DOI: 10.24996/ijs.2022.63.1.29

ISSN: 0067-2904

A Modified Advanced Encryption Standard for Color Images

Sarah Jassim*, Sarab M. Hameed

Department of Computer Sciences, College of Science, University of Baghdad, Baghdad, Iraq

Received: 13/11/2020 Accepted: 14/1/2021

Abstract

The widespread use of images, especially color images and rapid advancement of computer science, have led to an emphasis on securing these images and defending them against intruders. One of the most popular ways to protect images is to use encryption algorithms that convert data in a way that is not recognized by someone other than the intended user. The Advanced Encryption Standard algorithm (AES) is one of the most protected encryption algorithms. However, due to various types of theoretical and practical assaults, like a statistical attack, differential analysis, and brute force attack, its security is under attack.

In this paper, a modified AES coined as (M-AES) is proposed to improve the efficiency of the AES algorithm by increasing the algorithm's security to make the algorithm more suitable for color image encryption, and make it more resistant to many attacks. The modification is conducted on ShiftRows transformation of the original AES algorithm. To test the efficiency of the proposed M-AES algorithm, several images are drawn from the Signal and Image Processing Institute's (SIPI) image dataset. Moreover, the Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Entropy (H), Correlation Coefficient (CC), visual evaluation of histogram, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used as an evaluation metric. The results show that proposed modification to the AES algorithm makes the algorithm more appropriate to image and surpasses the original AES.

Keywords: Advanced Encryption Standard, Image Encryption, ShiftRows step.

تشفير معياري متقدم معدل لتشفير الصور الملونة

سارة جاسم*، سراب مجيد حميد

قسم علوم الحاسبات، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

أدى الاستعمال الواسع النطاق للصور ، وخاصة الصور الملونة والتقدم السريع في علوم الحاسوب ، إلى التركيز على تأمين هذه الصور والدفاع عنها ضد المتسللين. تتمثل إحدى الطرق الأكثر شيوعًا لحماية الصور في استخدام خوارزميات التشفير التي تحول البيانات بطريقة لا يتعرف عليها شخص آخر غير المستخدم المقصود. تعد خوارزمية معيار التشفير المتقدم (AES) واحدة من أكثر خوارزميات التشفير المحمية. ومع ذلك ، نظرًا لأنواع مختلفة من الهجمات النظرية والعملية ، مثل الهجوم الإحصائي والتحليل التفاضلي وهجوم القوة الغاشمة ، فإن أمنها يتعرض للهجوم ، في هذا البحث ، تم اقتراح AES معدل بصياغة (M–AES) لتحسين كفاءة خوارزمية AES عن طريق زيادة أمان الخوارزمية لجعل الخوارزمية أكثر ملاءمة لتشفير الصور

*Email: sarah.ahmed1301@sc.uobaghdad.edu.iq

الملونة وجعلها اكثر مقاومة ضد الهجمات. يتم إجراء التعديل على تحويل ShiftRows لخوارزمية AES الأصلية. لاختبار كفاءة خوارزمية M−AES المقترحة ، يتم رسم العديد من الصور من مجموعة بيانات صور معهد معالجة الإشارات والصور(SIPI) علاوة على ذلك ، متوسط الخطأ التربيعي (MSE) ، ذروة نسبة الإشارة إلى الضوضاء (PSNR) ، الانتروبيا (H) ، معامل الارتباط (CC) ، التقييم المرئي للرسم البياني ، معدل تغيير عدد البكسل (NPCR) ومتوسط شدة التغيير الموحد (UACI) تستعمل كمقاييس للتقييم. تظهر النتائج أن التعديل المقترح لخوارزمية AES يجعل الخوارزمية أكثر ملاءمة للصورة ويتجاوز AES الأصلي.

1. Introduction

The widespread usage of images on the Internet requires a fast, reliable, and robust security to store and transmit them over the network [1], and Image Security has become a critical issue [2]. One of emerging challenges in image processing especially color images is that encryption techniques need an additional requirement because image data have properties like high redundancy, bulk capacity, and high correlation between the pixels. Therefore, having an efficient cryptographic algorithm is considered to be imperative, to provide higher security in images, and to protect the images from any attacker [1].

Advanced Encryption Standard (AES) is one of the most commonly and widely symmetric block cipher algorithms used for protecting multimedia data such as images [3]. Attacks considered during design of AES includes statistical attacks, differential cryptanalysis, square attacks, and related key attacks. At the moment AES algorithm has not been broken. However, cryptanalysis of AES has not stopped [4]. But, since standardization of AES in NIST FIPS-197 and its adoption for use in a wide range of high-security applications has resulted in wide examination of vulnerabilities in AES and has also given rise to extended forms of attacks [5], so main focus of this paper is to supplement the standard AES and propose a new modification on AES design to enhance its security by increasing randomness and level of security of AES algorithm to make it more suitable for encrypting color image.

The rest of the paper is structured as follows. Section 2 presents related works. Original AES algorithm is explained in section 3. The proposed modification to AES algorithm for color image encryption is discussed in Section 4. Results and conclusions are provided in sections 5 and 6, respectively.

