International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Image Encryption Using AES with Modified Transformation

Harleen Kaur[1], Reena Mehla[2]

[1]Student, Department of Electronics & Communication, Kurukshetra University, India
[2]Assitant Professor, Department of Electronics & Communication, Kurukshetra University, India

Abstract: ***With the increased growth of internet, extensive exchange of data over the network has been made. Safe storage of digital images and secure transmission over the network is always been required, so as to protect the confidential data from unauthorized access. High transmission rate of the images using limited bandwidth makes the standard algorithms unsuitable for encryption. The work proposed in this paper is focussed on a new algorithm, which requires less encryption time, less computational power requirement and maintain a sufficient level of security. This paper proposes a modified version of AES. Various modifications have been made in the transformation steps of AES. Experimental results for encryption time using proposed AES have been shown and compared with original AES.***

Keywords: Advanced Encryption Standard (AES), Image Encryption, Computational time analysis, Modified mixing column transformation, Modified shift row transformation

1. Introduction

With the development of internet technology, applications such as multimedia data, video conferencing, broadcasting are being used more and more. For image security, encryption is used. Various algorithms for encryption have been proposed such as AES, RSA, IDEA [1, 2]. These algorithms are mostly used in text data. For multimedia data these algorithms are not suitable for real-time applications. This paper proposes a new modified version of AES algorithm. The modification is made on the various transformation steps in AES algorithm. Basically the modification is focussed on Shift row transformation, mixing column transformation and key expansion modification.

2. AES Algorithm

AES algorithm uses three cryptographic keys of 128, 192, 256 bits and accordingly AES is referred to as AES-128, AES-192, AES-256, operates in 10 rounds. At the beginning of encryption, the input bytes are mapped to state array. In the end, the final value is mapped to output array bytes.

AES has the following transformation steps:

1. Sub Byte Transformation
2. Shift Rows Transformation
3. Mix Column Transformation
4. Add Round Key Transformation

A. Sub Byte Transformation
In this step each byte of state is substituted using S-box, which is constructed by multiplicative inverse and affine transformations. Here S-box is used as a look up table.

B. Shift Rows Transformation
In this step the bytes are shifted cyclically to the left. The first row is kept un-shifted. Second, third and fourth rows are shifted cyclically 1, 2, 3 bytes to the left respectively.

C. Mix Column Transformation
This transformation step operates on state column-by-column. Each column is treated as a four term polynomial. Every column is considered as GF (2^8) polynomial and multiplied by polynomial a(x) modulo x^4+1, where a(x) = $\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$

D. Add Round Key Transformation
In this step simple XOR operation is done between each byte of state and each byte of sub key.
Key expansion transformation: AES algorithm takes the encryption key and performs a key expansion transformation to generate sub keys. Key expansion generates 11 sub key arrays of 16 words of 8 bits denoted by w_i (except w_0), previous w_{i-1}, Rcon and S-box are used.

Rcon[i]=[RC[i],0,0,0] with RC[1]=2*RC[i-1]

Table 1: Rcon Values

i	RC[i]
1	01
2	02
3	04
4	08
5	10
6	20
7	40
8	80
9	1b
10	36
11	6c
12	d8
13	a6
14	4d

Above table shows the different round constant values for RC[i], i=1 to 14

3. Related Work

Pankesh [1] proposed pixel shuffling method for encryption of grey scale images. The idea so proposed is simple and provides acceptable security level. Security of information is the main aim of the electronic data exchange. Security of coloured images is a difficult process. Sesha pallavi [2] proposed a new image encryption method based on random pixel permutation. With the advancement of technology, use of internet has been increased. For confidential transmission of data a strong algorithm is required. Subramanyam [3] demonstrated a new algorithm based on AES key expansion. This algorithm is a modified version of AES. In this encryption is done by performing XOR between the set of image pixels and 128 bits key. For every set of pixels, the key changes, this modified algorithm gives high sensitivity. For confidential video conferencing and confidential data transmission, it is required to use a strong algorithm. Kamali [4] proposed a modification in AES. The modification is done by adjusting shift row transformation. This modified algorithm gives better results in terms of security or external unauthorized attacks. Chin-Chen Chang [5] proposed an efficient cryptosystem that makes the use of image compression technique and vector quantization. Fridrich [6] presented a encryption technique based on two dimensional standard chaotic map. Mitra [7] used combination of bit, block and pixel permutations. Permutation of pixels and blocks gives high level of security.

