International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July 2018 www.irjet.net p-ISSN: 2395-0072

A SECURE AND TIME EFFICIENT IMAGE ENCRYPTION BASED ON AES USING MODIFIED LOOK UP TABLE

KAJAL S S[1], Prof .SUMIMOL L[2]

[1,2]*Department of Computer Science & Engineering, LBS Institute of Technology for Women , Poojappura ,Thiruvananthapuram ,India*

Abstract-*importance of images is increasing in people's day to day life, it is essential to protect the confidential image data from unauthorized access. The main objective of this work is to improve the security of images during communication. The proposed method uses Advanced Encryption Standard (AES) in Cipher Block Chaining Mode (CBC) to encrypt each block sequentially. Image encryption in AES–CBC mode currently uses a look up table method. It is a dynamical mapping of each block of the plain image using a pseudo code. In this work using a modified lookup table method is used to implement the AES algorithm rapidly in which finding of repeated patterns from the created look up table was done. This image cryptosystem, in the encryption phase the plain image is divided into various blocks each having size of 128bits. These blocks are encrypted with a secret key of size 256 bits in a domain of AES. Finally the secret key, modified lookup table and ciphertext are transmitted to the receiver through the public information channel. The decryption phase uses the secret key and modified look up table to decrypt the ciphertext to obtain the plain image.*

***Key Words*: AES, Cipher Block Chaining (CBC), Image Encryption, Look up table, Modified Look up Table.**

1. INTRODUCTION

With the fast evolution of digital communication methods, the security of information becomes more important in communication.Therefore we need to securely transfer images between secure transmissions over unsecured channels. In recent years there was a steady growth in the field of Image Encryption. Image encryption is a technique which provides security to images by converting the original image into an unreadable format that cannot be easily understood, thereby keeping it confidential between users. However, due to some special features of digital images such as huge data capacity, high redundancy and strong correlation among adjacent pixels, these traditional image encryption techniques are not very much suitable for image encryption[5]. The image encryption based on AES in CBC mode gives better image encryption.

Various algorithms have been proposed to encrypt and decrypt images. For this purpose various security algorithms like AES, DES, IDEA, Triple DES [2], etc. are used for encrypting and decrypting the image. To overcome the drawbacks of these algorithms, a secure mechanism based on Advanced Encryption Standard (AES) in CBC Mode [4] can be used to encrypt images, it can achieve higher encryption speed than some existing image cryptosystems.

2. IMAGE ENCRYPTION

Image encryption consists of few general steps which are as follows:

1. Select the plain image to be encrypted.

2. Apply Image encryption technique for the sender: There are various techniques to encrypt an image, which scrambles the plain image and generate the ciphered image as an output.

3. Apply Image decryption technique for the receiver: There are various techniques to decryption on ciphered image to obtain the plain image at the receiver end.

For image encryption process mainly two types of algorithms are used. They are symmetric and asymmetric. Symmetric cryptography use only one key for encryption and decryption. The sender and receiver of a message know and use the same secret key. The sender and the recipient must uses the (secret key) for the image encryption and the decryption. The asymmetric key cryptography uses both public key and private key [2]. The public key for encryption and private for decryption. In this work image encryption is done in the platform of symmetric key block cipher i.e. AES in CBC mode.

2.1 AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is a symmetric key block cipher published by the National Institute of standard and Technology (NIST) in December 2001.This algorithm based on the Rijndael cipher developed by Joan Daemen and Vincent Rijmen[2]. The AES is a Non Feistel cipher that encrypts and decrypt a data block of 128 bits. It supports three different key lengths of size 128,198,256 bits. In 1997 NIST replacement of DES and it is still used in world wide. The cipher consists of specific rounds, where the number of rounds depends upon key length: 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, 14 rounds for a 256-bit key.

The algorithm works on 4 x 4 matrix of bytes. AES consists of four major transformation functions: Sub bytes, Shift Rows, Mix columns and Add Round Key [2]. The final round consists

of three transformations. The Mix columns functions are not used in the final round. Each transformation takes one or more 4 x 4 matrices as input and it produces a 4 x4 matrix as output. Above four rounds are reversible, it is easy to prove that decryption does recover the plain text or image. The characteristics of AES algorithms are achieves higher encryption speed than any other cryptographic algorithms, safer and more secure encryption scheme, the block size is increased to 128 bits [2].

