A Proposed Cryptosystem Algorithm Based on Two Different Chaotic Systems (PCA2CS) for Securing the Colored Images

Osama M. Abu Zaid[1] , and Moussa Demba[2]

[1, 2] **Dept. of Computer Science, College of Computer Sciences and Information, Al-Jouf University, Sakakah, KSA.**

Abstract

In this paper, a proposed cryptosystem algorithm based on two different chaotic systems is presented. Chen's chaotic system and Henon chaotic system is used as different chaotic systems to obtain our proposed encryption algorithm; in order to meet the requirements of secure image transfer. The proposed encryption Algorithm will be designated as PCA2CS. It is applied on two different color's frequencies colored-images. The proposed algorithm (PCA2CS) contains confusion and diffusion procedures. Confusion procedure based on Chen 's chaotic system is used to shuffle the positions of pixels of the colored plain-image. Diffusion procedure based on mixing of Chen's chaotic system and Henon chaotic system is used to change the values of pixels of the shuffled-image. PCA2CS is applied on all color's channels of the image; Red, Green, and Blue with two modes of operations ECB and CFB. The expectant results of several experiments, statistical analysis, key sensitivity tests, NPCR and UACI analysis, and information entropy analysis will show that our proposed encryption algorithm (PCA2CS) is a good algorithm to provides an efficient and secure method for securing colored images.

Keywords *Image security; Chen's chaotic map; Henon chaotic system; and Modes of operations.*

1. Introduction

In this age of communications and information's exchange, Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the networks.

Chaotic maps are very complicated nonlinear dynamic systems, which are applied in the field of figure correspondence and encryption [1-3], because they are very sensitive to initial conditions and can generate good pseudorandom sequences.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography[4]. Therefore, chaotic cryptosystems have more useful and practical applications.

Recently, a number of chaos-based encryption schemes have been proposed. Some of them are based on one-dimensional chaotic maps and are applied to data sequence or document encryption [5,6]. For image encryption, two-dimensional (2D) or higher-dimensional chaotic maps are naturally employed as the image can be considered as a 2D array of pixels [7-9]. The colored image consist of three 2D arrays of pixels for the color channels R, G, and B.

This paper introduces a proposed cryptosystem algorithm which contains two steps, the first is shuffling pixels of the image by using our previous proposed confusion algorithm based on Chen's chaotic map system (CA3DCS)[10], and the second is changing values of pixels of shuffled-image by using diffusion procedure based on mixing of Chen's chaotic system and Henon chaotic system. A proposed cryptosystem algorithm is designated in this paper as (PCA2CS).

The proposed algorithm (PCA2CS) contains confusion and diffusion procedures; so it has the benefits of both of them. PCA2CS will be applied on Red, Green, and Blue channels of the colored-image with two modes of operations; Electronic Code Book (ECB), and Ciphering Feed Back (CFB).

This paper is organized as follows. Section 2 presents a brief overview on Chen's chaotic system. Section 3 presents a brief overview on Henon chaotic system. After this, Section 4 discuss a proposed cryptosystem (PCA2CS). Section 5 discuss the experimental results and analysis. In the final, Section 6 presents conclusion of the paper, and Section 7 presents acknowledgement.

2. Chen's Chaotic System

Chen’s chaotic map system is described by formula 1 which illustrates a set of the three differential equations of Chen's chaotic map system. [10-14]

$$\begin{cases} x = a(y_0 - x_0) \\ y = (c-a)x_0 - x_0 z_0 + c y_0 \\ z = x_0 y_0 - b z_0 \end{cases} \quad (1)$$

where $a > 0$, $b > 0$ and c such that ($2c > a$) are parameters of the system. Chen's system is chaotic when the parameters have the values; $a=35$, $b=3$ and $c \in$ [20, 28.4].

A very good performance for Chen's chaotic map at the parameters a=35, b=3, c=28, the initial values $x_0 = 0$, $y_0 = 1$, $z_0 = 0$, and $h = 0.055555$ such that h is the step of the sequence [10, 11].

