zied

Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box

Ashwak Mahmood Alabaichi
University of karbala, College of Sciences, Karbala, Iraq

Abstract
Techniques in encrypting digital images play a crucial role in the prevention of unauthorized access. This paper focuses on color image encryption and decryption using 3D chaotic map with AES key dependent S-Boxes. It contains four major parts which are Exclusive X-or forward and backward, 3D Logistic Map, 3D Chebyshev map, and 2D Arnold Cat Map, and Dynamic S-box of AES. Here, Exclusive X-or is used for image diffusing. 3D Logistic Map is employed for the generation of secret keys for the purpose of scrambling the image. 3D Chebyshev map is engaged for the generation secret keys for the purpose of diffusing the image. 2D Arnold Cat Map is utilized to scramble the coordinate values of AES S-Box to make it secret. The image is then substituted in the S-box. All these parts are to satisfy the high security level of the encrypted image. The suggestion algorithm is strictly tested using different criteria such as NPCR, UACI, Correlation Confection, Information Entropy, Histogram, MES, and Key sensitivity analysis. From the result it can be observed that the suggested algorithm shows good result in NPCR, UACI, Correlation Confection, Information Entropy, Histogram, MES, and Key sensitivity analysis. This means the proposed algorithm is resistant to different types of attacks. MATALAB programming (Mathworks R2012a) is used in the implementation of the proposed algorithm.

Keywords:
Chaotic map, 2D Arnold Cat Map, 3D logistic map, 3D Chebyshev map, AES key Dependent S-Boxes, NPCR, UACI, Correlation Confection, Information Entropy, Histogram, MES, and Key sensitivity analysis.

1. Introduction

Internet-based multimedia applications have become increasingly popular and this has led to an urgent need to protect digital information from access by unauthorized parties. Digital Images constitute the bulk of important information hat is shared and transmitted which must be protected by being encrypted. By nature, such images are large-sized with a tendency toward greater redundancy and correlation between the pixels. Due to the intrinsic characteristics of the images, the conventional schemes that provide encryption including DES, 3DES, RC5, AES and BA have now been proven to be both inappropriate and inadequate for their security (Gupta et al., 2014a; Jawad & Sulong, 2015b; Alabaichi et al., 2013). They have been a wide range of schemes developed by many researchers to provide protection for digital images from unauthorized access Among them are the chaotic system based on confusion and diffusion mechanisms, which is widely used and has shown superior performance in cryptography systems. Chaos implies random behavior and it is described as a study of nonlinear dynamic systems. The chaos systems are characteristically mainly sensitive to initial conditions and other system parameters. Being sensitive, the system acts in a rather random manner. Chaos-based encryption algorithms have been proven for their good security properties, complexity, and speed and computing ability. These properties make chaotic scrambling of an image an attractive option in comparison with conventional encryption algorithms (Tong el al., 2014; Mishra el al., 2014; Srividya & Nandakumar, 2011; Thampi & Jose, 2015). Currently, one dimensional chaotic system that is highly efficient and at the same offers the simplicity of the logistic map is being widely used. However, there are some inherent disadvantages: assigning a small key and inadequate security reduces the efficiency and performance of the system (Bremnavas el al., 2013). In recent years, numerous image encrypting systems have been introduced encompassing one, two or higher dimensional have come with chaotic maps. In comparison with one and two dimensional maps, three-dimensional maps offer higher security and randomness (Thampi & Jose, 2015) .

Shannon (1949) agreed on the necessity of all block ciphers possessing diffusion and confusion properties. The argument is that confusion would make new arrangements of the bits in the plaintext, spreading out the associated redundancy over the whole ciphertext. Diffusion, on the other hand, is planned to hide the relationship between the key and ciphertext as multifaceted a manner as possible. As such, even, the common block cryptosystems can possess good confusion and diffusion by substituting and permutation every round. The permutation-box (P-box) is linear, whereas the substitution-box (S-box) is nonlinear in nature (Jawad & Sulong, 2015b).

Despite the fact that AES and DES are ineffective for encrypting images, the S-box concept of AES can be useful for substitution in the encryption of images (Gupta et al., 2014a).

Key-dependent S-box indicates that the S-box is changed in every round based on the key and number of rounds. Although the design of fixed S-boxes allows them to resist differential and linear cryptanalysis, dynamic S-boxes, on the other hand, are better and able to resist these attacks (Alabaichi & Salih, 2015).

Manuscript received October 5, 2016
Manuscript revised October 20, 2016

Here we propose an algorithm for the purpose of encrypting and decrypting a color image on the basis of the chaotic theory system that is a combination of confusion and diffusion mechanisms, The proposed algorithm firstly, diffuses the image pixels by applying forward Exclusive X-or and Backward Exclusive X-or. Secondly, the 3D logistic map is utilized to generate secrets keys. These secret keys are used to rotate a plain image using a specific approach that confuses the relationships among adjacent pixels by changing the location of pixels within an image by employing image pixel scrambling. This disturbs the pixel correlations and hides the statistical structure of the pixels. Consequently, the algorithm provides security in the face of a statistical attack. Thirdly, the use of a 3D Chebyshev map causes diffusion in the correlation of the encrypted and plain images and provides the algorithm became greater security against cryptanalytic attacks. Fourthly, applying Arnold cat transform on the S-box of AES makes it secret. Then the image in the S-box is substituted for each iteration of Arnold cat and a different S-box is generated in each iteration of Arnold cat.

In this paper, besides Section 1, there is Section 2, which reviews the literature in relation to this paper; Section 3 explains the chaotic map in detail; Section 4 details the AES key Dependent S-Boxes; Section 5 describes the proposed algorithm for encrypting and decrypting color image; Section 6 provides a detailed explanation of the security analysis of the algorithm we are proposing in this paper, while Section 7 presents the conclusion to this paper and suggestions for future related research.

2. Literature Review

There have been many proposed algorithms that deal with image encryption on the basis of chaos and we discuss the most relevant below.

Lv el al. (2009) employed the 3D Henon chaotic map and Cat map to design a symmetric image encryption scheme. The Cat map is used to create confusion in the image pixel positions. The 3D Henon chaotic map used causes diffusion of the image pixels; the confusion and diffusion process is then repeated to achieve greater resistance to statistical and related attacks. From the results of the experiment and analyzing the results in detail, the algorithm we propose is shown to demonstrate high security and rapid encrypting.

Khade and Narnaware (2012) suggested the use of 3D logistic map, 3D Chebyshev map, and 3D, 2D Arnolds cat map to encrypt color image. The 2D Arnolds cat map is used to scramble image pixels and 3D Arnold's cat map substitutes Red, Green, and Blue components. The use of 3D Chebyshev map is to generate keys while the 3D logistic map is to scramble images. Using the three-dimensional chaotic characteristics in the algorithm offer a more secure level of protection as the encrypted image is shuffled and substituted.

