International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

A New Image Encryption using Modified AES Algorithm and its Comparision with AES

Priyanka Sharma, Himani Sabharwal
Electronics & Communication Engineering
Guru Gobind Singh Indraprastha University
Delhi, India.

***Abstract*—In the present world optimisation is the only thing to be asked for. The relentless growth of Internet and Communication technologies has made the extensive use of images unavoidable. The specific characteristics of image like high transmission rate with limited bandwidth, redundancy, bulk capacity and correlation among pixels makes standard algorithms not suitable for image encryption. In order to overcome these limitations for real time applications, design of new algorithms that require less computational power while preserving a sufficient level of security has always been a subject of interest. This paper proposes an algorithm based on Modified AES Key Expansion in which the encryption process is a bitwise exclusive or operation of a set of image pixels along with the a 128 bit key which changes for every set of pixels . The keys to be used are generated independently at the sender and receiver side based on Modified AES Key Expansion process hence the initial key is alone shared rather than sharing the whole set of keys. The algorithm has been experimented with standard bench mark images proposed in USC-SIPI database. Experimental results and security analysis of the proposed algorithm shows that the proposed algorithm offers good resistance against brute force attack, key sensitivity tests and statistical crypt analysis**

Keywords—AES Key Expansion, Image Encryption, One time pads, Image confidentiality.

I. INTRODUCTION

A digital image is defined as a two dimensional rectangle array. The elements of this array are denoted as pixels. Each pixel has an intensity value (digital number) and a location address (row, column). Many applications like military image databases, confidential video conferencing, personal online photograph albums, medical imaging system, Cable TV requires a fast and efficient way of encrypting images for storage as well as in transmission. Many encryption methods have been proposed in literature, and the most common way to protect large multimedia files is by using conventional encryption techniques. Private key bulk encryption algorithms, such as Triple DES or Blowfish, are not suitable for transmission of large amounts of data. Due to the complexity of their internal structure, they are not particularly fast in terms of execution speed and cannot be applied for images in the real time scenario. Also traditional cryptographic techniques such as DES, AES, etc. cannot be applied to images due to the intrinsic properties of images such as bulk data capacity, redundancy and high correlation among pixels. Image encryption algorithms can become an integral part of the image delivery process if they aim towards efficiency and at the same time preserve the highest security level.

II. RELATED WORK

A wide variety of cryptographic algorithms for images have been proposed in the literature. Kuo [1] proposed an image encryption method known as image distortion which obtains the encrypted image by adding the phase spectra of the plain image with those of the key image. This method is safe but no image compression is considered. N.G. Bourbakis [2] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial- accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. Chin – Chen Chang [3] have used the popular image compression technique, vector quantization to design an efficient cryptosystem. The images are first decomposed into vectors and the sequentially encoded vector by vector. Fridrich [4] demonstrated the construction of a symmetric block encryption technique based on two dimensional standard chaotic map. Scharinger [5] designed a Kolmogorov flow based image encryption technique in which the whole image is taken as a block and permuted through a key controlled chaotic system. A shift register pseudo random generator is also used to provide confusion in data. Mitra [6] have used a random combinational of bit, pixel, and block permutations. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. Color image data is regarded in Zhang and Karim (1999), where a double-phase technique is utilized. Color images are encrypted from an indexed image and thereby decrypted back to its color format. The work of Wu and Kuo (2001) describes selective encryption based on a digital coefficients table. It was shown its limitation due to a less intelligible recovered image. Color and gray-scale images were considered in Koga and Yamamoto (1998), where a lattice-based extension to Visual Secret Sharing Scheme (VSSS) (Naor and Shamir, 1994) was developed. A hashing approach to image cryptography is taken in Venkatesan et al. (2000); wavelet representations of images are obtained, and a new randomized strategy for hashing is introduced. Several cryptosystems exist like as data encryption [3], steganography [14], digital signature (Aloka Sinha, Kehar Singh, 2003) and SCAN (S.S. Maniccama, N.G. Bourbakis 2004) have been proposed to increase the security of secret images. However, one common defect of these techniques is their policy of centralized storage, in that an entire protected image is usually maintained in a single information carrier. If a cracker detects

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

an abnormality in the information carrier in which the protected image resides, he or she may intercept it, attempt to decipher the secret inside or simply ruin the entire information carrier and once the information carrier is destroyed, the secret image is also lost forever.

II. PROPOSED ALGORITHM

The algorithm is based on MAES key expansion technique. Now let us see the modified key expansion technique.

A. AES Key Expansion

```
pth=im13;
 pt = hex2dec(pth);
 keyh = {'12' '4e' '15' '16' '28' 'ae' 'd2' 'a6'...'ab' 'f7' '15' '88' '09'
'cf' '4f' '3c'};
key = hex2dec(keyh);
 s = aesinit(key); %inserting key in a image
 ii=0;
% ------------------------------------------------------------------------
-
% ECB test of AES-128
 ct = aes(s, 'enc', 'ecb', pt);% encoding of image
 enc_time=toc(tstart);
 for i=1:s11(1)
    for j=1:s11(2)
       ii=ii+1;
       ct1(j,i)=ct(ii);
    end
end
ct1=uint8(ct1);
```

B. *Modifications in AES KeyExpansion*

Certain changes made in the above key expansion process improves the encryption quality, and also increases the avalanche effect in the resulting cipher image. The changes are

```
%%
pth=im13;
pt = hex2dec(pth);
keyh = {'12' '4e' '15' '16' '28' 'ae' 'd2' 'a6'...'ab' 'f7' '15' '88' '09'
'cf' '4f' '3c'};
key = hex2dec(keyh);
 s = aesinit(key); %inserting key in a image
 ii=0;
% % ECB test of AES-128
 ct = aes(s, 'enc', 'ecb', pt);% encoding of image
for i=1:s11(1)
    for j=1:s11(2)
       ii=ii+1;
       ct1(j,i)=ct(ii);
    end
end
ct1=uint8(ct1);
 pt2 = aes(s, 'dec', 'ecb', ct);
ii=0;
for i=1:s11(1)
    for j=1:s11(2)
       ii=ii+1;
       pp1(j,i)=pt2(ii);
    end
end
```

C. Steps Involved

1. *Key selection:*

The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block is 8-bits long (8*16=128 bits).

2. *Generation of Multiple keys:*

The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

3. *Encryption:*

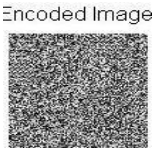
Encryption is done in spans, where we process 16 pixels in each span. We perform two XOR operations and a SubBytes Transformation for each set of pixels. Since we perform two XOR operations using our expanded key for every set of pixels it is impossible to get the key from plain image and cipher image, and to improve the non-linearity we also use the s-box values used in AES. Two XOR or Nor operations result into expansion of keys for decryption purpose.

4. *Decryption:*

The decryption process is similar as encryption, but we use Inverse SubByte Transformation and also the order of XOR operation using the expanded key is reversed.

IV. EXPERIMENTAL RESULTS

The algorithm has been implemented in MatLab 7.6.0 in windows environment with a system configuration of Intel Core i3 processor with 4 GB RAM. The proposed algorithm has been tested with various images. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute force attacks.



A. *Histogram Analysis*

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each colour intensity level.

The histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption.

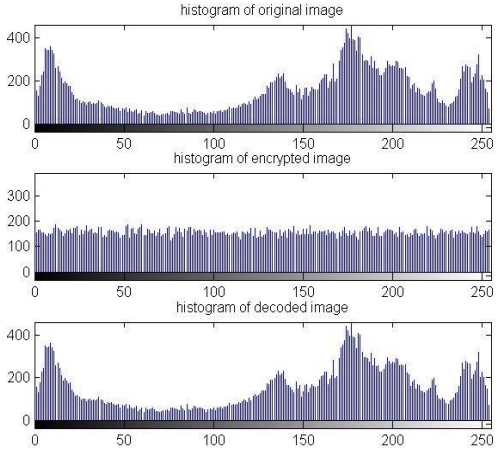
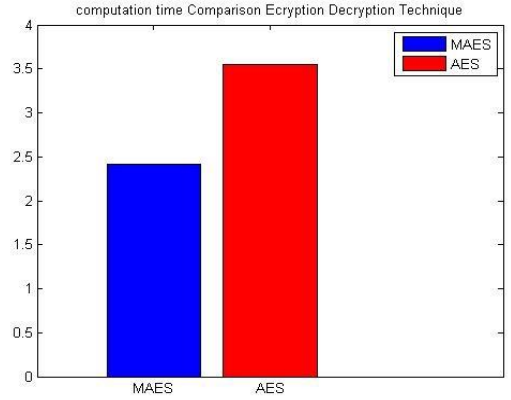
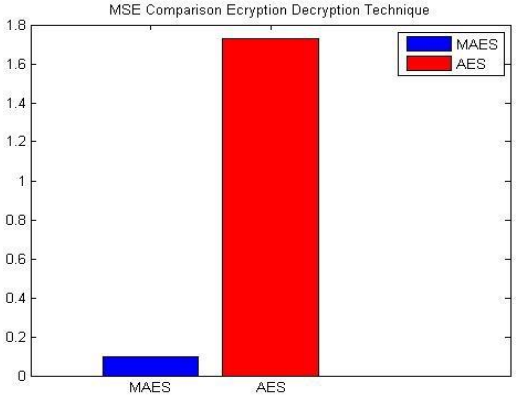


TABLE I ANALYSIS

AES ALGORITHM	MAES ALGORITHM
Noise : 69397.000000 MSE : 1.734925 PEAK : 255.000000 PSNR : 45.737997 NC : 0.998100 enc time : 34.112637 dec time : 4.460517 Entropy : 5.114933 total time of execution 43.058996	noise = 0 MSE =1.0000e-003 peak = 255 PSNR = 78.1308 Total time taken 5.641608





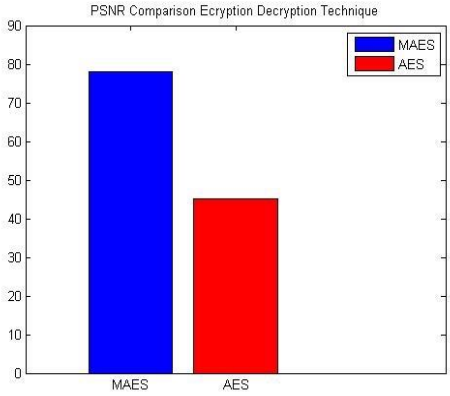


Fig. Pictorial comparision between AES and MAES Algorithm

V.CONCLUSION

In this paper a new modified version of AES, to design a secure symmetric image encryption technique, has been proposed. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms. Detailed analysis has shown that the new scheme offers high security, and can be realized easily in both hardware and software. The key stream generator has an important influence on the encryption performance.

ACKNOWLEDGMENT

I would like to thanks my mentor and teacher Mr. Akash Tayal (E.C.E. Dept., GGSIP University, Delhi) for his constant guidance and support to develop this paper.

REFERENCES

[1] C.J.Kuo, Novel image Encryption Technique and its application in progressive transmission. Journal of Electron imaging 24 1993 pp 345-351.
[2] N.J.Bourbakis , C.Alexopoulos, Picture data encryption using SCAN patterns. Pattern Recognition 256 1992 pp567 -581.
[3] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, “A new encryption algorithm for image cryptosystems”, The Journal of stemsand Software 58 (2001), 83-91.
[4] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (1998) (6), pp. 1259– 1284.
[5] J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, J. Electronic Eng 7 (1998) (2), pp. 318–325.
[6] Socek, S. Li, S. S. Magliveras, and B. Furht, Enhanced 1-D chaotic key-based algorithm for image encryption, IEEE/CreateNet SecureComm, pp. 406-408, September 5-9, 2005
[7] Mitra, Y. V. Subba Rao, and S. R. M. Prasanna, A new image encryption approach using combinational permutation techniques, International Journal of Computer Science, vol. 1, no. 2 , pp. 1306-4428, 2006.
[8] R. Ramasamy, et al., A new algorithm for encryption decryption for field applications, Computer Standards & Interfaces doi:10.1016/j.csi.2008.09.037,2008.
[9] J.C Yen, J.I Guo, A new image encryption algorithm and its VLSI architecture in proceedings of IEEE workshop signal processing ystems, 1999 pp 430-437.
[10] N.K.Pareek, Vinod Patidar, K.K.Sud Image Encryption using chaotic logistic map image and Vision Computing ,24 pp 926-934 N. Bourbakis, A. Dollas, Scan-based compression-encryption hiding for video on demand. *IEEE Multimedia Mag*. 10, 79–87, 2003.
[11] A. Canteaut and E. Filiol, "Ciphertext Only Reconstruction of LFSRbased Stream Ciphers ", Institut national de recherche en informatique et en automatique (INRIA), Technical report No 3887, Feb. 2000 Theme 2.
[12] H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. *IEEE Trans. Signal Process.* 48 (8), 2439–2451, 2000.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

[13] J. Daemen, V. Rijmen, "The block cipher Rijindael", *Proceedings of the Third International Conference on smart card Research and Applications*, *CARDIS'98*, Lecture Notes in computer Science, vol.1820, Springer, Berlin, 2000, pp.277_284.

[14] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Wagner, and D. Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *Proceedings of Fast Software Encryption – FSE'00*, number 1978 in Lecture Notes in Computer Science, pages 213–230. Springer-Verlag, 2000.

[15] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.

[16] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the Encryption algorithm and AES".