3. Henon Chaotic System

The Henon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. The Henon map takes a point (x_i, y_i) in the plane and maps it to a new point.[15]

The well-studied Henon map presents a simple two dimensional map with quadratic nonlinearity. This map gave a first example of the strange attractor with a fractal structure. Because of its simplicity, the Henon map easily lends itself to numerical studies. Thus a large amount of computer investigations followed. Nevertheless, the complete picture of all possible bifurcations under the change of the parameters a and b is far from completion. Where $a = 0.3$, $b \in$[1.07, 1.4]. If one chooses $a=0.3$, $b=1.4$, the system is chaotic, subsequently This feature is very useful in image encryption. [15-17]

Formula 2 illustrates the two equations of Henon chaotic map system.

$$\begin{aligned} x_{i+1} &= 1 - a x_i^2 + y_i \\ y_{i+1} &= b x_i \end{aligned} \quad (2)$$

4. The Proposed Cryptosystem (PCA2CS)

In this part of the paper, the proposed cryptosystem algorithm based on two different chaotic systems (PCA2CS) is presented. The proposed cryptosystem (PCA2CS) consists of encryption and decryption schemes. Here, the encryption scheme only is discussed because The decryption scheme is the reverse technique of the encryption scheme.

To resist statistical analysis, Shannon suggests that confusion and diffusion should be utilized in any cryptosystem [11]. The encryption scheme of the proposed cryptosystem (PCA2CS) consists of two procedures, the first is the confusion procedure, and the second is the diffusion procedure.

4.1 The Confusion Procedure

The confusion procedure (CA3DCS)[10], is the first part of designing of the encryption process of the proposed cryptosystem(PCA2CS). It is designed to produce shuffled-image. This algorithm consists of five steps of operations. [10]

4.2 The Diffusion Procedure

The diffusion procedure is the second part of the encryption scheme of the proposed cryptosystem (PCA2CS). It is designed to encrypt the pixels of the shuffled-image which is produced from the confusion procedure in the previous section. The diffusion procedure consists of seven steps of operations as following:

Step1: There are three sequences X, Y and Z of size $\boldsymbol{m \times n}$ which are generated by Chen's chaotic system and are used to confuse (shuffle) $\boldsymbol{R}$, $\boldsymbol{G}$ and $\boldsymbol{B}$ matrixes of the plain-image. Also, there are $\boldsymbol{CR}$, $\boldsymbol{CG}$, and $\boldsymbol{CB}$ matrixes of colors of the shuffled-image which is produced from the confusion procedure.

Step2: The Henon chaotic system is converted into one dimensional chaotic system [15]. The one dimensional Henon chaotic system is defined as in formula 3:

$$u_{i+2} = 1 - a u_{i+1}^2 + b u_i \quad (3)$$

Obtain $\boldsymbol{u_2}$, where the initial value $\boldsymbol{u_0}$ = 0.01, and the initial value $\boldsymbol{u_1}$ = 0.02. values of parameters a, and b are the same values of a, and b for Chen's chaotic system.

Step3: The Chen's chaotic system is defined as in the following formula:

$$\begin{aligned} x_2 &= a(y_1 - x_1) \\ y_2 &= (c-a)x_1 - x_1 z_1 + c y_1 \\ z_2 &= x_1 y_1 - b z_1 \end{aligned} \quad (4)$$

Obtain $\boldsymbol{x_2}$, $\boldsymbol{y_2}$, and $\boldsymbol{z_2}$, where values of the parameters are a =35, b =3, c =28. Also, The three initial values are $\boldsymbol{x_1}$= X (100), $\boldsymbol{y_1}$= Y (500) and $\boldsymbol{z_1}$= Z (800) which are generated by the Chen's chaotic system.

Step4: Obtain two sequences (1-D matrix) MH and MC of size $\boldsymbol{si}$ = $m \times n$, where MH is generated by Henon chaotic system according to the equations in formula 5, and MC is generated by Chen's chaotic system according to the equations in formula 6. Where $\boldsymbol{i}$ is the variable of the counter for loop, i.e. $\boldsymbol{i}$ = 1,…, $\boldsymbol{si}$ at value of the step of the counter is three. And in formula 6 the constant is adopted equal to $\boldsymbol{10^{14}}$.

$$\begin{aligned} MH(i) &= mod(floor(u_0*z_1), 256);\\ MH(i+1) &= mod(floor(u_1*x_1), 256);\\ MH(i+2) &= mod(floor(u_2*y_1), 256); \end{aligned} \quad (5)$$

$$\begin{aligned} MC(i) &= floor(mod((abs(x_2)*MH(i)-\\ &\quad floor(abs(x_2)))* constant , 256));\\ MC(i+1) &= floor(mod((abs(y_2)*MH(i+1)-\\ &\quad floor(abs(y_2)))* constant , 256));\\ MC(i+2) &= floor(mod((abs(z_2)*MH(i+2)-\\ &\quad floor(abs(z_2)))* constant , 256)); \end{aligned} \quad (6)$$

At the end of each loop of the counter, the initial values u_0 , u_1, x_1 , y_1, and z_1 are changed according to the following formula:

$$\begin{aligned} x_1 &= x_2 * u_0;\\ y_1 &= y_2 * u_1;\\ z_1 &= z_2 * u_2;\\ u_0 &= u_1;\\ u_1 &= u_2; \end{aligned} \quad (7)$$

Step5: Obtain three sequences (1-D matrixes) *XC*, *YC*, and *ZC* of size $si = m \times n$, where these sequences based on the sequence *MC* which is produced in step4 and the values of *v1*, *v2*, and *v3* which has been produced in the confusion procedure in[10]. *XC*, *YC*, and *ZC* are generated according to the equations in formula 8.

$$\begin{aligned} XC(i) &= mod(((v1+v2)*MC(i)) , 256);\\ YC(i) &= mod(((v2+v3)*MC(i)) , 256);\\ ZC(i) &= mod(((v3+v1)*MC(i)) , 256); \end{aligned} \quad (8)$$

Step6: *XC*, *YC* and *ZC* are changed based on exclusive OR operation for themselves with the sequence *MH* which is produced in step4. A new sequences *XC*, *YC*, and *ZC* are generated according to the equations in formula 9.

$$\begin{aligned} XC(i) &= bitxor(XC(i) , MH(i));\\ YC(i) &= bitxor(YC(i) , MH(i));\\ ZC(i) &= bitxor(ZC(i) , MH(i)); \end{aligned} \quad (9)$$

Step7: Then the matrixes of colors of the encrypted image can be obtained by the following formula:

$$\begin{aligned} EN_R(i , j) &= bitxor(CR(i , j) , XC(t));\\ EN_G(i , j) &= bitxor(CG(i , j) , YC(t));\\ EN_B(i , j) &= bitxor(CB(i , j) , ZC(t)); \end{aligned} \quad (10)$$

Where ***CR***, ***CG***, and ***CB*** are the color's matrixes of the shuffled-image which are generated in the last step of the confusion procedure. Also, ***i*** is the first dimension of the matrixes where $i = 1,\ldots,m$ and ***j*** is the second dimension of the matrixes where $j = 1,\ldots,n$. Also, $t = 1,\ldots si$, where $si = m \times n$.

5. Experimental Results and Analysis

In this paper, a practical programs of a proposed cryptosystem algorithm (PCA2CS) with the modes of operations and a practical programs of all experimental and security analysis tests are designed by MATLAB 7.0 on windows 7 system on Intel CORE I_3 Processor, and 3.0 GB RAM. All programs have been applied on two colored-images are different in frequency of colors (*flower.bmp* and *fruit.bmp*) as a plain-images of the size *120×120* pixels, which are shown in Fig. 1(a) and Fig. 1(b) respectively.

5.1 Statistical Analysis

To examine the quality of encryption and the stability via statistical attacks, the histogram is calculated for all color's channels *R*, *G*, *B* of the plain-images, correlation coefficient analysis (CCA) between each of color's channels *R*, *G*, *B* of the plain-image and the corresponding channels of the encrypted-image, the correlation analysis of two adjacent pixels with the directions horizontal (CAH), and vertical (CAV) for all color's channels *R*, *G*, *B* of the encrypted-image.

5.1.1 Histogram Analysis

The application of the proposed cryptosystem (PCA2CS) on these plain-images has two sequent steps; first is the confusion procedure and second is the diffusion procedure.

(a)  (b) 

Fig. 1 The plain colored-image: (a) the image (flower.bmp); (b) the image (fruit.bmp).

Figure 2(a) illustrates the encrypted-image for *flower.bmp* which is produced from applying the proposed cryptosystem (PCA2CS) with ECB mode. The histogram for *R*, *G*, *B* of this encrypted-image is shown in Fig. 2(b, c, d). Figure 3(a) illustrates the encrypted-image for *flower.bmp* which is produced from applying the proposed cryptosystem (PCA2CS) with CFB mode. The histogram for *R*, *G*, *B* of this encrypted-image is shown in Fig. 3(b, c, d).

Figure 4(a) illustrates the encrypted-image for *fruit.bmp* which is produced from applying the proposed cryptosystem (PCA2CS) with ECB mode. The histogram for *R*, *G*, *B* of this encrypted-image is shown in Fig. 4(b, c, d). Figure 5(a) illustrates the encrypted-image for *fruit.bmp* which is produced from applying the proposed cryptosystem (PCA2CS) with CFB mode.

The histogram for *R*, *G*, *B* of this encrypted-image is shown in Fig. 5(b, c, d).

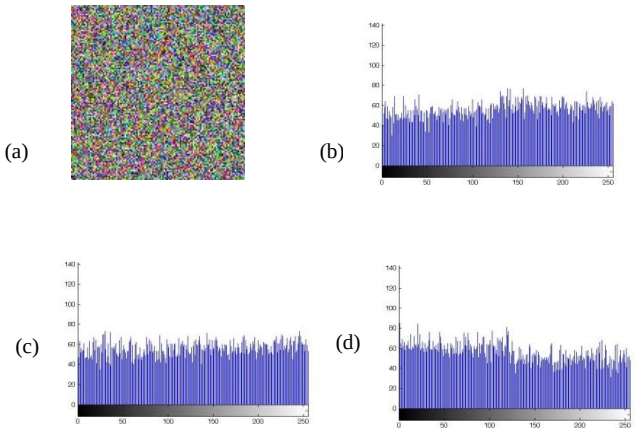

Fig. 2 The encrypted-image for flower.bmp which is produced by applying PCA2CS with ECB mode: (a) the encrypted-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

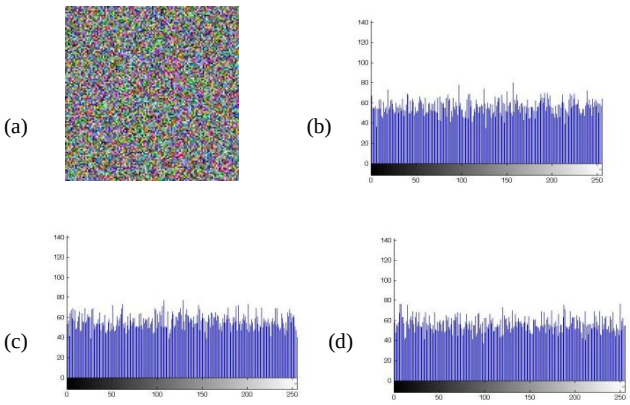

Fig. 3 The encrypted-image for flower.bmp which is produced by applying PCA2CS with CFB mode: (a) the encrypted-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