2.2 Cipher Block Chaining Mode (CBC)

Cipher block chaining mode is a technique used to encode and decode the information which is applied on a chunk of data. In CBC mode each plaintext block is exclusive-or with the previous cipher text block before being encrypted .when a block is enciphered, the block is sent, but a copy of it is kept in memory to be used in the encryption of the next block. A initialization vector (IV) is used [4]. CBC mode is as secure against standard attacks. CBC overcomes the security deficiency of the other mode. It more difficult for a cryptanalyst to beak the code using strategies that look for patterns in the cipher text, patterns that may correspond to the known structure of the plaintext. With this chaining scheme, the cipher text block for any given plaintext block becomes a function of all the previous cipher text blocks. The process is visualized in figure1.

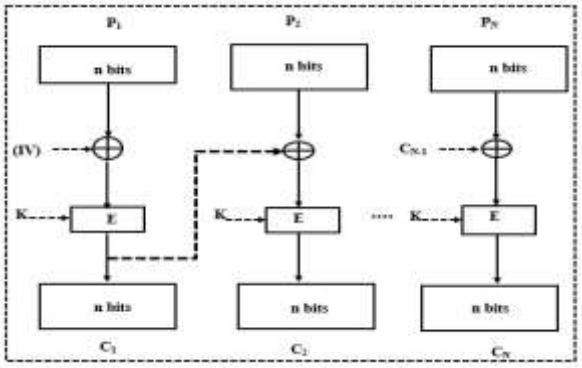
The relation between plaintext and ciphertext blocks is shown below, where E is the Encryption, P_i is the i^{th} plain text block i, K is Secret key, D is Decryption, C_i is the i^{th} Cipher text block i, IV is the Initial vector.

Encryption: C_0=IV,

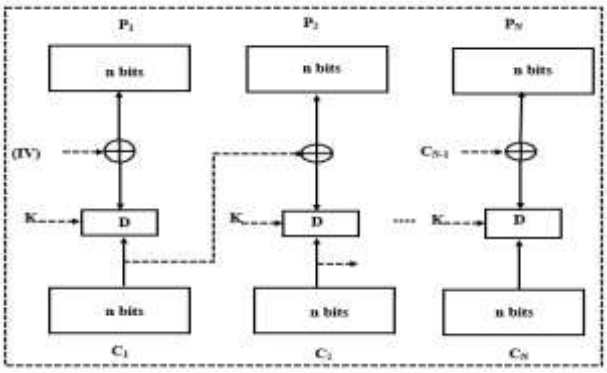
$C_i=E_K (P_i \text{ XOR } C_{i-1})$.

Decryption: C_0=IV,

$P_i=D_K (Ci) \text{ XOR } C_{i-1}$.



Encryption



Decryption

Fig -1: Cipher block chaining (CBC) mode.

3. METHODOLOGY

In the day to day life, the security of confidential images are the major concern. The traditional image encryption scheme doesn't have a time efficient and secure. The proposed method uses AES encryption method in CBC mode with an efficient look table method to overcome the attacks.

3.1 Proposed Method

With the fast evolution of digital data exchange, information security becomes much important in data storage and transmission. So image encryption is a process of encrypting the image into unreadable format. The proposed work is time efficient and secure. In this work, the plain image P is the RGB image which is encrypt using AES, the current text data encryption standard, is a block cipher. The length of each block is fixed to128 bits, whereas the key length is 256 bits. Here, AES can be fast implemented via the modified look-up table method for image encryption.

Assume that the plain image P is the RGB image have size of M xN. At first the image is preprocessed and divide P into n pieces of small blocks of length 16 bytes (i.e. 128 bits), where, n=ceil (MN/16), and ceil(x) returns the smallest integer which is greater than x. The image blocks are denoted by P_i, i=1, 2,..., n[16]. The redundant bytes in the n^{th} block is filled with 0. For faster AES encryption each blocks are replaced through a dynamic pseudo code mapping called Look up table. After image encryption secret key, Modified lookup table and the cipher text are transmitted to the receiver by public information channel. After receiving these files to decrypting the plain image successfully.

3.2 Phases of Proposed Method

In this work to implement an efficient technique to transmit an image from the sender to the receiver resisting image attacks by using AES in cipher block chaining (CBC) mode. This method is better time efficient by using a modified look up table.

In order to achieve such security standard, the proposed method consists of four phases.

- Image pre-processing phase
- Generation of Modified look up table
- Encryption phase
- Decryption phase.

