Stego App: Android based Image Steganography Application using LSB Algorithm

Azmat Ullah[1], Mohsin Ijaz[2]

University of Sargodha Mandi Bahauddin Campus, Punjab 50400, Pakistan
Department of Computer Science & Information Technology

Abstract: – *Communication technology is developing much faster than any other thing in this world with greater uses of handheld smartphone devices. Smartphones are the big sources of communication for sharing pictures, videos and documents etc. But secrecy and successful transmission of secret information or data remains on risk. Hence there is high need to secure the data from unauthorized viewing and to keep secrecy while transferring the data.*

*We have developed a **Stego App** application for android platform that is able to hide secret text and secret image into the cover image efficiently. Images in the format of JPEG, PNG and BMP can be used in this application as a cover image and secret image. If image of any type use as a cover image then this application will keeps the image type same as the original after hiding text and image in it. LSB algorithm of steganography is used to hide text and image into cover image. And to protect stego image from unauthorized access in case of when specification of algorithm revealed, this application allow user to set password on stego image.*

***Key Words*: Least significant bit algorithm, Stego App, Android, Secret text message, Secret image, LSB.**

1. INTRODUCTION

Now-a-days smart phones have become a very important part of every person in this world because they serve human being in variety of ways. They provide reliable and efficient functionality like desktop or laptop computers. As technology grows, smaller in size and performance enrich smartphones have been developed. Technology makes easier and cheaper the access, processing and storing and transmitting of information from one place to another place. Due to this untrusty and continuously evolving environment, demanding need to secure data, information and communication is an important subject of study and research for researchers [1].

Two techniques cryptography and steganography are used to guarantee that user's confidential and important data/messages will be safe. Cryptography is method of storing and transmitting data in particular form so that only those for whom it is intended can read and use it. But due to generated cipher text, one can tell message has been encrypted [2]. And attacker try to recover secret message by performing a series of attack on cipher text. And if attacker couldn't succeed, then might be possible that during attack encrypted secret message will be destroy. Steganography is an art of covering secret and confidential information within a carrier which could be an image file. This technique provide an invisible form of communication since an image file which has the secret information embedded within it is delivered to receiver instead of secret information itself. It hide the existence of secret message, only the sender and receiver can suspect the existence of secret information [3]. To use cryptography and steganography are advantageous, but both techniques have few limitations. In this paper we propose an android based application named as **"Stego App"**, which encodes secret message into an image in such a way that quality of cover image will not be affected and secret message is protected in cover image by applying password on it and encoded image can be transmitted to any communication medium i.e. the Gmail, WhatsApp, Facebook, and Bluetooth etc. In this proposed android application, user not only can hide the secret message into an image file but can also hide important image into cover image file without changing the cover image type.

2. WHY TO CHOOSE ANDROID?

Android is a mobile operating system developed by Google, designed primarily for touchscreen mobile devices such as smartphone and tablets. Number of android smartphones devices is greater than any other smartphones devices. Android is much more powerful and it is widely accepted by many handset manufacturers around the world than any other operating system i.e. Apple iOS and BlackBerry etc. [4]. Android OS is used by mobile phones manufacturers as describe in Table 1

Table-1: Worldwide Smartphones Sales Worldwide smartphones sales in the fourth quarter of 2016. (Thousands of units.) Source: Gartner [5].

Operating System	4Q16 Units	4Q16 Market Share (%)	4Q15 Units	4Q15 Market Share (%)
Android	352,669.9	81.7	325,394.4	80.7
iOS	77,038.9	17.9	71,525.9	17.7
Windows	1,092.2	0.3	4395.0	1.1
BlackBerry	207.9	0.0	906.9	0.2
Other OS	530.4	0.1	887.3	0.2
Total	**431,539.3**	**100.0**	**403,109.4**	**100.0**

As described above Android is very popular operating system. Study shows that approximately 432 million smart devices sold in fourth quarter 2016, 352 million ran Android operating system (81.7 percent) and 77 million smart devices ran iOS (17.9 percent) [5]. So it is clear that Android is number one than others. Android is java based and have a huge set of API that can be used for multiple purposes. And android has API related to multimedia and images [6]. By considering all above factor Android seems the best option for developing such application which serves great number of peoples for their secret communication or for transmitting of secret text and secret image from one place to other or from one user to other user.

3. RELATED WORK

Image steganography is very interesting and important technique which attracts many researcher to perform research on it to find and suggest new and better solution to make important information more secure, and developers to make dreams of researcher true by developing useful applications and tools for desktop computer and smart phones. For Android smartphones, there are few projects regarding image steganography. They are described below.

Android application developed by White and Martina that allow user to hide short text message in an audio message that is recorded by user and then user can send this message to anybody [7] and [1].

Another Android based application is MobiStego using steganography algorithm, that only hide message into an image. But MobiStego hide only text message in image [8].

