ISSN 2277-3061

A Modified Advanced Encryption Standard Algorithm for Image Encryption

Ari Shawakat Tahir
University of Zakho,Department of Computer Science

ABSTRACT

Cryptography algorithms are becoming more necessary to ensure secure data transmission, which can be used in several applications. Increasing use of images in industrial process therefore it is essential to protect the confidential image data from unauthorized access. Advanced Encryption Standard (AES) is a well- known block cipher that has many benefits in data encryption process. In this paper, proposed some modification to the Advanced Encryption Standard (M-AES) to increase and reaching high level security and enhance image encryption. The modification is done by modifying the ShiftRow Transformation. Detailed results in terms of security analysis and implementation are given. Comparing the proposed algorithm with the original AES encryption algorithm shows that the proposed M-AES has more security from the cryptographic view and gives better result of security against statistical attack.

Indexing terms/Keywords

Cryptography; AES; Image encryption

Academic Discipline And Sub-Disciplines

Computer Science;

SUBJECT CLASSIFICATION

Data Security, Cryptography

TYPE (METHOD/APPROACH)

AES encryption for encrypting Image,

ISSN 2277-3061

I. INTRODUCTION

Encryption is the basic method to ensure information confidentiality in a communication system. Nowadays, different algorithms are used for data encryption, with public encryption keys, like RSA (Rivest-Shamir-Adleman), or secret encryption keys, such as AES (Advanced Encryption Standard). The robustness of an encryption algorithm depends on the key length, the number of rounds, and its mathematic complexity but also on its weaknesses. AES is considered the most efficient and robust encryption algorithm of our days. It is applied on octets, on the 8-bit Galois Field GF (256)[1].

With the continuing development of both computer and Internet technology, multimedia data (images, videos, audios, etc.) is being used more and more widely, in applications such as video-on-demand, video conferencing, broadcasting, etc. Now, multimedia data is closely related to many aspects of daily life, including education, commerce, and politics. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA [2,3], most of which are used in text or binary data. It is difficult to use them directly in multimedia data, for multimedia data [4] are often of high redundancy, of large volumes and require real-time interactions, such as displaying, cutting, copying, bit rate conversion, etc.

In This paper proposes a modification of AES algorithm. The modification is focused on ShiftRow Transformations. In the ShiftRow Transformation, if the round number odd, it operates as normal ShiftRow transformation, else if the round number is even, each column are cyclically shifted bottom over different number of byte as offset. This modification allows for more security.

The rest of this paper is organized as follows: Section 2 gives brief survey of AES algorithm. Section 3 shows the proposed AES algorithm (ShiftRow transformation). Section 4 discusses the experimental results. Section 5 evaluates the performance of AES algorithm and Section 6 concludes the paper.

II. AES AlGORITHM

In cryptography, the Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. Back in 1997 the National Institute of Standards and Technology (NIST) made a public call for new cipher algorithms that could replace the DES. A rough summary of the requirements made by NIST for the new AES were the following:

- Symmetric-key cipher
- Block cipher
- Support for 128-bit block sizes

Support for 128-, 192-, and 256-bit key lengths finally in October 2000, the Rijndael algorithm was chosen as the basis for the new standard encryption algorithm. The original Rijndael algorithm also supported both fixed-size and variable-size bit cipher blocks. However, currently the Federal Information Processing Standards specification for the AES algorithm supports only the fixed-size, 128-bit blocks. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each AES cipher has a 128- bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).

In AES algorithm, the encryption step uses a key that converts the data into an unreadable ciphertext, and then the decryption step uses the same key to convert the ciphertext back into the original data. This type of key is a symmetric key; other algorithms require a different key for encryption and decryption. Generally speaking, the strength of an encryption byproduct ciphers can be heightened by increasing the number of rounds used to process the data. The AES standard specifies that the number of rounds is determined by the length of the cipher key, as shown in Table 1.