Chen el al. (2014) provided a continuous diffusion strategy, which is an improvement of the diffusion strategy. The proposed scheme adds a further diffusion process following the standard diffusing step. Meanwhile the controlling factors are modified by the cipher image following the initial diffusing step. Furthermore, to supplement and improve the effectiveness of the confusion and the diffusion procedure, a rigorous diffusion technique is introduced employing stretched key stream components to create a cyclic shift of the pixels in the cipher. Experimental results show that the novel approach offers excellent security and rapid encrypting speed for practical image encryption.

Mishra el al. (2014) proposed a new algorithm for encrypting images by combining pixel shuffling and three chaotic maps. This proposal involves dividing the plain image into 8x8 sized blocks and then shuffling them, followed by encryption of the shuffled image employing chaotic sequence produced by a different chaotic map. The results of the experiment demonstrate that this proposed approach provides greater key sensitivity and good resistance against statistical attacks and brute-force.

Gupta et al. (2014a) proposal involved an algorithm to encrypt image that combined Arnold map and S-box of AES. In this proposal the Arnold cat map shuffles the locations of the pixels in the image spatial domain. After the shuffling, the image is encrypted using S-box. From the experiential results the proposed scheme does provide appropriate security against statistical attacks but falls short against differential analysis.

Gupta et al. (2014 b) created a scheme to apply confusion and diffusion whereby the diffusion scheme is produced randomly by the number generator using Gaussian distribution as a basis. This approach employs Bakers map to provide key length of 64 bits. Based on the security analysis and experiments these types of chaos-based image encryption approaches are pragmatic and have great potential for imaging in real-time and communicating via video with high security, an advantage which is crucial for use by the military, various industries, and business environments.

Tong el al. (2014) offered a novel technique for encrypting image and a novel combination of chaotic characteristics with a 2 of 1D dynamic shifting chaotic characteristic. In addition the pseudo-random generator is combined with the LFSR and compound chaotic. A novel reporting system for encrypting image is designed that provides better security compared with traditional encryption schemes and one-dimensional logistic chaotic maps. The novel image encryption scheme has superior performance speed, complexity, and security.

Wang and Wang (2014) introduced an algorithm to encrypt image using dynamic S-boxes whereby thee cipher image

is separated into groups, with individual groups using an S-box. The image is divided into less than ten groups and scanning of the image is done four times and less than 50 S-boxes are constructed. Prior to construct a novel S-box the starting position is modified by the earlier group that has been subjected to encryption. From the results of the experiment it is shown that the newly-introduced algorithm is faster and has superior resistance to resist differential attacks.

Jawad and Sulong(2015a) introduced proposal which is included a new technique to generate keys that were dynamically non-linear and secret for a symmetrically-based block cipher with XOR-operation. The method of generating the secret keys combines logistic and piecewise chaotic maps together with novel automatically generated initial seed values using the improved new strategy for seeds generation on the basis of sunflower spiral points. The outcomes of the experiment demonstrate that the suggested key generator algorithm can provide large key space as well as security against brute force attack.

Thampi and Jose (2015) suggested scheme to encrypt color image depends on 3D chaotic maps. Initial conditions for 3D maps are produced with a method involving three keys. The randomly generated keys employed for encryption purpose. 3D maps offer higher security and randomness in comparison with 1D and 2D maps.

Jawad and Sulong (2015b) proposed a novel F-function of BA to improve the security level for color image encryption. The key dependent S-box and XOR operators are derived from the F-function through 4D hyper-chaotic map with a drastic reduction in the frequency of iterations to 4 from 16 to achieve a less complex process. The secret keys of the block which are of varying space sizes are randomly generated. Compared with earlier works, this algorithm outperforms the conventional BA in terms of encrypting color image.

3. Chaotic map

Scientifically, chaos theory emphasizes the investigation of systems that are nonlinear, with high sensitivity to initial conditions, with similarity to randomness, and permanent systems. The initial involvement of chaos theory in the fields of cryptography was first seen in the 1980s. Digital chaotic systems provide options to improve cryptographic algorithm security levels. The suitability of chaos maps for the development of cipher techniques with chaos map concepts has been noted by many researchers (Srividya & Nandakumar, 2011).

The chaotic maps generate numbers in a pseudo-random generator to assist in generating sequence keys (Wang et al., 2009). The inherent properties of the chaotic maps have encouraged cryptographers to create novel encryption systems. The chaos-based approaches combine velocity, complexity, high security, and acceptance efficiency in a beneficial way. On the other hand, the majorities of current security systems continue to exhibit significant shortcomings including slight keys size, and not very secure. In efforts to improve confidentiality and security, many researchers have resorted to a combination of different chaotic systems with a system that encrypts images for better confidentiality (Jawad & Sulong, 2015a). Furthermore, current image encryptions systems depend on the chaotic sequence but mostly in low-dimensional domains. They offer limited security and provide inadequate key space and have inherent disadvantages. 3D functions offer greater security against cryptanalytic attacks. For instance, an image encryption using logistic map has been popularly used but although these systems do have positive features like simplicity, speed in generating the chaotic sequence, and ease of release. Under some conditions such as the key space is too slight it is vulnerable to attack. As a result, higher dimensional chaotic system is now the focus of new research (Thampi & Jose, 2015; Tong el al., 2014; Khade & Narnaware, 2012).

The encrypting system using three-dimensional baker map provides higher speed compared to two-dimensional baker map, so the former is frequently utilized in crypto systems. Also, the cipher-image of the encryption algorithm with 3D baker is faster, better balance, and avalanche effect (Tong el al., 2014; Lv el al., 2009; Khade & Narnaware, 2012). Thus, in this paper 3D chaotic map is adopted for the proposed algorithm.

The chaotic systems properties are as follows:

1. Chaos based encryption is deterministic; they some regulating mathematical equations that control their behavior.
2. They are unpredictable and non-linear, exhibit sensitivity to initial conditions including small changes, which can result in considerably varied results.
3. They may seem to behave randomly but in fact, beneath their random behavior there is organization.

The high unpredictability and apparently random properties of chaotic outcomes constitute an intriguing aspect of the deterministic chaotic system that could encourage different new uses (Mishra et al., 2014; Jawad & Sulong, 2015 a).

3.1 3D Logistic Map

A distinct feature of the logistic map is the simplicity. Its chaotic behavior and is explained by the equation

$$X_{n+1}=\lambda X_n(1-X_n) \qquad \text{eq.(1)}$$

Here, the chaos is evident when $0<X_n<1$ and $\lambda=4$ and a 3D logistic map is employed as follows:

$xi+1 = \lambda\ xi\ (1- xi) + \beta yi^2 xi + \alpha zi^3$ eq.(2)
$yi+1 = \lambda\ yi\ (1-yi) + \beta zi^2 yi + \alpha xi^3$ eq.(3)
$zi+1 = \lambda\ zi\ (1- zi) + \beta xi^2 zi + \alpha yi^3$ eq.(4)

The equations above show possess good chaotic properties when $3.53<\lambda<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$ and its values are in the range [0, 1] (Thampi & Jose, 2015; Khade & Narnaware, 2012).