MoBiSiS is an Android application that enables the user to send the image which contain secret message through Multimedia Messaging Services (MMS). But this application has a limitation that the size of the cover image with the secret message embedded in it, must be less than 30 KB [9]. If image is larger than 10 KB then this application compress the image and send it. This application hide short text message in image. Another application is PixelKnot available on the internet which only hide message into image using F5 algorithm but this application takes too much processing time and only use to encode message into image [10] and [11]. SmartSteg is based on steganography and cryptography. This application is also android based that access the original image stored in device storage rather than using its copy in order to avoid damaging the dimension of cover image. Because by using the copy of original image, image type will be change in (.png) no matter the type of original image. SmartSteg encrypt the message first then hide it in image [1]. But we are not agree with idea of SmartSteg application. Copy of original image works as same as the original image. And almost all applications that require access to images are using the copy of original image for their purposes, to avoid damaging the original image. And it is possible to set the image type same as original image type after hiding text in image. On the basis of these issues we are developing an android based application that not only hide text into cover image but also hide image into cover image. This application will set the same image type of cover image after hiding text or image in it.

4. PROPOSED WORK

Most of applications are develop used to only hide text message into an image which must be smaller in size, not more than few words. These applications don't hide the image into cover image. And these applications change the original image type into other type e.g. if image have jpg extension, these applications will convert it into other data type e.g. png extension after hiding text message in it. Our proposed application works on Android smartphones. Proposed application can hide long text message up to 100 words into cover image and also can hide image with the size of 7KB into cover image and then same application will be used to recover the image or text message hidden in cover image. To hide the text message and image into cover image, we are using Least Significant Bit (LSB) algorithm. LSB algorithm adjust the least significant bit of cover image. Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, last bit which is 8th bit in byte of image is changed to the bit of secret message. For 24 bit image, the colors of each component i.e. RGB (red, green and blue) are changed. Image is made up of multiple pixels and each pixel made up of string of bits. For hiding text message or image in an image algorithm convert text message and image into bits then store these bits in an array. LSB replace the last bit of the cover image with the bit of information we are hiding either image or text as a secret. This algorithm replace the last bit of the cover image with the bit of text message or image to be encoded, which means the 8th number bit of each byte of the cover image become the bit of the secret text message or image.

To resolve the extension issue and to keep the extension of cover image and stego image same, proposed application get the complete path from cover image then split this path into slash. To get extension from image path we use the method named as **LastIndexOf**, which find the position of dot (.) in image path and extension that comes right after the dot will be temporary store in a variable. Then that variable will concatenate with the dot of stego image. Hence both cover image and after encoding the stego image will have same extension. Cover and stego images that become suspicious because of their extension, this technique will reduces these kind of chances. Password is used to protect the secret text message and secret image which user hide in the cover image. Bits of password will be hidden in the same way in the cover image as the bits of secret text message and image are store in the cover image. To keep secrets text message and secret image safe we use the method of android that provide services of **Hidesoftinputfrom** which protect the password by revealing during any kind of attack on cover image.

Proposed application can successfully encode secret or important image into the cover image. Hiding/encoding secret image is beneficial, when user want to covertly send important image from one place to other using internet, without anybody intention or want to keep important image safe from other.

To hide text message and image into the cover image,

Stego App follow these steps.

- Cover image, secret data (text or image) and password needed to be loaded into the application.
- In case of secret text message, Stego App first extract the bits of cover image, password and input text message. After this application will replace the last bit of cover image with each and every bit of password and secret text.
- In case of secret image, Stego App compare the size of input secret image with the cover image. If image size is smaller than the cover image than it can be easily hide in cover image. If size of input secret image is greater than the cover image, then application show the message to user to select image which must be smaller in size than the cover image. When user add secret image which is smaller in size than the cover image then application extract the bits of cover image and secret image. Then LSB algorithm replace the last bit of every byte of cover image with secret image.
- After embedding data (text or image) into the cover image successfully, application allow its user to easily share the image instantly via any communicating application installed in user smartphone device, to whom it concern or to save that image into gallery by pressing the save button in the application.

Application encode and decode secret text message and image into and from the cover image.

To encode text message and image into cover image, user need to first load cover image into application.

After this user can add password in password field of application if user want it. Then user can write text message in text area to encode/hide it in the cover image. If user want to hide image into cover image then user can add image from gallery into application and by pressing encode button text message and image will be successfully encode into cover image.

Remember that only one secret either text message or image can be encoded into cover image at a time.

For decoding stego or encoded image will need to be loaded in the application then by pressing decode button encoded secret text message or image will be display to user.