Table 1. Key Length and the number of Rounds

Key Length	Number of Rounds(Nr)
AES-128	10
AES-192	12
AES-256	14

However, The AES algorithm is divided into four different phases, which are executed in a sequential way forming rounds. The encryption is achieved by passing the plaintext through an initial round, 9 equal rounds and a final round. In all of the phases of each round, the algorithm operates on a 4x4 array of bytes (called the State). In Fig. 1 we can see the structure of this algorithm [5].

An initial XOR operation is performed between the State and the Key matrices. These atrices are then processed using two independent functions, respectively the Round function and the Key Expansion function (not represented on the figure). The Round function is executed 10 times and parameterized using the result of the Key Expansion function that

ISSN 2277-3061

generates R (1•R•10) 128-bits round keys K(R) from the 128-bits original secret key. Details of this function can be found in[6].

The Round function is composed of 4 operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. As shown in Figure 1, all rounds are identical with the exception of the final one which does not include the MixColumns transformation [7].

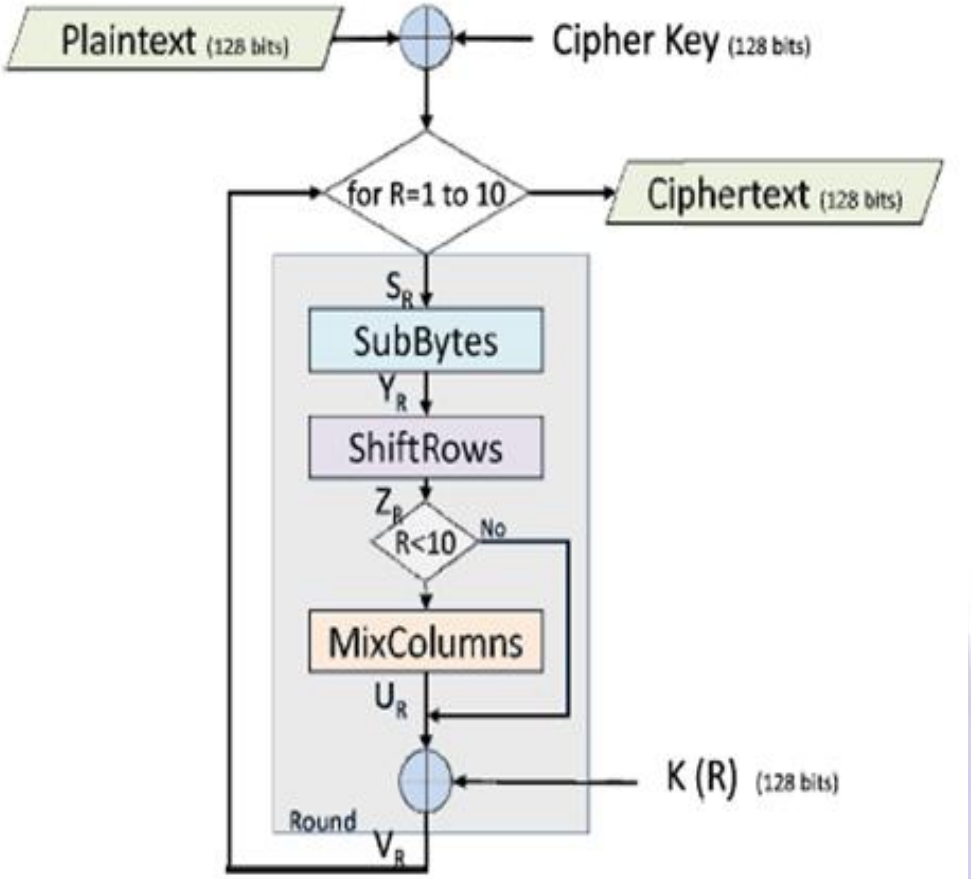


Figure 1. AES Algorithm

Let's denote S_R the *State* matrix at the beginning of every round R (1•R•10):

$$S_R = \begin{bmatrix} S_0 & S_4 & S_8 & S_{12} \\ S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \end{bmatrix} \quad (1)$$