3.2 Image Pre-Processing

The image processing phase, the plain image is the RGB images with size M*N. The image pre-processing consists of the following steps.

STEPS:

1. Read the Plain Image P having size M*N.

2. Display the histogram, which is the graphical representation of the pixel intensity values.

3.3 Generation of Modified Look up Table

In this phase refers to the process of converting image to binary blocks and performing XOR operations required for cipher block chaining and it consists of the following steps:

STEPS:

1. Convert the image into hex stream which forms the byte code equivalent.

Takes input in the form of pixel values of Red, Green, Blue ranging from 0 to 255 and then converts those values to hex stream.

2. Convert the hex stream values into binary form & count the number of digits in bit stream.

3. Divide the bit stream into blocks, each of size 128 bits (same as the data block size of AES) and count the number of blocks.

4. Perform XOR operation between the adjacent blocks.

5. Form a Modified Look up table.

It is an array that replaces the runtime computation. Here it is a dynamical mapping of each block by a pseudo code mapping (the combination of alphabets from A to Z and numbers from 0 to 9) randomly generated by a pseudo random function.

6. These blocks forms the base for AES encryption algorithm

3.2 Encryption Phase

In the encryption phase, the encryption process is done i.e. the replaced plain text block are encrypted using AES algorithm in cipher block chaining. It is represented in give figure 3.1

$$C_1=AES_e(K, IV \text{ XOR } P_1) \quad (3.1)$$

Here, the secret key K, IV is the initial vector which is randomly generated. AES_e represent the AES encryption algorithm, C_1 is the first cipher text. For i^{th} plain text block P_i is

$$C_i=AES\ e\ (K, C_{i-1} \text{ XOR } P_i) \quad i=2,\ldots,n \quad (3.2)$$

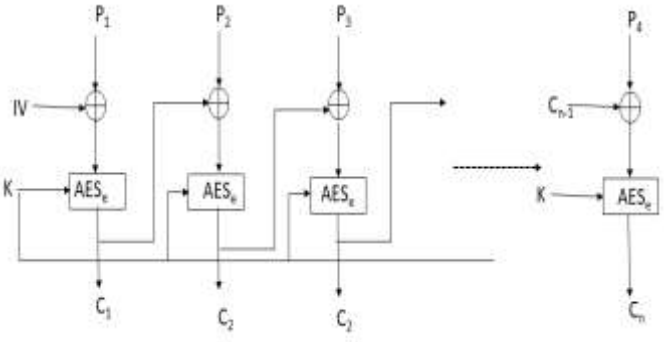


Fig -3.1: Encryption Process.

The secret key K is encrypted with each plain text block. The secret key of size 256 bit long. After encryption, the files containing cipher text of image, secret key and modified look-up table are transmitted to the receiver end.

3.3Decryption Phase

The decryption process is the inverse of encryption process. It is represented in give figure 3.2

$$P_1=AES_d(K, C_1) \text{ XOR } IV \quad (3.3)$$

Where, AES_d represents the AES decryption algorithm with the inputs of secret key K and cipher text block C_1. For the i^{th} text block C_i of ciphered text C, to decrypt it, namely

$$P_i = AES_d(K, C_i) \text{ XOR } C_{i-1},\ i=1,2,3\ldots,n. \quad (3.4)$$

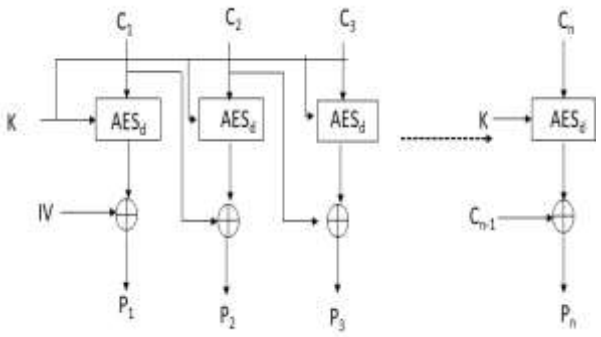


Fig -3.2: Decryption Process.

The deconstruct plain text blocks are performing inverse XOR operation .After these blocks are change into bit stream .These bits stream values converted into hex stream and finally get the original secret image.

4. EXPERIMENTAL EVALUVATION

Standard test image of size 512*512 is used to demonstrate the feasibility of proposed method.20 natural images were used to test the feasibility of proposed algorithm. The images are taken from the SIPI digital image database [8]. The proposed method is implemented and executed in Visual studio 2010 in Windows operating system with 4 GB RAM and a 2 GHz processor.

