# AN IMPROVED GEO-ENCRYPTION ALGORITHM IN LOCATION BASED SERVICES

**Pranjala G Kolapwar**[1]

[1]*CSE Department, SGGSIET, Nanded, Maharashtra, India*

## Abstract

*Wireless technology is used in many applications with location based data encryption techniques to secure the communication. The use of knowledge of the mobile user's location called Geo-encryption, produces more secure systems that can be used in different mobile 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 position, time, latitude coordinates and longitude coordinates of mobile nodes and uses 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. The Advanced Encryption Standard in Geo-encryption with Dynamic Tolerance Distance (AES-GEDTD) is an approach which gives higher security with a great throughput. This approach mainly uses the AES algorithm, symmetric key encryption algorithm. But applying this algorithm to more complex data like images, videos, etc. like in Digital Film Distribution, we might face the problem of computational overhead. To overcome this problem, we analyze AES and modify it, to reduce the computational overhead. In the modified AES algorithm (M-AES), we omit the calculation of mix column operations and hence the M-AES-GEDTD is a fast and lightweight algorithm for multimedia data.*

***Keywords:*** *Geo-encryption; LBDEM; LBS, Geo-locked Keys .*

----------***----------

## 1. INTRODUCTION

In todays world, the use of wireless technology goes on increasing as an increase in the wireless applications. To provide a higher layer of security to such wireless application, 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. Much research has been done on the LBDEM approaches and developed number of Geo-protocols. The paper cites the reference [1] gives the survey of such Geo-encryption techniques. There will be malicious users trying to exploit and find new holes in a network. Therefore, we need to look into the future so that we are able to face these security issues before they cause damage. In the paper [2], we try to improve the existing Geo-protocol, Data Encryption Standard in Geo-encryption with Dynamic Tolerence Distance (DES-GEDTD) and improve its performance by using AES-GEDTD. As AES is one of the best contemporary algorithm, AES-GEDTD giver higher level of security with enhancement in the performance of the network.

In this paper, we try to modify the existing AES-GEDTD approach which has complex computability and higher cost and evolved a new algorithm called M-AES-GEDTD with lower complexity and lower cost.

In digital film distribution, the same large (25 to 190 Gbyte), encrypted media file might be used in multiple theatre by using the Geo-encryption technique [3]. This provides a secure and efficient point-to-multipoint distribution model for delivery via satellite. At the exhibition hall, robust watermark or stenographic techniques can introduce location, time and exhibition license information into the exhibition for subsequent use in piracy investigations. AES-GEDTD approach [2] gives the best performance in this application.

The paper is organized as: Section 2 gives the related study. Section 3 gives the detail of the role of LBDEM in digital film distribution. Section 4 gives the Basic working of the AES algorithm. Section 5 gives the different flaws of existing approaches in digital film distribution. Section 6 explains the modified approach. Section 7 explains the results and analysis of M-AES-GEDTD. And finally we conclude in Section 8.

## 2. RELATED STUDY

Cryptography is the study of technique for secure communication. It works in two phases called encryption and decryption. These two processes are vice-vesra of each other. Encryption is a process carried out at receiver side and decryption is performed at the transmitter side. Traditional cryptographic algorithms are location independent and hence the technique of Geo-encryption is evolved. Figure 1 gives the general concept of Geo-encryption and steps involved in its working.

This Geo-encryption technique is location dependent means encryption and decryption work as-

### 2.1 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 and tags it to the ciphertext. The sender broadcasts the ciphertext and the Geo-tag.

### 2.2 Decryption Process

The receiver requires a communication channel to receive the ciphertext and Geo-tag. The receiver uses an RF antenna and receiver to capture and condition signals. The receiver applies a feature extraction algorithm and key generation algorithm to compute a Geo-tag based on the collected RF signals. If the location check is bypassed, the receiver is authorized to the decryption