2. Related works

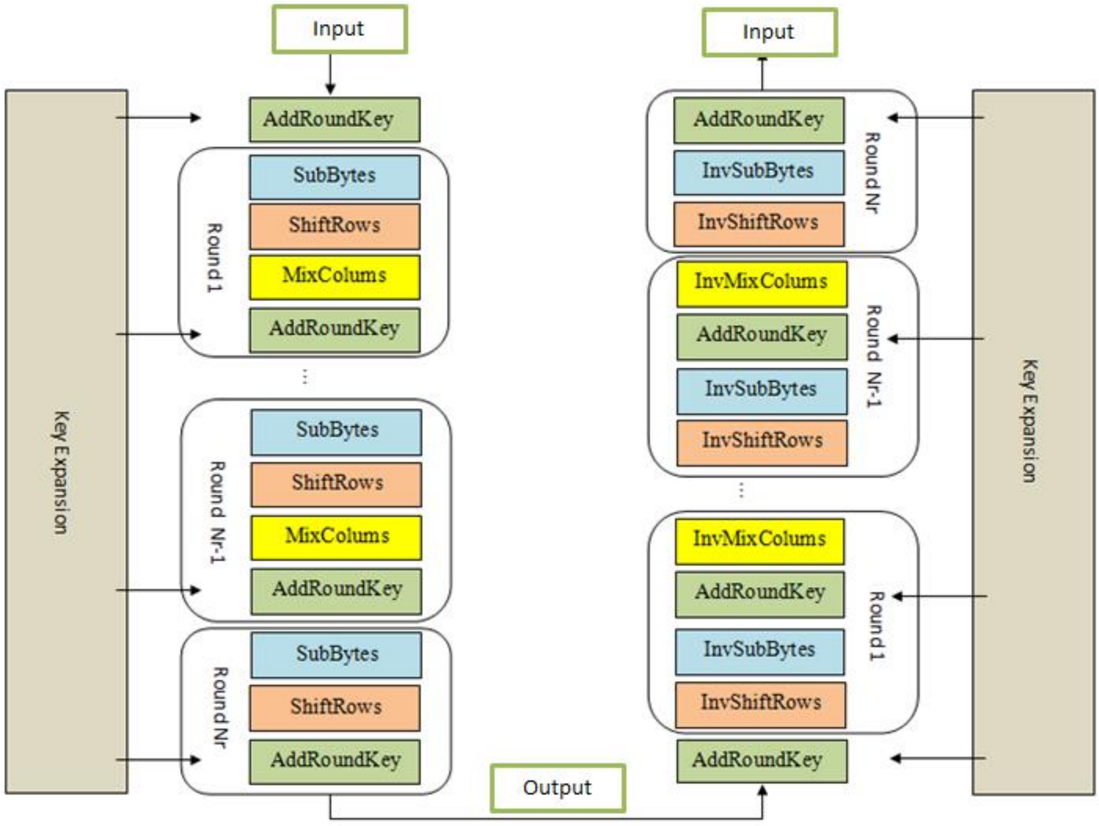
In the last years, various approaches and techniques have been introduced for modifying Advanced Encryption Standard (AES) algorithm [6]. Wadi & Zainal in 2014 proposed a modification on standard AES by conducting three modifications, first by using MixColumns transformation in five rounds rather than ten rounds in the original AES-128. The second modification is changing the key schedule operation by adding MixColumns transformation to the operation. The third modification is a simple S-box used for encryption and decryption instead of S-box in the original AES [7]. Kaur & Mehla in 2014 proposed a revised version of AES algorithm. The alteration is made on various transformation steps in AES algorithm. Basically, the modification is focused on ShiftRows transformation, MixColumns transformation, and key expansion modification. The modified algorithm takes less time than the original, and it is secured against brute force attack [8]. In 2015, Vaidehi & Rabi made modifications to AES algorithm for reducing hardware complexity and energy consumption of AES Encryption to strengthen AES encryption using Common Subexpression Elimination (CSE) technique to develop the Enhanced MixColumns transformation for AES encryption. Enhanced MixColumns transformation results showed a 10.93% decrease in Slices, a 13.6 % decrease in LUTs, and a 1.19% decrease in delay consumption compared to conventional MixColumns [3]. In 2015, Abdulgader et al. suggested modifications to enhance the AES algorithm's performance and make it more suitable for secured image storage and transmission. The modification includes a circular shift and a round key to make S-box depends on secret keys and the MixColumns is replaced by chaotic maps. The comparison shows that the proposed method offers strong encryption efficiency and takes less time to encrypt images [9]. In 2015, Alabaichi & Salih proposed an update to AES algorithm, which included AES dynamic S-box generation. The produced S-box is more dynamic and key-dependent, making it more challenging for differential and linear cryptanalysis. Compared to the original AES, result of that enhancement showed that it provided more security [2]. In 2016, Hoomod & Zewayr suggested a new chaotic method for improving AES by removing the transformation of MixColumns to decrease the time needed for this process. Compared to traditional MixColumns operation, result of the new method showed the enhancement of protection by providing more entropy and better correlation [10]. Riyaldhi & Kurniawan in 2017 proposed a modification that has been made by reducing ShiftRows circular process and S-box modification for MixColumns transformation. Result showed that the percentage improvement in the encryption process is 86.143% and the decryption process is 13.085%, and the method needs to consume a bigger memory to store two modified S-box map and Array ShiftRows map [11]. D'Souza & Panchal in 2017, proposed AES for the message transmission algorithm using a hybrid method to dynamic key generation and dynamic S-box generation. Results showed that the proposed change offers high security and increases the uncertainty of the ciphertext. In addition, it defends the message from brute-force, algebraic, linear, and differential attacks [12]. In 2018, Felicisimo & Wenceslao proposed a modified AES algorithm using many substitution boxes (S-boxes), Where the Rijndael S-box is the first S-box and the second S-box is built via an XOR operation and affine transformation, the MixColumns operation is replaced within the cipher's internal rounds. Results of simulation testing showed that a substantial difference in speed efficiency has been found between the two versions that favor the proposed AES algorithm using multiple S-boxes. The results also revealed that AES-2S-box performed more efficiently compared to the original AES [1]. A modified AES algorithm that addresses necessity image encryption was proposed by Gamido et al. in 2018. The modified algorithm used bit permutation instead of Mixcolumn to reduce the algorithm's computational requirement for encrypting images. The result showed that an entirely different encrypted image was generated by the modified algorithm and that whenever there is a slight change in the plaintext image, there is a major difference in the encrypted image. The result also revealed that the proposed algorithm is faster than AES and is amenable to statistical and differential attacks, causing it more suitable for image encryption [4]. In 2019, Thinn & Thwin suggested AES modification by including an extra or second key. As well as another change to the original SubBytes operation is done by using transportation operation. The proposed algorithm gave a good performance, high security and it can be applied to applications that share sensitive data via an insecure network [13]. Singh et al. in 2019 proposed modification on AES algorithm by using a new Dynamic AES algorithm developed that done by generates dynamic key-dependent S-boxes with dynamic irreducible polynomial and affine constant. Singh et al, in 2019, proposed a modification on AES algorithm by generating dynamic key-dependent S-boxes with dynamic irreducible polynomial and affine constant. Modified AES and standard AES algorithms are used for encrypting a color and grayscale image. It observed that both algorithms did well [14]. Kumar & Karthigaikumar in 2020, proposed to change the AES algorithm by using dynamic ShiftRows, SubBytes, and MixColumns operations in 2020. The security of the AES algorithm has been improved by achieving a larger avalanche effect than that of the traditional AES [5]. In 2020, Lavanya & Karpagam suggested a change to AES algorithm through a change in cipher processing and key expansion. The modified AES key schedule algorithm with an active key added sub-function has shown a gradual increase in unpredictability and distribution features. The modified AES produced an improved performance in terms of balance and hamming distance and reduces the ciphertext's statistical cryptanalysis when compared with the original AES. It also raises the algorithm's complexity.

3. Advanced encryption standard

AES is a cipher algorithm for symmetric-key blocks. It has been selected as a standard among symmetric cipher algorithms because of its high performance [4]. In AES, rounds consist of four encryption transformations. SubBytes, ShiftRows, MixColumns, and AddRoundKey. The cipher rounds are shown in the following four transformations.

1. The SubBytes transformation is a non-linear byte substitution that applies to each byte of the State independently [12]. This transformation includes substituting different values for the bytes of the state matrix. Using a substitution table called S-box. The AES S-box is a permutation of 8-bit values with a total of 256 entries constructed as a 16 x 16 lookup table. For the 16-byte state array, substitution is performed byte-by-byte. The left half of the selected byte selects the rows in the s-box, and the right half of the selected byte selects the s-box column. The corresponding row and column crossing point on the s-box table is the byte that substitutes the corresponding byte. In order to substitute all the contents of the state array, this step is repeated in the same way [5].
2. The transformation of ShiftRows is a simple byte transposition [12]. Based on their row location, every row of the state matrix except the first row is cyclically left-shifted [5]. The second row is shifted by one byte, the third row is shifted by 2 bytes, and the fourth row by three bytes [11].
3. The MixColumns transformation is done by combining each state column by carrying out matrix multiplication with a fixed square matrix, and it operates on the state column by column [15].
4. AddRoundKey transformation, the round key is XORed with the state array after SubBytes, ShiftRows, and MixColumns transformation to generate the intermediate cipher results [5].

Reverse operations of the encryption method are the decryption of the AES. Every round consists of four processes carried out in reverse order during decryption: InvAddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes [4]. In all rounds, the four transformations are present. Inverse MixColumns will no longer perform in the final round [12]. Figure 1 illustrates the structure of AES algorithm.



(a) (b)

Figure 1- AES algorithm structure. (a) Encryption process. (b) Decryption process.

4. The proposed modified AES (M − AES) for color image

The proposed image encryption aim is to get a cipher image from a plain image by modifying the original AES. The following subsections present the proposed AES and how it is used to encrypt an image.

4.1 Modified AES (M − AES)

The characteristics of the proposed modified AES ($M - AES$) concentrate on increasing level of security of AES algorithm. Core of the proposed method is to replace ShiftRows transformation of original AES by another one coined as *mShiftRows*. Structure of the $M - AES$ algorithm is like the original AES completely except replacement of ShiftRows step by (*mShiftRows)* step, which will be explained in next subsection. Figure 2 illustrates overall structure of the proposed modified AES ($M - AES$) algorithm.

