An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems

Abdulkarim Amer Shtewi[†], Bahaa Eldin M. Hasan, Abd El Fatah .A. Hegazy

[†]Arab Academy for science &Technology College of Computing and Information Technology, Cairo branch, Egypt.
[††] Arab Security Consultants (ASC)
[†††] Arab Academy for science &Technology College of Computing and Information Technology, Cairo branch, Egypt.

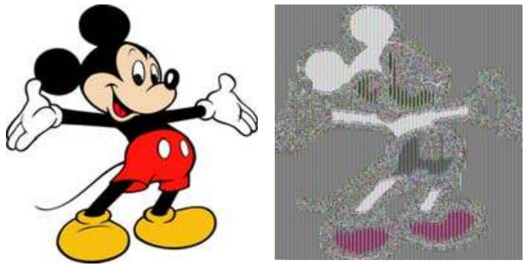
Abstract
Security in transmission storage of digital images has its importance in today's image communications and confidential video conferencing. Advanced Encryption Standard (AES) is a well known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications. In this paper, we present a modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption. The modification is done by adjusting the ShiftRow phase. Experimental results verify and prove that the proposed modification to image cryptosystem is highly secure from the cryptographic viewpoint. The results also prove that with a comparison to original AES encryption algorithm the modified algorithm (MAES) gives better encryption results in terms of security against statistical attacks.

Keywords:
AES, MAES, image encryption, security analysis

1. Introduction

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 [1, 2], most of which are used in text or binary data. It is difficult to use them directly in multimedia data, for multimedia data [3] are often of high redundancy, of large volumes and require real-time interactions, such as displaying, cutting, copying, bit rate conversion, etc. For example, the image shown in Figure 1(a) is encrypted into that shown in Figure 1(b) by AES algorithm directly (ECB mode). As can be seen, Figure 1(b) is still intelligible to some extent.

This is because the adjacent pixels in an image are of close relation which cannot be removed by AES algorithm. Besides the security issue, encrypting images or videos with these ciphers directly is time consuming and not suitable for real-time applications. Therefore, for multimedia data, some new encryption algorithms need to be studied.



a) b)

Fig. 1 Application of the AES cipher to Mickey plain image/cipher image.

This paper proposes a new encryption scheme as a modification of AES algorithm. The modification is mainly focused on both ShiftRow phase. In the ShiftRow 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.

2. AES Algorithm

2.1 Tables and Figures

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 [4]. This standard is based on the Rijndael algorithm [5], a symmetric block cipher. As the AES algorithm may be used with three different key lengths, these three different ‘‘flavors’’ are generally referred to as ‘‘AES-128’’, ‘‘AES-192’’, and ‘‘AES-256’’.

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).

Manuscript received February 5, 2010
Manuscript revised February 20, 2010

In Fig. 2 we can see the structure of this algorithm. Let us see every phase of the algorithm.

2.1 KeyExpansion phase

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 wi, taking into account that the first sub-key is the initial key. To calculate every wi (except w0) 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 GF(2^8). On the other hand, S-Box is a non-linear and invertible substitution table used to perform a one-by-one substitution of a byte value.

2.2 AddRoundKey phase

The AddRoundKey phase performs an operation on the State with one of the sub-keys. The operation is a simple XOR between each byte of the State and each byte of the sub-key.

2.3 SubByte phase

The SubByte transformation is a non-linear byte substitution that operates independently on each byte of the State using the SBox table.

2.4 ShiftRow phase

In the ShiftRow transformation, the bytes in the last three rows of the State are cyclically shifted over 1, 2 and 3 bytes, respectively. The first row is not shifted.

2.5 MixColumns phase

The MixColumns transformation operates on the State column by column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF$(2^8)$and multi- plied by a fixed polynomial a(x) modulo x^4+1given by

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \qquad (1)$$

This can be written as a matrix multiplication as follows:

$$S'(x) = A(x) \otimes S(x) \begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix}$$

$$= \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < 4 \qquad (2)$$

As a result of this multiplication, the four bytes in a column are replaced as follows:

$$\begin{aligned} S'_{0,c} &= (\{02\} \cdot S_{0,c}) \oplus (\{03\} \cdot S_{1,c}) \oplus S_{2,c} \oplus S_{3,c} \\ S'_{1,c} &= S_{0,c} \oplus (\{02\} \cdot S_{1,c}) \oplus (\{03\} \cdot S_{2,c}) \oplus S_{3,c} \\ S'_{2,c} &= S_{0,c} \oplus S_{1,c} \oplus (\{02\} \cdot S_{2,c}) \oplus (\{03\} \cdot S_{3,c}) \\ S'_{3,c} &= (\{03\} \cdot S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\} \cdot S_{3,c}) \end{aligned} \qquad (3)$$

Where $\oplus$is the XOR operation and the. is a multiplication modulo the irreducible polynomial $m(x) = x^8+x^4+x^3+x+1$ .Fig.2 shows the implementation of the function $B = xtime(A)$ which will be used to make the multiplications of a number by 2 modulo m(x).

