Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCEMENT OF AES ALGORITHM BASED ON CHAOTIC MAPS AND SHIFT OPERATION FOR IMAGE ENCRYPTION

[1]ALI ABDULGADER, [2]MAHAMOD ISMAIL, [3]NASHARUDDIN ZAINAL, [4]TARIK IDBEAA
[1,2,3,4] Department of Electrical, Electronic and Systems Engineering, Faculty of Engineering,
Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
E-mail: [1]aliabdulgader2004@yahoo.com, [2]mahamod@eng.ukm.my,[3] nash@eng.ukm.my, [4]tidbeaa@yahoo.com

ABSTRACT

With the rapid development of the Internet and communication networks, the confidentiality of digital images transmitted over public networks must be preserved by using encryption techniques. Advanced Encryption Standard (AES) is one of the most commonly used encryption algorithms at present. Although AES has several advantages, such as security in data encryption, it also has a number of drawbacks, such as high computations, pattern problems when used for encrypting images, and fixed S-box weak points. This paper proposes a method that overcomes the fixed S-box weak points and improves the performance of AES when used for encrypting images, particularly when the image data are large. In addition, the MixColumn stage is replaced by chaotic mapping and XOR operation to reduce the high computations in MixColumn transform. The proposed method is tested on several images, and the results show that the proposed method efficiently generated cipher images with very low correlation coefficients of adjacent pixels and provided better encryption speed and high security as a result of the dependence of the S-box on the key characteristics of the chaotic system.

Keywords: *AES, S-Box, Cyclic Shifting Operation, Inverse S-Box, Round Key, Chaotic Map.*

1. INTRODUCTION

This With the continuing development of both computer and Internet technology, multimedia data (images, videos, audios, etc.) are being widely used in applications, such as video on demand, video conferencing, broadcasting, and so on. Nowadays, multimedia data are highly associated with many aspects of daily life, including education, commerce, and politics. Thus, multimedia data must be protected against unauthorized access. Multimedia contents are protected by using various security methods before being stored or transmitted over the network [2]. However, encryption is hindered by the large size of images or videos. Large volume of multimedia data would be difficult to encrypt using a traditional encryption algorithm. Algorithms that require less computation and have good level security are necessary in encrypting any multimedia data [1]-[3]. Advanced Encryption Standard (AES) is one of the methods for protecting multimedia data. However, AES has a number of drawbacks, such as high computations, pattern appearance problems and very slow when used for encrypting images.

Several methods and techniques have been proposed to modify the AES algorithm for image encryption. Muhaya and Fahad [4] proposed a new modified version of the AES algorithm, which uses chaotic key generator for satellite imagery security. The chaotic key generator uses six chaotic maps, namely, Logistic, Tent, Henon, Sine, Cubic, and Chebyshev, to achieve high-level security, sufficiently large key space with improved confusion and diffusion properties, and key sensitivity encryption process. Tran et al. and Chen et al. [5] proposed enhanced the security of the S-box by adding binary Gray code transformation as a preprocessing step to the original AES S-box. This approach increases the security of the S-box against algebraic and interpolation attacks. In this method, the Gray S-box inherits all of the advantages and efficiencies of any existing optimized implementation of the AES S-box. Zeghid and Medien [6] proposed a method that adds a key

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

stream generator (A5/1, W7) to AES to increase its image encryption security and performance. This technique offers high security and can be easily achieved in both hardware and software. Ghulam Murtaza and Azhar Ali [7] proposed replacing MixColumn transformation with dynamic Mix-Column transformation in AES encryption by using dynamic MDS (Maximum Distance Separable) matrices based on m-bit additional secret key. This mechanism increases a brute force attack complexity by m-bit to the original key. Two direct methods were proposed by Huang et al. [8] and Telegraph et al. to modify the AES–ECB mode operation and overcome the pattern appearance problem of an encrypted image. In the first method, an additional key is used to ensure that each block in the image file is different, and that the original secret key input before encryption or decryption is used for each round within a block. The second approach uses image compression to decrease image size and prevent pattern appearance. Kamali et al. [9] and Telagarapu et al. [10] modified the AES algorithm by adjusting the ShiftRow transformation to increase the security of the algorithm. Depending on whether the value on the first row and the first column of the stats is odd or even,the two rows of the state are shifted to the left with a certain offset. Salim Wadi and Nasharuddin Zaina [11] proposed two modifications for enhancing the performance of the AES algorithm and making it more suitable for encrypting HD images. The first modification is performed by decreasing the number of rounds to one instead of ten to reduce encryption time. The second modification is replacing the S-box with a new one to decrease the computation amount and to satisfy the hardware requirements.

This paper is concerned with enhancing the existing standards of cryptography (AES) to encrypt image data. Modifications are made on the S-box and on MixColumn transformation. In the proposed method, the S-box changes in each round depending on the round key to increase the difficulty of an attacker in performing any offline analysis of the S-box. This modification increases the efficiency of encryption and speeds up the algorithm. This paper is organized as follows. Brief introductions on AES and chaotic maps are presented in Sections 2 and 3, respectively. The proposed method is discussed in Section 4. The experimental results are discussed in Section 5. The paper is concluded in Section 6.