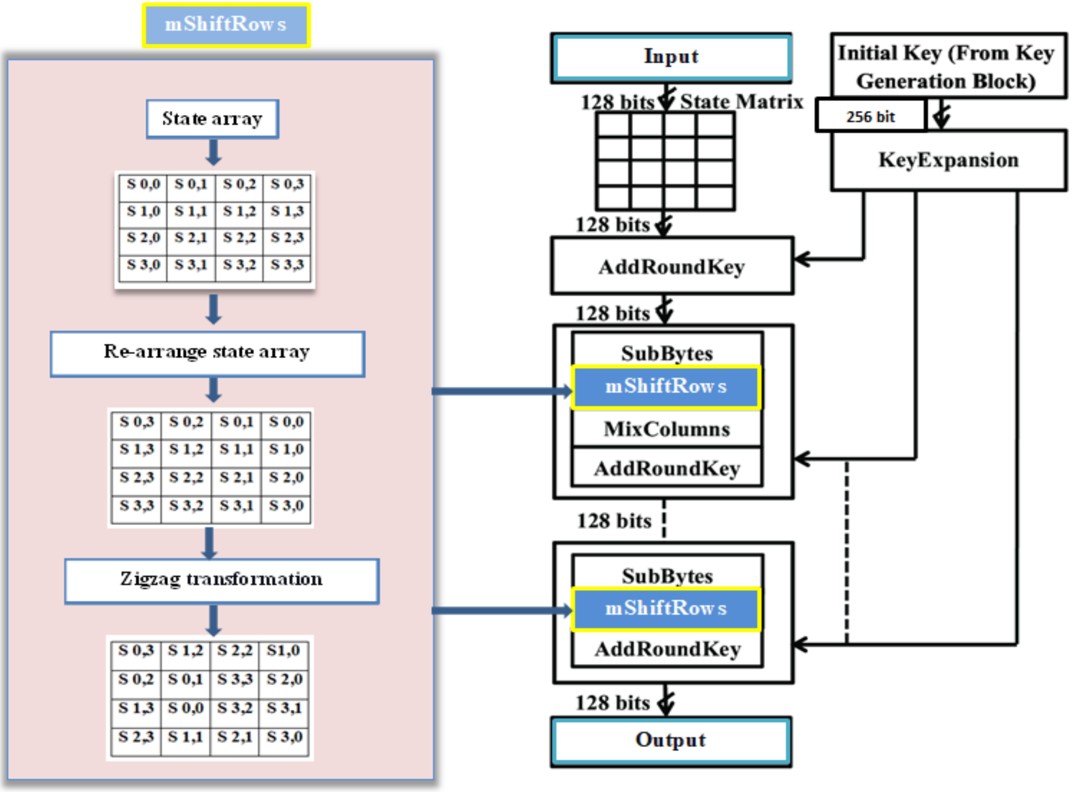


Figure 2- The overall structure of the proposed modified AES ($M - AES$) algorithm.

4.1.1 Modified ShiftRows (mShiftRows)

The proposed *mShiftRows* transformation tries to make statistical relationship between both plaintext and ciphertext as complicated as possible to impede the key from being inferred. This can be done by performing the following two steps:

1. Re-arrange the column transformation is used to re-arrange the columns of the state array by replacing the first column with the fourth. The fourth column takes the first position, the third column is replaced by the second column, and the second column takes its place (see Figure 3). In this scenario, the diffusion property will be improved by the permutation process on the value of a state array. Figure 4 provides an example illustration of the proposed idea of this transformation.

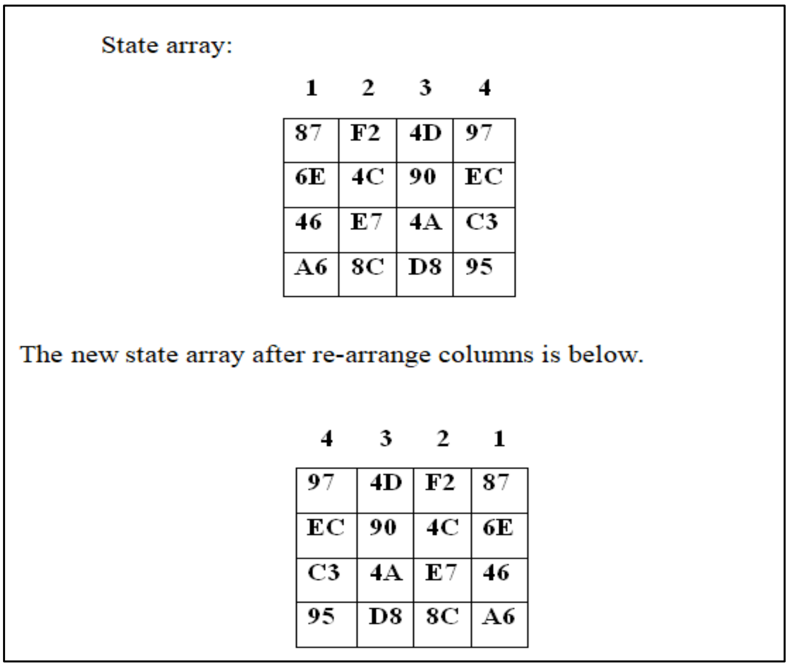
S 0,0	S 0,1	S 0,2	S 0,3
S 1,0	S 1,1	S 1,2	S 1,3
S 2,0	S 2,1	S 2,2	S 2,3
S 3,0	S 3,1	S 3,2	S 3,3

(a)

S 0,3	S 0,2	S 0,1	S 0,0
S 1,3	S 1,2	S 1,1	S 1,0
S 2,3	S 2,2	S 2,1	S 2,0
S 3,3	S 3,2	S 3,1	S 3,0

(b)

Figure 3-(a) State array. (b) After re-arrange column.



State array:

1	2	3	4
87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

The new state array after re-arrange columns is below.

4	3	2	1
97	4D	F2	87
EC	90	4C	6E
C3	4A	E7	46
95	D8	8C	A6

Figure 4- Re-arrange columns step of $M - AES$ algorithm

2-Zigzag transformation aims to perform a scrambling process that can only handle matrix of size N × N. There are several zigzag transformations. In this paper, the zigzag transformation shown in Figure 5 is adopted. It's used to confuse the sparse coefficient matrix and increase the security level of the encryption algorithm. The position of the starting pixel in the matrix is very important for zigzag transformation, and different locations can cause different effects of confusion. Figure 6 gives an example illustration of the proposed idea of this transformation.

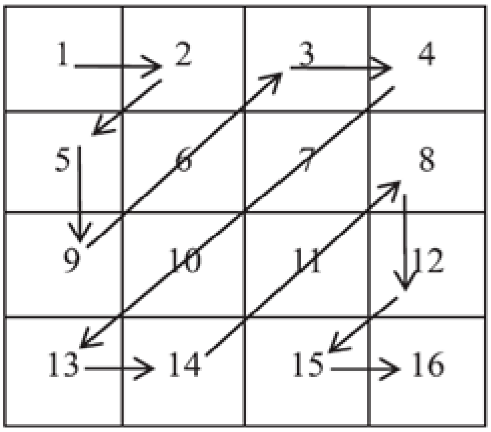
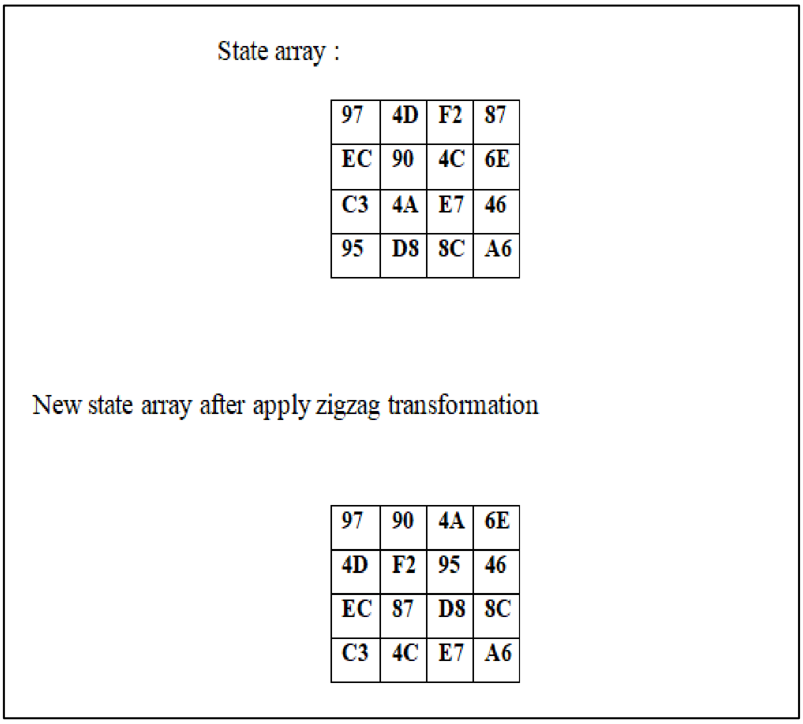


