iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4187

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Android Based Steganography Using Navigation

Ammar Mukadam[1], Danish Shaikh[2], Waleed Parkar[3], Tauheed Maniar[4], Prof. Dinesh Deore[5]
[1,2,3,4]*Department of Computer, Engineering Rizvi College of Engineering, Mumbai, India*
[5]*Associate Professor, Department of Computer Engineering Mumbai, India*

Abstract - In today's world of technology, Data security is essential. In many organizations information is critical. One of the ways to ensure security is by ensuring that the data is not visible to the intruder. This can be done by hiding the message behind some other objects. Here we achieve data security through the technique of Watermarking, also known as, Steganography. An algorithm for image Steganography has been proposed to hide a large amount of confidential data presented by secret color image. This algorithm is based on least significant bits (LSB), a technique used to hide data behind an image. An extra layer of security is added to the above algorithm where in-built technology of android, i.e. GPS is used so that the file can only be decrypted at specific location.

Keywords – Steganography, Least Significant Bit (LSB)

I. INTRODUCTION

Secured Transmission of data from one place to another is biggest challenges in communication. Various methods are available for providing security. One of the best methods is steganography. Steganography is a technique of hiding messages in other files for secured transmission in a manner that an intruder could not identify the confidential data inside the transmitted file. It includes various techniques for secret communications. The growing possibilities of the modern communications need the special security on computer network system. The network security is becoming more important because nowadays the number of data being exchanged on the Internet increases. Therefore, the important and confidential data are required to protect against unauthorized access and use.

The purpose of steganography is covert communication to hide a message from unauthorized users. Although messages embedded into an image are imperceptible to the human eye, they often disturb the statistical nature of an image. The choice of the cover image is very important in steganography as it influences the security of the technique in a huge way. Some steganographic experts recommend grayscale images as the best to use as cover images.

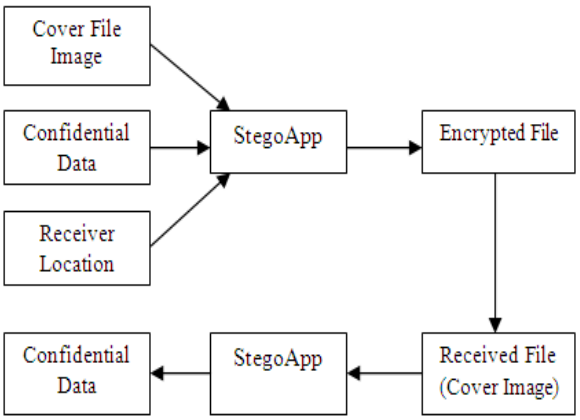


Figure1.1: Steganography Process

Images are the most popular medium for hiding data. The more detailed an image is, the fewer constraints there are on how much data it can hide before it becomes suspect.

II. PROPOSED METHODOLOGY

Considering the existing system, Steganography, which is implemented using LSB, is worldwide known algorithm and hence sending confidential data using LSB is not completely secure and so we are adding another layer of security over LSB using inbuilt GPS android module.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The sender encrypts the confidential data according to the location of the receiver and hides the encrypted data behind an image using Steganography(LSB), so that receiver can decrypt the data only at the specified location.

III. TECHNIQUE USED

A. *Least Significant Bit*

Sometimes abbreviated as LSB, the least significant bit insertion is a simple approach to embedding information in image file. This simplest Steganography technique embeds the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the LSB does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity of an algorithm can be increased by using two or more least significant bits. At the same time, the image fidelity degrades and the risk of making the embedded message statistically detectable increase. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding depends on the local characteristics of the pixel. The advantage of LSB-based method is that it is easy to implement and high message pay-load.

Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity and awareness of the technique. Therefore, intruders can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret/confidential information that was embedded in the image.

Therefore, a system named *Secure Information Hiding System (SIHS)* is proposed to improve and advance the LSB scheme. It overcomes the sequence-mapping problem by embedding the message into a set of random pixels, which are randomly distributed on the cover-image.