2. ADVANCED ENCRYPTION STANDARD ALGORITHM

This section provides a brief overview of the AES algorithm. The AES algorithm is a symmetric encryption algorithm that operates on a 4×4 array of bytes (128 bits), called a state with key length of 128, 192, or 256 bits. The state is encrypted or decrypted by applying four transformations for a specific number of rounds (10, 12, or 14) depending on the key length (128, 192, or 256 bits). The AES cipher uses plaintext as input along with the cipher key, and its output is the encrypted data [12]. The AES algorithm as shown in Figure 1 consists of the following phases:

- Key Expansion, in which the round keys are derived from the cipher key by using the Key Expansion algorithm.
- Initial Round, which consists of AddRoundKey, where each byte of the state is combined with the round key using a bitwise operation

The other rounds (Nr = 1 toNr-1) repeatedly perform the following transformations:

- SubBytes transformation is a non-linear substitution where each byte is replaced with another on the basis of the S-box. The numbers inside the S-box are calculated by a finite field inversion followed by an affine transformation.
- ShiftRows transformation is a cyclic shifting operation that rotates the rows of the state with different numbers of bytes (offsets). The offset is equal to the row index: the second row is shifted one byte to the left, the third row two bytes to the left, the fourth row three bytes to the left, and the first row four bytes to the left.
- MixColumn transformation mixes the bytes in each column by multiplying the state with the polynomial modulo x^4+1. The state bytes are the coefficients of the polynomial.
- AddRoundKey transformation is an XOR operation that adds the round key to the results of MixColumn. Final Round consists of SubBytes, ShiftRows, and AddRoundKey [1, 2,11].

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

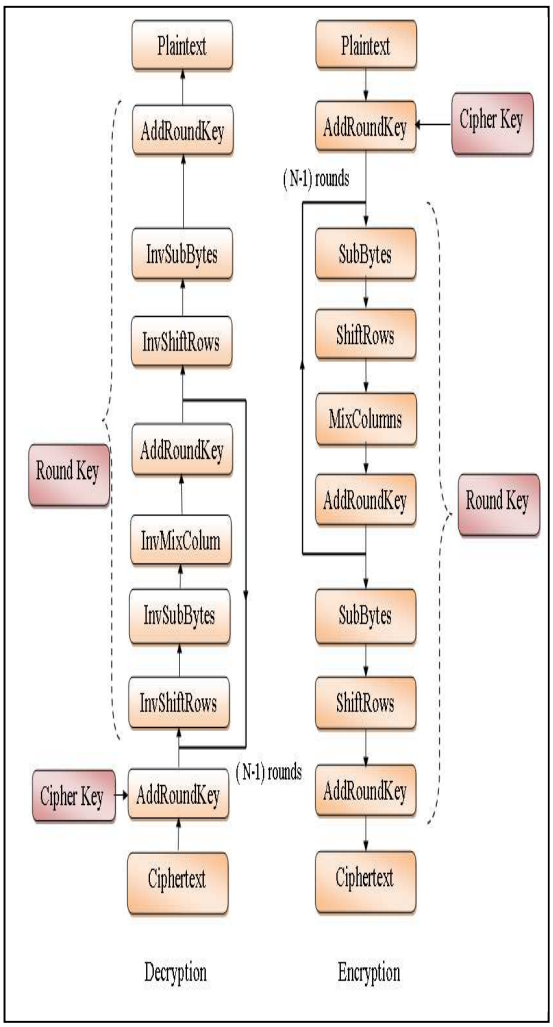


Figure 1: Block Diagram Of The Advanced Encryption Standard Algorithm

3. CHAOTIC MAPS

Chaotic maps have gained considerable attention from cryptography researchers who wish to develop encryption schemes. Chaotic encryption schemes can be developed by using properties of chaos, including deterministic dynamics, random behavior, and nonlinear transform [13–15]. These features allow chaos-based encryption to perform better confusion and diffusion in the encryption system. A type of chaotic map is the Arnold Cat Map, which can be expressed in matrix form in Equation 1.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \quad (1)$$

where x and y are the positions of the element of the $N \times N$ matrix, and p and q are the positive integer parameters. The Arnold Cat Map has the property of shuffling the position of the matrix and then returning the same position of the element as in the original matrix after a certain number of iterations. In this paper, the encryption method is based on the Arnold Cat Map to fulfill the requirements of secure image transmission. The Arnold Cat Map did not change the pixel values but changed their positions. The shuffling parameters in the Arnold Cat Map p and q and number of iterations are important in shuffling the image, and they can be used as secret keys in the encryption algorithm [16–18].

4. PROPOSED MODIFICATIONS IN THE AES ALGORITHM

The proposed encryption algorithm is a block cipher that combines a chaotic system with the conventional encryption algorithms, such as AES, in CBC mode. This paper aims to increase the efficiency of the image encryption system by making some modifications within the AES. These modifications aim to reduce the encryption and decryption time in the image encryption because the AES takes a very long time to encrypt color image. These modifications are as follows:

- The implementation of some circular shift on the S-box based on the round keys to overcome the weakness of the fixed S-box and high calculation in the AES and improve key sensitivity.
- The replacement of the MixColumn step with the chaotic system to reduce the computation amount in the AES. The MixColumn stage that is used to diffuse the data in the AES algorithm takes large calculations that slow down the AES algorithm. The other two stages remain unchanged within the AES.

