ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Image Encryption using AES Encryption Algorithm

Vijay S Karwande
Assistant Professor,
Computer Science and Engineering, EESCOE&T,
Aurangabad.

Nida Mirza
ME Student,
Computer Science and Engineering, EESCOE&T,
Aurangabad.

Absract:

The goal of this paper is security of information which is important in data storage and transmission. Images are used widely in industrial process, so it is necessary to provide safety, accuracy and integrity of images and to protect images from unauthorized access. In this paper we have applied AES (Advanced Encryption Algorithm) for images encrypting to enhance security in communication area for sending data.

The image file is selected first and then we perform splitting of the images. Then we apply AES Algorithm on the split images. Decryption mechanism is applied on the same image and achieves the split image and combines it to form original image.

Keywords:

Cryptography, Encryption, Decryption, Image encryption, AES (Advanced Encrypting Standard) Algorithm.

I. INTRODUCTION:

In today's world, Security is important factor for data storage and transferring of data on public network. We can use cryptography to keep our files and communication secure. The cryptography is the art and science of encrypting the data in such a way that no-one apart from the sender and intended recipient even realizes the original data, a form of security through obscurity [1]. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption.

A. Symmetric Encryption:

One type of encryption is symmetric encryption. It also called as single key cryptography. It uses a single key also known as private key that is used for both encryption and decryption sometimes also called as secret key. The sender can encrypt data with private key and send it to receiver who can decrypt data with that key. Symmetric Encryption is very common in database applications. Symmetric Encryption is very fast as compared to asymmetric encryption. Symmetric encryption covers a number of algorithms such as Blowfish, AES, DES and 3DES which are still in use.

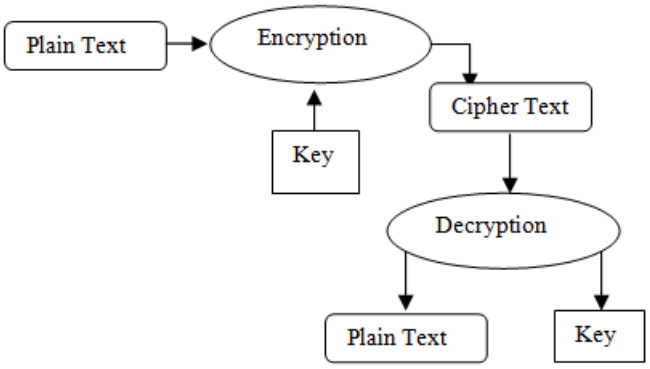

Fig. 1.1 Symmetric Encryption

B. Asymmetric Encryption:

It is also called as public key cryptography. It uses two keys: public key and a private key, public and private key have unique characteristics in asymmetric encryption in which we can encrypt with public key and there is matching private key which is used for decryption. Typically there is a public key which the sender use to encrypt data, and data is send in encrypted format to the receiver who uses the private key to decrypt the data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Thus asymmetric encryption uses a pair of keys, public and private to encrypt the information. We can encrypt with public key and decrypt with private key (vice versa). Asymmetric encryption works very well when there is two different end points. Examples of asymmetric encryption are web browsers, VPN, secure FTP.

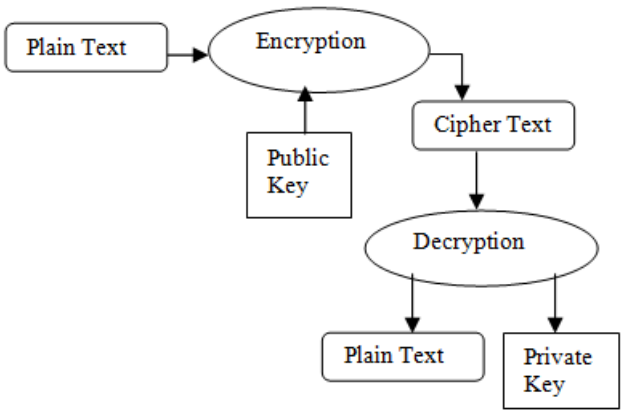

Fig. 1.2 Asymmetric Encryption

C.Introduction to AES Algorithm:

Advanced Encryption Standard, also known as the Rijndael (pronounced as Rain Doll) algorithm is adopted worldwide.AES Algorithm is used to protect Electronic data. The first thing AES Algorithm needs is data as input and the other thing it needs is key(encryption key). When these two combined are called as input and are feed into Cipher Engine produces Encrypted data in binary format called as cipher text. To recover the encrypted data it has to reverse the process in which the cipher text and key is feed into Cipher Engine to get back the original data. AES is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys.

Rounds:

There are 10, 12, 14 rounds for 128.192 and 256 bit keys. Regular rounds are 9,11and 13.Final round is 10th, 12th, 14th. Each round has certain processing involved. Following are the transformation involved.

1.SubBytes Transformation:-It uses substitution table which includes nonlinear substitution which operate on each byte of the state.

2.ShiftRows Transformation:- In ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row. The first row doesn't change.