Fig -4: Lena (1. Plain Image, 2.Decrypted image).

4.1 Encryption/Decryption Time Analysis

For analyzing the results obtained, this image cryptosystem uses AES to achieve better encryption and decryption. As shown in the table 1. The proposed system with AES-CBC mode using with modified look up table method had taken less encryption and decryption time compared to AES-CBC encryption/decryption with normal look up table method. So this image cryptosystem is better than the traditional look up table method. The comparison chart 1 &2 is given below.

Table -1: Encryption/Decryption Time in ms

IMAGES (M*N)	Encryption time(ms)in LUT method	Encryption time (ms) in MLUT method	Decryption time (ms) in LUT method	Decryption time (ms) in MLUTmethod
Image 1 (512*512)	75 ms	43 ms	57 ms	10 ms
Image 2 (500*480)	91 ms	56ms	225ms	25ms
Image 3 (490*360)	63ms	39ms	47ms	8ms
Image 4 (251*201)	54ms	31ms	14ms	5ms
Image 5 (225*225)	49 ms	26 ms	9 ms	2 ms
Image 6 (300*168)	54 ms	25 ms	20 ms	5 ms
Image 7 (318*159)	52 ms	28 ms	20 ms	5 ms

Chart -1: Time Taken for Encryption

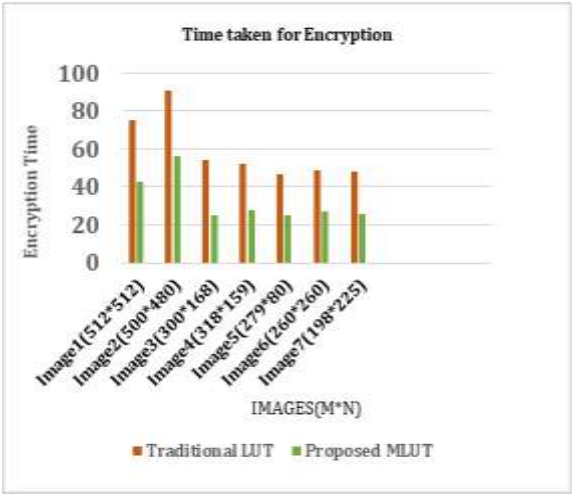
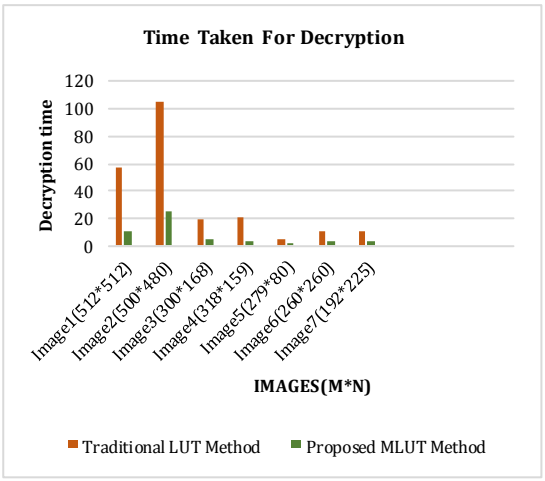


Chart -2: Time Taken for Decryption



In this work, this proposed system preserves the privacy and security assured. The secret key of size 256 bit was used in this image cryptosystem so it is secure against the brute-force attack. Also AES algorithm in CBC mode is used to encrypt and decrypt the image block. Modified look table improves the time efficiency. After decryption of the secret image, it can able to produce the image which is exactly same as the original image without any loss.

5. CONCLUSION

Image encryption is a technique that provides security to images by converting the original image into an unreadable format that cannot be easily understood, thereby keeping it confidential between users. In this paper, the image encryption based on AES in CBC mode was used for ensuring security. So by using AES-CBC mode with a modified look up table technique, we can construct an image cryptosystem which is more secure and time efficient. The experimental analysis shows that the AES-CBC mode with a modified look

up table method is faster and secure than the current encryption methods.

REFERENCES

[1] Yong Zhang, Xueqian Li, Wengang Hou, "A Fast Image Encryption Scheme Based on AES ", IEEE 2nd International Conference on Image, Vision ,and Computing vol 3, feb2017.