The proposed algorithm uses the principle of the shift register technique. During the encryption, the values in the AES S-box circularly right shift with a shift amount, which is based on the round secret key that is produced by the key schedule algorithm in the AES algorithm. At each round, the new AES S-box that is based on the secret key will be used for a byte substitution. The following is an example that shows how the AES S-box is circularly shifted to the left: Assuming the round key in i^{th} round as in Figure 2 (a) and the original

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AES S-box as in Figure 2(b) will be circularly shifted using the shift amount computed by Equation 2, then the new AES S-box now depends on the round key, as shown in Figure 2 (c).

$$sh = \left(\sum_{m=1}^{m=16} round_{key_i}(m) \right) \bmod 16 \qquad (2)$$

48	52	56	99
49	53	57	100
50	54	97	101
48	52	56	99

(a)

99	202	183	4	9	83	208	81	205	96	224	231	186	112	225	140
124	130	253	199	131	209	239	163	12	129	50	200	120	62	248	161
119	201	147	35	44	0	170	64	19	79	58	55	37	181	152	137
123	125	38	195	26	237	251	143	236	220	10	109	46	102	17	13
242	250	54	24	27	32	67	146	95	34	73	141	28	72	105	191
107	89	63	150	110	252	77	157	151	42	6	213	166	3	217	230
111	71	247	5	90	177	51	56	68	144	36	78	180	246	142	66
197	240	204	154	160	91	133	245	23	136	92	169	198	14	148	104
48	173	52	7	82	106	69	188	196	70	194	108	232	97	155	65
1	212	165	18	59	203	249	182	167	238	211	86	221	53	30	153
103	162	229	128	214	190	2	218	126	184	172	244	116	87	135	45
43	175	241	226	179	57	127	33	61	20	98	234	31	185	233	15
254	156	113	235	41	74	80	16	100	222	145	101	75	134	206	176
215	164	216	39	227	76	60	255	93	94	149	122	189	193	85	84
171	114	49	178	47	88	159	243	25	11	228	174	139	29	40	187
118	192	21	117	132	207	168	210	115	219	121	8	138	158	223	22

(b)

21	117	132	207	168	210	115	219	121	8	138	158	223	22	99	202
183	4	9	83	208	81	205	96	224	231	186	112	225	140	118	192
253	199	131	209	239	163	12	129	50	200	120	62	248	161	124	130
147	35	44	0	170	64	19	79	58	55	37	181	152	137	119	201
38	195	26	237	251	143	236	220	10	109	46	102	17	13	123	125
54	24	27	32	67	146	95	34	73	141	28	72	105	191	242	250
63	150	110	252	77	157	151	42	6	213	166	3	217	230	107	89
247	5	90	177	51	56	68	144	36	78	180	246	142	66	111	71
204	154	160	91	133	245	23	136	92	169	198	14	148	104	197	240
52	7	82	106	69	188	196	70	194	108	232	97	155	65	48	173
165	18	59	203	249	182	167	238	211	86	221	53	30	153	1	212
229	128	214	190	2	218	126	184	172	244	116	87	135	45	103	162
241	226	179	57	127	33	61	20	98	234	31	185	233	15	43	175
113	235	41	74	80	16	100	222	145	101	75	134	206	176	254	156
216	39	227	76	60	255	93	94	149	122	189	193	85	84	215	164
49	178	47	88	159	243	25	11	228	174	139	29	40	187	171	114

(c)

Figure 2: Shift Process Of The AES S-Box. (A) Example Of The Round Key. (B) S-Box Before Shift Process. (C) S-Box After Shift Process (Sh = 98 Mod 16).

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the permutation process, the positions of the element of the state array after the shift row stage are scrambled using an Arnold Cat Map. Fig.3 shows an example of scrambling the position of the element of the state array by applying the cat map with two parameters (p=5, q=17) and one-time iteration.

21	177	42	112
147	252	25	88
164	233	151	164
202	132	74	2

(a)

164	132	112	252
202	42	147	151
177	88	233	2
25	164	74	21

(b)

Figure 3: (A) State Array Before Permutation. (B) State Array After Permutation.

The general structure of the proposed algorithm is shown in Fig.4. The complete description of each step of the proposed method for encryption and decryption is as follows:

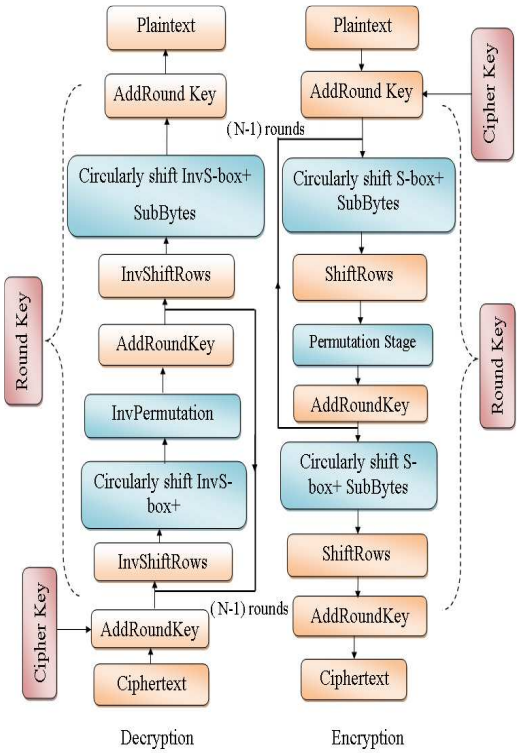


Fig.4. General Structure Of The Proposed Modified AES Algorithm

4.1 Encryption Steps

1. Read and divide the original image into several blocks of the size 128 bits. Each block is placed into the state array that is changed at every stage of the encryption process. At the end, the state is placed within the output matrix.
2. Input the secret key and the two positive integer parameters of the Arnold Cat Map (p and q).
3. The key length in the proposed algorithm is 128 bits. The input secret key has been expanded into a matrix of 44 words (176 bytes) by using the key expansion algorithm to provide a 4-word round key for each round in the encryption process.
4. AddRound key: The 16 bytes in the current block will be bitwise XOR with the 16 bytes of the round key.
5. Circularly shift the S-box value with a shift value that is derived from the round key using the sum of all round key bytes at each round.