3.MixColumnsTransformation:-MixColumns step operates on the column level. It is equivalent to the multiplication of matrix at column level. Each column of the state I multiplied with fixed polynomial.

4.AddRoundKeyTransformation:-In dd RoundKey step, the state is combined with roundkey using XOR operation.

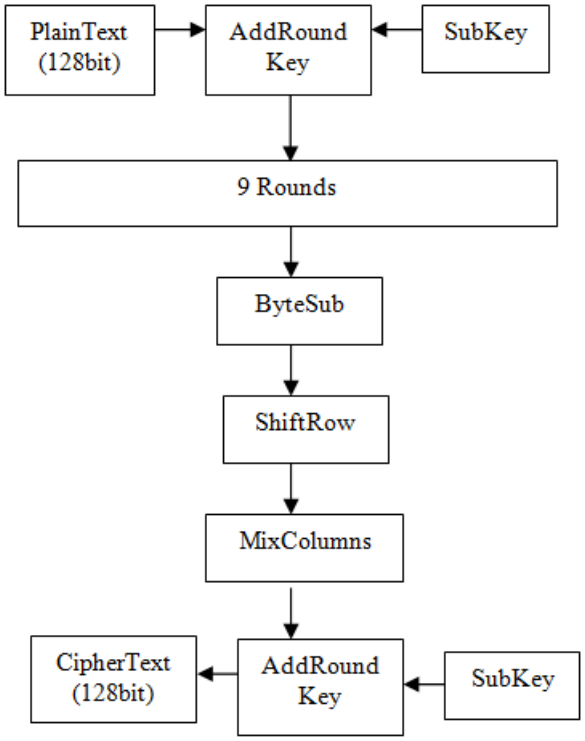

Fig. 1.3 Algorithm Encryption structure

5.Expansion Key:-In AES algorithm, the sender and receiver is known about the key. The AES algorithm remains secure, the key cannot be determined any intruder even if he knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk).The keys can be 128 bits, 192 bits, 256 bits.128 bits means (16 bytes, 4 words) ,192 bits means (24 bytes, 6 words), 256 bits means (32 bytes, 8 words). These are the key sizes which are supported by AES Encryption. The larger the key the stronger is the encryption.The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

ii Literature Survey:

HiralRathod, Mahendra Singh Sisodia proposed Image Encryption Approach using Combination of Permutation Technique Followed by Encryption where security and efficiency of data is the goal of the algorithm. It can be used in Encryption process of any image as it can provide 70% better entropy of encrypted image as compared to any other algorithm. The algorithm is very simple, direct mapping algorithm using Feistal Structure and logical operation [2].

In 2013 Saurabh Singh and Anurag Jain Proposed a method which when implemented provides highly secure transmission of data. If the intruder decrypts the image he gets another image which confuses him whether the actual data is in text format or in image format. Conversion of text into image and then applying AES encryption provides security during transmission of data [3].

In 2007 R. Tourki and M. Zeghid proposed a simplified version of AES, which design secure symmetric image encryption technique. The AES is modified to support a key stream [4].

III. Proposed Method:

First consider image. Then applying pre-processing on the same image so that image is divided in several 9 equal parts. The purpose of chopping the image is to enhance the security two times: First by chopping image into several parts and second by encryption. Then AES algorithm is applied on each chopped grid. After encrypting each grid, all the grids are combined to form one image so that eavesdropper can't guess about image chopping. On the receiver side reverse mechanism is applied. The encrypted image is first chopped into 9 equal parts and secondly AES algorithm is applied on each grid. To obtain the original image these 9 grids are sequentially combined.

Pre-processing:

Step 1: Select a image
Step 2: Divide the image into grid format
Step 3: First select first 86 pixels of rows and columns.
Step4: Then form a grid of first pixels of rows and columns.

```
Loop  rows= 0 to 85, rows= rows +86,   rows<=255;
Loop  cols= 0 to 85, rows= rows +86, rows<=255;
                    Grid[]= rows*cols;
                    End;
          End;
```

Step 5: Repeat the step 4 to form 9 grids as shown in fig 3.2.

Fig 3.1: Original Image.

Fig 3.2: Chopping of image into 9 grids.

Encryption Process:

1.Now applying AES algorithm to each grid.
2.Here, using 2 round keys, we encrypt a set of 16 pixels (128bits).
3.No of pixels to encrypt whole image N=2*{(m*n)/16}.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

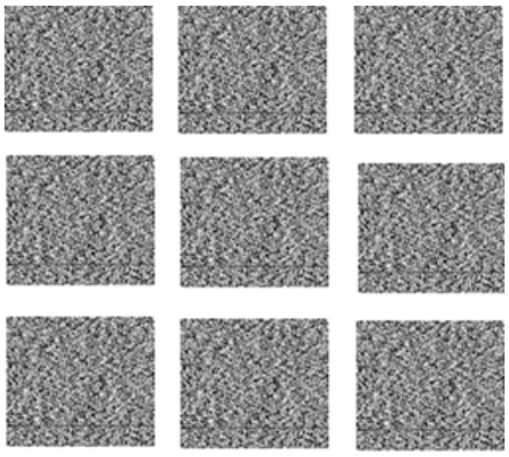

Fig 3.3: After applying AES on each grid.