Figure 5-Zigzag transformation



State array :

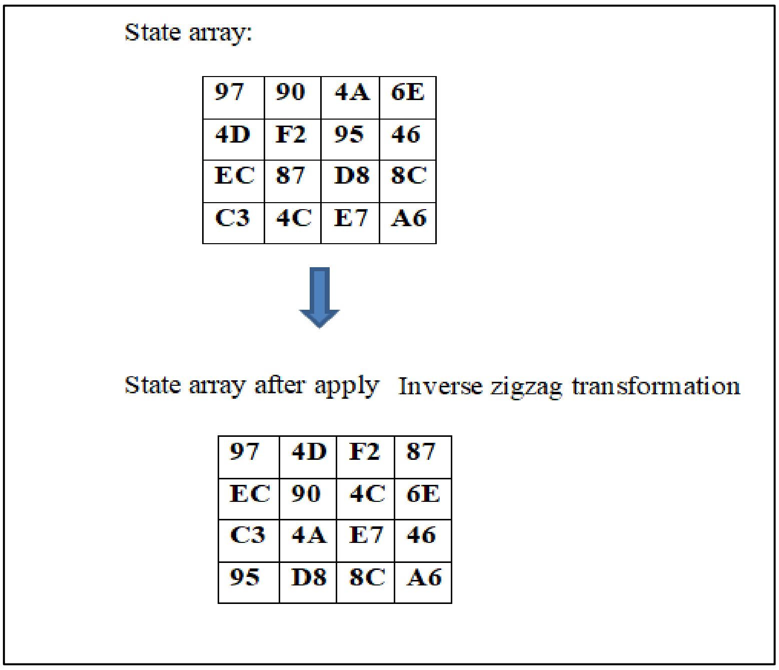
97	4D	F2	87
EC	90	4C	6E
C3	4A	E7	46
95	D8	8C	A6

New state array after apply zigzag transformation

97	90	4A	6E
4D	F2	95	46
EC	87	D8	8C
C3	4C	E7	A6

Figure 6-An example of zigzag transformation.

For the decryption process, the proposed *InvShiftRows* transformation is adopted. In which same structure of *mShiftRows* with reverse process is applied. That means Inverse zigzag process is applied to the state array. Then Inverse of the re-arranged the column is performed. Figure 7 and 8 give an example illustration of Inverse zigzag transformation and Inverse re-arrange columns transformation, respectively.



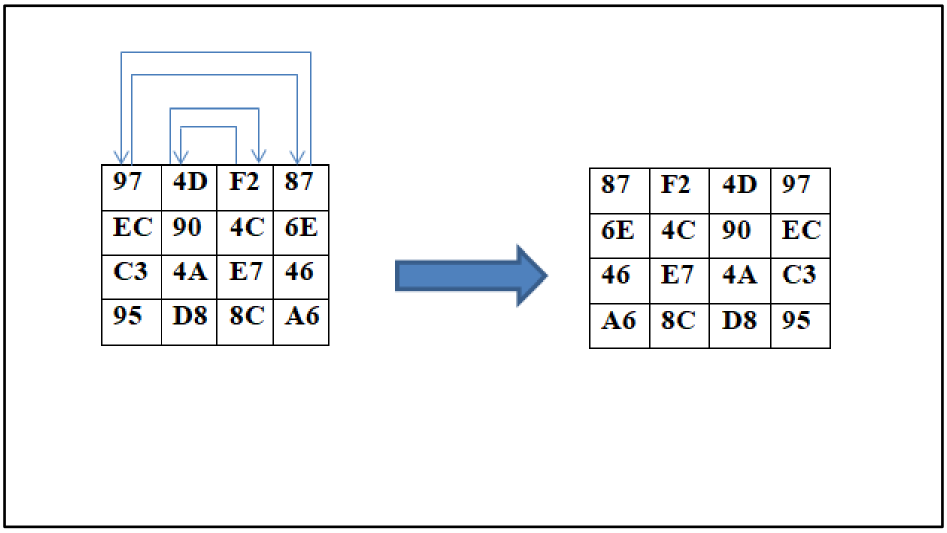
State array:

97	90	4A	6E
4D	F2	95	46
EC	87	D8	8C
C3	4C	E7	A6

State array after apply Inverse zigzag transformation

97	4D	F2	87
EC	90	4C	6E
C3	4A	E7	46
95	D8	8C	A6

Figure 7- An example of inverse zigzag transformation



97	4D	F2	87
EC	90	4C	6E
C3	4A	E7	46
95	D8	8C	A6

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Figure 8-An example of inverse re-arrange columns transformation

4. 2 Encryption color image by using $M - AES$ algorithm

For Encrypting color image using $M - AES$ algorithm, first A color image I_p of size $w \times h$ is disintegrated into three components $R, G,$ and $B.$ Then, each component is encrypted independently using $M - AES$ with a secret key of 256 bits to produce three encrypted components R_E, G_E and B_E . Finally, the three encrypted components are merged to produce a ciphered image I_c . Figure 9 depicts the whole encryption process of the proposed method.

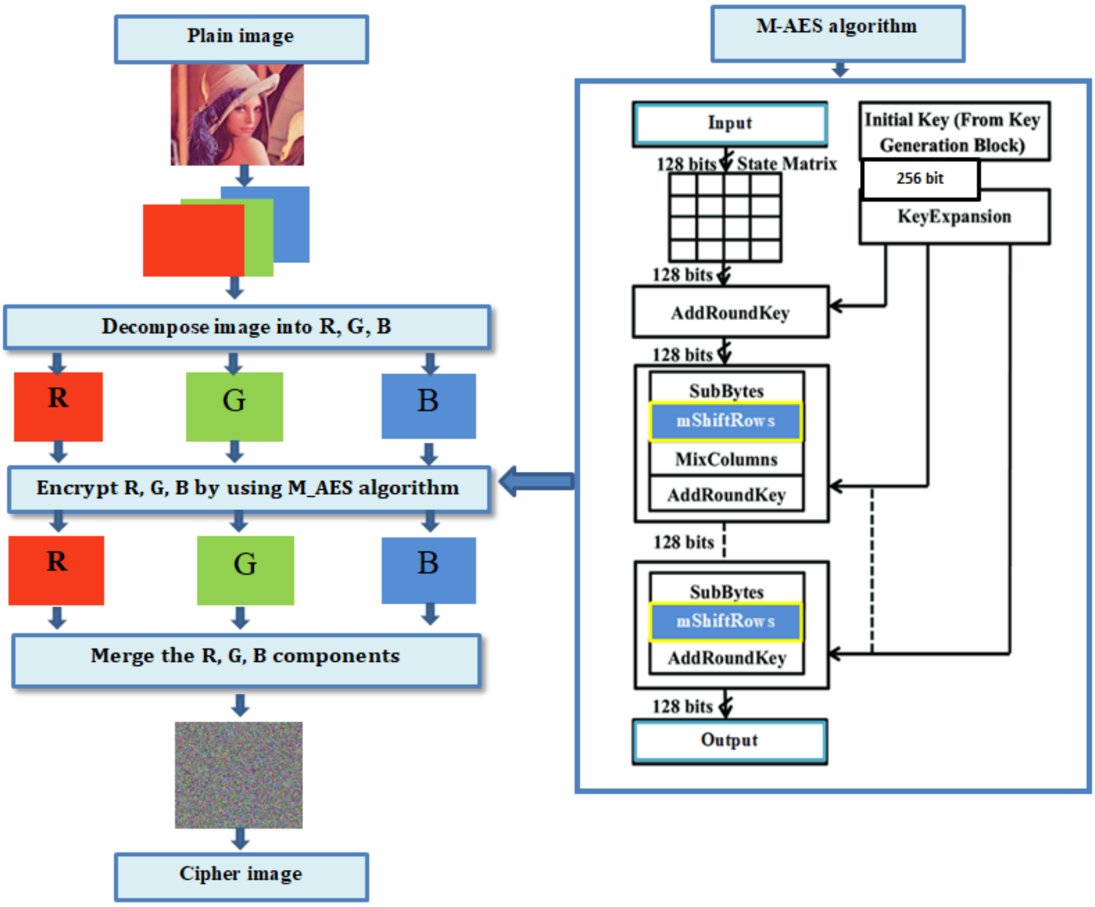


Figure 9- The overall structure of the color image encryption by $M - AES$ algorithm.