$$shift_{value} = (\sum round_{key}) \bmod 256 \quad (3)$$

The new S-box now depends on the key, and it will be used to perform a byte-to-byte substitution of the state.

6. Shift rows: A simple permutation of the state array. In the shift row stage, the first row of the state array is not changed. In the second row of the state array, 1byte is shifted to the left. In the third row, 2bytes are shifted to the left. In the fourth row, 3 bytes are shifted to the left.
7. Use an Arnold Cat Map instead of MixColumn to perform a scramble of the state array. The scramble of the state array depends on the number of iterations that are based on the number of rounds (in this paper, the number of rounds is 10) and two positive integer parameters of the Arnold Cat Map (p>=1andq>=1).
8. The diffusion process is performed as follows: For vertical diffusion, the first row of state array is not changed, and the second row is changed by XOR of the bytes in the first row with bytes of the second row. The third row is modified by XOR of the new second and third rows. The fourth row is changed by XOR on the new third and fourth rows. For horizontal diffusion, the modification of the second column in the state array is made by XOR of the first and second columns and the

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

modification of the third column by XOR of the modified second and third columns. The fourth column is changed by using the XOR operation between the new third and fourth columns.

9. Add the round key to the current block.
10. The output is an encrypted image.

4.2 Decryption Steps

1. Read an encrypted image file.
2. The same secret keys and two parameters of the Arnold Cat Map (p and q) will be used as inputs in the decryption process.
3. Add the round key to the state array.
4. Perform inverse Shift rows in the state array.
5. Use an inverse S-box in performing a byte-to-byte substitution of the block,
6. Subtract each byte in the state array from the shift value that is derived from the round key. The result is new state array as in equation

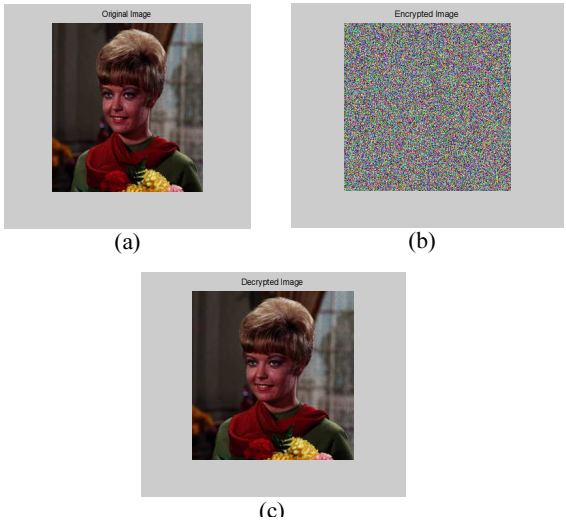
$$st_{array} = (st_{array} - sh_{value}) \bmod 256 \quad (4)$$

Where *st* is state array and *sh* is shift value.

7. Add the round key to the state array.
8. Perform the diffusion process in the reverse direction for every last three rows and for every last three columns in the state array (the first row should remain unchanged).
9. Descramble the state array by using an Arnold Cat Map instead of the inverse MixColumn; descrambling the state array depends on the number of iterations that are based on the number of rounds and two parameters of the Arnold Cat Map (p and q).
10. After N rounds, add the round key to the state array. The result is the decrypted image.

5. EXPERIMENTAL RESULTS

A series of experiments were conducted using different 24-bit color images in different sizes, as shown in Figure 5 (a).These images are available at the USC–SIPI image database in TIFF format [19]. Many experiments performed in this section show the efficiency of the proposed algorithm. The experiments are performed on a computer with Intel Core i5 CPU @ 3 GHz, 4G RAM with Windows 7 using MATLAB. The original images are encrypted using the proposed method with a key = {023456789ABCDEF} and p=5, q=17. Figure 5 (b) and (c) show the encrypted and decrypted images using the proposed method.



(a) (b) (c)

Figure 5: (A) Original Image. (B) Encrypted Image Using The Proposed Method. (C) Decrypted Image Using The Proposed Method

5.1 Histogram Analysis

The histogram is a graphical representation show the distribution of pixels within the image at every different intensity value in that image [13, 15, 18]. In this test, the image *(Giral.tiff)* is encrypted with the same key by using the AES algorithm and the proposed method. The histogram graphs of the original and encrypted images of the different channels are shown in Figure 6(a) to 6(i). Figure 6 clearly shows that the histogram of the encrypted image is different from that of the original image, and it is uniformly distributed. Therefore, the encrypted image that results from using the proposed method does not offer any trace that may be exploited by any statistical attacker.

