IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 12, PP 31-33

Secure Steganography Using Geo-Fence

Abhishek Galinde[1],Ishwar Suryawanshi[2],Pritesh Sisale[3],Shweta Sharma[4]
[1,2,3](Student, Computer Engineering, Atharva College of Engineering/ Mumbai University, India)
[4](Professor, Computer Engineering, Atharva College of Engineering/ Mumbai University, India)

***Abstract**: This paper is based on a new steganography application to hide the secret message behind the image with the help of Geo-Fence technique. This application is design to share secret message/information behind the image and that image is stenograph along with the Geo-Coordinates. This purposed system provide an image platform for the user to input image and a text box to insert a secret message. The system encrypt the secret message and image file with geo-coordinates of receiver using modified LSB technique. Once the process is done user can send the stego image to receiver using same application. At the time of retrieving stego file its checks the geo coordinates using in built technology of android i.e GPS so that the file can only be decrypted at particular location.*

***Keywords** – Least Significant Bit (LSB), Steganography, Stego file, Geo-fence.*

I. Introduction

In today's world of technology data security is very necessary. Secured transmission of data from one location to another is biggest challenges in communication. In most of the organizations information is critical. Different methods are available for providing security. 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 image using steganography and that message retrieve at particular location using geo-fence.

Steganography is a technique of hiding messages in other files for secured transmission in a manner that an intruder could not identify the secret data inside the transmitted file. Steganography works by replacing bits of useless or unused data in image files with bits of different information. Steganography differs from cryptography in a way that it masks the existence of the message where cryptography works to mask the content of the message.

Least Significant Bit (LSB) insertion is most widely known algorithm for steganography. it involves the modification of LSB layer of image. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise. Thus, altering them does not have any obvious effect to the image.

Geo-fencing uses the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries. Geo-fencing is paired with a hardware/software application that responds to the boundary with same parameters. If we add geo-coordinates at the time of encryption using geo-fence then at the time of retrieve the data application matched the geo-coordinates so that the file can only be decrypted at particular location.

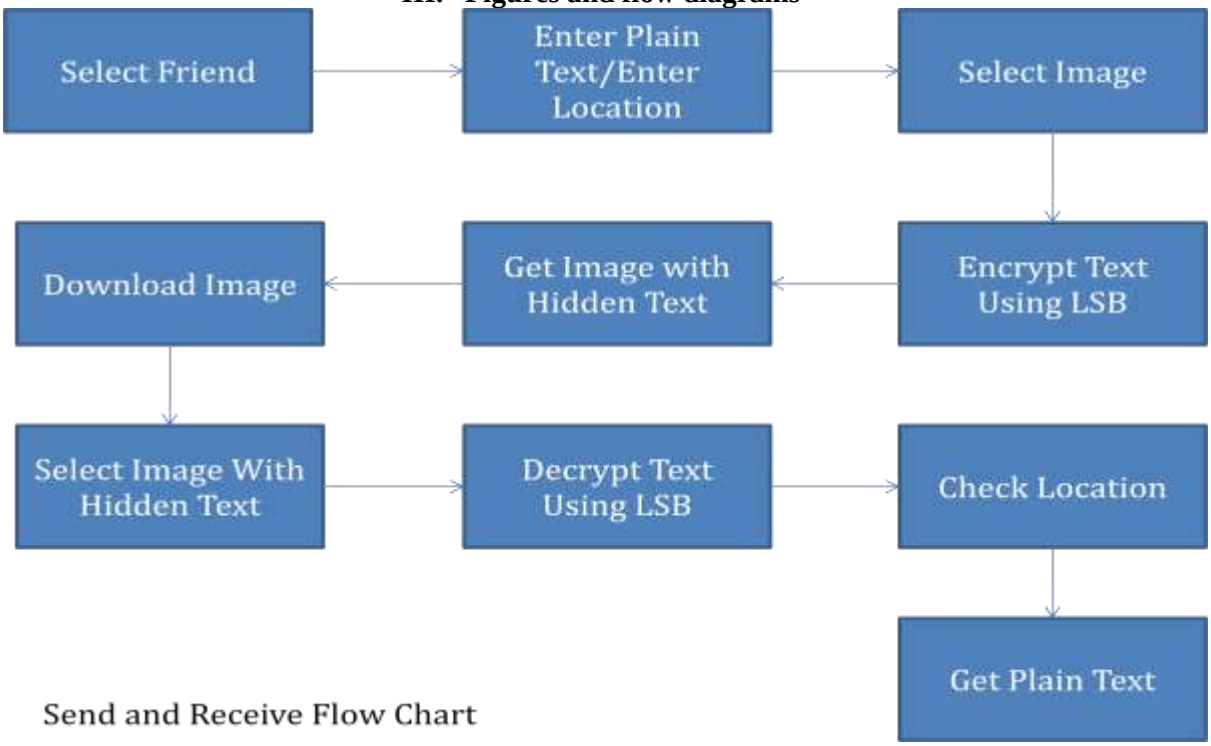
we are Proposing smart steganography android application. This application can encrypt message behind image using modified LSB steganography technique and geo-coordinates of the receiver are encrypted with image using in-built technology of android, i.e. GPS. After encryption file can be send to another user who use same application. The file can be decrypted using same application after geo-coordinates matched.