In this paper 3D Logistic Map is employed to create private keys to rotate Red, Green, Blue components distinctly by a specific approach. This is then followed by the decomposition of each component Read, Green, and Blue of the image distinctly into 16x16 blocks to rotate them based on generated private keys as will be explained in section 5 below.

3.2 3D Chebyshev map

Chebyshev polynomial is used for the purpose of generating the secret keys needed in encryption process. Chebyshev polynomial Fn (x) of the first type, which is a polynomial in *x* of degree n, as prototype of a chaotic map, the definition of which is as follows:

$Fn(x) = \cos n\theta$ where $x=\cos\theta$.
Putting n=0, 1, 2, 3, 4 we get $\cos 0\theta = 1$, $\cos 1\theta = \cos\theta$, $\cos 2\theta = 2\cos 2\theta - 1$, $\cos 3\theta = 4\cos 3\theta - 3\cos\theta$, $\cos 4\theta = 8\cos 4\theta - 8\cos 2\theta + 1$.
By putting $\cos\theta = x$ we get
$F0(x) = 1$,
$F1(x) = x$,
$F2(x) = 2x^2 - 1$,
$F3(x) = 4x^3 - 3x$,
$F4(x) = 8x^4 - 8x^2 + 1$.
This is transformed as
$F2(x) = 2x^2 - 1$ eq.(5)
$F3(y) = 4y^3 - 3y$ eq.(6)
$F4(z) = 8z^4 - 8z^2 + 1$ eq.(7)

Chebyshev polynomial map Fp:[-1,1] → [-1, 1] of degree *p*, when p > 1 (Kocarev & Tasev, 2003; Thampi & Jose, 2015; Khade & Narnaware, 2012).
In this paper, eq. (5), eq. (6), and eq. (7) are used to generate secrets keys for Red, Green, and Blue components distinctly. These secret keys are used to diffuse the image pixels by exclusive X-or with the image pixels in the three components R, G, and B respectively. This process changes the value of the image pixels.

3.3 2D Arnold Cat Map

Arnold transform is simple and often utilized in information hiding technology. However it can also be utilized for encrypting image. Arnold Cat Map transformation is employed to shuffle the pixels of images and for the performance of additional security for the cipher system. The two-dimensional Arnolds cat transform has no covered in modifying the image pixels' gray scale value; it is only involved in shuffling the data of the image without changing the value. Arnold transform, also referred to as cat map transform, is only suited to the encryption of N×N images. It is described as eq.(8) (Chen el al., 2014; Choudhary & Gupta, 2014; Ramesh et al, 2013).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \qquad \text{eq.(8)}$$

p, q , and the number of iterations can be the secret keys.

The inverse transform is used for decryption as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \qquad \text{eq.(9)}$$

4. AES key Dependent S-Boxes

The S-box has been proven to be the keystone of contemporary symmetric such as block and stream ciphers and is a primary constituent in any block system layout. However, some weaknesses in the S-box render it vulnerable to cryptanalysis. Thus, several studies have attempted to enhance the security by replacing the fixed S-box with key Dependent S-Box (Alabaichi & Salih, 2015). S-Box of AES is developed by composing a pair of transformations. Firstly, it considers the multiplicative inverse in GF (28), with '00' mapping onto itself. Secondly, application of an affine transformation according to the definition by Gupta et al, (2014a).

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

In this paper, 2D Arnold Cat Map is utilized in shuffling the values of S-box instead of the value of the image pixel as shown in previous studies. This approach is different from all previous studies.
Xn, Yn in eq.(8) represents the coordinate (original row and column) of the values of the S-box before shuffling it, while Xn+1, Yn+1 represents the new coordinates (row and column) of the values of the S-box after shuffling it as well as N is 16. Thus, it can generate a different S-box that depends on a key with each iteration of the 2D Arnold Cat Map as will be explained in section 5 below.

5. Proposed algorithm

The focus of this part of the present paper is on the proposed algorithm which is used to encrypt and decrypt color images in different sizes as will be described in detail. It includes four major parts as follows:

Part One: this part is suitable for the diffusion of the image pixels. It is done by applying the forward Exclusive X-or and Backward Exclusive as follows:

1. Decompose the Red (R), Green (G), Blue (B) components of the image and store them in three arrays with size N*M, where N and M are rows and columns of the image.
2. Apply the following eq.(10) for forward Exclusive X-or on each of the image components respectively.

C1(1)=P(1) where P(1) is the first pixel of the plain image which is used as seed.

$C1(i)=C1(i-1)\oplus P(i)$ eq.(10)

Where i =2…N*M where P(i), C1(i) are the present pixels in the plain and cipher images respectively and C1(i-1) is the previous cipher pixel .

While the backward Exclusive X-or is applied on the resulted image as follows using eq.(11)

$C2(i-1)= C2(i) \oplus C1(i-1)$ eq.(11)

where K=N*M, i =K…2, C2(K)=C1(K) as seed.

Fig.1 illustrates the plain image and images after forward Exclusive and back Exclusive.

Part Two: this part is suitable for disturbing the relationships between the neighboring pixels by altering their position but not making any change to the pixel value so the histogram of the image is stable. Scrambling of image pixels is done in the following steps.

1. decompose each component into 16 x 16 sizes blocks
2. Initialize the secret parameters of 3D logistic map to generate secrets keys separately for R, G, and B components and each block in the component as follows:
3. Where x for Red, y for Green, and z for Blue. x0=0.976, y0=0.677 , z0=0.973 λ=3.8414991 , β=0.024, α=0.017. Table 1.illustrates the sample of them.

Table 1. Samples of keys are between [0, 1]

0.9321	0.2953	0.8097
0.2733	0.7077	0.5972
0.9493	0.9221	0.1869
0.8107	0.6039	0.5898
0.7638	0.6020	0.1891

4. Convert the secret keys to decimal number using the following eq.(12) as

$X_{i,j} = floor(X_{i,j} * 10^4)$ eq.(12)

5. Exclusive X-or between the digits of the number.
6. Rotate each of the components (R, G, and B) left or right on the basis of the first bit of the number in step 5. Hence, Rotate is right if the first bit is 1 otherwise Rotate is left.
7. Rotate each block (16x16) of components right or left based on the first bit of the number in step 5; hence rotate right when the first bit is 1 otherwise Rotate left. Fig.2 illustrates the images after Rotating the components as well as blocks respectively.

In the decryption part the rotation process is done in reverse order hence rotate left when the first bit is 1, otherwise rotate right.