4. Proposed Work

With the increased use of internet and transmission of images over the network, for confidential video conferencing and secure data transmission, the system demands a strong algorithm. The proposed work is focussed on modifying the original AES so that the encryption computational time requirement decreases but the level of encryption remains maintained. The modification is done on the shift row transformation, mix column transformation and key expansion transformation steps of AES.

Modified shift rows transformation:

In proposed AES, if the first element of state array is even, than the shifting is same as that of original AES. But, if the first element of the state array is odd, than first and fourth rows of the state array are kept un-shifted and second and third rows are shifted cyclically one and two bytes to the left.

Modified key expansion transformation:

In proposed AES the Rcon value is not constant but it is formed from initial key itself. This improves the reliability of algorithm.

Modified mix column transformation:

In proposed AES transpose of state matrix is taken before applying mixing column operation.

5. Experimental Results

The proposed algorithm has been tested for various images of different sizes.

Beach Scene Encrypted Beach Scene

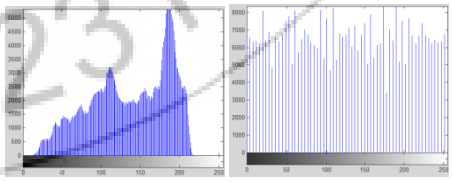
Sunflower Encrypted Sunflower

Toy Encrypted Toy

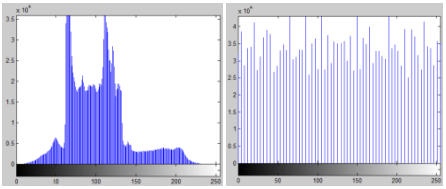
Figure1: Original and Encrypted Image Samples

A. Histogram Analysis

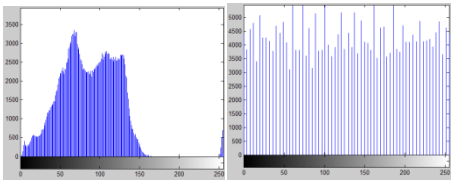
For security of information in the image it is required that the encrypted image bears little or no statistical similarity with the original image. Histogram of the image illustrates how the pixels of the image are distributed. Histogram of the encrypted is fairly uniform and different from the histogram of the original image and it does not provide any information to the third person. Figure 2 shows the histogram of original and encrypted image. The encryption algorithm covered all the information of original image and complicated the relation between original image and its encrypted version.



Beach Scene Encrypted Beach Scene



Sunflower Encrypted Sunflower



Toy Encrypted Toy

Figure 2: Histogarm of Original and Encrypted Image

B. Key Sensitivity Analysis

High key sensitivity is required by cryptosystems for the security of the image so that unauthorized people could not access the information. The proposed algorithm is experimented for different keys. If there is negligible small difference in the encryption key and decryption key the decryption of the image could not be performed successfully. The strength of the algorithm is justified by, if there is even a single bit change in the encryption and decryption key, the algorithm does not perform the successful decryption. Figure 3 illustrates the high key sensitivity of the algorithm.