- SubByte: A non-linear substitution step where each byte is replaced with another according to a lookup table called S-Box. The AES S-Box is a 256 entry table composed of two transformations such as multiplicative inverse in GF (2^8) and an affine Transformation. For decryption, inverse S-Box is obtained by applying inverse affine transformation followed by multiplicative inversion in GF (2^8). Where Affine Transformation is a transformation consisting of multiplication by a matrix followed by the addition of a vector[8].
- The ShiftRows: This step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset as shown in Fig. 2. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three, respectively. For the block of size 128 bits, the shifting pattern is the same. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state.[9]

ISSN 2277-3061

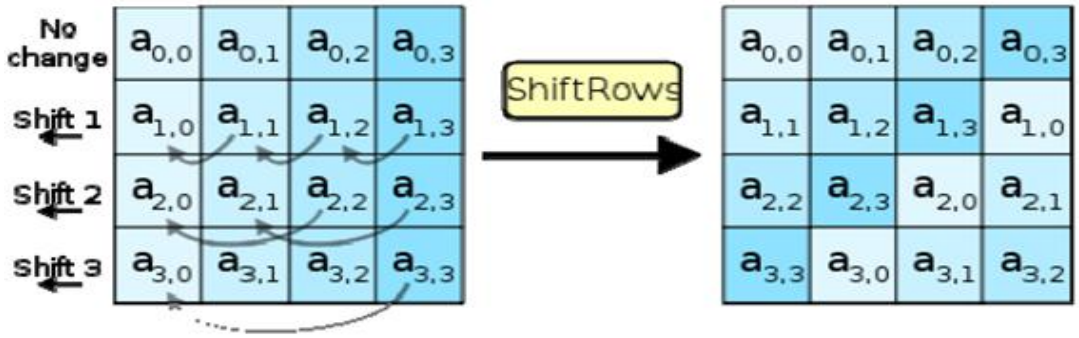


Fig 2 The ShiftRow transformation representation

- The MixColumn : In this step, the MixColumns step, the four bytes of each column of the State are combined using an invertible linear transformation as shown in Fig. 3. The MixColumns function takes four bytes as input and output, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher.[9]

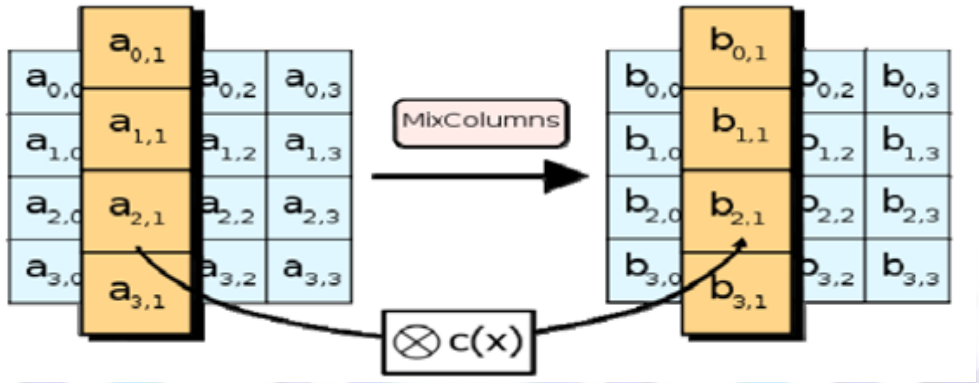


Fig 3 The MixColumn transformation representation

- AddRound Key: In this step, the subkey is combined with the State. For each round, a subkey is derived from the main key using Rijndael's key schedule where each subkey has the same size as the State. The subkey is added by combining each byte of the State with the corresponding byte of the subkey using bitwise XOR. This process is indicated in Fig. 4.[9]

