Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 1, January -2015

A SURVEY ON ENHANCE SECURITY USING AES WITH MULTIPLE CHAOTIC MAPS

Zankhana Mistry[1], Asst.Prof Hiren V Mer[2]

[1]PG Student,CSE Department, CSE Department, Parul Institute of Technology,Limda, zmistry.4435@gmail.com
[2]Assistant Professor, Parul Institute of Technology,Limda, prof.hirenmer@gmail.com

Abstract*--Geographic Information System contains Geospatial data which is related to space or Earth surface related data.GIS data is used in many fields like military aspects, satellite sensor Technologies, Government Organizations, Disaster Defence, Public Security, etc. GIS Images or Satellite images contains huge data about some particular area & spatial database is totally depend on the Geological Image. GIS data contains such confidential information which must be kept away from unauthorized user. So Geospatial data i.e GIS Images requires more Security policies against unauthorized user. Here in this report such security policies for Geospatial data are discussed. Here we discuss some techniques of encryption on Geological images such as AES algorithm. Chaotic Series and logistic Maps are used to perform Encryption and Decryption operation with composition with AES algorithm. The encrypted cipher images always display the uniformly distributed RGB pixels. Uniform histogram of encrypted image shows high security of data.*

Key words: *GIS, Geospatial data, Satellite Images, AES algorithm, Chaotic series/map*

I. INTRODUCTION

In the recent days, Image encryption has found a lot of focus in the field of security. It is well known that images are different from text data, but in GIS (Geographic Information System) Images are very important then Text data because in GIS from Geospatial Images

Different types of data can be collected by analysing, manipulating storing, capturing The GIS Images. It is very important to Protect the GIS Images or Data from two threats. First, since the GIS data or Images are too expensive, we have to prevent illegal replication and distribution of it. Second, since the data is sensitive and must not be accessed by unauthorised users.[4]

Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code[5].some conventional encryption Algorithms are used in digital Image cryptography such as DES,RSA (Rivest-Shamir-Adleman), IDEA, etc.but the drawback of these conventional algorithms are that they are not Suitable for Digital Image cryptography. Here we use satellite Images or GIS images for Encryption so they are quite different from digital images and the quality is very high then digital Images. So we use AES(Advance Encryption Standard) with composition of Multiple Chaotic Maps for GIS Images.AES is suitable for Image Encryption and Decryption with is closely related to some dynamics of its own characteristics[5].

As name suggest Image encryption, it is clearly that we have to work pixels. In most of the Images, the value of the pixels can be predicted from its nearby pixel values. Encoding the image is the process in which we have to change image from its original content and make some secure cryptograph, while Decoding is the process to obtain or recover the Original Image from the encoded Image[6]. Encryption can be done by two way such as

1. Fully Encryption
2. Partial Encryption

Full Encryption algorithm encrypts complete data, which can obtain high security. but they are of high compute complexity and change the file format[6].It is the drawback of Full Image Encryption. Where as Partial Encryption algorithm obtain high Speed by encrypting only some sensitive data so it is more suitable for Image encryption[6]. But we use GIS Images for Encryption, The GIS images contains Confidential data and it is in Different Format then other Digital Images. so it is very necessary to Secure full Images without changing its File Format. Another drawback of Full encryption is that after decrypting the Image into original Image it is not maintaining the original quality of Image, it is not suitable for our GIS images because GIS images are confidential an should be highly secure from some unauthorised user.

II. LITERATURE SURVEY

For data encryption AES encrypts a plain text by using Secret key into cipher text. The cipher text can be seen very different from the plain Text and give no clue to the original text or data. Same way in the application of Image Encryption and decryption, the encrypted image should be different from and give no clue to the original one[5].

AES(Advance Encryption Standard)

AES(Advance Encryption Standard) algorithm is 128 bit Symmetric algorithm. The main advantage of AES algorithm is its flexibility.AES is supporting any combination of data and key size of 128, 192, 256 bits.AES allows a 128 bits data length that can be divided into four basic operation blocks. Here Some transformation Steps are given.

1. Subbyte Transformation
2. Shift rows Transformation
3. Mix columns Transformation
4. Add round key Transformation

Expansion Key

With AES Encryption, the secret key is known to both Sender and receiver. The keys are expanded via a key expansion routine for use in the AES cipher algorithm. The key expansion routine can be performed all at once or "on the fly" calculating words as they are needed[5].