Below is the figure (Fig-1) of application flowchart that describe how Stego App works:

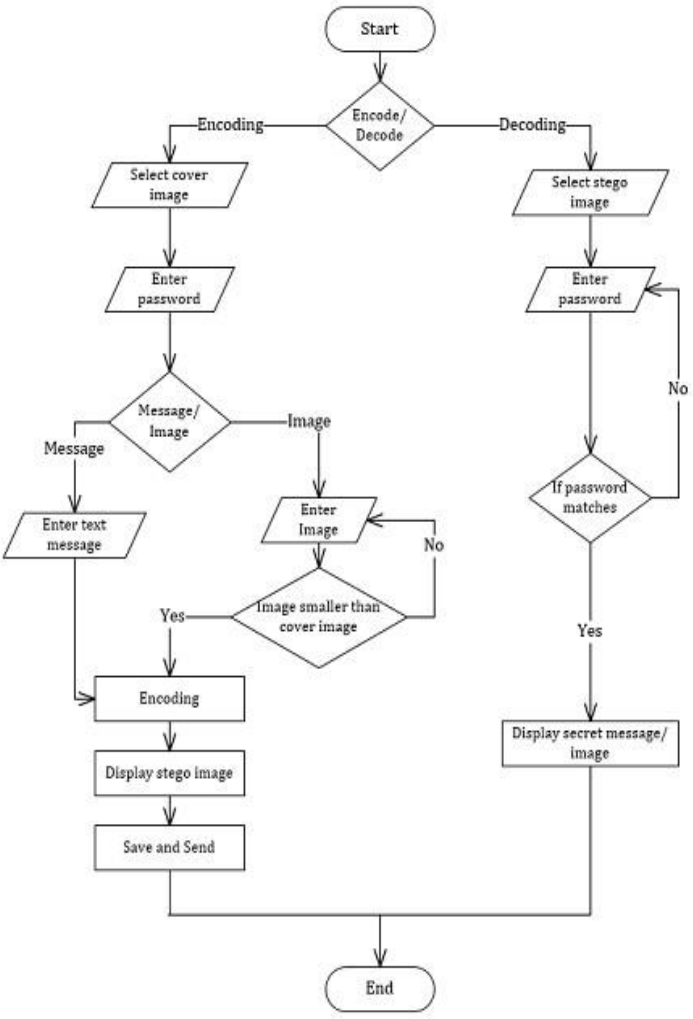

Fig-1: Flowchart of Stego App

5. DESIGN AND IMPLEMENTATION

The IDE and smartphones are used to develop and test this application are describe below:

- Android Studio application development tool used to develop the application.
- Huawei and Oppo Android smartphones with 7.0 and 5.0 version are used to test the application.

The cover image following characteristics is used for encoding:

- JPEG, PNG type.
- Size: up to 7MB.

The characteristics of secret data (text, image).

- Text: approximately 100 words.
- Image size: 7KB.

Fig-2: Cover image: Original image and with secret text message and image embedded.

6. CONCLUSION AND FUTURE WORK

Image steganography allows two individuals to communicate privately. We have develop an android application using this technique to securely send secret image and text message by hiding them in image without worrying about man-in-the-middle attack by protecting image with password. This provide security from attacker. We use LSB algorithm that is efficient algorithm in Stego App. Image of JPEG, BMP and PNG type can be used in our application as cover image and as an input secret image. This application didn't change the type of original image after hiding secret information in it.

Advantage of proposed model:

- Execution time is fast.
- Information hidden in cover image cannot be detected from steganalysis attack.
- Hide large size of text in cover image.
- Hide smaller image into larger cover image.
- Sender can protect secret information in image by setting password on cover image.
- Woks on all version of android operating system.

Application run successfully and perform it's require functionality.

Future work of our research is to develop new version of Stego App that works on Apple operating system.

And enable the application to hide MB dimension of image in cover image.

7. REFERENCE

1) SmartSteg: A New Android Based Steganography Application.

2) https://www.clear.rice.edu/elec301/Projects01/steganosaurus/background.html.

3) Data Security Using Image Steganography And Weighing Its Techniques.

4) International Journal of Mobile & Adhoc Network|Vol2|issue 2|May 2012 150 Steganography on Android Based Smart Phones.

5) https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016.

6) https://developer.android.com/reference/android/media/Image.html.

7) T. F. M. White, J. E. Martina, Mobile Steganography Embedder, 11 SBSeg Simposio Brasileiro Em Seguranca Da Informacao E De Sistemas Computacionais, Bsalia-DF, 6 a 11de Novembro de 2011.

8) MobiStego:http://play.google.com/store/apps/details?id=it.mobistego, visited on 04.06.2018.

9) I.Rosziati, L. C. Kee, MoBiSiS: An Android-based Application for Sending Stego Image through MMS, ICCGI 2012: The Seventh International Multi Conference on Computing in the Global Information Technology, 115–120, 2012.

10) Google play.

11) Android-Based Digital Image Steganography and Steganalysis.

BIOGRAPHIES

Azmat Ullah. Graduated in Engineering from University of Sargodha Mandi-Bahauddin Campus. He write a research paper and also working on other research article, "How to improve Waterfall model".

Mohsin Ijaz. Graduated in Software Engineering from University of Sargodha Mandi- Bahauddin Campus. He write a research paper and also working on other research article, "How to improve Waterfall model" with primary author.