AES based Image Encryption and Decryption using Matlab

Meghashree B. S
PG Student
Department of ECE,
Malnad College of engineeringHassan

B. R Sujatha
Head of Department
Department of ECE,
Malnad College of Engineering Hassan

***Abstract*:- Image data security is the essential portion in communication and multimedia world. During storing and sharing, avoid third party access of data is the challenge one. Providing security of data is the clever work and art also. Many protection algorithms are used in recent years. Protection may be given of a data is converting the original in to some unknown form, signals, sketch etc., which is not understand by any one. Cryptography is the best technique of image data security. In Greek, 'crypto' refers 'hidden' and 'graphy' refers 'script'. Cryptography has two processes namely encryption and decryption. Encryption achieves the conversion by possessing a key of original data into unreadable form called encoding. Restoring of encrypted data in to original is decoding or decryption. Key, code or password is the vital role in cryptography. This paper presents the performance of encryption and decryption of an image using AES algorithm and tested on image and results are shown.**

Keywords:- AES, cipher, image encryption, image decryption, MATLAB

1. INTRODUCTION

Security of image data has become increasingly important for many applications like video conferencing secure facsimile, medical, military applications etc. It is hard to prevent unauthorized people from eavesdropping in any communication system including internet. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. Thus, image information transmission has increased rapidly and image encryption technology has drawn more attention.Images are generally the collection of pixels. Encryption (sometimes called as Encipherment) is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment).With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Transmission of sensitive data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity and non-reproduction of exchanged information.

2. CRYPTOGRAPHY

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables us to store sensitive information or transmit across insecure networks, so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis invokes an interesting combination of analytical reasoning, application of mathematical tools, determination and luck. Cryptanalysis also called as attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptography can be strong or weak, its strength is measured in the time and resources, and it would require recovering the plaintext. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. A cryptographic algorithm is a mathematical function used in the encryption and decryption process. It works in the combination with a key-a word, number, or face- to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is thus entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. Cryptography includes the following process such as Encryption and Decryption.

Encryption: It is the process of converting plaintext into unreadable form called cipher text.

Decryption: It is the process of converting cipher text into readable form called plain text.

3. AES ALGORITHM

3.1 AES Encryption and Decryption

For each round of AES, 128 bit input data and 128 bit key is required i.e., it needs 4 words of key in one round thus the input key must be expanded to the required number of words depending upon the number of rounds. The output of each round serves as input to the next stage. In AES system, same secret key is used for both encryption and decryption, thus simplifies the design. For both its cipher and inverse cipher, the AES algorithm uses a round function i.e. composed from four different byte-oriented transformations:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The above four transformations are looped Nr-1 times. In the last round Mix column is not performed.

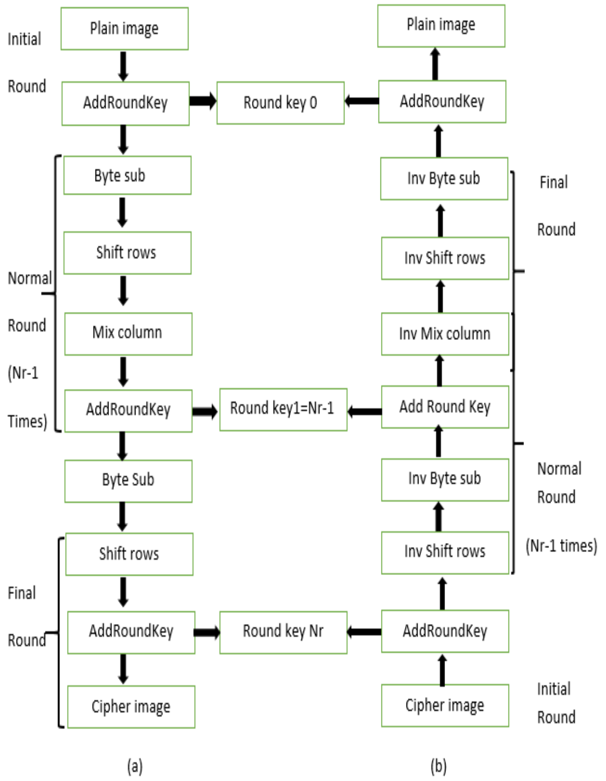


Figure 1: Design flow of AES algorithm (a) Encryption Process (b) Decryption process.

The tenth round Mix columns stage is not included. The nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

3.2 AES Transformation

3.2.1. Substitute Bytes:

It is a nonlinear byte substitution, using a substation table (S-box) each bytefrom the input state is replaced by another byte. The substitution is invertible and is constructed by the composition of two transformations as described below. The substitute bytes operation is as shown in Figure 2.

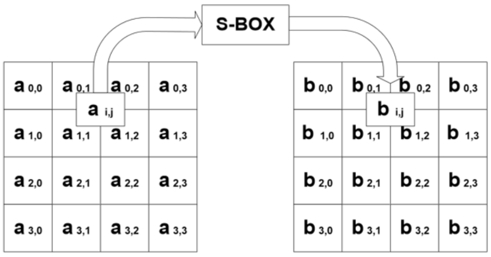


Figure.2: Substitution Bytes.

3.2.1.1 Inverse Substitute Bytes:

It is the reverse operation of the Substitute Bytes transformation, in which the inverse S-box is applied to each byte of the state. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (28).

3.2.2. Shift rows:

Shift rows operate on individual rows of the state. It provides diffusion throughout the AES algorithm. In the Shift Rows transformation, the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the left, respectively as shown in Figure 3.

