International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 01-04 www.ijaem.net ISSN: 2395-5252

"Android Based Image Steganography"

Shubhangi Kuhikar, Pooja Bhaisare, Priyanka Somankar, Achal Landekar, Prashant Khetade.

Date of Submission: 25-12-2023 Date of Acceptance: 05-01-2024

ABSTRACT
Basically, Image Steganography is the process of hiding information which can be text, images or video inside the cover image. Android based Image Steganography is a simple android application that implements steganography concepts. In this project Image Steganography is used so that text-messages can be hidden securely in an image. Here, the sender is uploading an image which hide the secret message. Sender should upload image, add a secret message and a secret key in order to encode the message and hide it in the image. Receiver can decode the message with secrete key shared by sender. The main advantage of steganography algorithms is because of its simple security mechanism. The project is good in secreting communication and in effective information hiding while maintaining Authentication and Confidentiality.. The main aim of developing this application is to facilitate secure secrete communication without generating curiosity. Proper and effective use of steganography can prove to be one of the best solutions for information hiding, Authentication and Confidentiality

Keywords: Steganography, Upload Image, Encoding, Decoding, Secret Message, Secret Key, Encryption technology, Android Application.

I. INTRODUCTION

Android-based image steganography is a method of hiding information within images on devices running the Android operating system. Android-based image steganography involves concealing information within images on Android devices. Theimportant concept of cyberspace is maintaining confidentiality. Here comes the importance of hiding information. Image Steganography is the concept of hiding a secret file within another non secret and normal-looking image. Steganography is veryuseful concept for maintaining the security principles like authentication and confidentiality. Our Android Based Image Steganography is a simple android system that implements the steganography concept. In this project, Image Steganography is used so that a text message can be hidden securely in a cover image. The system is good in secreting communication and in effective information hidingwhile maintaining authentication and Confidentiality. Our Android Based Image Steganography project comprises 2 modules:1) Encoding 2) Decoding. The users will have access to encode as well as decode secrete messages. The user would require registering first to Login. Users need to enter Username and Password to Login for registration. After registration User Id will generate automatically by the system. After that user can Login into the system. Users can add the process list byuploading the image, entering the text message and the secret key.

II. METHODOLOGY

Android-based image steganography involves hiding secret information within an image in such a way that it is difficult to detect. Here is a general methodology for implementing steganography on the Android platform.

Software and Hardware Requirements:

The software and hardware requirements for developing and running an Android-based image steganography application can vary based on your specific implementation and the features you plan to incorporate.

Cloud hosting is used so that no database is used to integrate the system.

1 Development Environment: - Android Studio,the official IDE for Android app development.
2. Java Development Kit (JDK): Android apps are typically written in Java.
3. Programming Languages: - Java
4.Frontend: - XML for Android layout files.
5.Backend: - MSSQL

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 01-04 www.ijaem.net ISSN: 2395-5252

In this project, an android application is developed using Android Studio Software. In this android app, options like Encoding and Decoding the data are provided.

This can be done by hiding the data behind an image. Images in the application can be used by dual options either by mobile gallery or by mobile camera.

Besides, we are also going to add an extra feature which is login id and password to both the sender and the receiver.

In this android app, the User interface (UI) will have a Register option in which the user must enter the Login Id or Name and Password.

When a user opens the app, user will get to sign up or if already registered then directly sign in.

Once the user has signed in, the user will get the next interface in which will get options like encode, decode.

After selecting the Encode option, image can be selected from the camera and then, the user is provided a Text Box for writing the secret text message to be encoded with the image using AES algorithm converting into Stego image. and after user will need to enter the secret key.After this user can send the stego image to its intended person.

On the receiver side, by selecting the Decode option, it can select the Stego image file and then by entering the secret key provided by the sender, secret message can be decoded easily.

SYSTEM ARCHITECTURE

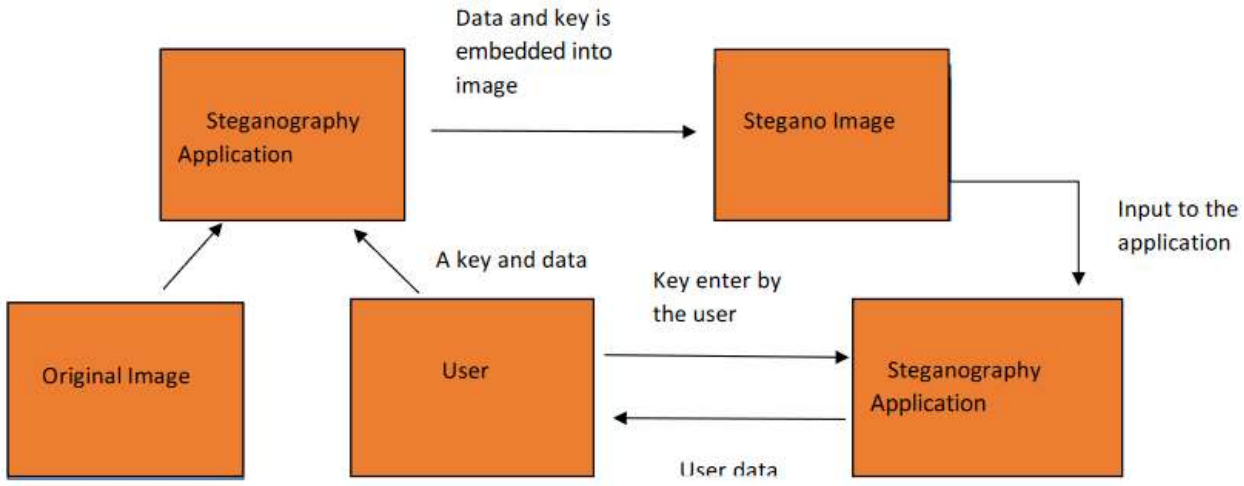


Figure:- Architecture Diagram

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 01-04 www.ijaem.net ISSN: 2395-5252