5. Experimental results

The proposed $M-AES$ has been tested for various 24-bit color images of size (256×256) pixels. These images are available at the USC-SIPI image database in bmp format. The evaluation of the encrypted image is based on histogram analysis, correlation coefficient, information entropy, NPCR, UACI, PSNR, and MSE. The experiments are conducted on a computer with Intel Core i5 CPU @ 2.70 MHZ with Windows 10 using MATLAB software. All the experiments encrypt the original images with a key of length 256 bits.

$$K = \{7A24432646294A404E635266546A576E5A7234753778214125442A472D4B6150\}$$

5.1 Evaluation concerning statistical attack

In the statistical attack, the attacker utilizes statistical weaknesses in a cryptographic scheme to identify data that is confidential. The $M-AES$ is evaluated regarding entropy (H), histogram analysis, and correlation coefficient to illustrate its ability to withstand statistical attacks.

Information entropy is one of the quantitative measurement kinds that evince how random a signal source. It can be defined as in Equation 1.

$$\mathrm{H}\,(\mathrm{m}) = -\sum_{i-0}^{N} \mathrm{P}\,(\mathrm{m\ i})\ \mathrm{lo\ g\ 2\ P}\,(\mathrm{m\ i}) \quad \textbf{(1)}$$

In which P (m i) and log refer to the probability of occurrence of symbol m i and the base 2 logarithm, respectively [16].

Correlation coefficient (CC) is calculated as in Equation 2 which measures the correlation of adjacent pixels [17].

$$\mathrm{r}_{\mathrm{xy}} = \frac{\mathrm{cov(x,y)}}{\sqrt{\mathrm{D(x)D(y)}}} \quad \textbf{(2)}$$

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

$$\mathrm{D(x)} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i=1}}^{\mathrm{N}} \left(\mathrm{x_i} - \mathrm{E(x_i)}\right)^2$$

$$\mathrm{cov(x,y)} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i=1}}^{\mathrm{N}} \left(\mathrm{x_i} - \mathrm{E(x_i)}\right)\left(\mathrm{y_i} - \mathrm{E(y_i)}\right)$$

Where y is the horizontal adjacent pixel of x, N is the total number of pixels in N ×N image, cov(x, y) is covariance at pixels positions x and y,$\sqrt{\mathrm{D\ (x}}$) is standard deviation, D(x) is variance, also E(x) is mean.

Histogram analysis (Figure 10 and 11) show that histogram of plain images and encrypted image respectively. Obviously, histogram of ciphered image and plain image are completely different in all components (red, green, and blue).The encrypted image has a uniformly distributed histogram, indicating only a limited amount of data information is identified. The consequence of the histogram analysis indicates that $M-AES$ is immune from the statistical attack.

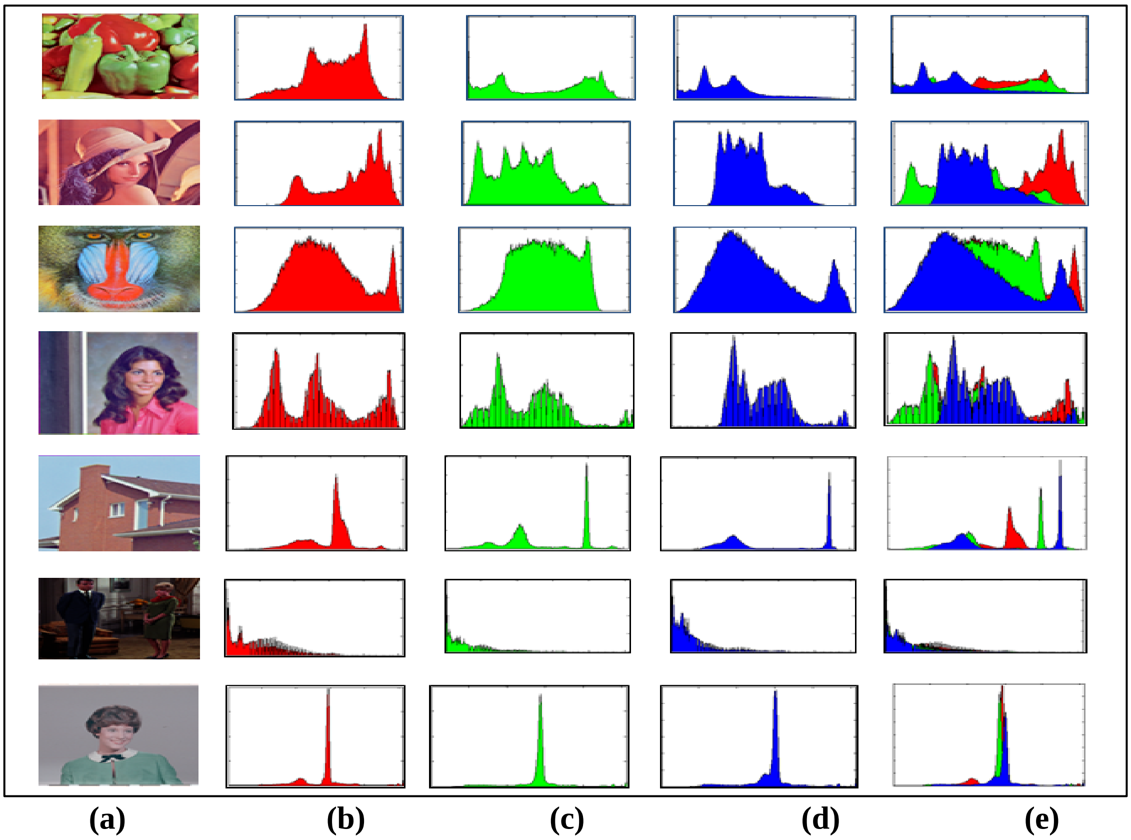


Figure 10-Histogram of the plain images. (a) The plain image. (b), (c) and (d) represent the histogram for red, green and blue components respectively. (e) Combining the histogram of all components.

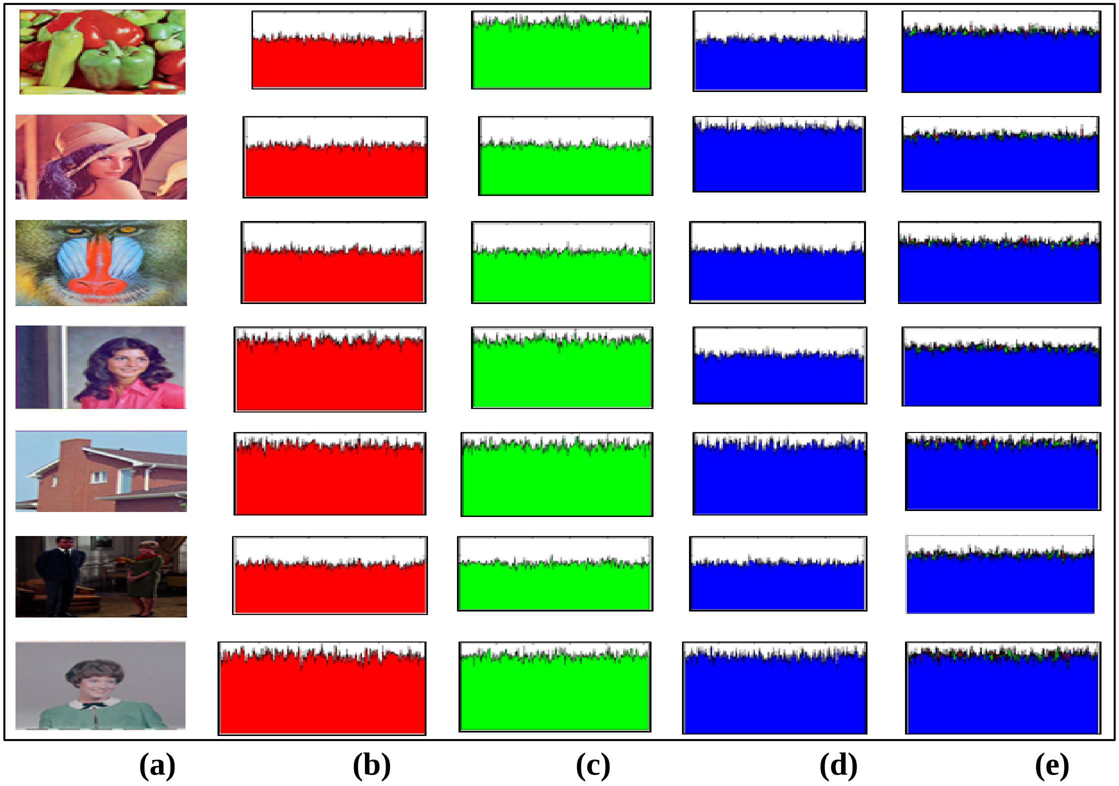


Figure 11- Histogram of the encrypted images using $M - AES$. (a) The plain image. (b), (c) and (d) represent the histogram for red, green and blue components respectively. (e) Combining the histogram of all components.