II. Literature Survey

In this paper the drawback of existing steganography methods is describes. It alters the bits used for storing color information. Some of the examples include Least Significant Bit or MSB based steganography. There are also many existing methods like Dynamic RGB Intensity based steganography scheme [1] Says that if a person views the object in which the information is hidden inward, he or she will have no indication that there is any hidden information. So the person can not be able to decode the data. Steganography can be divided into text steganography, image steganography, and audio/video steganography. Image steganography is one of the typical methods used for hiding the information in the cover image. Least Significant Bit is very dynamic algorithm used to embed the information in a cover file. This paper presents the detail knowledge about the Least Significant Bit based image steganography and its applications to various file formats. In this paper we also analyses the available image based steganography along with cryptography technique to achieve security. [2] In this paper an improvement in the plain Least Significant Bit based image steganography is proposed and implemented. In this paper the use of bit inversion technique to improve the stego image quality is proposes. Two schemes of the bit inversion techniques are proposed and implemented. In these techniques, Least Significant Bit of some pixels of cover image are inverted if they occur with a particular pattern of some bits of the pixels. In this way, less number of pixels is modified in comparison to plain Least Significant Bit method.

So PSNR of stego image is improved. The proposed bit inversion technique provides good improvement to Least Significant Bit steganography. This technique can be combined with other methods to improve the steganography else[3] The main purpose of Steganography, which means 'writing in hiding' is to hide data in a cover media so that others will not be able to notice it. While cryptography is about protecting the content of messages, steganography is about concealing their very existence [6].Geo-fencing is a promising technique for emerging location based services. Geo-fencing is concept that uses the global positioning system (GPS) to define geographical boundaries. It is a virtual barrier. A geo-fence could be dynamically generated as in a geographical radius around a store or point location. Or a geofence can be a predefined set of boundaries, like school attendance zones or neighborhood boundaries.[4]. Geofences can be used to target customers in physical locations, allowing you to trigger the right message, the right campaign, at the right time and place.[7] One of the more advanced (and often underutilized) features of a GPS tracking system is the ability to create geofences with triggered alerts . Geofences are designated areas that you can define on a map. They can either be a certain radius around a single point, or any shape that you create from several points.[8]

III. Figures and flow diagrams



Send and Receive Flow Chart

Fig.1 selecting geo-fence

Fig. 2 decryption of data at particular location

IV. Project Scope

In this project we have used steganography along with geofence to share files. Geofence is nothing but a mark of latitude and longitude. Using GeoFence we get names of the persons who are in the area of GeoFence. Steganography is hiding information along with image or text. We have implemented use of steganography to make sharing of file in a secure manner over the internet. Hence using GeoFence and Steganography files can be shared over internet in a secured way.

V. Applications

1. Confidential communication and secret data sharing.

   In military, confidentiality of communication is important, If the confidentiality get alter by terrorist then nation's will be in danger. This smart stenography application helps in confidential communication. It also help organization to share secret data.

2. Protection from data alteration.

   This application provides protection from data alteration. Its use's geo-fence technique that's why the data can only be decrypted at specific location.

3. Data integrity

   In this application integrity of data is maintained. The data send by sender is remain same at receiver side. Unauthorized person can not access the data due to geo-fence technique.

VI. Conclusion

Smart Steganography application software provided for the purpose , how to use embed message into image along with Geo-Coordinates. The master work of this application is in supporting the facility of compressing of output file, even encrypt the output file with geo-coordinates, so that the message can be retrieved at a particular area.

REFERENCES

[1] R. Rejani, D. Murugan, Deepu V. Krishnan, "Pixel Pattern Based Steganography on Images", ICTACT Journal on Image and Video Processing, Volume: 05, Issue: 03, pp. 991-997, February 2015.
[2] K.Thangadurai, G.Sudha Devi, "An analysis of LSB Based Image Steganography Techniques", International Conference on Computer Communication and Informatics (ICCCI -2014), Coimbatore, INDIA, 2014.
[3] Nadeem Akhtar, Shahbaaz Khan, PragatiJohri, "An Improved Inverted LSB image Steganography", Internationai Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 749-755, 2014
[4] Subramanya A. Iyer, "Location Based Steganographic Algorithm", Subramanya A. Iyer Department of Telecommunication Engineering, Dr.AIT,Bengaluru
[5] https://thehackernews.com/2015/06/Stegosploit-malware.html
[6] Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security series, Boston, London.
[7] http://academy.pulsatehq.com/7-things-about-geofencing
[8] https://gpstrackit.com/how-to-use-geofences-and-triggered-alerts-with-your-gps-tracking-system/