So, we will only have binary operations as follows:

$$\begin{aligned} \{02\} \cdot S'_{x,c} &= xtime(S'_{x,c}) \\ \{03\} \cdot S'_{x,c} &= xtime(S'_{x,c}) \oplus S'_{x,c} \end{aligned} \qquad (4)$$

See [6] for a complete mathematical explanation of the AES algorithm.

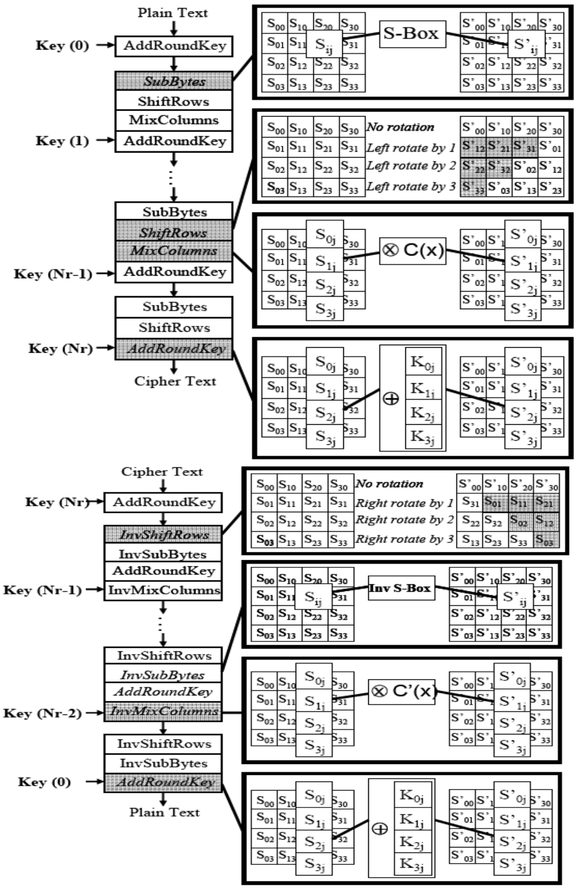


Fig. 2 Description of the AES cryptographic algorithm

3. A Modified AES (MAES)

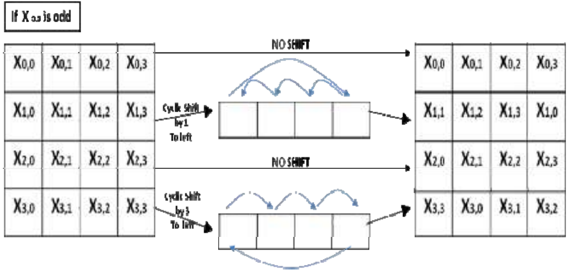
Here, we modify the AES to be more efficient and secure way by adjusting the ShiftRow phase.

3.1 ShiftRow Phase:

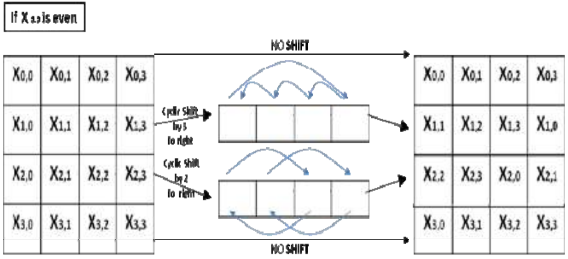
Instead of the original Shiftrow, we modify it as:

a- Examine the value in the first row and first column,(state [0][0]) is even or odd?

b- If it is odd, The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For MAES, the first and third rows are unchanged and each byte of the second row is shifted one to the left. Similarly, the fourth row is shifted by three to the left respectively.



c- If it is even, The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. The first and fourth rows are unchanged and each byte of the second row is shifted three to the right. Similarly, the third row is shifted by tow respectively on to the right.