B. *GPS (Global Positioning System)*

Android devices are equipped with GPS hardware and provide a very straight forward API to access Location information using LOCATION MANAGER derived from GPS hardware along with Wi-Fi and Cellular network that helps provide location information. These API needs to get the users permission for the application to access this service.

In our App sender needs to input the confidential data along with receiver's location (latitude & longitude values) so that the data is encrypted using receiver's location as key and hide it behind the image using Steganography. On receiver's side our app internally gets the location (latitude & longitude values) and if receiver is on the specified location then our app decrypts the data hidden behind the image using receiver's location (latitude & longitude values) as key.

IV. DESIGN OF EXISTING SYSTEM

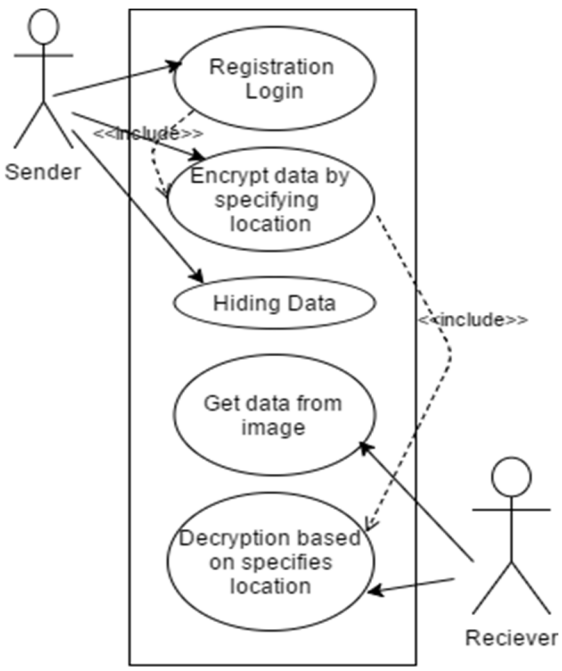


Fig. 4.1: Use case diagram of Steganography process based on navigation

V. FEATURES OF THE PROJECT

A. Sender Activities

1) *Registration/Login:* Sender register himself using his credentials and sets username & Password. Then sender will LOGIN into our android app using his username & password.
2) *Encrypt message:* Sender will input the confidential data and location (Latitude & Longitude values) of receiver. This will encrypt the confidential data using receiver's location (Latitude & Longitude values) as key.

Latitude is distance north or south of the equator (an imaginary circle around the Earth halfway between the North Pole and the South Pole) and longitude is distance east or west of the prime meridian (an imaginary line running from north to south through Greenwich, England).

3) *Steganography:* Sender then hides the encrypted data behind an image using Steganography and sends the image to receiver.