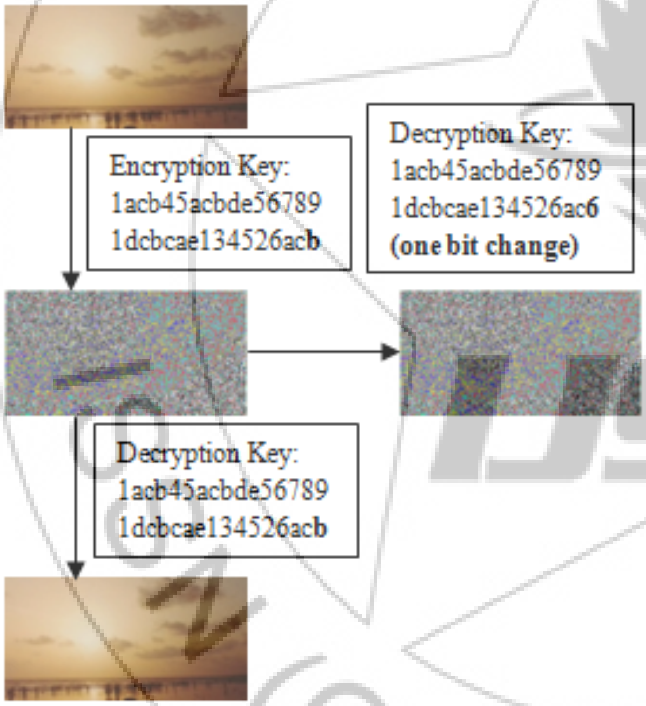


Figure 3: Key Sensitivity

C. Computational Time Analysis:

Another factor that evaluates the efficiency of the proposed algorithm is the computation time it takes for the encryption of the image. Results for the time taken for the encryption of images are considered. The algorithm is experimented for various images of different sizes and the time taken for encryption by using proposed algorithm is compared with the original AES algorithm. Experimental results show that the encryption time reduces in proposed AES.

Table 2: Encryption Time analysis

Image Size on Disk	Encryption Time (in sec) With AES	Encryption Time With Proposed AES
Toy (104 KB)	6.9554	4.3102
Beach Scene (280 KB)	8.6713	4.8913
Sunflower (760 KB)	19.0792	16.3566

6. Conclusion

The proposed work in this paper makes the use of modified AES. On the basis of experimental results it can be observed that the modified algorithm takes less encryption time than the original AES algorithm. The key sensitivity of the algorithm is also discussed, which makes the modified AES secure against brute attacks. Key sensitivity and less computation time requirement make the proposed AES with modified transformations better than the original AES.

7. Future Scope

The field of image processing is growing at a fast rate. With the ever increasing advancement in technology and revolution in image processing, it is demanded that the previous work should further be refined. The proposed work can be enhanced if the proposed AES is hybrid with DES or RSA, so that the efficiency of the algorithms can further be improved more. The proposed AES can be used to make the Wi-Fi service more secure.

References

[1] Pankesh, Image Encryption Using Pixel Shuffling, International Journal of Advance Research in Computer Science and Software Engineering, December 2012, pp. 279-282.
[2] Sesha Pallavi Indrakanti and P.S. Avadhani, Permutation Based Image Encryption Technique, International Journal of Computer Applications (0975-8887), Volume 28- No. 8, August 2011.
[3] B.Subramanyam, Vivek M. Chhabria, T.G. Shankar Babu , Image Encryption On AES Key Expansion, 2011 Second International Conference on Emerging Applications of Information Technology, pp. 217-220.
[4] Seyed Hossein Kamali, Maysam Hedayati, Reza Shakerian, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", ICEIE, Vol 1, pp. 141-145.
[5] 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.
[6] Jiri Fridrich, Symmetric Ciphers Based on Two-Dimensional Chaotic Maps, International Journal of Bifurcation and Chaos, Vol 8, 1998.
[7] Mitra, Y.V. Subba Rao and S.R.M. Parsanna, A New Image Encryption approach using Combinational Permutation Techniques, International Journal of Computer Science, Vol. 1, No. 2, pp. 1306-4428, 2006

Author Profile

Harleen Kaur, Student (M.Tech), Doon Valley Institute of Engineering and Technology, Kurukshetra University, Haryana, India.

Reena Mehla, M.Tech (ECE), Assistant Professor, Doon Valley Institute of Engineering and Technology, Kurkshetra University, Haryana, India