The entropy of encrypted images of the $M - AES$ is reported in Table 1. The result clarifies that it is protected against the statistical attack.

Table 1- Information entropy result for AES and $M - AES$

Method	**Image Name**	**R**	**G**	**B**	**Average**
Original AES	**Peppers**	7.9975	7.9970	7.9972	7.9972
	Lena	7.9970	7.9970	7.9974	7.9971
	Baboon	7.9973	7.9973	7.9975	**7.9974**
	Female	7.9974	7.9971	7.9972	**7.9972**
	House	7.9972	7.9970	7.9975	7.9972
	Couple	7.9968	7.9976	7.9970	**7.9971**
	Female(from Bell Labs)	7.9972	7.9969	7.9972	7.9971
$M - AES$	**Peppers**	7.9971	7.9974	7.9971	**7.9972**
	Lena	7.9974	7.9973	7.9973	**7.9973**
	Baboon	7.9971	7.9972	7.9972	7.9972
	Female	7.9971	7.9968	7.9970	7.9970
	House	7.9974	7.9970	7.9973	**7.9972**
	Couple	7.9970	7.9971	7.9968	7.9970
	Female (from Bell Labs)	7.9976	7.9975	7.9976	**7.9976**

Table 2 quantifies the average correlation coefficient in horizontal (H), vertical (V), and diagonal (D) directions for cipher image of $M - AES$. The results indicate that $M - AES$ are better than the AES to resist the statistical attack.

Figure 12 and 13 show the distribution of two adjacent pixels in V, H, and D of plain and encrypted images respectively. The figures obviously reveal that correlation coefficients between pixels in three components of the plain image and its corresponding encrypted image are very small which clarify that the encrypted image presents the properties of a random image and the M-AES surpasses the original AES in correlation which provides a high random image.

Table 2- Correlation coefficient result for AES and the $M - AES$

Image name	Direction	Original AES	$M - AES$
Peppers	H	-0.0173	**-0.0056**
	V	0.0062	**0.0001**
	D	0.0152	**-0.0017**
Lena	H	0.0044	**-0.0262**
	V	-0.0090	**-0.0019**
	D	**-0.0132**	-0.0200
Baboon	H	-0.0164	**-0.0071**
	V	-0.0036	**-0.0019**
	D	0.0062	**0.0007**
Female	H	-0.0170	**-0.0100**
	V	**-0.0062**	-0.0069
	D	**-0.0017**	-0.0082
House	H	0.0093	**0.0004**
	V	0.0132	**0.0098**
	D	-0.0288	**-0.0038**
Couple	H	-0.0013	**-0.0003**
	V	-0.0029	**-0.0025**
	D	-0.0196	**-0.0027**
Female(from Bell Labs)	H	0.0039	**-0.0119**
	V	-0.0033	**-0.0010**
	D	-0.0074	**-0.0042**

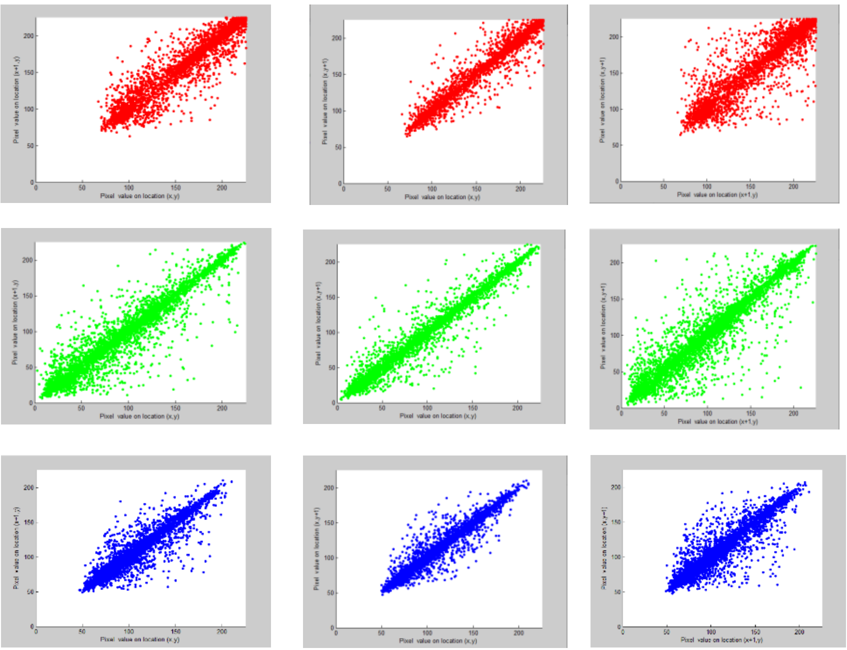


Figure 12-Correlation coefficient for Lena plain image. The 1st column presents vertical direction. The 2nd column presents horizontal direction. The 3rd column presents diagonal direction.

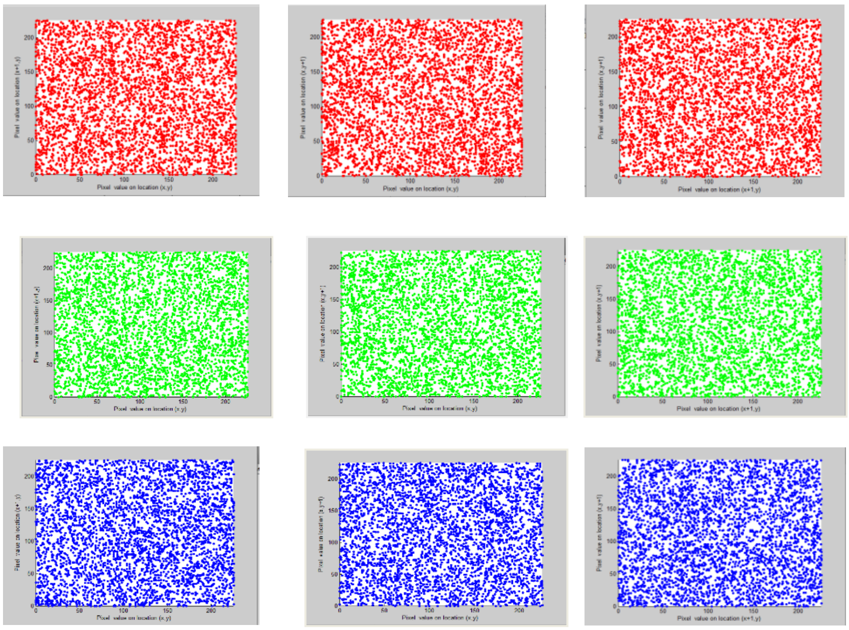


Figure 13- Correlation coefficient for Lena cipher image using $M-AES$. The 1st column presents vertical direction. The 2nd column presents horizontal direction. The 3rd column presents diagonal direction.

5.2 Evaluation concerning the differential attack

NPCR and UACI metrics are applied to analyze the impact of altering one pixel in the plain image on the cipher image that are calculated as in Equations 3 and 4 respectively [3].