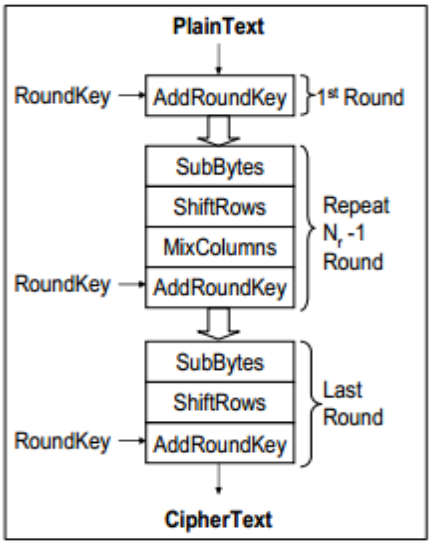

Figure-1: Diagram of AES encryption algorithm[5]

In the other paper the author has discussed about the Partial Image Encryption using Chaotic Logistic maps. Images can be encrypted by two ways such as

1. Full Image Encryption
2. Partial Image Encryption

Strengths of AES:

- AES is extremely fast then other block ciphers.
- The cipher does not use arithmetic operations[5]
- AES is fully self supporting, does not use S-Boxes of other ciphers, bits from RAND tables[5]
- AES allows any sizes of key like 128,256.
- AES is used in Image Encryption then other Conventional algorithms because conventional algorithms like RSA,DES,IDEA are not suitable for Real time image encryption[6]

The Full Encryption algorithm encrypts complete data, which can obtain high security. But they are of high compute complexity and change the file format whereas partial encryption algorithm obtain high speed by encrypting only some sensitive data. As chaotic maps have many fundamental properties such as ergodicity, mixing property and sensitivity to initial condition/system parameter[6].

A new partial image encryption scheme is used Chaotic Logistic maps for more secure image encryption. In this encryption scheme, 80 bit secret key and 2 Chaotic Logistic maps are used. The initial conditions for both logistic maps are derived using the secret key by providing different weightage to its bits. The first logistic map is used to generate numbers ranging from 1 to 24[6]. The loss of even a small part of encryption image cause greater distortion in the encrypted image. In fact the part of the encrypted image which is distorted constitutes pixels that will be scattered in the decrypted image.

Chaos theory shows the difficulty of predicting their long range behaviour. Logistic map is written as[6]

$$f(x_n) = rx_n(1 - x_n)$$
$$x_{n+1} = f(x_n) \quad (1)$$

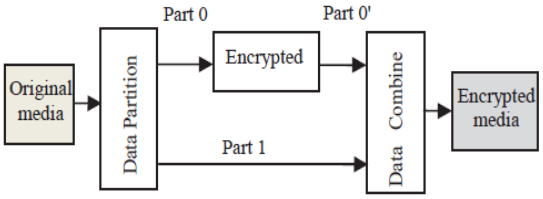

Figure-2: Partial Encryption

Where,
X_n = Chaotic sequence $(0< X_n < 1)$
$X_0 \in [0,1]$
r = positive real number $(0 < r < 4)$

Image encryption technique in composition of AES and Chaotic Series. Chaotic series act as a key for AES Encryption. In the spatial domain, we present a new method of deriving a space transform matrix with chaotic Series. There is no damage cause the decrypted image[7]. Here Chaos base encryption can be done by confusion and Diffusion techniques.

Chaos signals are very sensitive to parameters and the initial value, in principle, using them as encryption key would produce a huge key space. Their key spaces are definite and their security performances are easy to evaluate[7]. Combination of Chaotic series and conventional algorithm provide high security to the images. Combination of conventional algorithm and chaotic series can be applied by two way

1. Chaotic encryption in series with Conventional Encryption
2. Chaotic encryption in parallel with Conventional Encryption

we have discussed about the Encryption scheme for the Medical Images. As we know that Encryption can be done on such confidential and Important data which could be kept away from unauthorised user. Among the various images Medical images are such types of Confidential data which contains Information about the patients' Medical History and their disease.