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

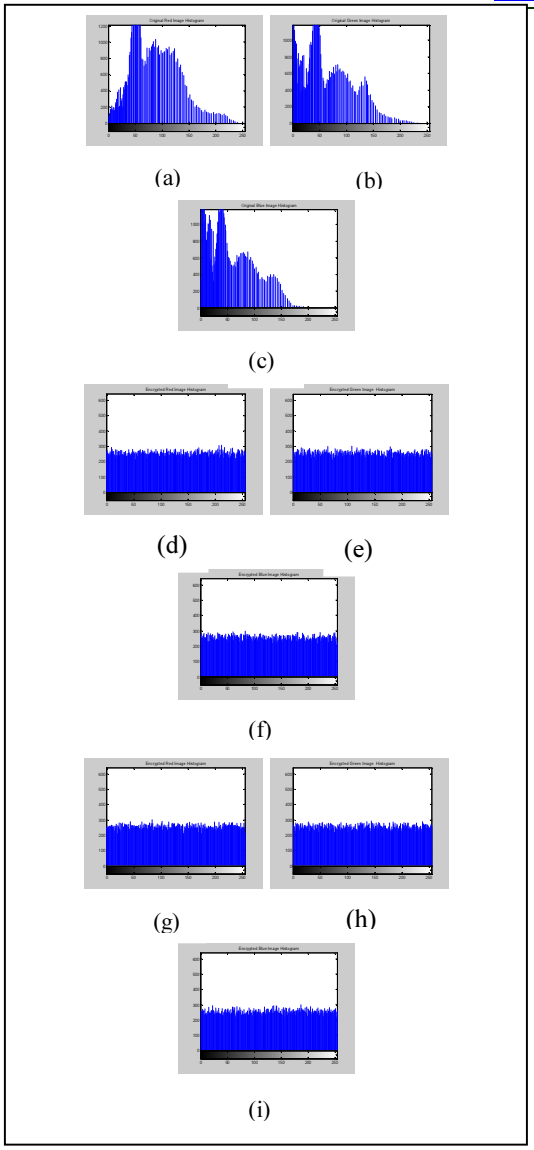


Figure 6: Histogram Analysis: (A), (B), And (C) Are The Histograms Of The Original Image (Red, Green, And Blue Channels). (D), (E), And (F) Are The Histograms Of The Encrypted Image Using The AES Algorithm (Red, Green, And Blue Channels). (G), (H), And (I) Are The Histograms Of The Encrypted Image Using The Proposed Method (Red. Green. And Blue Channels).

5.2 Correlation Coefficient Analysis

The correlation coefficient is a statistical calculation with a range value between −1 and+1, and it is used to study the relationship between two variables of data [20]. The pixels in the image are usually strongly correlated with the adjacent pixels whether in horizontal, vertical, or diagonal directions. The correlation coefficient between pixels in the original and encrypted images is computed by Eq 5:

$$C = \frac{\sum_m \sum_n \left(A_{mn} - \bar{A}\right)\left(B_{mn} - \bar{B}\right)}{\sqrt{\left[\sum_m \sum_n \left(A_{mn} - \bar{A}\right)^2\right]\left[\sum_m \sum_n \left(B_{mn} - \bar{B}\right)^2\right]}} \quad (5)$$

where A and B are the matrices of the same size and $\bar{A} = mean(A)$ and $\bar{B} = mean(B)$. In this test, 2000 pairs of pixels in the original and encrypted images were randomly selected and their correlation coefficient was computed. Table 1 shows the correlation coefficients for both original image (Girl.tiff) and its corresponding encrypted image in horizontal, vertical, and diagonal directions that are encrypted by the AES algorithm, the proposed AES version by Kamali and Shakerian [9], and the proposed method in this paper. Table 1 clearly shows that the value of correlation coefficients of the proposed method is very low compared with the method of Kamali and Shakerian [9]. The correlation coefficient near zero indicates that very little correlation exists between the pixels, which mean these methods are secure against various attacks.

Table 1: Correlation Coefficient of Two Adjacent Pixels in the Original and Encrypted Images.

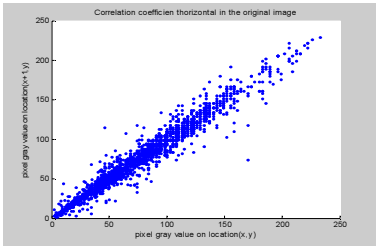
	Correlation coefficient analysis of adjacent pixels		
	Horizontal	Vertical	Diagonal
Original image *(Girl.tiff)*	0.9729	0.9622	0.9482
Original AES	−0.0024	0.0009	−0.0023
Method by Kamali [9]	−0.0019	−0.0030	−0.0012
Proposed method	−0.0013	−0.0020	0.0080

Figure 7(a) to Figure 7 (f) shows the distribution of two adjacent pixels in horizontal, vertical, and diagonal directions in the original and encrypted images. Figure 7 obviously show that the correlation coefficients are very small between pixels in different channels of the original image and its corresponding encrypted image. This result indicates that the encrypted

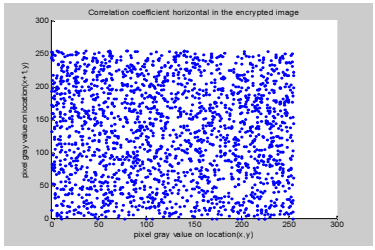
Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

image exhibits the characteristics of a random image.



(a)



(b)

Figure 7: (A) And (B) Show The Distribution Of Two Horizontal Adjacent Pixels In Red Channel Of The Original And Encrypted Image (Girl.Tiff).