Part Three: it is suited to the diffusion of the relation between the plain and cipher mages by changing the pixel values. This part has the steps as indicated below:

1. Initialization of the three secret parameters of 3D Chebyshev to generate individual secret keys for R, G, and B of the scrambled image as follows:

Where x for R, y for G, z for B and x0=0.234; y0=-0.398; z0=-0.88

2. Convert them to values between 0…255 using the following eq.(13)

$X_{i,j} = floor(X_{i,j} * 10^{10} \ mod \ 256)$ eq.(13)

Table 2 shows the key samples

Table 2 Samples of keys are between [0, 255]

148	125	151
171	93	209
166	231	212
199	254	29
10	127	124

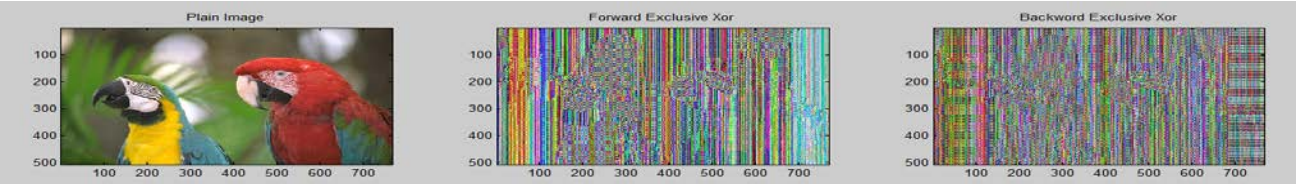


Fig.1 The plain image and images after forward Exclusive and back exclusive

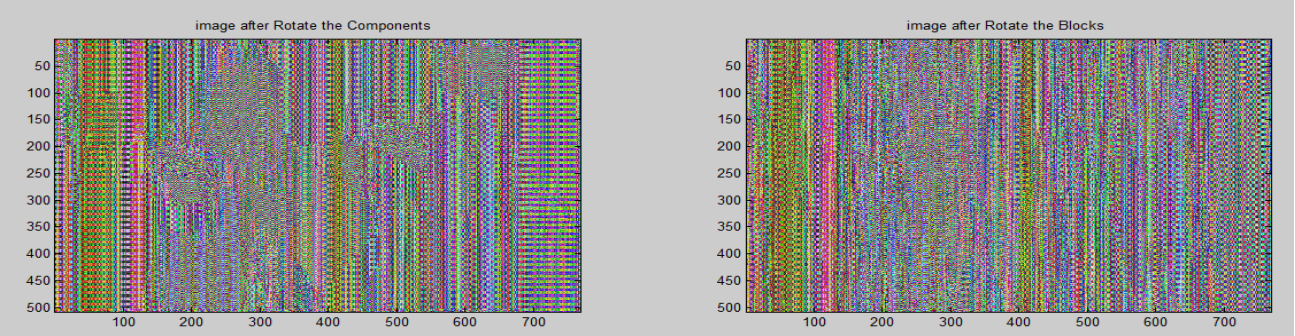


Fig.2 The image after Rotating the components and blocks

3. Exclusive X-or between secrets keys and components of the scrambled image. Fig.(3) illustrates this part.

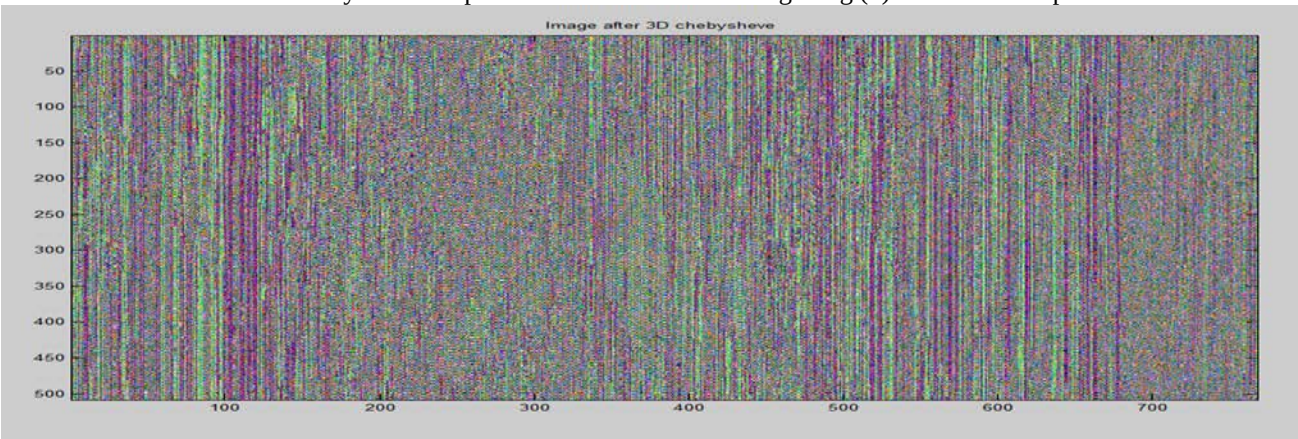


Fig.3 Image after 3D Chebyshev

Part Four: to provide additional security of the encrypted image 2D Arnolds Cat Map and S-box in AES, which are used as illustrated in the following steps:

1. Initializing the secret parameters of 2D Arnolds Cat Map as follows:
   p=5, q=10, number of iterations is 4.
2. Changing the coordinates of the values in the S-box to convert it from public to secret using 2D Arnolds Cat Map. Fig.4 (a…d) illustrates the original S-box and S-boxes after applying 2D Arnolds Cat Map on it for the three iterations.
3. Substituting the pixels values of the three components of the resultant image from the second part into secret S-box.
4. Repeating five times (k) the steps 2 and 3.
5. Combining all components into a single image.

```
orignal Sbox
63 7C 77 7B F2 6B 6F C5 30 01 67 2B FE D7 AB 76
CA 82 C9 7D FA 59 47 F0 AD D4 A2 AF 9C A4 72 C0
B7 FD 93 26 36 3F F7 CC 34 A5 E5 F1 71 D8 31 15
04 C7 23 C3 18 96 05 9A 07 12 80 E2 EB 27 B2 75
09 83 2C 1A 1B 6E 5A A0 52 3B D6 B3 29 E3 2F 84
53 D1 00 ED 20 FC B1 5B 6A CB BE 39 4A 4C 58 CF
D0 EF AA FB 43 4D 33 85 45 F9 02 7F 50 3C 9F A8
51 A3 40 8F 92 9D 38 F5 BC B6 DA 21 10 FF F3 D2
CD 0C 13 EC 5F 97 44 17 C4 A7 7E 3D 64 5D 19 73
60 81 4F DC 22 2A 90 88 46 EE B8 14 DE 5E 0B DB
E0 32 3A 0A 49 06 24 5C C2 D3 AC 62 91 95 E4 79
E7 C8 37 6D 8D D5 4E A9 6C 56 F4 EA 65 7A AE 08
BA 78 25 2E 1C A6 B4 C6 E8 DD 74 1F 4B BD 8B 8A
70 3E B5 66 48 03 F6 0E 61 35 57 B9 86 C1 1D 9E
E1 F8 98 11 69 D9 8E 94 9B 1E 87 E9 CE 55 28 DF
8C A1 89 0D BF E6 42 68 41 99 2D 0F B0 54 BB 16
```