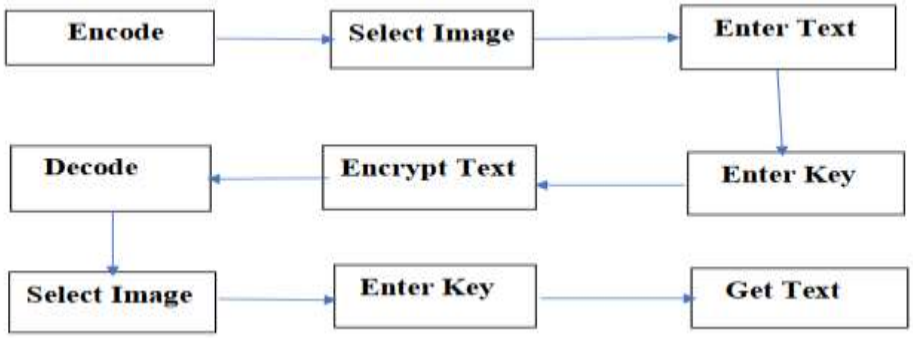


Figure: -Flow Diagram

III. TEST AND RESULTS

Test and Result

Testing an Android-based image steganography application involves various aspects, including functionality, security, performance, and user experience. Below is a broad outline of test scenarios and expected results as below screenshots from actual application.

1. Functional Testing:

Image Selection:

Test Scenario: User can select an image as a cover.

Expected Result: Selected image is loaded and displayed correctly.

Steps for this testing as below:

Step 1: The user opens the application and enters their email address and password. If this is their first time using it, they can register first and then log in.

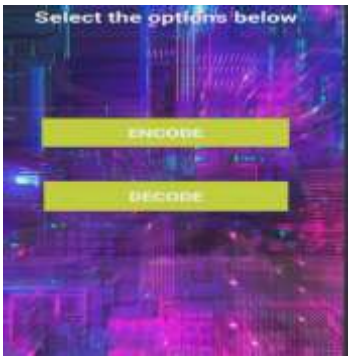
Step 2: The user must choose the encoding after providing his or her credentials.

Step 3: After choosing the encoding, the user must choose the image in which the message is to be hidden by clicking on the selected image button. Enter the secret key created during the registration and hide the image, along with the username, for the reference once it has been selected. After click on the encode button and save the image.

Input:Contacts us for more details

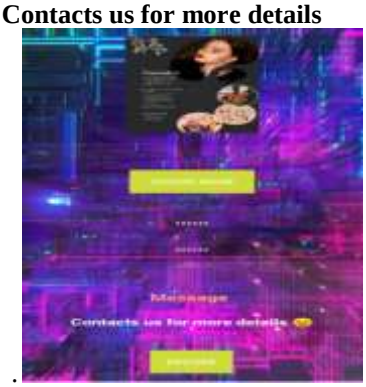
Step 4: After saving the image, return to the application's main screen and click the decoding button.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 01-04 www.ijaem.net ISSN: 2395-5252



Step 5: After selecting the decode button, the user must select the same image to add the hidden massage, secret key, and username, and click the decode button to view the hidden massage.

Output:Contacts us for more details



Data Hiding:
Test Scenario: User can hide data within the selected image.
Expected Result: Data is successfully hidden, and the resulting image maintains reasonablequality.
Data Extraction: Test Scenario: User can extract hidden data from a stenographic image.
Expected Result: Hidden data is accurately extracted.

IV. CONCLUSION

In conclusion, Image Steganography application software provided for the purpose, how to use embed message into image. It can be extended to a level such that it can be used for the different types of images formats like bmp, jpeg, .tiff etc. So other image formats can also be used in steganography. Proper and Effective use of steganography can prove to be one of the best solutions for hiding information, confidentiality and authentication.

REFERENCES

[1]. Parag Himatlal Rughani (2016) "Steganography on Android Based Smart Phone" International Journal of Mobile & Adhoc Network Volume 02 issue 2|May 2016
[2]. Pawan Sharma, Srishanth Shetty,Om Kadam, Prof.Ritu Sharma (2018) "Android Based Image Steganography" International Journal of Creative Research Thoughs (IJCRT)ISSN: 2320-2882 Volume 6, Issue 2 April 2018
[3]. Anjana Menon (2020) "Android Image Steganography" International Journal of Interdisciplinary Innovative Research &Development (IJIIRD) SSN: 2456-236X Volume 05 Issue 01 | 2020
[4]. Dr.K.Jayasakthi velmurugan, S,Daniel Visuvasam, Akash K (2022) "Android Application for Image Steganography using Android Studio" International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue V May 2022.
[5]. C. K. Chan, L. M. Cheng, "Hiding data in image by simple LSB substitution", pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.
[6]. R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al
[7]. Thanikkal, J. G., Danish, M., & Sarwar, S. A. (October 2014) New Android Based Steganography Application for Smartphone's. Journal of Basic and Applied Engineering Research. Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 8; pp. 32-35.
[8]. Savithri G, K.L.Sudha.(July 2014). Android Application for Secret Image Transmission and Reception Using Chaotic Steganography. International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 7,
[9]. Bucerzan, D., Raţiu, C., & Manolescu, M. J. (2013). SmartSteg: A New Android Based Steganography Application. International Journal of Computers, Communications & Control, 8(5).