5.3 Entropy Analysis

Entropy is a measurement of the uncertainty associated with a random variable in information theory [21]. The entropy is computed in bits. The entropy (E) of the image is calculated using Eq 6:

$$E = \sum \left[P(m_i) \times log_2 \left(\frac{1}{P(m_i)} \right) \right] \quad (6)$$

Where $P(m_i)$ represents the probability of the symbol m_i . If 2^8 symbols with equal probability and after applying Eq 6, the ideal entropy of encrypted messages should be equal to 8, corresponding to a truly random source. Indeed, the entropy value of the practical information source is lower than the ideal because a random message generated by a practical information source is not often random. In most cases, breaking an encryption system is difficult to perform if the entropy value of the cipher algorithm is close to the ideal. Table 3 shows the entropy values of the original and encrypted images using the AES algorithm, the method by Kamali and Shakerian [9], and the proposed method in this paper. The results in Table 3 prove that the entropy values for the proposed method and that proposed method by Kamali and Shakerian [9] are very close to the ideal value and better than values of the original AES algorithm exhibits the best values. From the result and compared with the AES algorithm, the proposed method has good encryption quality and is secure against entropy-based attacks.

Table 3: Entropy Values of The Original and Encrypted Images

Image		Girl 256×256	Mandrill 512×512	Flower 1024×1024
Original image	R	6.4200	7.7066	6.3959
	G	6.4456	7.4744	6.4962
	B	6.3807	7.7522	6.5232
Original AES	R	7.9971	7.9993	7.9998
	G	7.9971	7.9993	7.9998
	B	7.9971	7.9992	7.9998
Method by Kamali [9]	R	7.9972	7.9992	7.9999
	G	7.9970	7.9993	7.9999
	B	7.9974	7.9993	7.9999
Proposed method	R	7.9974	7.9993	7.9999
	G	7.9975	7.9992	7.9999
	B	7.9972	7.9992	7.9999

5.4 Difference between Encrypted and Original Images (Differential Attack)

In differential attack analysis, attackers try to determine a relationship between the plain and the cipher images by studying how differences in an input can affect the resultant difference at the output to obtain the key [22]. To maintain high security, a big difference among encrypted forms is expected, which also measures the efficiency of the diffusion phase. Two common measures are used to test the influence of one pixel change on the whole encrypted image by the proposed scheme: number of pixel change rate (NPCR) and unified average changing intensity (UACI). NPCR means the number of pixels that change in the cipher image when only one pixel is changed

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in the plain image. UACI measures the average intensity of differences between the plain and the cipher images. NPCR is given by the following:

$$NPCR = \frac{\sum_{r=1}^{H}\sum_{c=1}^{W} D(r,c)}{H \times W} \times 100 \quad (7)$$

where $D(r, c)$ indicates the modification in the pixel of the image because of the encryption of a monochrome image, as shown below:

$$D(r,c) = \begin{cases} 0 & if \quad P(r,c) = C(r,c) \\ 1 & if \quad P(r,c) \neq C(r,c) \end{cases} \quad (8)$$

The UACI is represented by Eq 9:

$$UACI = \frac{1}{H \times W} \sum_{r=1}^{H}\sum_{c=1}^{W} \frac{|P(r,c) - C(r,c)|}{255} \times 100 \quad (9)$$

The results from the NPCR and UACI computations in Table 4 and Table 5 indicate that the proposed method for image encryption is highly sensitive with respect to small changes in the plain images. Therefore, the three methods are strongly capable of resisting the differential attack.

Table 4:NPCR Values of AES and The Proposed Modified AES.

		NPCR (%)		
Image	Color channels	Original AES	Method by Kamali	Proposed method
Girl	R	99.4430	99.484	99.461
	G	99.6017	99.623	99.641
	B	99.6261	99.600	99.592
Mandrill	R	99.5796	99.565	99.580
	G	99.5903	99.588	99.604
	B	99.6009	99.627	99.614
Flower	R	99.6014	99.599	99.601
	G	99.6060	99.610	99.621
	B	99.6157	99.617	99.612

Table 5:UACI Values of AES and The Proposed Modified AES

		UACI (%)		
Image	Color channels	Original AES	Method by Kamali	Proposed method
Girl	R	33.3622	33.4007	33.4948
	G	33.4800	33.5740	33.4955
	B	33.4052	33.3635	33.5165
Mandrill	R	33.3398	33.5295	33.4439
	G	33.4070	33.4733	33.5012
	B	33.4232	33.4897	33.5328
Flower	R	33.4505	33.4869	33.4749
	G	33.4703	33.4875	33.5063
	B	33.4255	33.4402	33.4698

5.5 Key Sensitivity and Key Space Analysis

The secret keys in the encryption algorithm should be very sensitive, and the key space should be large enough to prevent brute force attacks. The conception of the key space is the total number of the different keys, which can be employed during the encryption/decryption process. The secret key space of the proposed method consists of the user secret key of size of 2^{16} bits, two parameters of the Arnold Cat Map. It is large and necessary to resist all types of brute force attacks.