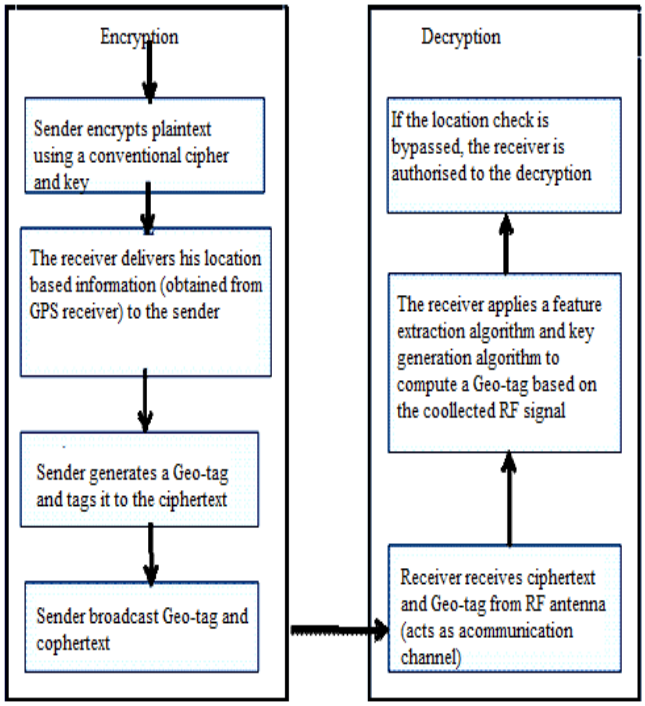


**Fig -1**: Basic Geo-encryption Working

### 2.3 Literature Survey

Karimi and Kalantari developed a new Geo-protocol called as Data Encryption Stadarad GEDTD (DES-GEDTD which makes the use of Dynamic Tolerence Distance as a key parameter and DES encryption-decryption algorithm. DTD is nothing but a fractional number with small interval which makes the key more secure in encryption decryption process. But, if the transmitted file is bulky and require higher security, then this protocol not able to handle this situation efficiently. Moreover, AES is one of the best contemporary algorithm and used to meet the above mentioned demands, [2] designed the new Geo-protocol called as AES-EDTD.

There are a number of location based services requiring security during data transmission with higher throughputs. Scott and Dening [3], explains the use of these location based data encryption techniques in digital film distribution. LBDEM also plays a very important role to enhance the security. But when we apply the AES-GEDTD technique for more complex and large data like video files in digital film distribution, it produces significant computational overhead and require much processing time. And hence need to optimize the existing AES-GEDTD as M-AES-GEDTD.

## 3. ROLE OF LBDEM IN DIGITAL FILM DISTRIBUTION

Digital Film refers to the use of digital technology to distribute or project motion pictures as opposed to the historical use of motion picture film. In this application, the same large encrypted media file is used at multiple theatre locations nationwide, but with different Geo-locked keys, specific to the intended recipient location and its exhibition license. This provides a secure, efficient point to multipoint distribution model applicable to distributions via satellite or DVD. At the exhibition hall, robust stenographic techniques can introduced signed location, time and exhibition license information into the exhibition for subsequent use in piracy investigations [2].

LBDEM plays an important role in the DFD. Because in a DFD, require a high level of security and the also the input file is also very large. Hence the proposed approach [2] called AES-GEDTD works very efficiently. But as we are using AES is the main symmetric cryptographic algorithm in AES-GEDTD approach, increases the complexity in the DFD. Hence, we try to modify it as M-AES.

## 4. BASIC WORKING OF AES ALGORITHM

AES algorithm is one of the best contemporary algorithm that can be used to enhance the security in data communication. There are three versions of AES algorithms depending on the length of the key called AES128, AES192 and AES256. These different length keys are arranged in a matrix with sizes 4×4, 4×6 and 4×8 respectively, and 128 bit block data which constructed in 4×4 matrix called state. AES algorithm is divided into four sequential operations where these operations are made on a state with (10, 12, 14) rounds based on key length as shown in Figure. 2. The AES algorithm involves following steps [16].

### 4.1 AES Steps

#### 4.1.1 Sub Byte Transformation

SubByte operation is a nonlinear byte substitution that state bytes independently using substitution tables called the S box. The box is constructed by taking the multiplicative inverse in the Galois field (GF).

#### 4.1.2 Shift Row Transformation

In this step, shifting operation applies to state rows, where the first row remains as it is, second row shifted to right one time, third row shifted to the right two times and the fourth row shifted to the right three times.

### 4.1.3 Mix Column Transformation

Mix column transformation carries out on the state column by column. In this operation, each byte is replaced by the value depends on all 4 bytes in the same column through the multiplication state matrix in GF.

### 4.1.4 Add Round Key Transformation

The final operation in the AES round is the Add Round Key (ARK) transformation. ARK transformation is nothing but the simple bitwise XOR between state matrix and sub key.