The pseudo code for ShiftRows is as follows.

```
ShiftRows ( byte state [4, Nb] )
begin  byte t[Nb]
 if state[0][0]   odd numbers
   for r = 1  step 1, 3
       x = r mod 4
        if x = 0  step  0 to  x + 1
          for c = 0  step 1 to Nb – 1
             t[c] = state[r, (c + x) mod Nb]
          end for
           for c = 0 step 1 to Nb – 1
             state[r,c] = t[c]
              end for
    end for
else
    for r = 2  step 2, 4
         k = 0
         x = r mod 4
         if x = 0  step 0 to 3
            for  c = Nb - 1, c >= 0 ,  c -1
       t[c] = state[x, (c + x) mod Nb   , k + 1
            end for
              for  c = 0 ,  c < Nb  , c + 1
                state[x,c] = t[c]
              end for
    end for
end
```

4. Experimental results

Results of some experiments are given to prove its efficiency of application to digital images. We use several images as the original images (plain images). The encrypted images are depicted in Figs. 3b-5b. As shown, the encrypted images (cipher image) regions are totally invisible. The decrypted images are shown in Figs. 3c-5c. The visual inspection of Figs.3-5 shows the possibility of applying the proposed MAES successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them.

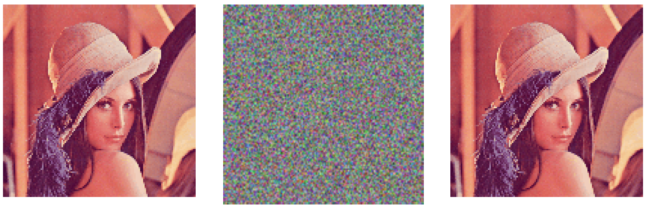

a) Original image b) Encrypted image c) Decrypted image

Fig. 3 Application of the modified cipher to Lena plain image/cipher image

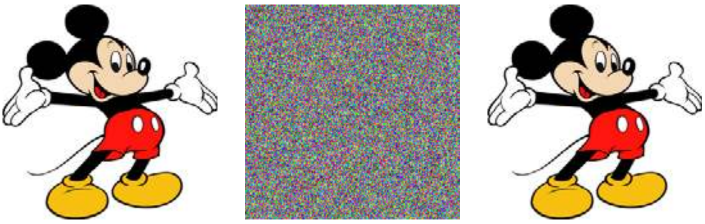
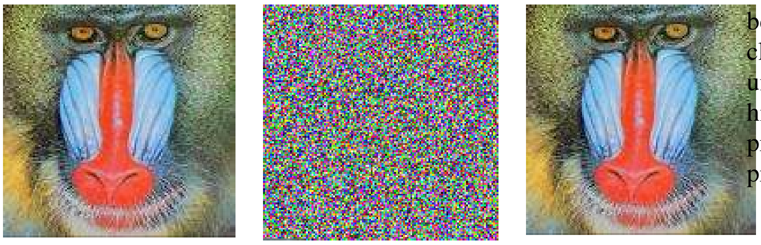

a) Original image b) Encrypted image c) Decrypted image

Fig. 4 Application of the modified cipher to Mickey plain image/cipher image



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

Fig. 5 Application of the modified cipher to Baboon plain image/cipher image

5. Security analysis

The security of an image cryptosystem is determined by its confusion and diffusion capabilities. It is usually evaluated by the following quantitative measures [7-15].

5.1 Key space analysis

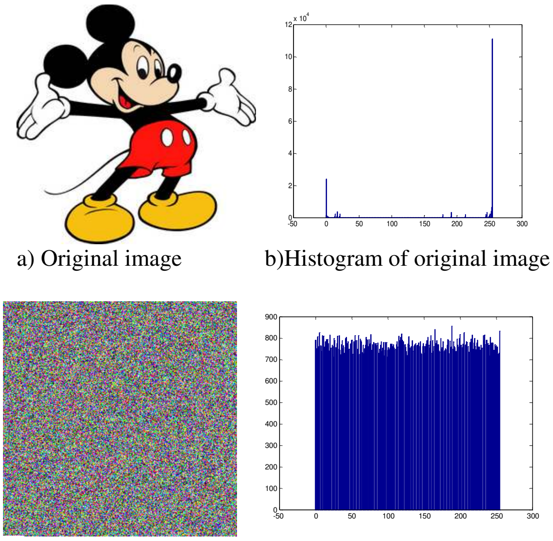
Key space size is the total number of different keys that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [20]. The proposed cipher has 2128 different combinations of the secret key. An image cipher with such a long key space is sufficient for reliable practical use.