When a small change occurs between keys that are used for encryption and decryption, the encrypted image cannot be correctly decrypted. This condition is called sensitivity to secret keys. The proposed method in this paper is tested for different values of key, which are different from the original key in one digit to decrypt the encrypted image. The output image is totally different from the original image. Figure 8(a) and Figure 8 (b) show the original *(Girl.tiff)* and decrypted images by using the original secret key {023456789ABCDEF} (p=5, q=17). Figure 8(c) and Figure 8 (d) show the decryption image by using the secret key, which only slightly changes from the original {123456789ABCDEF} (p=5,q=17) (the first digit being 1 instead of 0) or has change in the Arnold Cat Map parameters (p and q) respectively. Obviously, the decrypted image by using a slightly different key is completely different from the original image. This result shows that the proposed method is

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

highly sensitive to any changes that occur to the secret key.

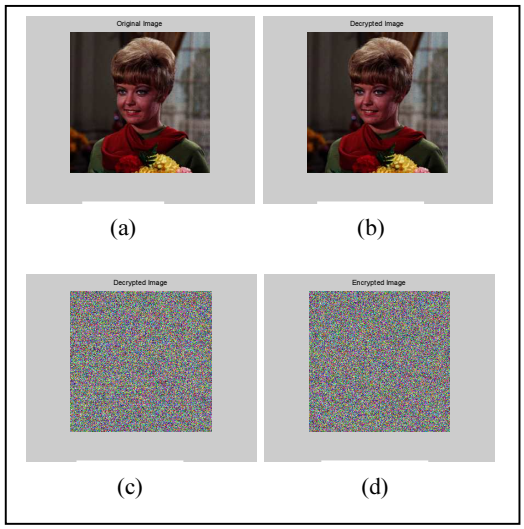


Figure 8: Key sensitivity test result. (a) Original image. (b) Decrypted image by the original secret key {023456789ABCDEF}(p=5;q=17). (c) Decrypted image by using the key {12345678ABCDEF} (p=5;qs=17). (d) Decrypted image by using the key has change in the Arnold Cat Map parameters {023456789ABCDEF} (p=5;q=7).

5.6 Encryption Quality Analysis

Peak Signal-to-Noise Ratio (PSNR) and structural similarity index measure (SSIM) calculations are performed to determine the encryption quality of the proposed method.

5.6.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR is one of the methods used to estimate the encryption quality in the image encryption system. PSNR measures the changes between each pixel in the original image and its corresponding encrypted image. Mathematically, PSNR is defined in Eq 10, and its unit measurement is decibel (dB).

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

M and N are the width and height respectively of the original image. P(i, j) is the pixel value of the original image at the point (i, j), and C (i, j) is the pixel value of the encrypted image. The PSNR values based on the proposed method compared with the values in the original AES are illustrated in Table 5. The table shows that the PSNR values for test images in the proposed method and the AES version by Kamali and Shakerian [9] are nearly similar and are best from the AES algorithm. The lower value of PSNR represents better encryption quality. This fact shows the high security of the proposed method.

Table 5: PSNR Values of Plain and Cipher Images.

Algorithm	Image File	PSNR for Red channel (dB)	PSNR for Green channel (dB)	PSNR for Blue channel (dB)
Original AES	Girl	8.1649	7.0802	6.8836
	Mandrill	8.8214	9.2707	8.4020
	Flower	5.5556	8.4563	7.5333
Method by Kamali [9]	Girl	8.1144	7.0460	6.8444
	Mandrill	8.8005	9.2728	8.4041
	Flower	5.5534	8.4598	7.5459
Proposed method	Girl	8.1141	7.0445	6.8141
	Mandrill	8.7547	9.2433	8.3636
	Flower	5.5554	8.4583	7.5432

5.6.2 Structural Similarity Index Measure (SSIM) Analysis

The SSIM is a quality metric used to measure the similarity between two images. It was developed by Wang et al. [23] and is considered to be correlated with the quality perception of the human visual system. Instead of using traditional error summation methods, the SSIM is designed by modeling any image distortion as a combination of three factors, namely, loss of correlation, luminance distortion, and contrast distortion. The SSIM metric is calculated using Eq 11:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (11)$$

where x is the original image, y the encrypted one, μ the average, σ the variance, and c1 and c2 the two constants. This formula applies to the luminance image to evaluate the image quality with a maximum value of 1 showing excellent quality. The SSIM values of the test image with and without encryption are shown in Table 6.The results clearly show that the proposed method and that proposed method by Kamali and Shakerian [9] have very low SSIM values compared with the AES algorithm.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 6: SIMM values of plain and cipher images

Algorithms	File description	Dimensions (w × h) pixels	SIMM
Original AES	Girl	256 × 256	0.0072
	Mandrill	512 × 512	0.0105
	Flower	1024×1024	0.0086
Method by Kamali [9]	Girl	256 × 256	0.0065
	Mandrill	512 × 512	0.0092
	Flower	1024×1024	0.0086
Proposed method	Girl	256 × 256	0.0068
	Mandrill	512 × 512	0.0087
	Flower	1024×1024	0.0086

5.7 Encryption/Decryption Speed Test

The encryption speed in this paper is analyzed by comparing the encryption and decryption time of the proposed algorithm with the AES algorithm and the proposed method by Kamali and Shakerian. The experiments are conducted under MATLAB in a computer with Intel Core i5 3 GHz CPU, 4 GB RAM running on Windows 7 Home Premium. Table 7 shows the encryption time of three algorithms for different image sizes. The proposed method performs faster than the two existing ones. The average execution time of the proposed method decreases approximately 68% of the AES algorithm.

