International Journal of Infinite Innovations in Technology|ISSN:2278-9057
IJIIT|Volume-V|Issue-IV|2016-2017 April|Paper-02
Reg. No.:20170302|DOI:V5I4P02

GEO-ENCRYPTION

Bhairavi Jadhav
Department of Computer Engineering,
Datta Meghe College of Engineering,
Airoli, Navi Mumbai.
bhairavijadhav1796@gmail.com

Pranjali Gawade
Department of Computer Engineering,
Datta Meghe College of Engineering,
Airoli, Navi Mumbai.
pranjaligawade7695@gmail.com

Srushti Patel
Department of Computer Engineering,
Datta Meghe College of Engineering,
Airoli, Navi Mumbai.
pshrush86410@gmail.com

Prof. J.A. Gaikwad
Department of Computer Engineering,
Datta Meghe College of Engineering,
Airoli, Navi Mumbai.
jag.cm.dmce@gmail.com

***Abstract* - Nowadays data security is making a way into market. New techniques of data security have gained interest of many researchers. The use of knowledge of the user's location called Geo-encryption, produces more secure systems that can be used in different applications. Location Based Data Encryption Methods (LBDEM) is a technique used to enhance the security of such applications called as Location Based Services (LBS). It collects latitude coordinates and longitude coordinates of mobile nodes and uses it for the encryption and decryption process. Geo-encryption plays an important role to raise the security of LBS. Different Geo-protocols have been developed in the same area to add security with better throughput. To increase the security by another fold, image steganography can be used to store the encrypted data and transfer it to the receiver through an image. In this paper, we will study how location based encryption works.**

Keywords* - *image steganography, NMEA protocol.

I. INTRODUCTION

In recent years, mobile networks have received tremendous attention because of their self-configuration and self-maintenance capabilities. The penetration of mobile wireless technologies has resulted in larger usage of wireless data services in the recent past. For secure communication, different data encryption algorithms are used. But traditional data encryption algorithms are location independent. Data encrypted with such techniques can be decrypted anywhere. They cannot restrict the location of mobile clients for data decryption. So, for secure communication the concept of “geo-encryption” is introduced which is location dependent. It is an enhancement to traditional encryption that makes use of physical location as a mean to produce additional security. It allows data to be encrypted for a specific place or broad geographic area. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing. The geo-encryption algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security.

This paper provides a threefold security mechanism to protect the data by first encrypting the data with cryptographic algorithms, second restricting the number of users by adding location coordinates and area of access and third protecting the data from spoofing while being transferred by image steganography. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

II. LITERATURE SURVEY

Location information has many properties good for encryption and authentication [3]. Logan Scott and Dorothy Denning [1] discussed an innovative encryption. The capability has tremendous potential benefits to applications such as location based services, managing secure data and digital movie distribution where controlling access is the main concern [2] scheme that integrates position into the encryption and decryption processes. Their geo-encryption approach builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for one or more specific locations or areas such as a corporation’s campus area. Geo-encryption can be used with both fixed and mobile applications and supports a wide range of data sharing and distribution policies such as providing location-based security for digital cinema distribution and forensic analysis in cases of piracy.

III. PROPOSED METHOD

Process method comprises of encryption process and decryption process.

A. Encryption process

The sender encrypts the plaintext using a conventional cipher and a key. The receiver delivers his location based information to the sender. The sender generates a Geo-tag that includes latitude, longitude and radius which is tagged to the encrypted text. This encrypted text is further concealed in an image using image steganography techniques and is send to the intended receiver.

B. Decryption process

The receiver requires a communication channel to receive the Geo-tag. The receiver uses a GPS adapter that uses NMEA protocol to capture the Geo-tag. I f the location check is bypassed, the receiver is authorized for the decryption process. Further the receiver requires initialization vector and password to decrypt the data from the image and if the condition satisfies data is decrypted.

C. Working of technologies used

i. GPS

GPS is a global navigation satellite system that provides geo-location and time information to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

ii. NMEA protocol

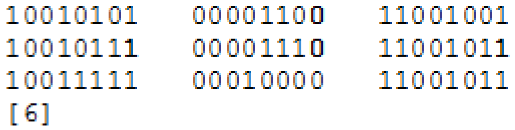
NMEA is an acronym for the **National Marine Electronics Association.** NMEA existed well before GPS was invented. According to the NMEA website, the association was formed in 1957 by a group of electronic dealers to create better communications with manufacturers. Today in the world of GPS, NMEA is a standard data format supporter by all GPS manufacturers, much like ASCII is the standard for digital computer characters in the computer world. The purpose of NMEA is to give equipment users the ability to mix and match hardware and software.

