on Steganography.* Kolkata: Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata.
19. T. Morkel, J. E. (2005). *A Review of Image Steganography.* Pretoria: Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria.
20. U.K. Essays. (2018). *Encoding Secret Messages In Text Information Technology Essay.* London: U.K. Essays.