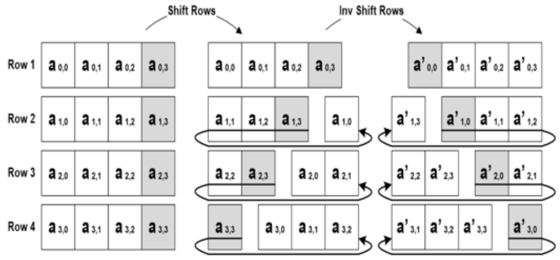


Figure 3: Shift row operation.

3.2.2.1 Inverse Shift rows:

It is the inverse of the shift rows; the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the right, respectively.

3.2.3. Mix columns:

In the Mix Columns transformation, every column of the state array is considered as polynomial over GF (28). After multiplying modulo x4+1 with a fixed polynomial a(x), the operation of Mix Column is as shown in Figure 4.

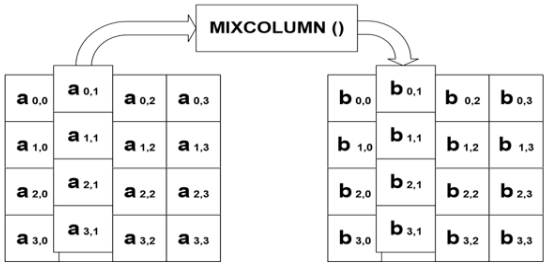


Figure 4: Mix column operation.

3.2.3.1 Inverse Mix columns:

In the Inverse Mix Columns transformation, every column of the state array is considered a polynomial over GF (28). After multiplying modulo x4+1 with a fixed polynomial

b(x), b(x) =0B*x3 + 0D*x2 +09*x + 0E

The result is the corresponding column of the output state. As it is not so straightforward hardware implementation as Mix column, so if we compare both, Inv Mix Col requires more logic resources for implementation.

3.2.4. Add round key:

The Add Round Key operation is as shown in Figure, which is asimple XOR operation between the State and the Round Key. The Round Keyis derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element: b (i, j) = a (i, j) k (i, j) Where a is the current State, b the next State and k is the round key.

$$\begin{array}{|c|c|c|c|}\hline K_{0,0} & K_{0,1} & K_{0,2} & K_{0,3} \\ \hline K_{1,0} & K_{1,1} & K_{1,2} & K_{1,3} \\ \hline K_{2,0} & K_{2,1} & K_{2,2} & K_{2,3} \\ \hline K_{3,0} & K_{3,1} & K_{3,2} & K_{3,3} \\ \hline \end{array} \otimes \begin{array}{|c|c|c|c|}\hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array}$$

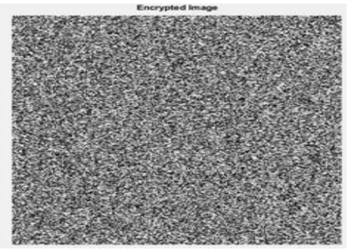
$$= \begin{array}{|c|c|c|c|}\hline B_{0,0} & B_{0,1} & B_{0,2} & B_{0,3} \\ \hline B_{1,0} & B_{1,1} & B_{1,2} & B_{1,3} \\ \hline B_{2,0} & B_{2,1} & B_{2,2} & B_{2,3} \\ \hline B_{3,0} & B_{3,1} & B_{3,2} & B_{3,3} \\ \hline \end{array}$$

Figure 5: Add round key

4. RESULTS

AES algorithm is implemented using the MATLAB platform. Here image is taken as input, applying the AES encryption algorithm creates a cipher mage and this cipher image is input to the decryption algorithm which reconstructs the original image back. Result for camera man image is as shown below.

(a) Input image



(b) Encrypted image

(c) Decrypted image

5. CONCLUSION

In this paper, Image Encryption and Decryption using AES algorithm is implemented to secure the image data from an unauthorized access. A Successful implementation of symmetric key AES algorithm is one of the best encryption and decryption standard available in market. With the help of MATLAB coding implementation of an AES algorithm is synthesized and simulated for Image Encryption and Decryption. The original images can also be completely reconstructed without any distortion. It has shown that the algorithms have extremely large security key space and can withstand most common attacks such as the brute force attack, cipher attacks and plaintext attacks.

REFERENCES

[1] Manoj. B, Manjula N Harihar, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-1, Issue-5, June 2012.

[2] Kundankumar Rameswar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra,International Journal of Emerging Trends and Technology in Computer Science(IJETICS) ISSN: 2278 6856, Volume 3, Issue 3, May June 2014.

[3] Seyed Hossein Kamali, Reza Shakerian, maysam Hedayati, Mohsen Rahamani, ANew Modi_ed Version of Advanced Encryption Standard(AES) based algorithmfor image encryption.

[4] B Subramanyan, Vivek M Chhabria, T G Shankar babu, Image Encryption BasedOn AES Key Expansion, 2011 Second International Conference on EmergingApplications of Information Technology.

[5] Komal D Patel, Sonal Belani, International Journal of Emerging Technology andAdvanced Engineering ISSN: 2250 2459, Volume 1, Issue 1, November 2011.

[6] P.Karthigaikumar, Soumiya Rasheed, IJCA Special Issue on Computational Science New Dimensions and Perspectives, NCCSE, 2011.

[7] Think Python, Allen B. Downey, ISBN 13:978-93-5023-863-9.

[8] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush A NovelImage Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm International Journal ofComputer Science Issues (IJCSI); Vol. 9 Issue 4,p41 Jul2012.

[9] Ahmad Abusukhon Mohammad Talib A Novel Network Security AlgorithmBased on Private Key Encryption IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 .

[10] Praveen.H.L , H.S Jayaramu, M.Z.Kurian Satellite Image Encryption Using AESInternational Journal of Computer Science and Electrical Engineering (IJCSEE),Vol-1, Iss-2, 2012.