iii. Image steganography

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit colour, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

```
10010101   00001101   11001001
10010110   00001111   11001010
10011111   00010000   11001011
```

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed)



```
10010101   00001100   11001001
10010111   00001110   11001011
10011111   00010000   11001011
[6]
```

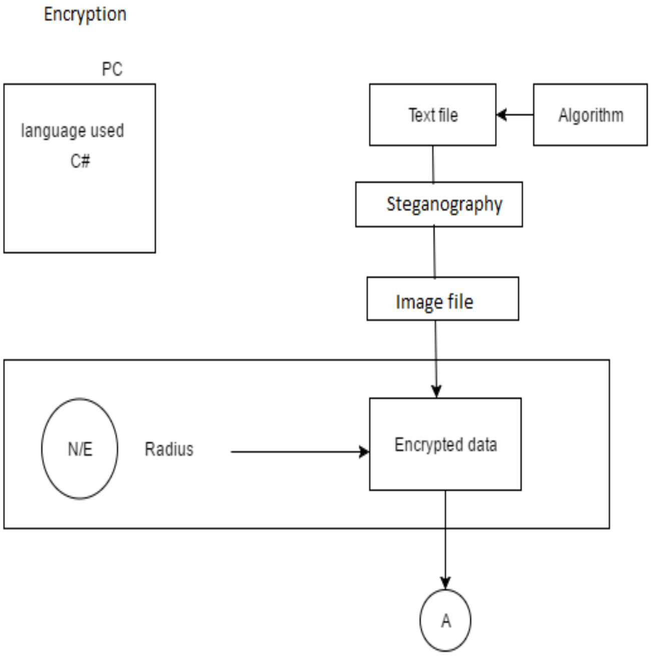


Figure 1: Block diagram for Encryption

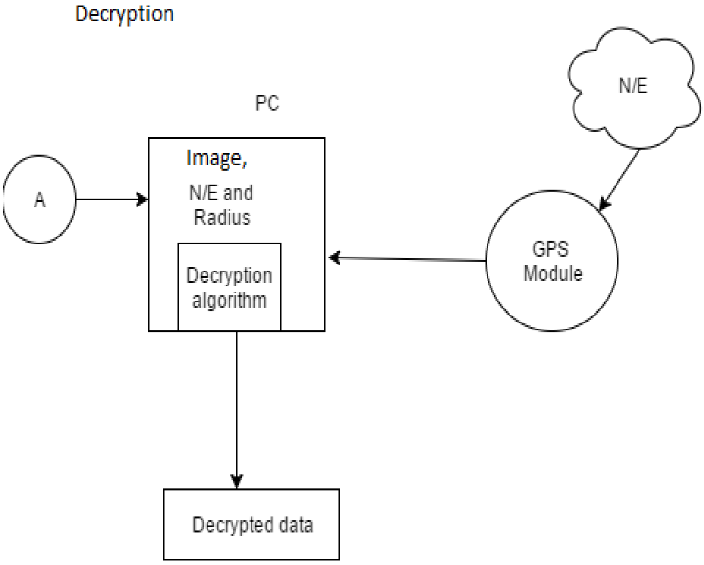


Figure 2: Block diagram for Decryption

IV. CONCLUSION

This paper proposed a simple but effective method of providing security to the data by location based services and image steganography. The aim of the study was to develop an encryption system that allows secure transmission of data from the sender to receiver. Our system provides three-fold mechanism for the same.

ACKNOWLEDGEMENT

A special thanks to my guide Prof J.A. Gaikwad who gave me best of her support in my paper work. I am also thankful to Prof. Dr.S.D.Sawarkar and Prof. Amol Pande for the motivation that they gave me.

REFERENCES

[1] Logan Scott, Dorothy Denning, "A Location Based Encryption Techniques and some its Application", ION NTM,
pp. 734-740, 2003.
[2] Hsien-Chou Liao and Yun-Hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile
Users", Information Technology Journal 7 (1), pp. 63-69, 2008.
[3] A Survey on Location Based Data Encryption Algorithms for
Mobile Devices. Volume 4, Issue 5, May 2014
[4] *Pahati, OJ (2001-11-29).* "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet. *Archived from* the original *on 2007-07-16.* Retrieved 2008-09-02.
[5] http://www.gpsinformation.org/dale/nmea.htm *-website*
[6] http://www.garykessler.net/library/steganography.html
[7] http://gpsworld.com/what-exactly-is-gps-nmea-data/