In this system we use symmetric cryptography and chaos for encrypt medical images such as MRI, X-ray, ultrasound, CT and PET. Symmetric cryptography algorithm that we used in this project is Simplified Advance Encryption Standard (S-AES)[8]. This extreme sensitivity to the initial conditions makes chaotic functions very important for application in cryptography and in this cryptosystem the key sensitivity are determined by the parameter sensitivity of chaotic map and the initial-value sensitivity of diffusion function[8].

The image pixels first scrambled via Cat Map chaotic mapping. Then the second stage provides diffusion for pixels values modification in the image by applying S-AES algorithm (with chaotic S-box) to every pixel. combining cat map with block cipher system can provides additional features for the system.[8]

In this paper we have used pixel position scrambling method before encryption. This step is called Confusion stage which permutes the pixels in the medical image without changing its values by applying scrambling algorithm.

In other paper, the encryption is done on GPU(Graphics Processing Unit) along with CPU. The encryption and decryption process can be Completely implemented on the GPU. The GPU acts as a valuable co-processor that relieves the load off the CPU[9]. In this paper, it is also represented a system for encryption and decryption of hybrid map tiles generated from GIS data sets. The method implements the entire encryption and decryption algorithm on the GPU and takes advantage of the parallel processing capabilities of the GPU. Once the data is loaded onto the GPU all other steps are implemented on the GPU. During decryption, we provide a method to display the decrypted data (text and images) directly on the screen without bringing it to the CPU memory[9]. Here the CPU and GPU both are act as Co-Processor. The GPU is comparable or better than that of the CPU.

In the other paper, the basic concept is Image encryption using Two Chaotic Scheme. The main advantage of two Chaotic Scheme is very wide encryption space. Another important thing of Chaotic Sequence is that Chaotic Sequences are easy to control and easy to generate. The highly unpredictable and random-look nature of chaotic signals is the most attractive feature of deterministic chaotic system that may lead to novel applications[10]. In this paper the image encryption technique is include Compression Methodology.

The advantages of Chaos based Encryption system are good properties in security, complexity, speed, computing power, computational overhead etc. The strong point of Chaotic System is that it is very difficult to predict the final position of one point from its initial position. Chaos theory can be exploited in the field of cryptography by taking such system parameters and initial condition as secret key s while considering the iteration of chaotic map equivalent to round of the encryption function[10]. There are some comparison between Chaotic System and Traditional Cryptography is shown in below table,

Chaotic system	Traditional cryptosystems
ergodicity	Confusion
Sensitivity to initial condition and system parameters	Diffusion
Parameters	Encryption key
Iterations	cipher

Table-1: Comparison between Chaotic system And traditional Cryptosystem[10]

Encryption and Decryption of Image:

Encryption of digital Images by using combination of Chaotic Scheme and Traditional Algorithm, the security of the encrypted image is high and effective. Instead of Encryption an image in a chaotic signal directly, the proposed scheme uses two chaotic system based on the thought of higher secrecy of multi system. Then this chaotic sequence is transformed into a binary stream by a threshold function. The other chaotic system is used to construct a permutation matrix[10].

Encryption can be used to provide high levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection. special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfil such a task, many image encryption methods have been proposed[11].

The new techniques for Digital Image Encryption are introduced in the paper are[11]

1. LSB Replacement Technique
2. Transform Domain Technique
3. Share Base Technique

III. RELATED WORK

Image encryption is very important in many applications where secret image consisting of secret information. Some images like GIS images contains such confidential and sensitive information which are very important in various aspects like army, defence ministry, space research centres, etc. So it is very important to secure these images very efficiently and kept away from unauthorised users. various techniques are used for Image encryption.

Novel partial Image encryption with the use of chaotic Logistic map is use for Partial Image encryption. In this technique partial Image encryption is more feasible then Full Image Encryption[6]. The drawback of full image encryption this related the quality of Image. After Decrypting the Image The original Quality of Image should not be maintained, and sometimes the file format of the Image should be changed after Decryption[6]. Sometimes only AES Algorithm is also used for Simple Image Encryption. In this the image should be encrypted with the help of secret key and some transformation steps of AES algorithm[5].

Geological Images contains such confidential data about some specific area, so it is important to secure it and give permission to access it only to the authorised user.Fast and robust image encryption is done with chaotic generator. some chaotic equations are generated by the Chaos generator and encrypt the blocks of Images[2]. Some Image encryption can be done based on Diffusion with multiple chaotic maps based on circular mapping[4]. Another technique for image encryption is composition of AES and Chaotic Series. In this technique Chaotic series and conventional algorithm is used in series and parallel manner[7].