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} D(i,j)}{MxN} \text{ x } 100\% \qquad \textbf{(3)}$$

Where: $\mathrm{D}\ (\mathrm{i},\mathrm{j}) = \begin{Bmatrix} 0, \text{if } C1(I,j) = C2(I,j) \\ 1, \text{if } C1(I,j) \neq C2(I,j) \end{Bmatrix}$

M and N are image width and height respectively, and $C1$ and $C2$ are encrypted images of the plain image and the modified one [18].

$$\mathrm{UACI} = \frac{1}{MxN}\left[\sum \frac{C1(i,j)-C2(i,j)}{255}\right] x\ 100\% \qquad \textbf{(4)}$$

Detailed results reported in Tables 3 and 4 clarify that $M-AES$ is very sensitive to a slight change of LSB of key and able to resist the differential attack.

Table 3-The value of NPCR for the cipher images using $M-AES$ after changing LSB of the secret key

Method	Image Name	R	G	B	Average
Original AES	**Peppers**	99.6323	99.5651	99.6048	99.6007
	Lena	99.6017	99.5789	99.5407	99.5738
	Baboon	99.6201	99.6429	99.6368	99.6333
	Female	99.6002	99.5865	99.5880	99.5916
	House	99.5987	99.6063	99.6384	99.6145
	Couple	99.6216	99.6399	99.6094	99.6236
	Female(from Bell Labs)	99.5865	99.5819	99.6323	99.6002

$M-AES$	**Peppers**	99.6002	99.6063	99.6140	**99.6068**
	Lena	99.6277	9.5987	99.6216	**99.6160**
	Baboon	99.5789	99.6368	99.6231	99.6129
	Female	99.6368	99.6536	99.5621	**99.6175**
	House	9.6460	9.6155	99.5911	**99.6175**
	Couple	99.6033	99.6338	99.6231	99.6201
	Female(from Bell Labs)	99.5956	99.5972	99.6155	**99.6028**

Table 4-UACI values of cipher images using $M-AES$ after changing LSB of the secret key

Method	**Image Name**	**R**	**G**	**B**	**Average**
Original AES	**Peppers**	33.4014	33.3982	33.3752	33.3916
	Lena	33.4410	33.4955	33.5230	33.4865
	Baboon	33.5588	33.3435	33.3404	33.4143
	Female	33.4608	33.6287	33.6418	33.5771
	House	33.4289	33.4042	33.5043	33.4458
	Couple	33.3567	33.3145	33.4543	33.3752
	Female(from Bell Labs)	33.3886	33.3892	33.5471	33.4416
$M-AES$	**Peppers**	33.4971	33.4445	33.5006	**33.4807**
	Lena	33.4761	33.5557	33.5782	**33.5367**
	Baboon	33.5738	33.4787	33.4770	**33.5098**
	Female	33.5242	33.4672	33.3680	33.4531
	House	33.4790	33.3363	33.5463	**33.4539**
	Couple	33.5911	33.5276	33.3132	**33.4773**
	Female(from Bell Labs)	33.4316	33.4344	33.6842	**33.5167**

5.1 Evaluation concerning MSE and PSNR

Mean Square Error (MSE) is used to assess the performance of using $M-AES$. MSE is denoted by Equation 5 [19].

$$\text{MSE} = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\text{C}\,(\text{i},\text{j})-\text{C}'(\text{i},\text{j}))^2\right) \qquad \textbf{(5)}$$

Where C (i, j) original image pixel, C′ (i, j) is encrypted image pixel and M and N are the size of the original or encrypted image.

Peak Signal-To-Noise Ratio (PSNR) is one of the metrics used to estimate encryption quality in the image encryption system [3]. PSNR is defined in Equation 6

$$PSNR = 10 \times log_{10}\left[\frac{M\times N\times 255^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(p(i,j)-c(i,j))2}\right] \quad \textbf{(6)}$$

The results from Table 5 point out that the MSE value between the cipher image and the plain image is large. This means $M - AES$ is more immunity to attacks than the original AES.

Table 5-MSE value between original images and the corresponding encrypted by the M-AES

Method	Image Name	R	G	B	Average
Original AES	**Peppers**	7978.1	1097.1	1097.2	9973.7
	Lena	1056.1	8933.2	7025.4	**8840.0**
	Baboon	8241.1	7195.9	8968.2	8135.1
	Female	9295.9	9123.0	7007.4	8475.4
	House	6844.5	8680.9	9545.9	8357.1
	Couple	1402.5	1593.4	1616.1	1537.3
	Female(from Bell Labs)	6753.5	6527.2	6538.4	**6606.4**
$M - AES$	**Peppers**	7893.9	1105.6	1103.8	**9996.2**
	Lena	1053.9	8890.3	7034.4	8821.4
	Baboon	8239.0	7260.5	8956.3	**8152.0**
	Female	9422.6	9092.8	7049.5	**8521.6**
	House	6819.7	8630.8	9625.0	**8358.5**
	Couple	1409.8	1592.6	1626.2	**1542.8**
	Female(from Bell Labs)	6642.5	6427.6	6549.8	6539.9

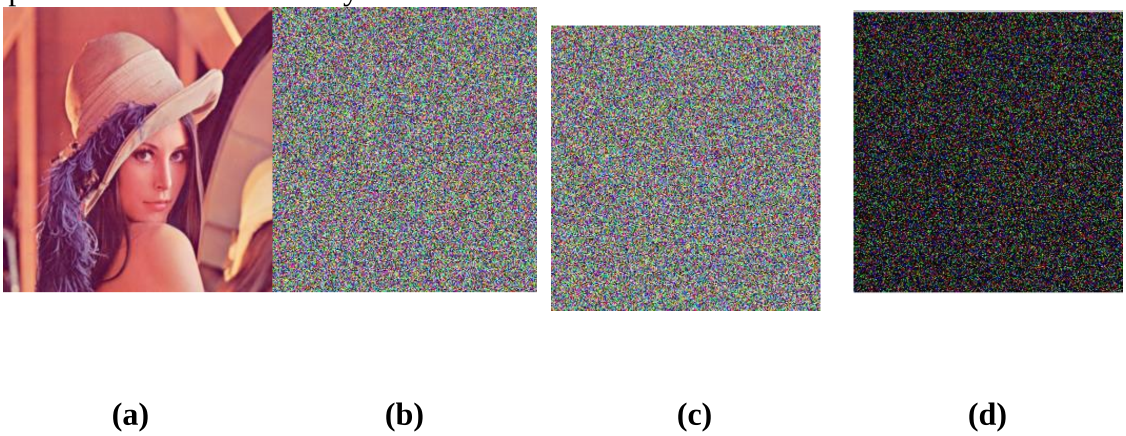
The PSNR value between the original image and the encrypted one is listed in Table 6. Results reveal that $PSNR$ values between the original and encrypted images via $M - AES$ are small and better than the original algorithm which means that the attacker unable to recognize the image.

Table 6-PSNR value between original images and the corresponding encrypted by the M-AES

Method	Image Name	R	G	B	Average
Original AES	**Peppers**	9.1118	7.7284	7.7279	8.1423
	Lena	7.8936	8.6207	9.6641	**8.6663**
	Baboon	8.9710	9.5599	8.6037	9.0272
	Female	8.4479	8.5294	9.6752	8.8492
	House	9.7774	8.7452	8.3326	8.9103
	Couple	6.6619	6.1075	6.0462	6.2631
	Female(from Bell Labs)	9.8355	9.9836	9.9761	**9.9312**
$\boldsymbol{M-AES}$	**Peppers**	9.1579	7.6947	7.7017	**8.1325**
	Lena	7.9026	8.6416	9.6585	8.6754
	Baboon	8.9720	9.5211	8.6095	**9.0182**
	Female	8.3891	8.5438	9.6492	**8.8256**
	House	9.7932	8.7703	8.2968	**8.9095**
	Couple	6.6394	6.1098	6.0191	**6.2476**
	Female(from Bell Labs)	9.9075	10.0503	9.9686	9.9751

5.4 Evaluation concerning the key sensitivity analysis

Key sensitivity is a significant influence on the security of the cryptosystem. The changes of one bit in the secret key have to be followed by the generation of a completely different encrypted result [18]. A good encryption algorithm should be highly sensitive to change in the secret key [20]. $M-AES$ proves the high sensitivity of the encryption key as shown in Figure 14 that depicts the key sensitivity of $M-AES$ regarding of encryption and decryption respectively, where the keys $K1$ and $K2$ and $K3$ are differed in one bit. The figure shows that decryption process is not capable of recovering the original image when a slightly change was performed to the secret key.



