International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 04, April 2016
www.ijates.com
ijates
ISSN 2348 - 7550

A NEW IMAGE ENCRYPTION APPROACH USING THE INTEGRATION OF A SHIFTING TECHNIQUE AND THE MAES ALGORITHM

Ms. Neha Yadav, Mr. Alok Kumar Singh

ABSTRACT

In this paper we present image encryption using Modified Advanced Encryption Standard (MAES). Encryption is a method to protect data from an unauthorized attack by using special algorithm, here modification to the Advanced Encryption Standard (AES) is done which show a high level security and excellent image encryption. This paper deal with Encryption of image using MAES. It provide great security for digital image.The image to encrypt is converted in to a matrix of scale values. The matrix is divided into sub matrices which are shuffled in a random order.This random order is serves as the shared secret between the two communicating person and then it is transmitted on a secure channel using Encryption techniques. On the receiver side sub matrices are shuffled back to original positions.

Result shows that the image encryption is highly secure and also prove that with a comparison to original AES Encryption the MAES gives better Encryption result in terms of security against hacker.

Keyword: Encryption, AES, MAES, Cryptography

I. INTRODUCTION

ENCRYPTIONAn Encryption image technique convert the original image in to an another image which is difficult to identify as the original image.The purpose is to keep the image confidential among users.With the continued growth of multimedia application security is an important issue in communication and image storage and Encrption is the best way to ensure security.

Uses of Encryption

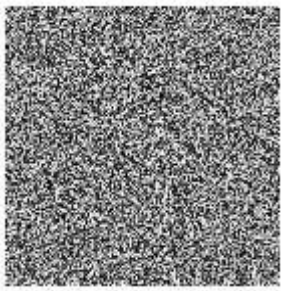
1. Military
2. Government Organization
3. Automatic Teller Machine
4. Internet, Bluetooth Devices
5. Mobile Telephones, Wireless Intercom

The current world depend on communication and internet. As a result there is a great demand of internet for exchanging the information and there is a requirement to provide security for all this information. Images play important role in multimedia data, digital images are being transferred and stored in great amounts through the internet and used in various application including military.

With the thecontinue growth of internet technology, multimedia data is being used in applications such as audio,video,images,broadcasting,viedoconferencing.Now a days multimedia data are used in daily life including

politics.Various data encryption algorithm have been used DES,AES.Most of them are used in grey scale image.It is difficult to use them directly in multimedia data. For Example , the image shown in figure 1(a) is encrypted into that shown in figure 1(b) by AES algorithm.In this figure image are of close relation which can not be removed by AES algorithm.Beside security issue,encrypted images are time consuming and not suitable for real time applications.Therefore,for this paper deals with a new encryption scheme as a modification of AES algorithm.This modification gives better security and increased performance.

Encoded Image



decoded Image

II. CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a form that only those it is intended can read.It is a science of protecting information by encoding it into an unreadable format.It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.The technology of encryption is called cryptography.The exchange of digital data in cryptography results in different algorithm that can be classified into two cryptographic mechanisms.Symmetric key in which same key is used for encryption and decryption.Symmetric key algorithms are much faster and easier to implement and generally requires less processing power when compared with assymetric key algortithms.

III. RELATEDWORK

In the past decade,as the use of images was increased, threats also increased to overcome these problems few encryption methods were also introduced to keep the image safe. But, as the technology is changing new encryption methods are developing, In the beginning, Chaotic encryption technique was introduced which was good on both images i.e. grey images and coloured images but due to its easy technology of shifting pixel from its position in horizontal and vertical direction to disorder the pixel from its position this method was easier to crack and more confusing so it is not safe to stick on one method as hackers keep them updated with current technology and this reason motivates researches to improve encryption methods time to time to beat there technology.

ChaoticMethod

This method is based on moving the complete pixel in horizontal and vertical direction based on some predefined key which is known to sender and receiver.Pixels shifts first in horizontal direction followed by vertical direction. To increase the confusing in encrypted image, horizontal and vertical shiftying performed more than one and number of time shifting is performed is kept confidential.But in this method one thing was movement of complete pixel from its position. So original color and value pixel remain same and decryption of same was not more that a tiny puzzle for hacker. So this method could not successful in image encryption.