(a)

```
Sbox 1
16 E0 D1 77 6D 43 59 B4 F5 34 35 7E E2 CE 5E 2F
3F F6 17 07 1E B8 B3 B0 95 58 76 E7 EF C9 2E 92
39 FE 7A 9F C0 BA A3 93 66 5F 96 8E 88 52 99 AC
0C 23 11 22 6E 42 5C 6A 01 F4 7F 9C BD F3 15 70
A9 45 D4 74 21 71 C1 19 75 E1 81 2C 0D 49 FC 6F
55 0B 84 8C 32 00 7B 8D 4D 47 C6 BC A5 57 3D EB
7D 1C 9D F7 0E C4 12 87 14 29 54 E4 CF 63 C8 AA
3B 2D 62 4A D7 AE A8 CA 78 40 26 48 97 05 94 46
D2 B7 3E 13 C3 69 2A 5A 68 C2 CB 67 EA 50 A4 8B
06 B1 C5 6C F9 A2 1F 10 D8 1D 73 04 F8 4F 1A BF
B9 64 27 28 DB 09 A1 3A ED F2 D5 33 F0 E8 B6 E5
7C 37 FB FA A6 38 CC 61 A7 80 E9 DE E3 BB 79 53
9A 9B EE D6 0F 91 4C AB 08 D0 82 25 8F 36 03 44
3C 72 8A 51 FD B5 EC 18 D9 90 A0 41 D3 BE 2B 65
DC 1B E6 24 5B 30 56 02 AF 4B FF 31 9E CD C7 98
DD DA F1 86 5D B2 DF 60 83 89 0A 20 6B 4E 85 AD
```

(b)

```
Sbox 2
AD B9 0B D1 FA 0E B8 4C CA 66 90 CB 9C 9E 4F FC
BA EC 5A 01 4B 73 2C 6B E8 3D 2F 7C 1C 17 D6 D7
BC E2 BB C8 92 9A 2D 7A 51 C3 42 56 10 75 89 D5
B7 11 24 F9 71 DF 3A 4D 34 E9 E4 EF 36 94 AC 3C
61 14 58 82 48 88 BE A4 70 DC B1 D4 86 DB 00 59
CD 1A 6F DD 64 84 77 A6 C4 B3 AB 78 5F A0 67 BD
07 0F AE A3 18 68 F4 FF 04 0D 4E B6 EB 16 37 9D
E1 0A 33 A5 CE 79 AA 3F 9B 62 9F FD 69 5C 02 D8
46 39 72 3E 22 5B A2 C1 60 ED 47 35 DE CF C9 03
09 7B B4 A7 29 76 25 97 52 2B 8B 0C 1B C5 74 5D
41 EA F3 C7 BF A9 DA 27 8C 6D 38 12 B0 08 40 96
E0 FB F7 1E 91 A8 93 D9 C2 7F 31 F8 49 85 E5 55
6A AF 1D 81 20 F0 57 5E 53 7D F6 EE 4A C0 B5 2A
63 2E 44 3B FE 8A 13 6E 30 1F 19 83 F2 C6 7E E3
6C 21 B2 A1 8D F5 80 54 E7 8F 05 99 65 D2 23 E6
D0 26 8E D3 50 15 98 06 45 F1 28 32 43 CC 87 95
```

(c)

```
Sbox 3
95 41 1A 0B 1E 18 73 57 3F 51 1F 47 EF 65 C5 00
9A 13 C1 34 8F 8B D4 43 08 67 FC E0 0F 5A 81 CE
78 9C 85 37 D7 6A 0A BB 3B 22 DF 80 97 70 F1 38
39 24 A1 29 88 98 27 C4 66 31 B6 1C C0 02 D5 63
D9 04 3D F6 FD 10 C6 C9 3C 6C 7B 58 D3 BF 84 B8
D2 74 59 D0 EA 6F D1 91 68 2C 5E 9B C3 19 35 36
01 20 79 2D 6E 60 E9 05 0C 86 CC 40 BD AD FB AE
DC 28 12 5F 9E E5 9D BA AF 33 C8 FE 5B 3A 54 52
D8 BC 2E 72 F9 8D 76 BE 06 8C B3 90 F8 EB 17 B5
A9 77 4C C2 0D 2F EE 69 75 7E 03 B7 21 B4 82 50
83 DE 94 23 5D 61 26 F3 DD FA A8 F4 6B 53 62 42
B9 F7 A3 4B F0 AA 7A 30 ED E4 99 1B DB 87 96 CD
4D E7 2B B1 32 B0 A0 4F 55 07 EC 1D A5 92 8A A2
16 D6 2A E1 E2 44 3E 71 F5 25 A4 45 6D AB CB 49
A7 48 15 DA A6 CA 7F 4E 7C 4A 5C 89 E3 46 11 B2
7D 9F 56 F2 CF AC E6 09 14 8E C7 64 0E 93 FF E8
```

(d)

Fig. 4(a-d): (a) the S-box of AES, (b) S-box of the first iteration, (c) S-box of the second iteration, (d) S-box of the third iteration.

Fig. 5 illustrates the images after the first to fourth substitutions.

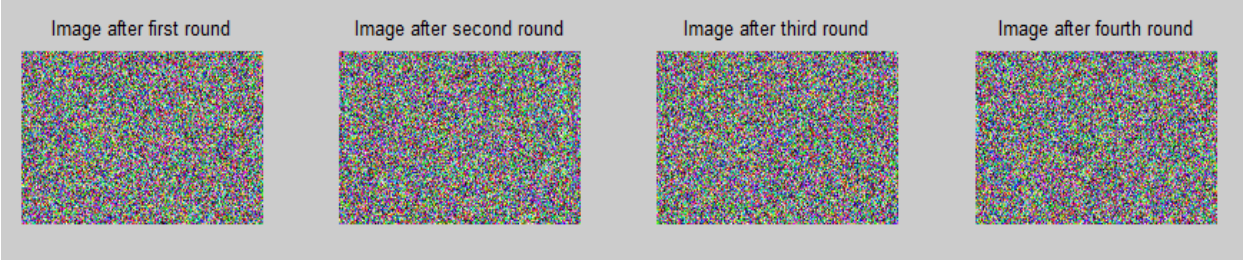


Fig. 5 image after the first to fourth substitutions.

Now, acquisition of the cipher image is achieved. The decrypting stages are nearly the same as the encrypting stage with reverse order where first substitution of the image into inverse S-boxes occurs and then reversal of image pixels must be done by rotating the block first followed by rotating the component; second, Exclusive X-or the secret keys of the 3D Chebyshev with cipher image; third applying Exclusive X-or with cipher image backward then forward.