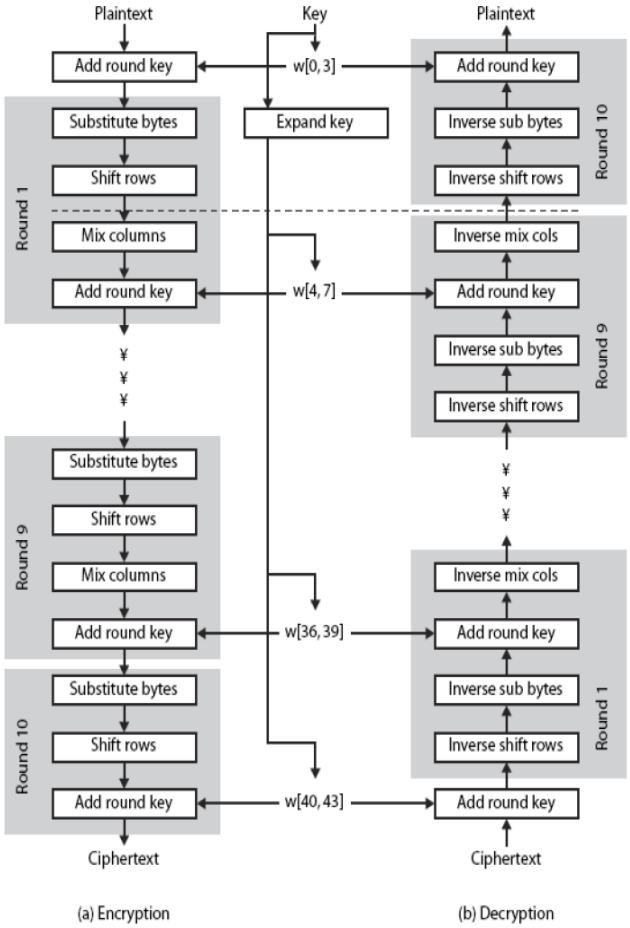


**Fig -2**: AES Structure (a) Encryption Operation (b) Decryption Operation

### 4.2 AES SKey Expansion

The AES key expansion operation takes a 4 word (16 byte)initial key and produces a linear array of words, providing 4 word round key for the initial AddRoundKey stage and each of the 10 or 12 or 14 rounds of the cipher. It copies the contents of initial key into the first group of 4 words and then construct subsequent groups of 4 words for each group depend on the values of the previous group.

## 5. FLAW OF EXISTING AES IN DFD

All the operations discussed in the above section require high mathematical calculations. Moreover, encryption and decryption use different time consuming operations to process the multimedia data. When we look into the detail of these operations, mix column operation is more complicated and require more time as compared to the other operation involved in AES round key process. Consider the scenario in which the input file is very large or if it is a video file like in DFD application, then it consumes more time to encrypt this input file as well as to decrypt.

Hence, to overcome the problem of high calculations and computation, we modify the existing AES algorithm as Modified-AES (M-AES) without affecting the security.

## 6. M-AES ALGORITHM IN GEDTD

The main aim of this modification is to reduce the calculations and hence encryption-decryption time is also reduced. As mentioned in the above sections, the round function contains four stages, among which we just skip the high computational step called mix column. So, in the M-AES round function, only three stages are there:

- Sub Byte Transformation
- Shift Row Transformation
- Add Round Key Transformation

In the process of M-AES decryption, the same inverse of all the above said operations is calculated except mix column. As we are applying this M-AES in location based applications called DFD in which we require security as well as less transmission time also. Both these requirements can be handled by this approach very efficiently.

## 7. RESULTS AND ANALYSIS OF M-AES IN DFD

For testing this algorithm, we apply the same input file to the AES and M-AES algorithm by using GEDTD protocol. To test the algorithm, we take the 71 byte input file and compare the execution time of the AES-GEDTD and M-AES-GEDTD. Table 1 shows the comparative analysis.

**Table -1:** Encryption results for the test file

| File Size | AES-GEDTD (min) | M-AES-GEDTD (min) | Efficiency (min) |
|---|---|---|---|
| 71 Bytes | 2.10 | 1.55 | 0.55 |

## 8. CONCLUSION

Normally, lightweight algorithms are very attractive for multimedia transmission as like requiring in DFD application. M-AES-GEDTD is such a lightweight algorithm having minimum computational overhead. So, by using M-AES-GEDTD approach, we can meet these demands of multimedia data transformation.

## REFERENCES

[1] Pranjala G Kolapwar, H P Ambulgekar (2014), "A Survey on Location Based Data Encryption Techniques of Mobile Nodes," ISCSSIT, pp. 1010-1015.

[2] Pranjala G Kolapwar, H P Ambulgekar(2014), "Use of Advanced Encryption Standard in Geo-protocol to enhance the performance of Location Based Data Networks," IJSR, pp. 2888-2890.
[3] Ilias Maglogiannis, Leonidas Mazatzopoulos Delakouridis(2009), "Enabling Location Privacy and Medical Data Encryption in Patient Telemonitoring System," IEEE Transaction Paper, pp. 1089-1098.
[4] Logan Scott, Dorothy Denning(2003), "A Location Based Encryption Techniques and Some its Application," ION NTM, pp. 734-740.
[5] Hsien-Chou Liao and Yun-Hsiang Chao(2008), "A New Data Encryption Algorithm Based on the Location of Mobile Users," Information Technology Journal, pp. 63-69.
[6] Hatem Hamad and SouhirElkourd (2010), "Data encryption using the dynamic location and speed of the mobile node," Journal Media and communication studies, pp. 67-75.
[7] Prasad Reddy. P.V.G.D, K. R. Sudha, P Sanyasi (2010), "A Modified Location-Dependent Image Encryption for Mobile Information System," IJEST, pp. 1060-1065.
[8] Rohollah Karimi and Mohammad Kalantari (2011), "Enhancing Security and Confidentiality in Locaion based Data Encryption Algorithm," IEEE Conference, pp. 30-35.
[9] V Rajeswari, V Murali and A.V.S. Anil (2012), "A novel approach to identify Geo-Encryption with GPS and Different Parameters (Location and Time)," IJCSIT, pp. 4917-4919.