Bitshifting

This is another method for image with shifting of pixel from its position as like in chaotc method. This method more focus on shifting of bits either left shift or right shift within pixel based on some key and this is known as secure image encryption. Shifting bits of pixel leads to change in color of pixel which creates confusion for hacker to decrypt the image but pixel movement is also necessary to increase the difficulty for decryption.Manipulation of bits value is not enough because either left shift or right shift will give the result after few treies.If pixel did not shifts from its position.

Inter pixel Displacement

In this method focus was more on the inter pixel displacement rather than just manipulation of pixel complete from its position to new position.

IV. AES

AES is Symmetric Key Algorithm that Encrypts and Decrypts the Informataion.AES is not only for text data but also applicable for images. Its original name is Rijndael. Basedon Rijndael Cipher developed by two Joan Daemen and Vincent Rijmen. Rijndael is a family of cipher with different key and block sizes. For AES, National Institute of Standards and Technology slected 3 members of the Rijndael Family, each with a block size of 128 bits, but 3 different key length : 128,192,256 bits.Aes has been adopted by the U.S. Government, and is now used worldwide.

The Advanced Encryption Standard (AES) algorithm is capable of using cryptographic keys of 128,192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. This standard is based on Rijndael algorithm. AES

algorithm used with three different key lengths, these three different are reffered to as "AES-128",AES-192", and AES-256".Encryption consists of 10 rounds of processing for 128 bit keys,12 rounds for 192 bit keys, and 14 rounds for 256 bit keys.Except last round, all other rounds are same.Each round of processing includes one single byte based substitution step,a row-wise permutation step,a column-wise mixing step and the addition of the round key.Theorde of these 4 steps are different for Encryption and Decryption.128-bit block consists 4*4 matrix.

byte0	byte4	byte8	byte12
byte1	byte5	byte9	byte13
byte2	byte6	byte10	byte14
byte3	byte7	byte11	byte15

yinvolves byte-level substitutions followed by word-level permutation.The nature of substitution and permutations in AES allows for a fast software implementation of algorithm.ForEncryption,each round consists of the following 4 steps.

1.Substitute bytes

2.Shift rows

3.Mix columns

4.Add round key

The last step consisting of xoring the output of the previous 3 steps with 4 word from the key schedule.

For Decryption,each round consists of the following 4 steps.

1.Inverse shift rows

2.Inverse substitute bytes

3.Add round key

4.Inverse mix column

The 3rdstep consists of xoring the output of the previous two steps with 4 words from the key schedule.

The Last rounds for Encryption does not involve the "mix columns" step.The last rounds for Decryption does not involve the "Inverse Mix Columns" step.

V. MODIFIEDAES

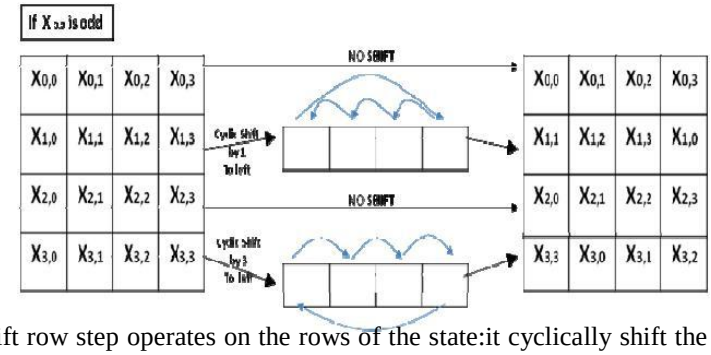
Here we use shift row phase.

Shift row phase:

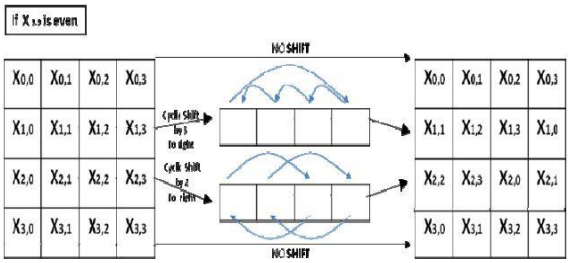
Instead of the original shift row,we modify it as:

(a) Examine the value in the first row and firstcolumn is even or odd.

(b) If it is odd,the Shift Rows Steps operates on the rows of the state ;it cyclically shifts the bytes in each row.For MAES, the first and third rows are unchanged and each byte of the second row is shifted to one to the left.Similarly,the fourth row is shifted by three to the left respectively.