6. Analyzing the security

In this part we analyze some criteria to check how effective and efficient the suggested algorithm is against different attacks. These criteria include Number of Pixels Change Rate (NPCR), and the Unified Average
Changing Intensity (UACI), Correlation Confection (CC), Information Entropy (IE), Histogram, Mean Square Error (MES), and Key sensitivity analysis (Wang & Wang, 2014; Gupta et al., 2014a; Tong el al., 2014; Chen el al., 2014).

6.1 NPCR and UACI

The ability to resist differential attack is one of the most important requirements of image encryption. A small alteration (e.g., changing a one pixel) of the plain image is always done by the attackers to gain some clues of the keys using the comparison between the changed cipher images. Thus, a good algorithm must have the ability to spread out any small alteration in the plain image to a more sizeable scale over the encrypted image; this will stop the attacker from discovering any critical information related to the keys. NPCR and UACI are utilized for this purpose. NPCR refers to the rate at which the pixels of the encrypted image are altered with the change one plain image pixel. UACI, however, measures the rate intensity of the variations between the plain and encrypted images. There is only one pixel difference between a pair of encrypted images, C1 and C2, with matching plain images. The NPCR of these two images is described in eq.(14) (Chen el al., 2014; Gupta et al., 2014a)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad \text{eq.(14)}$$

Where D(i, j) is defined as

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j) \\ 1, & if \quad C_1(i,j) \neq C_2(i,j) \end{cases}$$

The definition of UACI is as in eq.(15)

$$UACI = \frac{1}{M \times N} \sum_{i,j} \left[\frac{|C_1(i,j) - C_2(i,j)|}{L-1} \right] \times 100\% \qquad \text{eq.(15)}$$

Tests were conducted on the proposed algorithm, which involved the modification of a one plain image pixel. The

outcomes of the NPCR and UACI tests can be seen in Table 3. It is obvious from the results that a one alteration in the different plain image will effectively alter the encrypted images, which shows the robustness of the proposed algorithm in the face of differential analysis.

Table 3 NPCR and UACI of the different images

IMAGES	*NPCR*			*UACI*		
	R	*G*	*B*	*R*	*G*	*B*
Lena	99.6510	99.6267	99.5868	26.1619	28.9422	28.0849
Pepper	99.6399	99.6201	99.6063	30.8135	29.9082	34.9912
Baboon	99.6197	99.6204	99.5949	25.8224	26.6198	30.8858
Cat	99.6114	99.6155	99.6155	31.1145	32.2342	30.8283

6.2 Correlation Coefficient

A statistical analysis was carried out on the image that had been subjected to encryption and the Correlation Coefficients (CCs) were computed to establish how closely the two neighboring pixels were related. In general, every pixel of the original image has a strong correlation with its neighboring pixels are vertically, horizontally, diagonally, or anti-diagonally positioned. An algorithm that is ideal for encrypting images has the ability to break this relationship. Therefore, the neighboring pairs of pixels that are vertically, horizontally, diagonally, or anti-diagonally positioned are selected from the image to calculate the CCs using the following eq.(16):

$$r = \frac{\sum_{i=1}^{N}(x_i-\bar{A})(y_i-\bar{B})}{\sqrt{(\sum_{i=1}^{N}(x_i-\bar{A})^2)((y_i-\bar{B})^2)}}$$

$$\bar{A} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad \text{eq.(16)}$$

$$\bar{B} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

where N = number of selected neighboring pixels to calculate the relationship in an image, with xi and yi, which are the values of neighboring pixels in the vertically, horizontal, diagonal, and anti-diagonal positions in the image (Jawad & Sulong, 2015b; Wang &Wang, 2014; Gupta et al., 2014a).

Table 5 and Table 6 illustrate the CC in the original and encrypted image positioned vertically, horizontally and diagonally and anti-diagonally. It can be shown from the results that the relations between adjacent pixels are destroyed and near to zero.

6.3 Information Entropy

Entropy is an important characteristic that expresses the random nature of a source of information and also determines how unpredictable it is. The entropy serves the purpose of measuring the rate of potential threats in retrieving the original image with no knowledge of the key. A true random source with 2^N symbols possesses an entropy that is N. Therefore, to obtain a cryptosystem, the cipher image entropy with 256 gray level should optimally be H(s) = 8.

The entropies of the plain and cipher images generated by the algorithm developed in this study are computed and presented in Table 7. It is evident that the cipher image entropy is theoretically valued at around 8. The implication being that there is significant information loss when processing the encrypting, and the proposed algorithm offers security against entropy analysis. The entropy is defined in eq.(17):

$$(s) = \sum_{0}^{2^n-1} P(si)\, log_2 P(si) \qquad \text{eq.(17)}$$

Where: *P(si)* is the probability of the existing pixel *si* and n is the total number of image pixels (Chen, el al., 2014; Jawad & Sulong, 2015b; Tong el al., 2014).

6.4 Histogram

An image histogram is able to show how prevalent the values of the pixels are by indicating the number of pixels at each grayscale level. A robust image algorithm would produce a flat cipher image histogram.

The plain image and cipher image histograms of the Red, Green, and Blue components are shown in Figures 6 (a) and (b) respectively.

The encrypted image histograms are reasonably flat and differ significantly from the plain image histogram. Encryption removes the plain image's redundancy and therefore leaves no clue for any statistical attack to be launched (Wang &Wang, 2014; Chen, el al., 2014).

6.5 Mean Square Error (MSE)

Mean square error is defined as the variation between the plain image and the cipher image. This variation must be very high for a better performance. Mathematically it is calculated as in eq.(18)

$$\text{MSE}= \frac{1}{MN}\sum_{i=}^{M}\sum_{j=1}^{N}\big(x(i,\ j) - y(i,j)\big)^2 \qquad \text{eq.(18)}$$

where $x(i, j)$ expresses the plain image and y (i, j) expresses the cipher image and i and j are the pixel positions of the M×N image. MSE is zero when $x(i, j) = y(i, j)$ (Srivastava & Singh, 2015; Choudhary & Gupta, 2014). Table 8 illustrates the result of MSE for the different images.