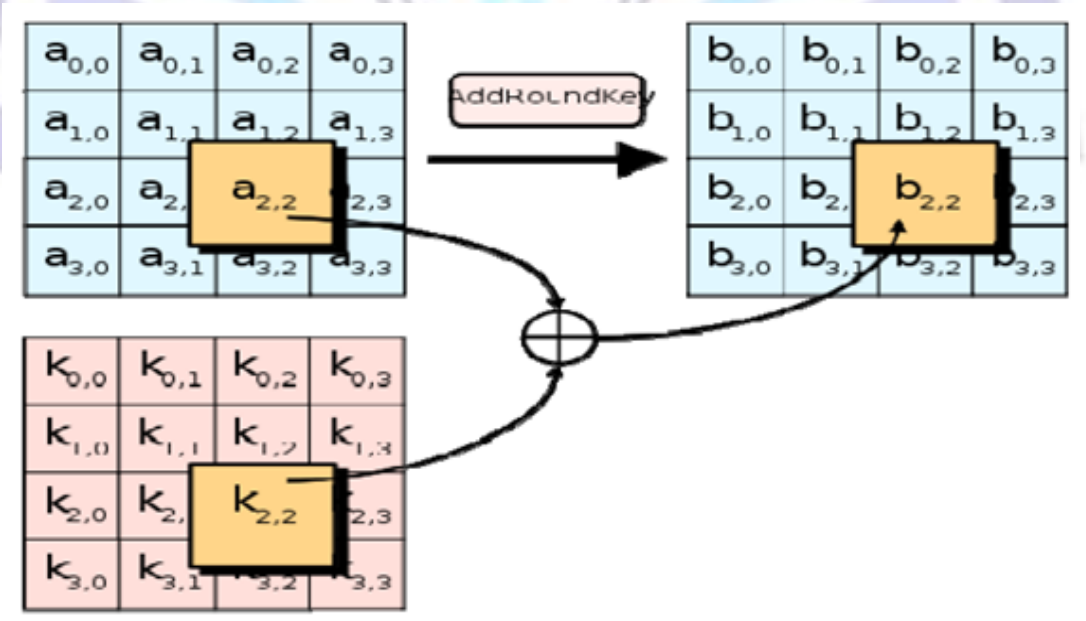


Fig 4 The AddRound Key transformation representation

ISSN 2277-3061

KeyExpansion Transformation

The AES algorithm takes the Master Key K, and performs a Key Expansion routine to generate a key schedule. The Key Expansion generates a total of 11 sub-key arrays of 16 words of 8 bits, denoted w_i , taking into account that the first sub-key is the initial key. To calculate every *wi* (except w_0) the routine uses the previous w_{i-1} and two tables, RCon and S-Box. RCon[i] contains the values given by $\{x^{i-1},\{00\},\{00\},\{00\}\}$, with x^{i-1} being powers of x (x is denoted as {02}) in the field (2^8) *GF* .[5]

III. A MODIFIED AES ALGORITHM (MAES)

The presented research modifies the AES algorithm (make modification in ShiftRow trans-formation) in order to make AES algorithm be more secure.

A. Modified ShiftRow Transformation

The proposed algorithm suggested checking the round number is odd or even:

1. When round number is odd, The ShiftRows transformation operates on the rows of the state array (as normal ShiftRow transformation); it cyclically shifts the bytes in each row by a certain offset. The first row unchanged, the second row is cyclically shifted by one to the left, the third row is cyclically shifted by tow to the left and the fourth row is cyclically shifted by three to the lift. As shown in fig 5