[2] D. Aruna kumari M. Chandrika and B. Surekha Ratnam Bharadwaj,"Magnified Cipher Block Chaining Mode using DES to Ensure Data Security in Cloud Computing", Journal of Science and Technology, Vol 9,mar 2016.

[3] K.W.Wong, "A fast chaotic cryptographic scheme with dynamic look-up table,Phys.Lett. vol. 298,jan 2012 pp. 238- 242.

[4] Y. Tsai, Y. Huang, R. Lin, and C. Chan, "An Adjustable Interpolation based Data Hiding Algorithm Based on LSB Substitution and Histogram Shifting", *International Journal of Digital Crime and Forensics*, vol. 8,dec 2016 no. 2, pp. 48–61.

[5] X. Wang, and Q. Yu," A block encryption algorithm based on dynamic sequences of multiple chaotic systems," Commun. Nonlinear Sci. Num. Simul., Vol. 14,sep 2009 pp. 574_81.

[6] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurc. Chaos,Vol. 8,feb 2007 pp. 1259_84.

[7] Lin QZ, Wong KW, Chen JY, " An enhanced variable-length arithmetic coding and encryption scheme using chaotic maps". J Syst Softw vol86, aug 2013:1384–1389.

[8] Allan G Weber The usc-sipi image

[9] PravinKawale,AvinashHiwase,MedKarimAbdmouleh"Modified Advanced Encryption Standard", International journalofSoft computing and Engineering(IJCSE),volume-4,feb 2014.

[10] C.Gayathri and V. Kalpana, "Study on image cryptography techniques", International Journal of Engineering and Technology (IJET), vol. 5, no. 2,mar2013 pp. 572–577.

[11] R. Chandramouli, M. Kharrazi, and N. Memon, "Image steganography and steganalysis: concepts and practice", Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 2939,sep 2004pp. 35–49.

[12] J.Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurc. Chaos,* Vol. 8,jan 2007 pp. 1259_84.

[13] G. R. Chen, Y. B. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps,"Chaos Solitons Fractals, Vol. 21 ,2004 pp. 749_61.

[14] Y. Tsai, Y. Huang, R. Lin, and C. Chan,"An Adjustable Interpolation based Data Hiding Algorithm Based on LSB Substitution and Histogram Shifting", International Journal of Digital Crime and Forensics, vol. 8,2016 no. 2, pp. 48–61.

[15] Yuen, C.-H., Wong, K.-W, "A chaos-based joint image compression and encryption scheme using DCT and SHA-1". Appl. Soft Comput vol 11,2011 5092–5098.

[16] Cai GL, Tan ZM, Zhou WH, Tu WT , "Dynamical analysis of a new chaotic system and its chaotic control". Acta Phys Sin,vol 56,2007:6230–6237.

[17] P. Cheng, H. Yang, P. Wei, and W. Zhang, " A fast image encryption algorithm based on chaotic and lookup table," Nonlinear Dyn., vol.79,2015 pp. 2121- 2131.

[18] G. R. Chen, Y. Mao, and C. K. Chui"A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos Soliton. Fract., vol. 21 ,2004 ,pp. 749- 761.

[19] Chao, H., Hsu, C. and Miaou, S., "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," IEEE Trans. Inf. Technol. Biomed., vol. 6, no. 1, (2002)46-53.

[20] DeVleeschouwer, C.,Delaigle, J., Macq, B., "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Trans Multimedia vol. 5, (2003) 97–105.

[21] Stallings, W. "Cryptography and Network Security—Principles and Practice". Englewood Cliffs, NJ: Prentice-Hall, 1999.

[22] Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud,M.M. "Performance Analysis of Symmetric Cryptography". pp. 1.

[23] Sunitha K, Prashanth K.S. "Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm". IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013). pp. 64.

[24] Singh Narjeet, Raj Gaurav. "Security On Bccp Through Aes Encryption Technique". International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-4, 813 – 819. pp. 817.

BIOGRAPHIES

"Kajal SS received her B. Tech degree in Computer Science and Engineering from the University of Kerala. She is now pursuing her M. Tech degree in Computer Science and Engineering from LBS Institute of Technology for Women, Thiruvananthapuram affiliated to APJ Abdul Kalam Technological University. Her areas of interest are Cryptography and Network Security."

Sumimol L, is working as an Assistant Professor in the Department of Computer Science and Engineering, LBS Institute of Technology for Women, Thiruvananthapuram affiliated to APJ Abdul Kalam Technological University. Her areas of interest are Network Security and Mobile Computing Networking.