5.2 Statistical analysis

It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack. To prove the robustness of the proposed cipher, we have performed statistical analysis by calculating the histograms and the correlations of two adjacent pixels in the plainimage/cipherimage.

5.2.1 Histograms analysis

To prevent the leakage of information to an opponent, it is also advantageous if the cipherimage bears little or no statistical similarity to the plainimage. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig.6b. The histogram of a plainimage (Mickey image(Fig.6a) of size 256x256 pixels) contains large spikes. The histogram of the cipherimage as shown in Fig.6d, is uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that 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 procedure.



a) Original image b)Histogram of original image

c) Encrypted image d) Histogram of Encrypted image

Fig. 6 Histograms of the plain image and ciphered image

5.2.2 Correlation of adjacent pixels

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plainimage/cipherimage respectively. The procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$\operatorname{cov}(x,y)=E(x-E(x))(y-E(y)), \qquad (5)$$

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \qquad (6)$$

where x and y are grey-scale values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \qquad (7)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2, \qquad (8)$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)), \qquad (9)$$

Fig. 7 shows the correlation distribution of two horizontally adjacent pixels in plainimage cipherimage (Micky image of size 256x256) for the modified cipher. The correlation coefficients are 0.9452 and -0.0112 respectively for both plainimage cipherimage, which are far apart. Similar results for diagonal and vertical directions were obtained as shown in Table 1. It is clear that from the Fig.7 and Table 1 that there is negligible correlation between the two adjacent pixels in the cipherimage. However, the two adjacent pixels in the plaintext are highly correlated.

Table 1 : Correlation coefficient of two adjacent pixels in original and encrypted image

Direction	Plainimage	Cipherimage
Horizontal	0,9452	-0,0112
Vertical	0,9471	-0,0813
Diagonal	0,9127	0,0009

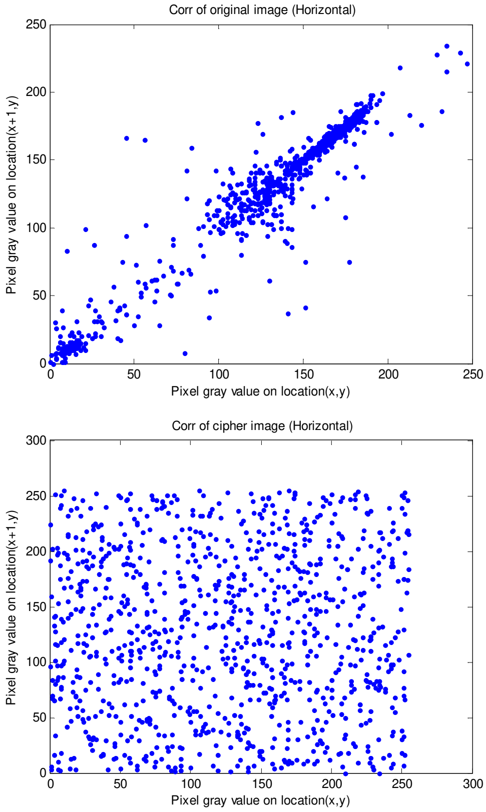


Fig. 7 Tow horizontally adjacent pixels Correlation in plainimage/cipherimage, respectively

5.3 Information entropy analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [16]. Modern information theory is concerned with error- correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy H (m) of a source m, we have:

$$H(m)=\sum_{i=0}^{2^N-1}P(m_i)\log_2\frac{1}{P(m_i)}\,bits \qquad (10)$$

Where p (mi) represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 28 symbols with equal probability, i.e., $m=\{m_1,m_2,\ldots\ldots,m_{2^8}\}$ after evaluating Eq. (10), we obtain its entropy H (m) = 8, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Let us consider the ciphertext of image encryption using the proposed block cipher, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed. We illustrate the entropy analysis of our scheme kept at the same word size w=32, number of rounds r= 10, and secret key length b=16 respectively, and compare it with other schemes. Table 2 indicates the various values of the entropies for encrypted images. It can be noted that the entropy of the encrypted image of MAES are very near to 8 compared to the other schemes.