B. Receiver Activities

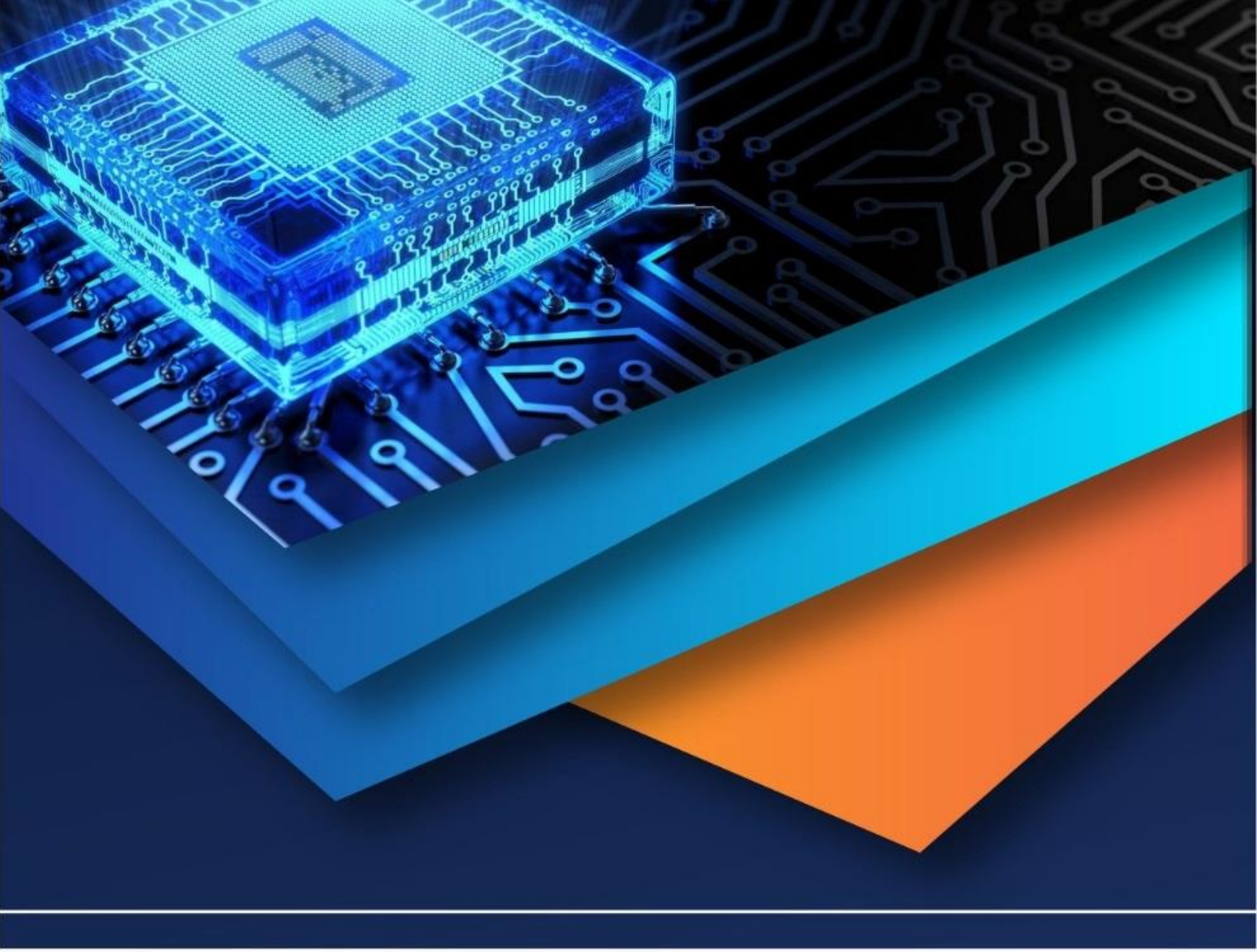
1) *Registration/Login:* Receiver register himself using his credentials and sets username & Password. Then receiver will LOGIN into our android app using his username & password.
2) *Selecting and Loading received image:* Receiver will then select and load the image in our app using android file chooser. After loading the image, our application will then try to locate the receiver's location using GPS.
3) *Based on location message will be visible:* If receiver is on the location specified by sender, receiver will be able to view the confidential data.

VI. CONCLUSION

The target of this paper is to add another layer of security to steganography. Implementation of the system will result in complete security of confidential information where the sender will hide the data behind an image and provide a location only where the data will be accessible to the receiver. This can help many organizations to share their confidential information to the legitimate user in a very secure manner. The main intention of the project is to develop an application that provides high security. The proposed approach provides higher security than other existing systems as receiver can only access data from specific location. So, it is very difficult for unauthorized personnel to access data.

REFERENCES

[1] Steganography Based Navigation of Missile- Volume 4, Issue 6, June 2015 International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
[2] A new hybrid encryption and steganography technique: a survey- Vol 3(14) ISSN (Print): 2394-5443 ISSN (Online): 23947454http://dx.doi.org/10.19101/IJATEE.2016.314005 International Journal of Advanced Technology and Engineering Exploration
[3] Comparative study of Edge Based LSB Matching Steganography for Color Images- Volume: 06, Issue: 03, ICTACT Journal on Image and Video Processing, February 2016



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY