Image Encryption Based On AES Key Expansion

B.Subramanyan*, Vivek.M.Chhabria*, T.G.Sankar babu*
*Student, Department of Information Technology, Thiagarajar College of Engineering, Madurai, India
becks.subbu2@gmail.com

***Abstract*— 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 AES Key Expansion in which the encryption process is a bit wise 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 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.

III. PROPOSED ALGORITHM

The algorithm is based on AES Key Expansion technique. Now let us see the AES Key Expansion in detail.

A. AES Key Expansion

Pseudo code for AES Key Expansion: The key-expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates $4x(N_r+1)$ words. Where N_r is the number of rounds.

The process is as follows

- The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k_0 to k_{15}). The first four bytes (k_0 to k_3) become w_0, the four bytes (k_4 to k_7) become w_1, and so on.

978-0-7695-4329-1/11 $26.00 © 2011 IEEE
DOI 10.1109/EAIT.2011.60

- The rest of the words (w_i for i=4 to 43) are made as follows
  - If (i mod 4)!=0, $w_i = w_{i-1} \oplus w_{i-4}$.
  - If (i mod 4)=0, $w_i = t \oplus w_{i-4}$. Here t is a temporary word result of applying SubByte transformation and rotate word on w_{i-1} and XORing the result with a round constant.

Pseudo code for AES Key Expansion:

```
Key Expansion (byte key[16], word w[44])
{
  word temp
   for (i = 0; i < 4; i++)
   w[i] = (key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]);

   for (i = 4; i < 44; i++)
   {
    temp = w[i-1];
    if (i mod 4 = 0)
    temp = Sub Word (Rot Word (temp)) ⊕ Rcon [i/4];
    w[i] = w[i-4] ⊕ temp;
   }
}
```

Where,

Sub Word: SubBytes Transformation table(S-Box) value for the Word.

Rcon: Round Constant used in AES Algorithm.

Rot Word: Rotate Word (circular left shift of 8bits).

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

- The initial key is not only expanded for 10 rounds as in AES process, but it is expanded based on the number of pixels in the image.
- The Rcon value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.
- Both the s-box and Inverse s-box are used for the Key Expansion process which improves non-linearity in the expanded key and also improves the encryption quality.
- We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key this improves the key sensitivity.

The above changes in the algorithm can be represented as

1) Key Expansion for the image

Let P be the plain gray-level image of size mxn. So we have m*n pixels in the image. We encrypt a set of 16 pixels (128 bits) using 2 round keys. So the number of keys to Encrypt the whole image N=2*{(m*n)/16}.

2) Formation of Rcon values

Rcon [0]=key[12:15]; Rcon [1]=key[4:7];
Rcon [2]=key[0:3]; Rcon [3]=key[8:11];

3) Using Inverse S-Box for key expansion

The 'temp' value used in the algorithm is formed as

temp = SubWord(RotWord(temp)) ⊕ InvSubWord(Rcon[i/4]);

Where InvSubWord: InverseSubByte transformation table value

4) Shifting of S-box and Inverse S-box

Sbox_offset = sum(key[0:15])mod256;
Inv_Sbox_offset = (sum(key[0:15])*mean(key[0:15]))mod256;

The initial key is represented as blocks key[0],key[1],..,key[15]. Where each block is 8bits long (8*16=128 bits).

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 8bits 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.

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.

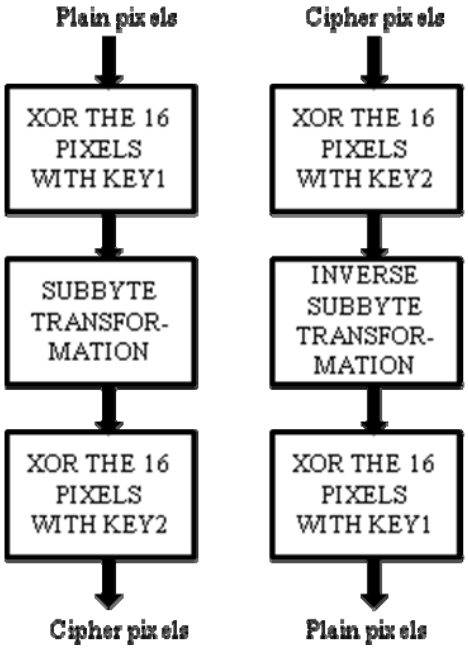
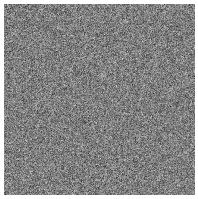


Figure 1. Block diagram for encryption and decryption process

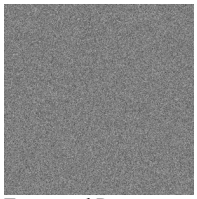
IV. EXPERIMENTAL RESULTS

The algorithm has been implemented in Mat Lab 6.0 in windows environment with a system configuration of PIV processor with 1 GB RAM. The proposed algorithm has been tested with various images in USC-SIPI repository which is a collection of digitized images primarily to support image processing, image analysis and machine vision. (http://sipi.usc.edu/database/). A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute force attacks.


Bridge


Encrypted Bridge


Pentagon


Encrypted Pentagon


Lena

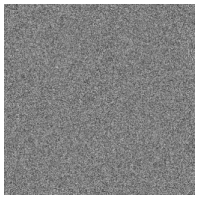

Encrypted Lena

Figure 2. Original and Encrypted Image samples

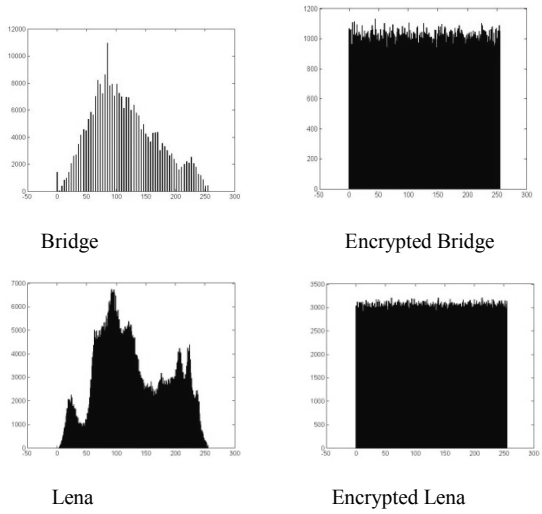
A. *Key Space Analysis*

The strength of any cryptographic algorithm depends upon key space which should be sufficiently large enough to make brute force attack infeasible. The proposed algorithm has a huge key space which is 2^128 possible keys. If an opponent tries for brute force attack, since the key sensitivity of this algorithm is very high he would have to try all combinations of keys for the image which is computationally infeasible.

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

Fig 3. Shows the histogram analysis of plain and original images. The histogram analysis shows that the histogram of the cipher image is fairly uniform and is significantly different from the original image. The encryption algorithm has covered up all the characters of the plain image and has complicated the statistical relationship between the plain image and its ciphered version.


Bridge Encrypted Bridge

Lena Encrypted Lena

Figure 3. Histogram analysis of plain and encrypted images

C. Key Sensitivity Analysis

High key sensitivity is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly even if there is only a slight difference between encryption or decryption keys. The proposed algorithm is experimented for various key values whose difference is negligibly small. This is similar to avalanche effect in text encryption where a small bit difference in the key could produce a significant difference in the cipher text produced. The strength of the algorithm is that even for a single bit change in the key value the image is not decrypted. Fig 4. Illustrates the key sensitivity of the proposed algorithm.

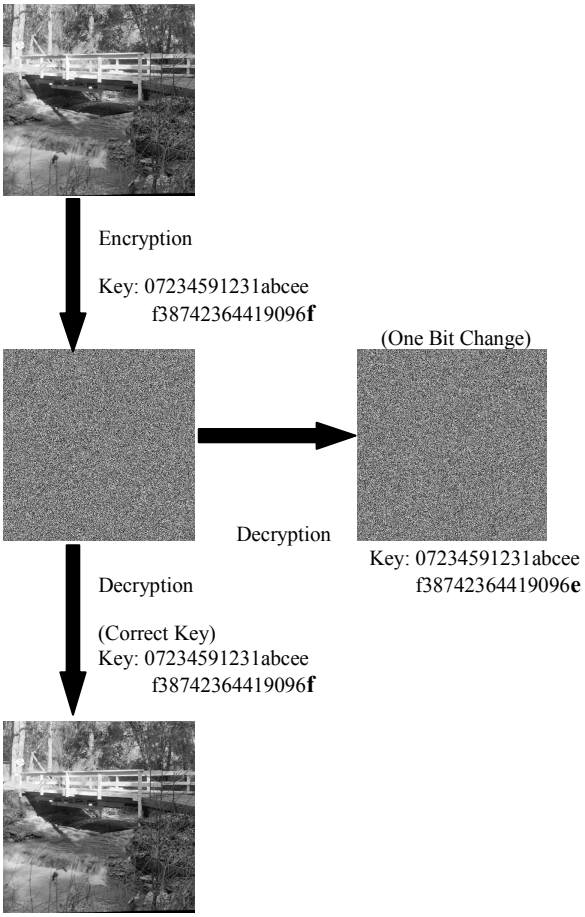


Figure 4. Key Sensitivity of the proposed Algorithm

D. Execution Time

Another important factor that evaluates the efficiency of algorithms is measuring the amount of time required to encrypt an image. The key generation is a one time process and the time taken for Lena image is 2.8146 seconds. These expanded keys can be used for future communications until they change their initial key. In this investigation, actual time in CPU cycles will be used as a measure of execution time.

TABLE I
COMPUTATIONAL TIME COMPLEXITY ANALYSIS

Algorithm	***Lena** (time in seconds)*
Socek[6]	*1.05*
Bourbakis[2]	*2.54*
Mitra[7]	*1.82*
Proposed Algorithm	*1.41*

V. CONCLUSION

The work proposed in this paper makes use of AES Key Expansion which is used to generate multiple non-linear keys for the encryption process. Based on the experimental results it can be observed that the proposed algorithm offers high encryption quality with minimal memory requirement and computational time. The key sensitivity and key space of the algorithm is very high which makes it resistant towards Brute force attack and statistical cryptanalysis of original and encrypted images. The time taken for encryption is relatively less in comparison with the algorithms proposed in the literature. The above mentioned features make the algorithm suitable for image encryption in real time applications.

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 Systems and 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 2006