Table 2: Entropies of the encrypted images of Mickey image (mickey.bmp)

Encryption algorithm	Entropy Value
AES	7.9989
MAES	7.9992

5.4 Differential attack

Two common measures, NPCR and UACI [17-19], are used to test the influence of changing a single pixel in the original image on the whole image encrypted by the proposed scheme. NPCR stands for the number of pixels change rate while–pixel of plain image are changed. Unified Average Changing Intensity (UACI) measures the average intensity of difference between the plain image and cipher image. For calculation of NPCR and UACI, let us assume two ciphered images C1 and C2 whose corresponding plain images have only one-pixel difference. The gray-scale values of the pixels of the ciphered image

C1 and C2 at grid (i,j) are labeled as C1(i,j) and C2(i,j), respectively. Define a bipolar array, D, with the same size as images C1 and C2. Then, D(i,j) is determined by C1(i,j) and C2(i,j), namely, if C1(i,j) = C2(i,j) then D(i,j) = 1; otherwise, D(i,j) = 0. NPCR and UACI are defined through the following formulas:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad (11)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%, \qquad (12)$$

Where W and H are the width and height of C1 or C2. Tests have been performed on the proposed algorithm, about one-pixel change influence on a 256 gray-scale image of size 256×256 .We obtained NPCR=99.58% and UACI=29.63 %. The results show that a swiftly change in the original image will result in a significant change in the ciphered image, so the algorithm proposed has a good ability to anti differential attack.

5.5 Performance of MAES w/r/b Encryption

Apart from security considerations, some other issues for image cryptosystem algorithm are also important. This includes the 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. 4a) is used as a plainimage and encryption of this image is shown in Fig. 4b. the personal computer used in all programs and test was Intel(R) Core™ 2Duo CPU T5800 2.00GHz with 3.00GB of memory and 230GB hard-disk capacity. Table 3 and Fig.8 shows Performance of AES and MAES w/r/b Encryption on 256 grey-scale image of different sizes, kept at the same word size w=32, number of round r=12 and secret key length b=16 and kept at CBC mode of operation.

Table 3 : Performance of AES and MAES w/r/b Encryption

Image size (in pixels)	*Image size on disk*	*Encryption time in ms with AES*	*Encryption time in ms with MAES*
256x256	192KB	6.443	6.349
512x512	257KB	8.643	8.565
512x512	768KB	25.256	25.007
1024x1024	2.25MB	75.862	75.114

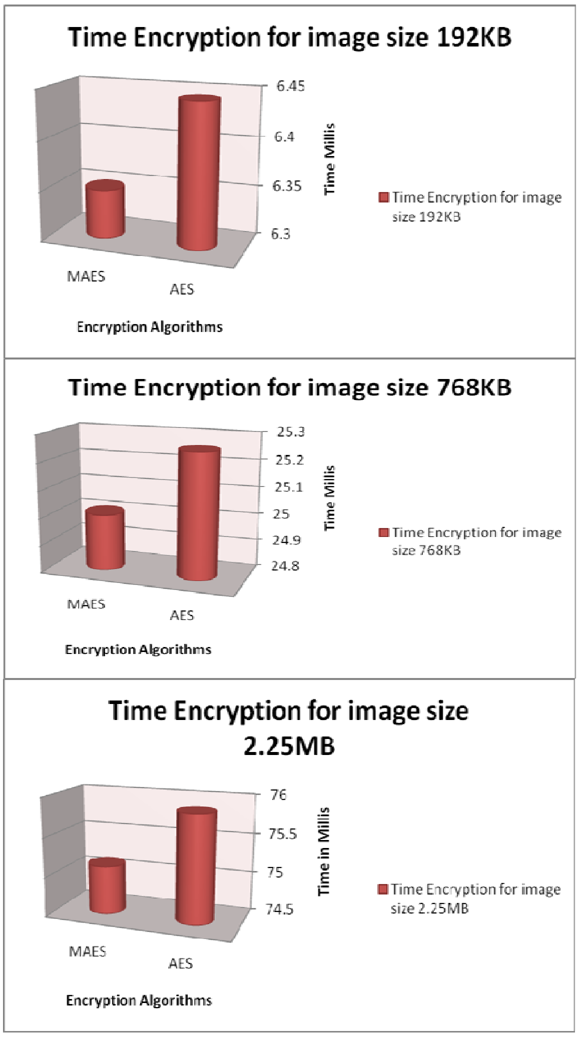


Fig. 8 Performances of AES and MAES

6. Conclusion

In this paper a modified version of AES, namely MAES, is proposed. The modification is done by adjusting ShiftRow phase. The proposed cryptosystem does not require any additional operations rather than the original AES. We have shown that MAES gives better encryption results in terms of security against statistical attacks.

References

[1] Shiguo Lian, Multimedia Content Encryption: Techniques and Applications. Taylor & Francis Group, LLC, 2009.