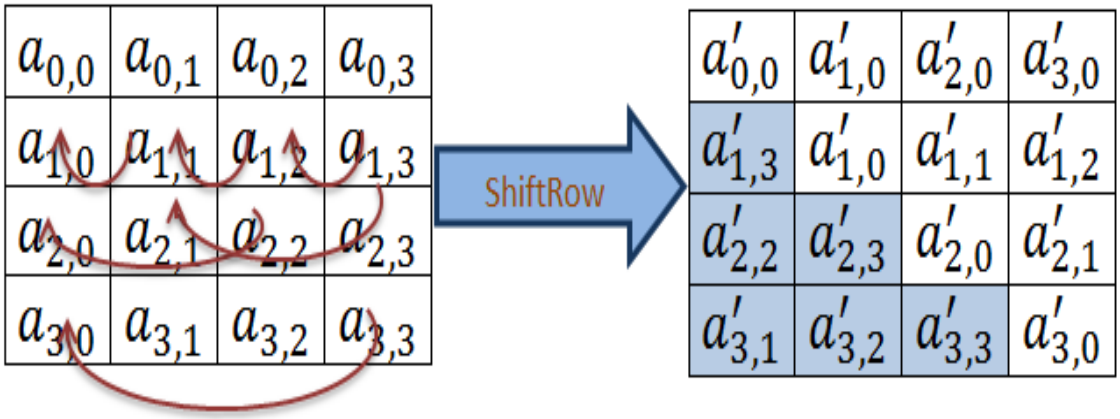


Fig 5 The ShiftRow transformation representation when Round number is odd

2. When round number is even, the ShiftRow transformation operates on the column of the state array; it shift the bytes in each column by a certain offset in circle. The first column unchanged, the second column is shift cyclically to the bottom by one byte, the third column is shifted cyclically to the bottom by two bytes and the last column is cyclically shifted to the bottom by three byte. As shown in fig 6

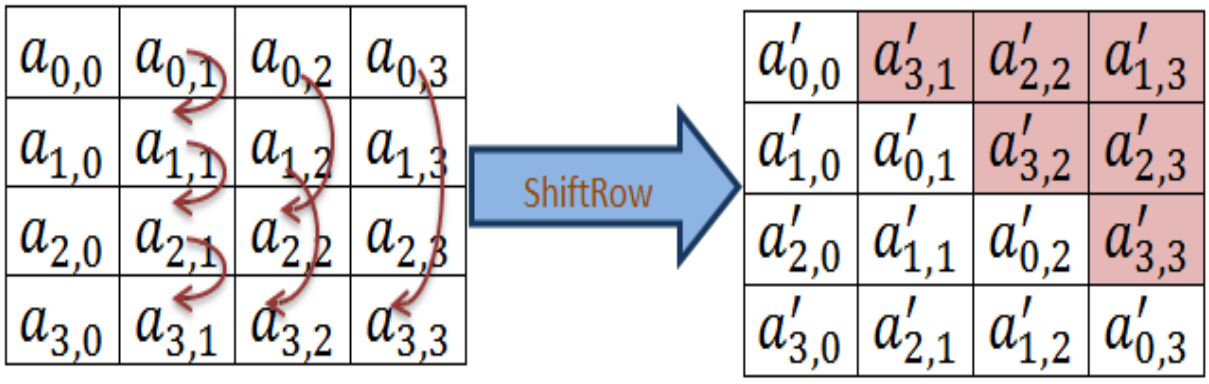


Fig 6 The ShiftRow transformation representation when Round number is odd

The pseudo code for ShiftRows transformation is as follows.

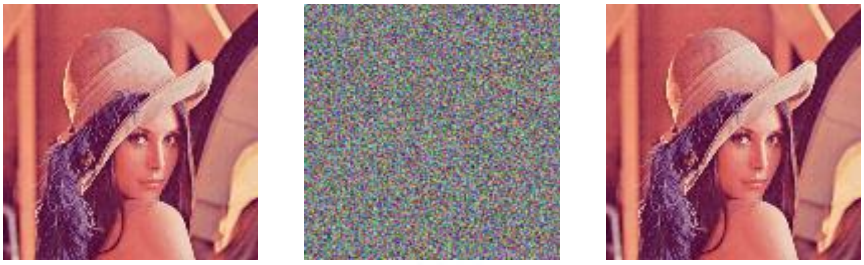
```
ShiftRows (state [4, Nb],round)
Begin
 t [Nb]
If round odd numbers
        For i = 0 to 4 loop
        If i=0
                First row unchanged
        Elseif i=1  // second row shift to left by one byte
                Set temp to state[i][0]
                For j=0 to 3 loop
                        Set state[i][j] to state[i][j+1]
                End loop
                Set state[i][j] to temp
        End if
        Elseif i=2 // third row shift to left by two byte
                For j=0 to 2 loop
                        Set temp to state[i][j]
                        Set state[i][j] to state[i][j+2]
                        Set state[i][j+2] to temp
                End loop
        End if
        Elseif i=3 // fourth row shift to left by three byte
                Set temp to state[i][3]
                For j=3 to 0 loop
                        Set state[i][j] to state[i][j-1]
                End loop
                Set state[i][j] to temp
        End if
End if

If round even number
        For j = 0 to 4 loop
        If j=0
                First column unchanged
        Elseif j=1  // second column shift to bottom by one byte
                Set temp to state[0][j]
                For i=0 to 3 loop
                        Set state[i][j] to state[i+1][j]
                End loop
                Set state[i][j] to temp
        End if
        Elseif j=2 // third column shift to bottom by two byte
                For i=0 to 2 loop
                        Set temp to state[i][j]
                        Set state[i][j] to state[i+2][j]
                        Set state[i+2][j] to temp
                End loop
        End if
        Elseif j=3 // fourth column shift to bottom by three byte
                Set temp to state[3][j]
                For i=3 to 0 loop
                        Set state[i][j] to state[i-1][j]
                End loop
                Set state[i][j] to temp
        End if
End if
```