Table 7: Encryption and Decryption Time (in seconds) For Different Image Sizes.

Image size		256 × 256	512 × 512	1024×1024
Original AES	Encryption time	96.92	382.09	1546.19
	Decryption time	118.51	469.48	1899.02
Method by Kamali [9]	Encryption time	91.15	361.93	1462.95
	Decryption time	113.63	454.57	1853.96
Proposed method	Encryption time	31.81	119.30	463.65
	Decryption time	31.69	110.82	446.64

6. CONCLUSION

This paper proposes the modification of the AES algorithm for image encryption. The modification of the AES based on circular shift and round key to make S-box depends on secret keys and replace the MixColumn by chaotic maps. The results show that the proposed method provides good encryption quality. Compared with the AES algorithm, proposed method required less time to encrypt the image. The proposed method has large key space and is sensitive to any changes that occur in the secret key, thus making the proposed method robust against any attack. The results clearly show that the proposed method exhibits the lowest correlation coefficients among pixels in the encrypted image of those in the AES algorithm. Differential analysis illustrates that the proposed method is robust, and that it prevents differential attacks. Therefore, the proposed method is highly secure, as a result of the S-box depending on the secret key and on characteristics of the chaotic system, and it is suitable for secure image storing and transmission.

ACKNOWLEDGMENTS

This study is sponsored by the Universiti Kebangsaan Malaysia through research grants OUP-2013-182 and DPP-2013-001.

REFRENCES:

[1] Lian, S. Multimedia content encryption: techniques and applications: CRC Press. 2008.

[2] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. "A modified AES based algorithm for image encryption." International Journal of Computer Science and Engineering, vol. 1, no. 1, 2007, pp.70-75.

[3] Kazlauskas, K., & Kazlauskas, J. "Key-dependent S-box generations in AES block cipher system." Informatica, vol. 20, no. 1, 2009, pp. 23-34.

[4] Muhaya, F. B., Usama, M., & Khan, M. K. "Modified AES using chaotic key generator for satellite imagery encryption." In Emerging Intelligent Computing Technology and Applications, Springer Berlin Heidelberg, 2009, pp. 1014-1024.

[5] Tran, M.-T., Bui, D. K., & Duong, A. D. "Gray S-box for advanced encryption standard," In Computational Intelligence and Security. CIS'08. International

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Conference on, 2008, Vol. 1, pp. 253-258, IEEE.

[6] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. "A modified AES based algorithm for image encryption." International Journal of Computer Science and Engineering, vol. 1, no. 1, 2007, pp. 70-75.

[7] Murtaza, G., Khan, A. A., Alam, S. W., & Farooqi, A. "Fortification of AES with Dynamic Mix-Column Transformation." IACR Cryptology ePrint Archive, 2011, 184.

[8] Huang, C. W., Tu, Y. H., Yeh, H. C., Liu, S. H., & Chang, C. J. "Image observation on the modified ECB operations in Advanced Encryption Standard. In Information Society (i-Society)," 2011 International Conference on, 2011, pp. 264-269. IEEE.

[9] Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. "A new modified version of Advanced Encryption Standard based algorithm for image encryption." In Electronics and Information Engineering (ICEIE), 2010 International Conference On, Vol. 1, 2010, pp. V1-141, IEEE.

[10] Telagarapu, P., Biswal, B., & Guntuku, V. S. Security of image in multimedia applications. In Energy, Automation, and Signal (ICEAS), 2011 International Conference on, 2011, pp. 1-5, IEEE.

[11] Wadi, S. M., & Zainal, N. "Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption." Procedia Technology, vol. 11, pp. 51-56.

[12] Stallings, W. (2002). "The advanced encryption standard." Cryptologia, 26, no. 3, pp. 165-188.

[13] Shu-Jiang, X., Ji-Zhi, W., & Su-Xiang, Y. "An improved image encryption algorithm based on chaotic maps." Chinese Physics B, vol. 17, no. 11, 2008, 4027.

[14] Gupta, K., & Silakari, S. "New Approach for Fast Color Image Encryption Using Chaotic Map." Journal of Information Security, vol. 2, no. 4, 2011, pp. 139.

[15] Jolfaei, A., & Mirghadri, A. "Image encryption using chaos and block cipher." Computer and Information Science, vol. 4, no. 1, 2010, pp172.

[16] Peterson, G.. Arnold's cat map. Math45-Linear algebra http://online. redwoods. cc. ca. us/instruct/darnold/maw/c atmap. htm. 1997.

[17] Chen, G., Mao, Y., & Chui, C. K. "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos, Solitons & Fractals, vol. 21, no. 3, 2004, pp. 749-761.

[18] Ahmad, M., Gupta, C., & Varshney, A. "Digital image encryption based on chaotic map for secure transmission." In Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT'09. International, 2009, pp. 292-295, IEEE.

[19] Weber, A. G. The USC-SIPI Image Database: Version 5, Original release, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering. October 1997.

[20] Rummel, Rudolph J. "Understanding correlation." Honolulu: Department of Political Science, University of Hawaii, 1976.

[21] Shannon, C. E. (1949). Communication Theory of Secrecy Systems*. Bell system technical journal, 28(4), 656-715.

[22] Wu, Y., Noonan, J. P., & Agaian, S. "NPCR and UACI randomness tests for image encryption." Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, pp. 31-38.

[23] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). "Image quality assessment: from error visibility to structural similarity". Image Processing, IEEE