Table 5 Correlation Coefficient (Horizontal, Vertical, Diagonal, and Anti-Diagonal) of the different plain images

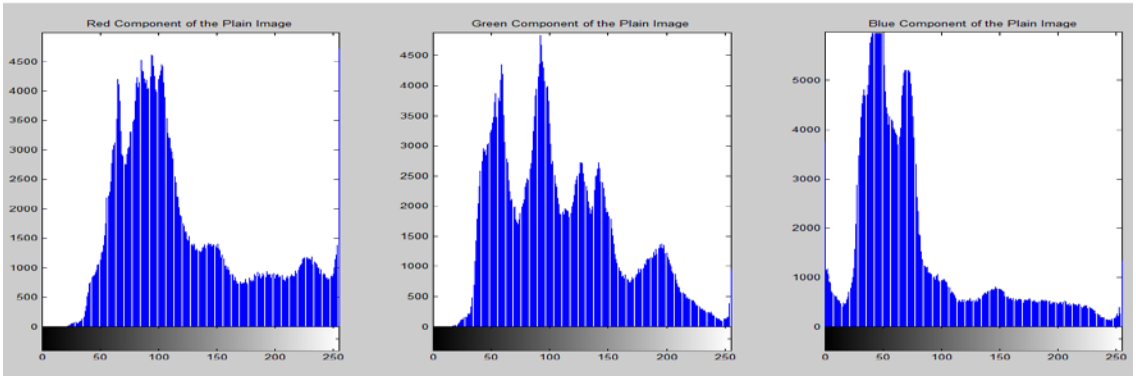
Direction	*Horizontal*			*Vertical*			*Diagonal*			*Anti-Diagonal*		
Images	R	G	B	R	G	B	R	G	B	R	G	B
Lena	0.9608	0.9511	0.9423	0.9811	0.9764	0.9659	0.9373	0.9276	0.9143	0.9588	0.9450	0.9272
Pepper	0.9943	0.9938	0.9887	0.9951	0.9945	0.9903	0.9888	0.9878	0.9779	0.9914	0.9903	0.9833
Baboon	0.9893	0.9824	0.9895	0.9867	0.9786	0.9882	0.9776	0.9635	0.9790	0.9771	0.9627	0.9788
Cat	0.9884	0.9857	0.9864	0.9878	0.9843	0.9855	0.9824	0.9776	0.9789	0.9785	0.9736	0.9750

Table 6 Correlation Coefficient (Horizontal, Vertical, Diagonal, and Anti-Diagonal) of the different cipher images

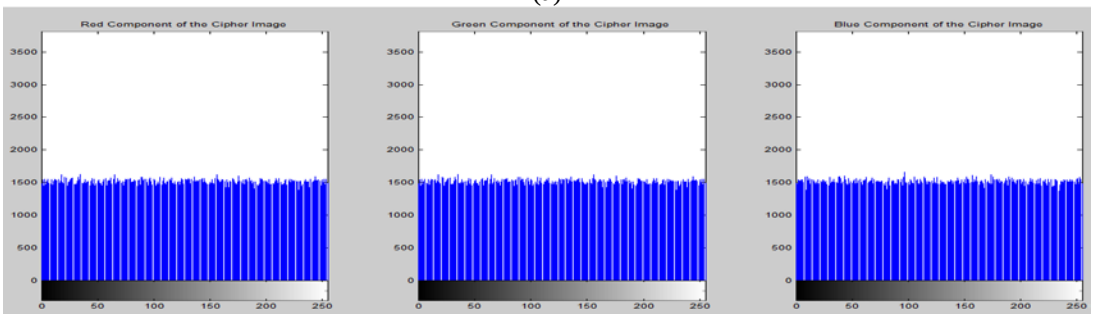
Direction	*Horizontal*			*Vertical*			*Diagonal*			*Anti-Diagonal*		
Images	*R*	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*
Lena	-0.0080	0.0039	0.0013	0.000029	-0.0034	0.00053	-0.0086	-0.0044	0.0027	0.0076	0.0018	0.0040
Pepper	0.00062	0.0062	0.0101	0.0020	0.0048	-0.0019	-0.0032	-0.000062	-0.0064	0.000030	-0.0039	0.0026
Baboon	0.0012	0.0019	-0.00021	0.0021	0.00061	-0.00075	-0.00072	-0.0016	0.0000095	-0.00082	0.00097	-0.000035
Cat	0.0019	0.00045	0.00061	0.00095	-0.0020	-0.00022	0.00034	0.00042	-0.00095	-0.000018	-0.0021	-0.00052

Table 7 Entropy of the different plain and cipher images

IMAGES	*Entropy / plain image*	*Entropy / cipher image*
Lena	7.7215	7.9985
Pepper	7.6776	7.9989
Baboon	7.6328	7.9997
Cat	7.6216	7.9997



(a)



(b)

Fig. 6(a-b): (a) the histogram of the plain image, (b) the histogram of the cipher image

Table 8 Result of MSE for the different images.

IMAGES	MSE		
	R	G	B
Lena	104.50	97.07	98.55
Pepper	99.274	102.44	138.26
Baboon	91.789	89.072	93.069
Cat	95.418	99.568	109.45

6.6 Analyzing key sensitivity

The sensitivity of a key can be determined in two approaches: firstly, compute the CC between cipher images, which result from the use of slightly different keys for the encryption of the same plain image; a good system should be with a very small CC; secondly it will not be possible to achieve correct decryption of the cipher image when there even a small variation exists between the encryption and decryption keys (Chen el al., 2014; Tong el al., 2014; Jawad & Sulong, 2015a)

For the first approach, the encryption of the plain image is in a pair of different keys. Assume that the selected key is (α=0.017, β=0.024, λ=3.8414991) whereas the keys with slight differences are (α=0.017000001, β=0.024, λ=3.8414991), (α=0.017, β=0.024000001, λ=3.8414991), and (α=0.017, β=0.024, λ=3.8414991000001). Finally, the correlation between the cipher images is computed as in table 9ز

Table 9 Result of CC for the different keys.

Keys	CC		
	R	G	B
α=0.017000001	0.000284	0.00066	0.000881
β=0.024000001	0.0974	0.0016	0.0640
λ=3.8414991000001	0.0284	0.0033	0.0881

It is shown that the CC is near to zero when there is a slight change in the key. For the second approach, encryption if first performed with the selected α=0.017, β=0.024, λ=3.8414991, while the slightly different keys (α=0.017000001, β=0.024, λ=3.8414991), (α=0.017, β=0.024000001, λ=3.8414991), and (α=0.017, β=0.024, λ=3.8414991000001) are used for decryption. The matching deciphered images are presented in Figures 7(a) to (c), respectively. It can be seen from Fig. 7, that even a small variation in the decryption key will prevent the decryption of the plain image. Thus, most keys do not display any plain image information and therefore it can be concluded that the algorithm introduced in this study is extremely key sensitive