Another image encryption is done on Medical images. The encryption is done with help of scrambling method[8]. Some Encryption of images and data are done not only in CPU but Also done on GPU(Graphics Processing Unit).While using GPU, CPU is used as a co-processor of GPU[9]. Some encryption can be done by various techniques like LSB Replacement Technique, Shared base Technique and Domain Transform technique[11].Most of images are encrypted by using Chaotic sequence or Chaotic maps because chaos system is highly unpredictable and sensitive for initial condition. So because of high unpredictability, the attacker can't be decrypt or access the image easily.

IV. PROBLEM DEFINITION

Now a day Data or Images are not so secure against various Attacks and malicious activities, so to provide high security and access of that confidential data only to the authorised user Some highly secure Encryption Technique is required. GIS data contains most of data about some particular Area. so to provide security to the GIS Images, we have to Encrypt the GIS images using AES Algorithm with multiple Chaotic Maps. Another problem facing in Full encryption is that

Quality of Image is not maintain after decryption of image. so by using Some series or parallel operation in composition of AES and Multiple Chaotic maps, try to maintain the quality of Image after full encryption and Decryption Of Image.

VI. CONCLUSION AND FUTURE SCOPE

Encryption of images by using composition of AES and Chaotic scheme has provide security to the image, but there may some problem occur in decryption. The Security of the chaotic sequence totally depends on the secret key. Chaotic sequences are employed as AES secret keys.

In our proposed algorithm of Image encryption, we have used AES algorithm in the composition of Multiple chaotic map parallely on some preprocessed satellite images by using some transformation technique for image.

For further security we can enlarge a secret key space by generating the chaotic scheme with a multi-dimensional chaotic map. Other problem is in full encryption of image, in full encryption picture quality is not maintain. We would try to maintain the quality of image after decryption. There is a little difference between encryption key & decryption key give totally different result. Sometimes image can't be decrypted into original image.

REFERENCES

[1] Sangita Zope- Chaudhari, P. Venkatachalam,"Conceptual Framework For Geospatial Data Security", International Journal of Database Management Systems(IJDMS) Vol.5,No.5,October 2013

[2] Hasan Naura, Safwan El Assad, Calin Vladeanu,"Design of a Fast & Robust Chaos-Based Crypto System For Image Encryption",IEEE 2010

[3] G.A.Sathishkumar, Dr. K Bhupathy Bagan, Dr. N. Sriraam,"Image Encryption based on Diffusion & multiple Chaotic maps",International Journal of Network Security & its Application,vol.3,March 2011

[4] P. Manali Singh Rajpoot, Pratik Patel,"A Comparative Study on Various Aspects of Security of Geospatial Data",A Fourth International Conference on Communication Systems & Network Technologies,IEEE 2014

[5] Nitumoni Hazarika, Monjul Saikia, "A Novel Partial Image Encryption Using Chaotic Logistic Map",2014 International Conference on Signal Processing & Integrated Networks(SPIN),IEEE,2014

[6] Xiao Huijuan,Qiu Shuisheng,Deng Chenglingang,"A Composite Image Encryption Scheme Using AES and Chaotic Series",First International Symposium on Data, privacy & E- Commerce,IEEE 2007

[7] Megdad Ashtiyani,Parmida Moradi Birgani,Hesam M. Hosseini,"Chaos Based Medical Image Encryption using Symmetric Cryptography" IEEE

[8] Manoj Sheshadrinathan,Kelly L Dempski,"Implemetation of Advanced Encryption Standard for Encryption & Decryption of Images and Text on a GPU",IEEE 2008

[9] Dr. Vivek Sharma, Hariom C. Agnihotri, Chetan H. Patil,"An Image Encryption & Decryption techniques using two chaotic schemes",Interbnational Journal of Research in Advent Technology,Vol.2,No.2,February 2014

[10] T. Sudha,B. Gopi,"Novel Spatial and transform Domain Image Encryption Algorithms",IOSR Journal of VLSI and Signal Processing(IOSR-JVSP),Vol.3,Issue.2,Ver.2, March-April 2014