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

[3] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook, February 2004.

[4] Federal Information Processing Standards Publication 197(FIPS197), http:// csrc.nist.gov/publications/fips/fips197/fips-197.pdfS, 2001.

[5] J. Daemen, V. Rijmen, The block cipher Rijndael, Smart Card Research and Applications (2000) 288–296.

[6] Zhang, Y. and D. Feng, Equivalent generation of the S-box of Rijndael, Chinese Journal of Computer, vol.27, no.12, pp.1593-1600, 2004.

[7] Liu, J., B. Wei and X. Wang, 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, 2005.

[8] Matsui M, Linear cryptanalysis method for DES cipher.Advances in Cryptology-EuroCrypt'93. Berlin: Springer- Verlag, 1994. 386-397.

[9] Eli Biham, Adi Shamir. Differential Cryptanalysis of DES-like Cryposystems, Advances in Cryptology— CRYPTO'90 Proceedings. Springer-Verlag, 1991. 3-72.

[10] H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. IEEE Trans. Signal Process. 48 (8), 2439–2451, 2000.

[11] L.M. Marvel, G.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process, 8 (8), 1075–1083, 1999.

[12] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, 1996.

[13] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Faragallah, "Encryption Efficiency Analysis and Security Evaluation of AES Block Cipher for Digital Images," International Journal of Computer, Information, And Systems Science, and Engineering, Vol. 1, No. 1, PP. 33-39, 2007, ISSN 1307-2331.

[14] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Faragallah, "An Efficient Chaos-Based Feedback Stream cipher (ECBFSC) for Image Encryption and Decryption", An International Journal of Computing and Informatics, Vol. 31, No. 1, PP. 121-129, 2007, ISSN 0350-5596.

[15] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps". Chaos, Solitons & Fractals 2004;21(3):749–61.

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

[17] S. Behnia, A. Akhshani, A.Akhshani, H. Mahmodi, A. Akhavan ."A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps". Physics Letters A 366 (2007) 391-396

[18] Fuyan Sun,Shutang Liu, Zhongqin Li, and Zongwang Lü, " A novel image encryption algorithm based on spatial chaos map," Chaos,Solitons and Fractals 38 (2008) 631-640.

[19] Ibrahim F. Elashry, Osama S. Farag Allah, Alaa M. Abbas, S. El-Rabaie, and Fathi E. Abd El-Samie, "Homomorphic image encryption," J. Electron. Imaging Vol. 18, 033002 (Jul. 14, 2009)

Abdulkarim Amer Shtewi received the Bachelor's degree in Engineering Sea Officer with the degree Excellent from Stralsund College graduated Engineer in Germany in 1985. Bachelor's degree in System Analysis with the degree very good from Dar Alalem University, College computer Science. in Libya in 2006. Now a Master student at college of computing and information technology at the Arab Academy for science &Technology in Egypt.

Bahaa Eldin M. Hasan received the B.Sc. and M.Sc. degrees, from faculty of Engineering (Shoubra), Zagazig University in 1978 and 1987, respectively. He received the Dr. Eng. degree from Ain Shams University under supervision of Tokyo institute of Technology in 1994. Bahaa has served the National Defense Council Service for 26 years. During his 26 years, he was engaged in general National Defense Council duties. He awarded the Order of Merit- Second grade from the president of Egypt. Bahaa left the National Defense Council in 2006 and went to work for his own privet business "Arab Security Consultants (ASC)".Bahaa is an expert specializing in such areas as: Data security, network security, computer security, Ethical hacking and countermeasures, and Smart card and smart token applications for securing the data and information. Bahaa is still involved in the training of security officers as well as for security staff for several Arab world organizations.

Abdelfatah A. Hegazy received the B.E. degrees, from the Military Technical Collage, Cairo, Egypt, 1978. In 1982 he received the M.Sc. In Computer Sciences from George Washington University, USA. Dr. Hegazy received the Ph.D. Degree Computer Sciences from George Washington University, USA, in 1985. After working as an assistant professor (from 1985) in the Dept. of computer enginering operation research, the Military Technical Collage., and an associate professor (from 1990), he has been a professor at College of Engineering at the Arab Academy for Science and technology. Since 1998. His research interest includes: Information Systems Planning; E-Commerce, E-Government, Information Systems Security, network security ,knowledge Management, Web Intelligent Systems and Enterprise Resource Planning Systems. He is a member of IEEE, ACM, AIS, AANIS, and CSS-Computer Scientific Society Egypt.