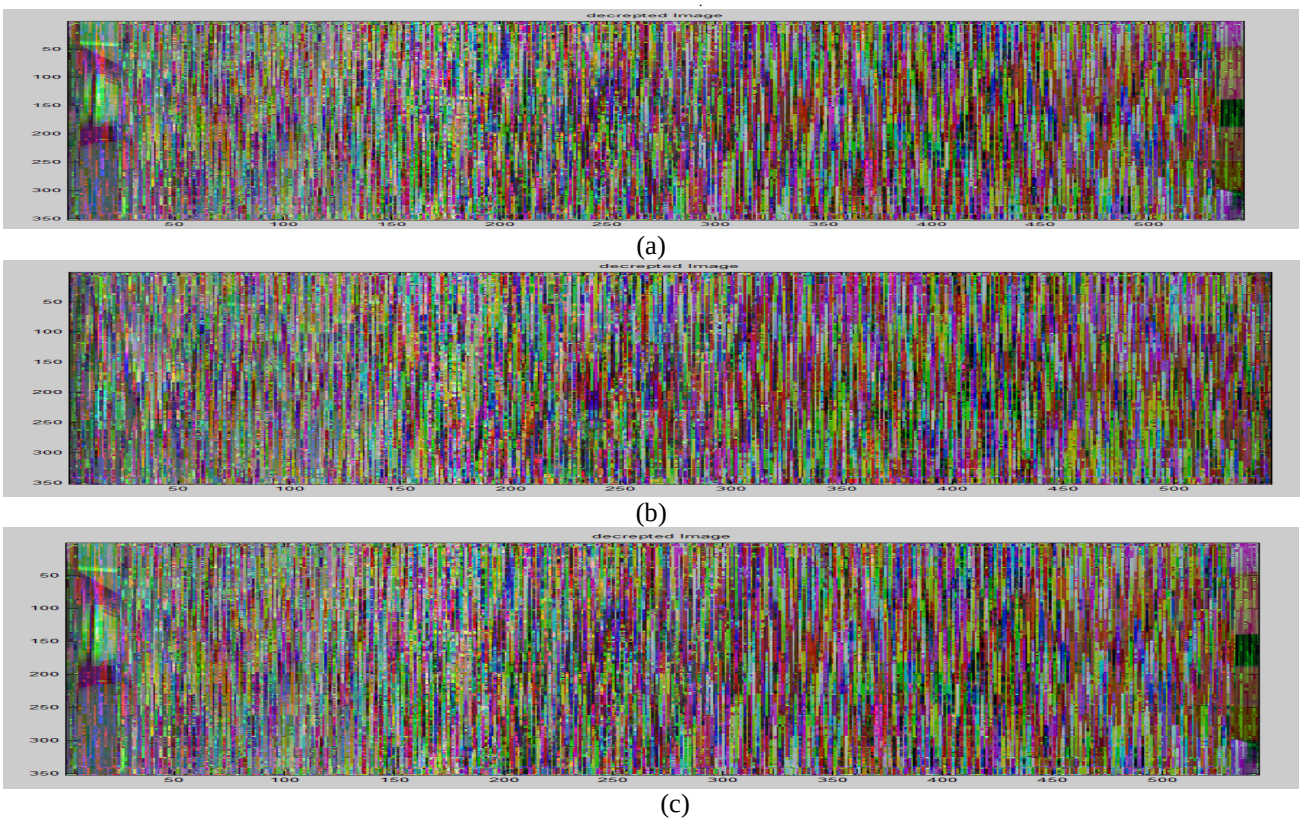


Fig. 7(a-b): (a) The decrypted image following there is a small alteration in value α, (b) the decrypted image following is a small alteration in value β, (c) the decrypted image following a small alteration in value λ

7 Conclusion and Recommendations

This paper proposes the use of 3D chaotic system and dynamic S-box of AES to encrypt and decrypt any color image of any size. Hence the proposed algorithm has four major parts which are Exclusive X- or forward and backward, three-dimensional Logistic Map, three-dimensional Chebyshev map and two-dimensional Arnold Cat Map, and dynamic S-box of AES. The aim of these parts is to diffuse and confuse the image more than once to ensure it has high security. The proposed algorithm is strictly tested as show in section 6 and from the results that were found, we can conclude that using 3D chaotic map with Dynamic S-box of AES can provide a high level of security and resistance against many types of attacks as well as increase the key spaces.
For future research we intend to investigate the application of the proposed algorithm on selective images.

References

Alabaichi, A. M., Mahmood, R., Ahmad, F., & Mechee, M. S. (2013). Randomness analysis on Blowfish block cipher using ECB and CBC modes. Journal of Applied Sciences, 13(6), 768.

Alabaichi, A., & Salih, A. I. (2015). Enhance security of advance encryption standard algorithm based on key-dependent S-box. Paper presented at the Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on.

Bremnavas, I., Poorna, B., & Mohamed, I. R. (2013). Secured medical image transmission using chaotic map. Elixir Comp. Sci. Eng, 54.

Chen, J.-x., Zhu, Z.-l., & Yu, H. (2014). A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme. Optik-International Journal for Light and Electron Optics, 125(11), 2472-2478.

Choudhary, N. Y., & Gupta, R. K. (2014). Partial Image Encryption based on Block wise Shuffling using Arnold Map. International Journal of Computer Applications, 97(10).

Gupta, L., Gupta, R., & Sharma, M. (2014b). Low Complexity Efficient Image Encryption Technique Based on Chaotic Map. International Journal of Information & Computation Technology

Gupta, P., Singh, S., & Mangal, I. (2014a). Image Encryption Based On Arnold Cat Map and S-Box. International Journal of Advanced Research in Computer Science and Software Engineering, 4(8)

Jawad, L. M., & Sulong, G. (2015b). Chaotic map-embedded Blowfish algorithm for security enhancement of colour image encryption. Nonlinear Dynamics, 81(4), 2079-2093.

Jawad, L. M., & Sulong, G. (2015a). A Novel Dynamic Secret Key Generation for an Efficient Image Encryption Algorithm. Modern Applied Science, 9(13), 85.

Khade, P. N., & Narnaware, M. (2012). 3D chaotic functions for image encryption. IJCSI International Journal of Computer Science Issues, 9(3), 323-328.

Kocarev, L., & Tasev, Z. (2003). Public-key encryption based on Chebyshev maps. Paper presented at the Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on.

Lv, Z., Zhang, L., & Guo, J. (2009). A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System. Paper presented at the IEEE Proceedings of the Second International Symposium on Computer Science and Computational Technology (ISCSCT'09).

Ramesh, K.Y,Singh B. K., Sinha S.K., and Pandey,K. K. (2013). A New Approach of Color Image Encryption Based on Henon like Chaoti Map. Journal of Information Engineering and Applications 3(6).

Shannon, C. E. (1949)). Communication theory of secrecy systems. Bell system technical journal, 28(4), 656-715.

Srividya, G., & Nandakumar, P. (2011). A Triple-Key chaotic image encryption method. Paper presented at the Communications and Signal Processing (ICCSP), 2011 International Conference on.

Srivastava, R., & Singh, O. P. (2015). Performance Analysis of Image Encryption Using Block Based Technique. International Journal of Advanced Research in Electrical, Electronics and instrumentation Engineering, 4(5), 4266–4271. Retrieved from http://www.ijareeie.com/upload/2015/may/52_9_Performance.pdf.

Tong, X.-J., Zhang, M., Wang, Z., & Liu, Y. (2014). A image encryption scheme based on dynamical perturbation and linear feedback shift register. Nonlinear Dynamics, 78(3), 2277-2291.

Thampi,C. & Jose, D. (2015).More Secure Color Image Encryption Scheme Based on 3D Chaotic Maps. International Journal for Advance Research in Engineering and Technology, 1(IX),1-5.

Wang, X., & Wang, Q. (2014). A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. Nonlinear Dynamics, 75(3), 567-576.