(c) If it is even,the shift row step operates on the rows of the state:it cyclically shift the bytes in each row.The first and fourth rows are unchanged and each byte of the second row is shifted three to the right.Similarly, the thord row is shifted by row respectively on to the right.



This paper gives a new encryption based on modification of Advanced Encryption Standard algorithm.The modification is focused on both shift row phase.In the shift row phase, if the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. This modification allows for greater security and increased performance.

There are different encryption algorithm used to encrypt and decrypt images.There is no particular encryption algorithm which satisfies the reuirements of all image. More existing encryption algorithm are suitable for text data.However,due to the large data size and real time constraints,algorithms that are good for textual data not for multimedia data.In majority of images the values of the neighbouring pixels are strongly correlated.This means that the value of each pixel may be predicted from the values of its neighbours.

To decrease the high correlation among pixels and increase the entropy value of an image we propose a technique base on shifting the rows and the columns with in the image.By using a MSE,NPCR as measures of testing the security,the shifting process and the MAES algorithm will be expected to results and improved security level of the encrypted images.

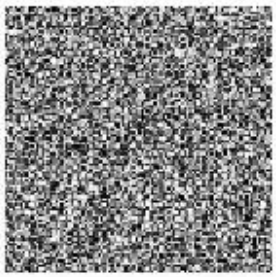
Experimental details and Results

A good encryption algorithm should be strong against all problems,includingnoise.Some experiments are given in this section to demonstrate the efficiency of the proposed technique.These are shown in table.

Technique	Time(second)	MSE	NOISE	PSNR
MAES	59.1	0.01	128	90
AES	87.09	0.9	3882	50.2

Original Image

Encoded Image



decoded Image

VI. CONCLUSION

The proposed algorithm in this paper has improved image security using an AES algorithm and MAES algorithm.To quantify the difference between the encrypted image and the plain image,three measures are used: MSE,NOISE,PSNR.The result show that a small change in the original image will result in a significant difference in the cipher image.Consequently,result show that the proposed algorithm has a high security level.It can withstand against known and choosen text, and is able to encrypt large data sets efficiently.The proposed method is expected to be useful for real time image encryption.

REFERENCES

[1] Shtewi, A.M,"AnEfficent Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems."IJCSNS International Journal of Computer Science and Network Security,Vol. 10.2 PP226-232 February 2010.

[2] Huag,C.W.,Tu,Y.H.,Yeh,H.C.,Liu,S.H.,&chang,C.J.,"Image Observation on the Modified ECB Operations in Advanced Encryption Standard.In Information Society(i-society)."2011 International Conference on,2011,PP.264-269 IEEE.

[3] Lian , S. Multimedia ,Content Encryption : Techniques and applications : CRC Press.2008.

[4] Neil F. Johnson and SushilOi Jajodia,1998,Steanalysis: The Investigation of Hidden Information Technology,PP.113-116,1998.

[5] A. Mitra , Y. V. Subbarao and S.R.M Prasanna," A new image encryption approach using combinational permutation techniques",Journal of Computer Science,Vol.1,no. 1,,2006,pp 127.

[6] William Stalling ,Cryptography and Network Security: Principles and Practices,4th ed. Prentice Hall, 2006.

[7] National Institute of Standards and Technology,"Federal Information Processing Standard Publication 197,the Advanced Encryption Standard(AES)" NOV. 2001.

[8] M. Mcone,J.V. Mc Canny, "Rijndael FPGA implementations utilizing look-up tables".,J. VLSI Signal Process,sites,34(3)(2003) 261-275.

[9] Shannon CE.,"Communication theory of secrecy system".Bell Syst. Tech J 1949; 28:656-715.

[10] G.Chen ,Y.Mao,C.K.Chui,"A Symmetric image encryption scheme based on 3D chaotic catmaps".chao,solitons& Fractals 2004;21(3):749-61.

[11] Domnik Engel Thomas Stutz, Andreas Uhl," A survey on JPEF 2000 encryption,"MultimediaSystems[online] Springer Link Verlag PP.1-29,2008.

[12] J. Daemen ,V.Rijmen,The block Cipher Rijndael,smart card Research and Applications,(2000).