(a) **(b)** **(c)** **(d)**

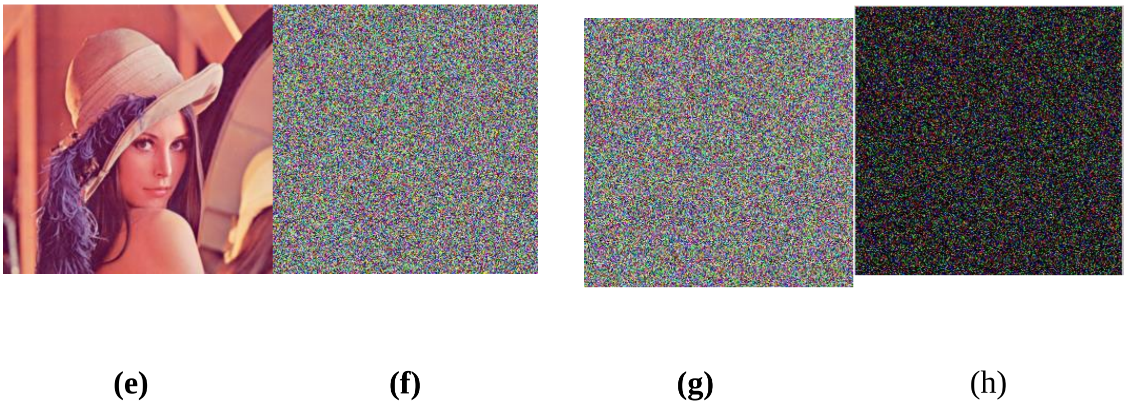


Figure 14-Key sensitivity results. (a) (plain image) Lena, (b) cipher image (*C1*) that encrypted with $K1$, (c) cipher image (*C2*) that encrypted with $K2$, (d) cipher image difference $C1 - C2$;(e) decipher image *D1* that decrypted (*C1*) with *K1*,(f) decipher image *D2* that decrypted (*C1*) with $K2$,(g) decipher image *D3* that decrypted (*C1*) with $K3$,(h) decipher image difference $D3 - D2$ ($K1$ and $K2$ are different only in one bit; $K2$ and $K3$ are also different only in one bit; and $K1 \neq K3$).

6. Conclusions

This paper proposed a modification to the AES algorithm for color image encryption, which is called a Modified Advanced Encryption Standard (M − AES) to improve the security level of the encryption process. The modification is conducting on the ShiftRows step of the original AES algorithm by replacing it with two steps. First step is done by re-arranging columns of the state array, and second step is done by conducting zigzag transformation on the state array. Through the evaluation of $M - AES$, the results clearly showed that the proposed method exhibits the lowest correlation coefficients among pixels in the encrypted image of the original AES algorithm ,and the results of some metrics, such as entropy, histogram distribution, proved that the $M - AES$ is strong against Statistical attacks. The results show that $M - AES$ method provides good encryption quality compared with the AES algorithm. The $M - AES$ is sensitive to any changes that occur in the secret key, thus making the $M - AES$ method robust against any attack. Differential analysis shows that the $M - AES$ is robust, and that it prevents differential attacks. Through the evaluation of $M - AES$, the results show that it provides a better security level when a comparison was made with AES. Therefore, M − AES is highly secure and is suitable for color image encryption.

References

[1] Gamido, H. V., Sison, A. M., & Medina, R. P., “Modified AES For Text And Image Encryption,” *Indonesian Journal Of Electrical Engineering and Computer Science*, vol. 11, no. 3, pp. 942-948, 2018.

[2] Hoomod, H. K., & Zewayr, M.H., “Image Encryption Using Modified AES with Bio-Chaotic,” *International Journal of Advances in Scientific Research and Engineering* (IJASRE) (pp.8-31), pp. 2454-8006, 2016.

[3] Abdulgader, A., Ismail, M., Zainal, N., & Idbeaa, T., “Enhancement of AES Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption,” *Journal of Theoretical and Applied Information Technology*, vol. 71, no. 1, 2005-2015 (pp. 1-12), 2015.

[4] Thinn, A. A., & Thwin, M. M. S., “Modification of AES Algorithm By Using Second Key And Modified Subbytes Operation For Text Encryption,” In *Computational Science and Technology* , Springer, Singapore, pp. 435-444, 2019.

[5] Lavanya, R., & Karpagam, M., "Enhancing the Security of AES Through Small Scale Confusion Operations for Data communication," *Microprocessors and Microsystems*, pp. pp. 1-11, 103041, 2020.

[6] Wadi, S. M., & Zainal, N., "High Definition Image Encryption Algorithm Based on AES Modification," *Wireless Personal Communications*, vol. 79, no. 2, pp. 811-829, 2014.

[7] Kaur, H., & Mehla, R., "Image Encryption Using AES with Modified Transformation," *International Journal of Science and Research* (IJSR), vol. 3, no. 7, pp. 360-363, 2014.

[8] Vaidehi, M., & Rabi, B. J., "Enhanced MixColumns Design for AES Encryption," *Indian Journal of Science and Technology*, vol. 8, no. 35, pp. 1-7, 2015.

[9] Alabaichi, A., & Salih, A. I. , "Enhance Security of Advance Encryption Standard Algorithm Based on Key-Dependent S-box," In 5th International Conference on Digital Information Processing and Communications (ICDIPC) ,IEEE, pp. 44-53, 2015.

[10] Riyaldhi, R., & Kurniawan, A., "Improvement of Advanced Encryption Standard Algorithm With Shift Row And S. Box Modification Mapping In Mix Column," *Procedia Computer Science*, vol. 116, pp. 401-407, 2017.

[11] D'Souza, F. J., & Panchal, D., "Advanced Encryption Standard (AES) Security Enhancement Using Hybrid Approach," International Conference on Computing, Communication and Automation (ICCCA), IEEE, pp. 647-652, 2017.

[12] Wenceslao Jr, F. V., "Enhancing the Performance of the Advanced Encryption Standard (AES) Algorithm Using Multiple Substitution Boxes," *International Journal of Communication Networks and Information Security*, vol. 10, no. 3, pp. 496-50, 2018.

[13] Singh, A., Agarwal, P., & Chand, M., "Image Encryption and Analysis Using Dynamic AES," In 5th International Conference on Optimization and Applications (ICOA), IEEE, pp. 1-6, 2019.

[14] Kumar, T. M., & Karthigaikumar, P., "A Novel Method Of Improvement In Advanced Encryption Standard Algorithm With Dynamic Shift Rows, Sub Byte And Mixcolumn Operations For The Secure Communication," *International Journal of Information Technology*, pp. 1-6, 2020.

[15] Hameed, M. E., Ibrahim, M. M., & Abd Manap, N., "Review on Improvement of Advanced Encryption Standard (AES) Algorithm Based on Time Execution, Differential Cryptanalysis and Level of Security," *Journal of Telecommunication, Electronic and Computer Engineering* (JTEC), vol. 10, no. 1, pp. 139-145, 2018.

[16] Arab, A., Rostami, M. J., & Ghavami, B., "An Image Encryption Method Based On Chaos System And AES Algorithm," *The Journal Of Supercomputing*, vol. 75, no. 10, pp. 6663-6682, 2019.

[17] Ghadirli, H. M., Nodehi, A., & Enayatifar, R., "An Overview Of Encryption Algorithms In Color Images,". *Signal Processing*, vol. 164, pp. 163-185, 2019.

[18] Zahmoul, R., Ejbali, R., & Zaied, M., "Image Encryption Based On New Beta Chaotic Maps," *Optics And Lasers In Engineering*, vol. 96, pp. 39-49, 2017.

[19] Taqi, I. A., & Hameed, S. M., "A New Beta Chaotic Map with DNA Encoding for Color Image Encryption," *Science*, vol. 61, no. 9, pp. 2371-2384, 2020.

[20] Gamido, H. V., Sison, A. M., & Medina, R. P., "Implementation of Modified AES as Image Encryption Scheme," *Indonesian Journal of Electrical Engineering and Informatics* (IJEEI), vol. 6, no. 3, pp. 301-308, 2018.