ISSN 2277-3061

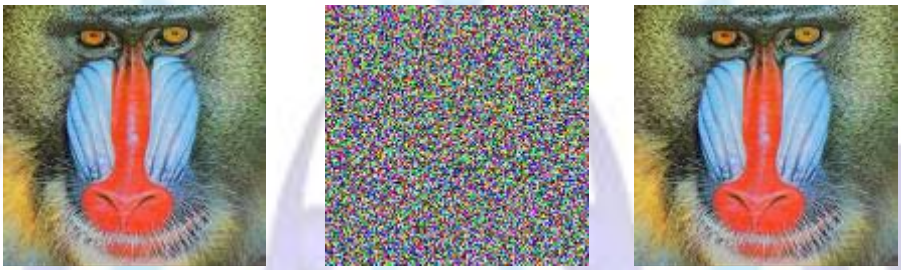
IV. EXPERIMENTAL RESULTS

The proposed modify AES encryption algorithm used to test and evaluate some bases image which uses in encryption process based on software simulation. Using some input images as the original images (plaint images) then encrypted by modified AES encryption algorithm in order to be not invisible. The encrypted images are depicted in Figs. 7b-9b. As shown, the encrypted images (cipher image) regions are totally invisible. The decrypted images are shown in Figs. 7c-9c. The figures below show the possibility of applying the proposed M-AES successfully in both encryption and decryption.



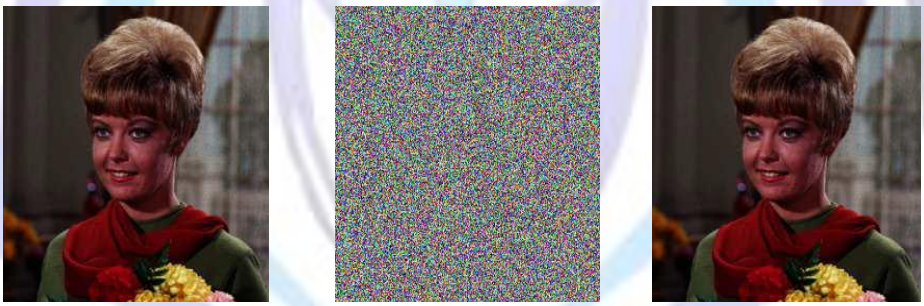
a) Original image **b) Encrypted image** **c) Decrypted image**

Fig 7. Application of the modified cipher to Lena plain image/cipher image.



a) Original image **b) Encrypted image** **c) Decrypted image**

Fig 8. Application of the modified cipher to Baboon plain image/cipher image.



a) Original image **b) Encrypted image** **c) Decrypted image**

Fig 9. Application of the modified cipher to Baboon plain image/cipher image.

I. Security Analysis By Statistical Approach

A good encryption scheme should resist all kinds of known attacks, such as known-plain-text attack, cipher-text attack, statistical attack, differential attack, and various brute-force attacks. Some security analysis techniques perform on the AES image encryption scheme, including the statistical analysis and key space analysis [10].

A. Statistical Analysis

Shannon suggested two methods of diffusion and confusion in order to frustrate the powerful attacks based on statistical analysis. Statistical analysis has been performed on the AES, demonstrating its superior confusion and diffusion properties which strongly defend against statistical attacks. This is shown by a test on the histograms of the enciphered image and on the correlation of adjacent pixels in the ciphered image [11, 12].

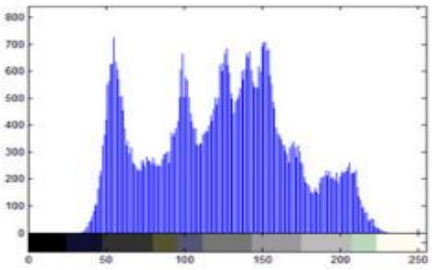
1) Histogram

An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each gray scale level. The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plain-text and should not leak any information about the plain-text or the relationship between plain-text and cipher-text.

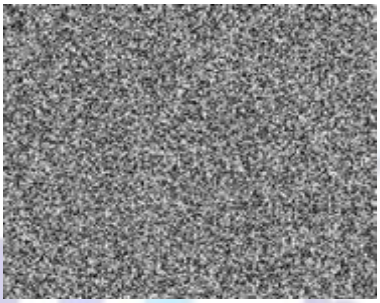
ISSN 2277-3061

The histograms of plain-image (Fig. 10(a)) and its ciphered image (Fig. 10(c)) produced by the proposed scheme are shown in Figs. 10(b) and 10(d), respectively. It's clear from Fig. 10(d) that the histograms of the cipher-image are fairly uniform and significantly different from that of the plain image and hence does not provide any clue to employ statistical attack.

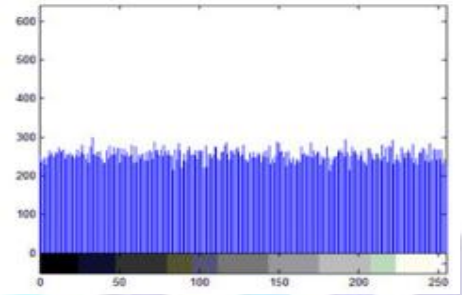
a) Original image



b) Histogram of original image



c) Encrypted image



d) Histogram of encrypted image

Figure 10 . Histograms of the plain image and ciphered image.

2) Correlation of Two Adjacent Pixels

Testing the correlation between two horizontally adjacent pixels, and two vertically adjacent pixels respectively, in a ciphered image. First, select n pairs of two adjacent pixels from an image randomly. And then the correlation coefficient of each pair uses the following formula calculated.

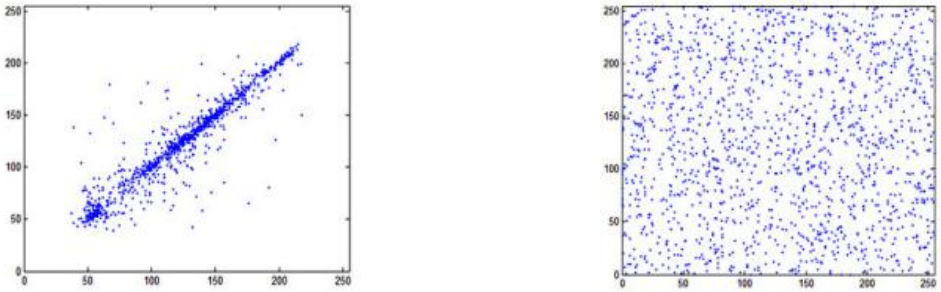
$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i - \overline{y})^2\right)}}, \tag{2}$$

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$\overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i,$$

Where x_i and y_i are grayscale values of ith pair of adjacent pixels, and N denotes the total number of samples. The results of the correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the plain-image and its cipher-image are show in Table 2 . The visual testing of the correlation distribution of two vertically adjacent pixels and the cipher image produced by the proposed scheme is shown in fig 11.

ISSN 2277-3061



(a) Plain image. (b) Ciphered image.

Fig 11 Correlation of vertical adjacent two pixels.

TABLE 2. correlation coefficient of two adjacent pixels in original and encrypted image.

Direction	Plain image	Ciphered image
horizantal	0.9404	0.0096
vertical	0.9471	-0.0614
Diagonal	0.9127	-0.0086

B. Key Space Analysis

Key space size is the total number of different keys that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [13]. The proposed encryption process uses 2128 different combinations of the secret key. Using such long key space to encrypt image is sufficient for reliable use.

C. Performance of M-AES

There are some other issues important to image cryptosystem algorithm such as running speed, particularly for real time Internet multimedia application. Some experimental tests are given to demonstrate the efficiency of our scheme. An indexed image of a "Mickey" (see Fig. 7a) is used as a plain image and encryption of this image is shown in Fig. 7b . The personal laptop used in all programs and experiments was Intel CORE i3 at 2.27GHz, with 4GB of RAM and 500 GB of hard disc capacity. Table 3 shows Performance of AES and Modified-AES $_{32/12/16}$ using CBC mode of operation.

Table 3 Performance of AES and Modified-AES $_{32/12/16}$ using CBC mode of operation.

Image size (pixels)	Image size on disk	Encryption time with AES in ms	Encryption time with M-AES in ms
256X256	192 KB	6.443	6.438
512X512	250 KB	8.638	8.630
512X512	742 KB	25.225	25.202
1024X1024	2.35 MB	76.854	76.782

V. Conclusion And Future Work

A new modified version of AES has been presented in this paper in order to design a secure symmetric image encryption technique. The proposed version does not tried to change or require any additional operations just it tried to adjust the Shift Row transformation. The modified AES tested and compared with the original AES algorithm and the results shows that M-AES gives better results in security.

In future, the proposed modify algorithm can be implemented on video in case of image as cover to hide the secret data. The algorithm can be modified to increasing speed to translating the encrypted data into decrypted and versa verse.

REFERENCES

[1] Luminița S., Petre-Daniel M., (2013), “On the Substitution Method of the AES Algorithm”, Signals, Circuits and Systems (ISSCS), 2013 International Symposium on, IEEE, 978-1-4799-3193-4.

[2] Shiguo L.,(2009), Multimedia Content Encryption: Techniques and Applications. Taylor & Francis Group, LLC, 2009.

[3] R. A. Mollin,(2006)." An introduction to cryptography", CRC Press Boca Raton FL USA.

[4]Shujun I., Guanrong C. and Xuan Z.,(2004) "Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook.

[5] Seyed H. K., Reza Sh., Maysam H. and Mohsen R.(2010), “A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption”, International Conference on Electronics and Information Engineering, IEEE, 978-1-4244-7681-7.

[6] FIPS-197 , (2001),"Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, http://csrc.nist.gov/publications/.

[7] K. Bousselam, G. Di Natale, M-L. Flottes, B. Rouzeyre, (2010), “Evaluation of Concurrent error detection techniques on the Advanced Encryption Standard”, On-Line Testing Symposium (IOLTS), 2010 IEEE 16th International, IEEE, 978-1-4244-7723-4.

[8] Sujatha Hiremath and M.S.Suma,(2009), “Advanced Encryption Standard Implemented on FPGA”, Second International Conference on Computer and Electrical Engineering, IEEE, 978-0-7695-3925-6/09.

[9] El-Sayed A. E., Waleed A. E., Amro M. and Alaa El-Din S. H.,(2007),” A New Chaos Advanced Encryption Standard (AES) Algorithm for Data Security”, institute of Electronics, Silesian University of Technology.

[10] Liu, J., B. Wei and X. Wang, (2005), “An AES S-box to increase complexity and cryptographic analysis”, Proc. of the 19th International Conference on Advances Information Networking and Application, Taiwan, pp.724-728.

[11] J.J. Amador, R. W.Green,(2005), “Symmetric-Key Block Cipher for Image and Text Cryptography”: International Journal of Imaging System and Technology, No. 3, , pp. 178-188.

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

[13] L. Shujun, Z. Xuan, M. Xuanqin, C. Yuanlong,(2002), "chaotic encryption scheme for real time digital video", SPIE vol.4666,p.149-160, Real-Time Imaging.