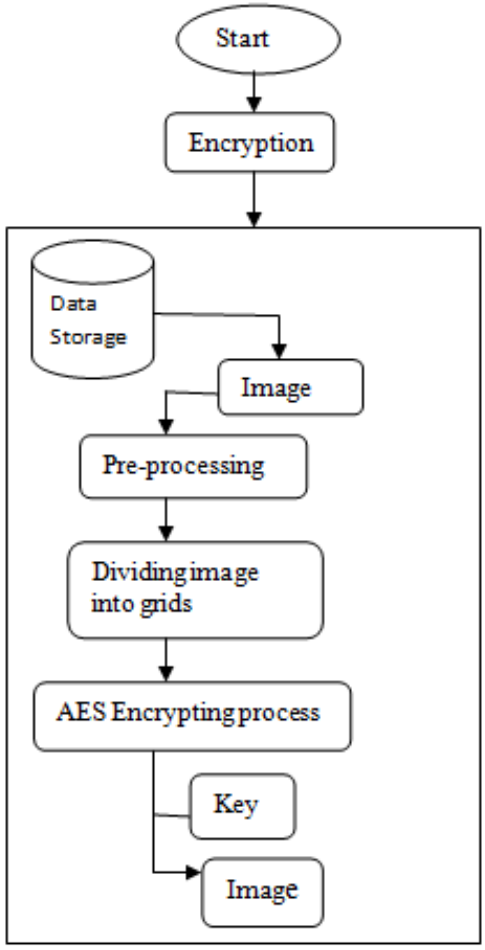

Fig 3.4: Graphical representation of Encryption Process.

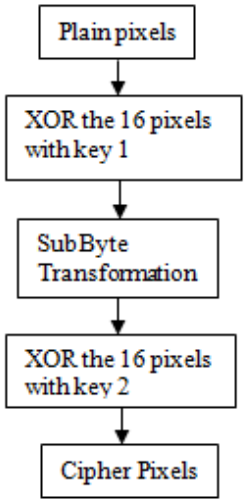

Fig 3.5: Encryption Process

Decryption Process:

Following is the process for decryption. It is reverse process of encryption.

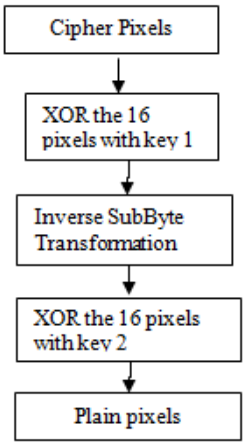

Fig 3.6: Decryption Process.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

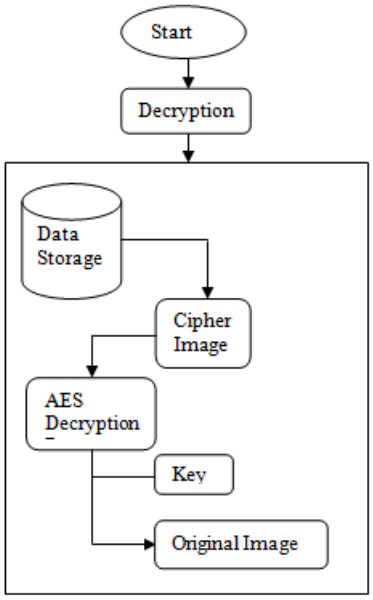

Fig 3.7: Graphical representation of Decryption Process.

V. Conclusion:

In this paper, AES Encryption algorithm is applied with pre-processing technique, which offers high encryption as well as decryption quality with minimum time period. It improves image security by splitting image into blocks o that the intruder cannot predict that the image is first split and then applying AES Encryption. The key sensitivity is very high which makes it resistant towards Brute force attack and statistical cryptanalysis.

ACKNOWLEDGMENT:

I would like to express my deepest appreciation to all those who provided me the possibility to complete this report. A special gratitude I give to the Prof. Vijay S. Karwande whose contribution in stimulating suggestions and encouragement helped me to coordinate my paper especially in writing this paper.

V. REFERENCES:

[1] Hamdan.O.Alanazi, B.B.Zaidan, .A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617.

[2] HiralRathod, Sanjay Kumar Sharma "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm", IJCTEE, Volume 1, Issue 3.

[3] Gajendra Singh, Pragna Patel "Image Encryption with RSA and RGB Randomized Images", IJAREEIE, Volume 3, Issue 5, May 2014.

[4] Saurabh Singh, Anurag Jain "An Enhanced Text and Image Encryption Technique using RGB Substitution and AES", IJETT, Volume4, Issue 5-May 2013

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES based Algorithm for Image Encryption", Volume1, Issue 3, 2007

[6] Radhadev and P. Kalpana proposed "Secure Image Encryption using AES", IJRET, Volume1, and Issue 2012.