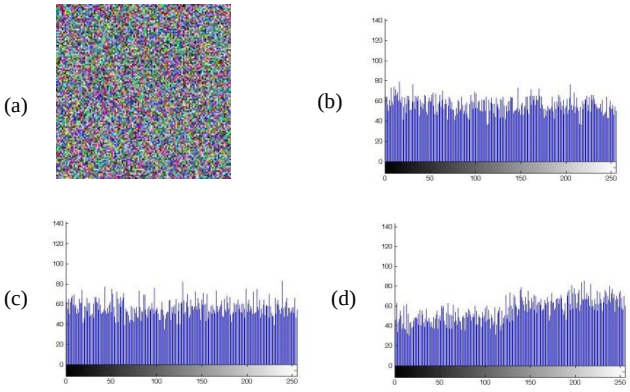

Fig. 4 The encrypted-image for fruit.bmp which is produced by applying PCA2CS with ECB mode: (a) the encrypted-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

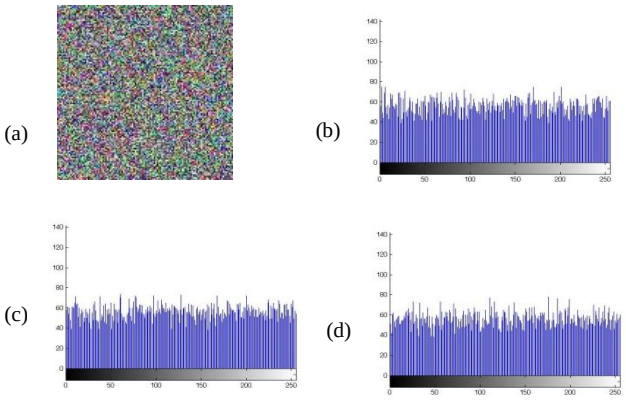

Fig. 5 The encrypted-image for fruit.bmp which are produced by applying PCA2CS with CFB mode: (a) the encrypted-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

From all previous figures of histograms the encrypted-images, the proposed cryptosystem (PCA2CS) is a complicated and very good algorithm for disguise any countenance of the images.

5.1.2 Correlation Coefficient Analysis

The correlation coefficient equals one if they are highly dependent, i.e. the encryption process failed in hiding the details of the plain-image. If the correlation coefficient equals zero, then the plain-image and its encryption are totally different. So, success of the encryption process means smaller values of the CCA [10,15]. The CCA is measured by formula 11:

$$\mathbf{CCA} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \qquad (11)$$

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

where *x* and *y* are gray-scale pixel values of the plain and encrypted images. The CCA is measured for each color's channel (*R*, *G*, *B*) of any colored-image.

Tables 1, 2 illustrate that the proposed cryptosystem (PCA2CS) achieves very small values (near to zero) of CCA with all modes of operations for two colored-images, so a PCA2CS is a complicated and a good cryptosystem for encrypting the images. Also, the results of CCA for CFB mode is better than the results for ECB mode. The results of CCA is better with the high frequencies colors image than the other with all modes.

Table 1: Results of CCA analysis for encrypting flower.bmp by PCA2CS with the modes.

Modes	**CCA for encrypting *flower.bmp***		
	R	***G***	***B***
ECB	-0.0162	-0.0035	-0.0065
CFB	-0.0089	-0.0035	-0.0059

Table 2: Results of CCA analysis for encrypting fruit.bmp by PCA2CS with the modes.

Modes	CCA for encrypting *fruit.bmp*		
	R	***G***	***B***
ECB	0.0012	-0.0029	-0.0069
CFB	0.0012	-0.0020	0.00095

5.1.3 Correlation Analysis of Two Adjacent Pixels

It is well known that the adjacent pixels of an image have very high correlation coefficients in horizontal and vertical directions. The following formulas is employed to test the correlation analysis between two horizontally adjacent pixels (designed as **CAH**), and two vertically adjacent pixels (designed as **CAV**) respectively. In plain images and encrypted images, the following procedure was carried out. First, select 900 pairs of two adjacent pixels from an image. Then, calculate the correlation coefficient $\boldsymbol{C}_{xy}$ of each pair by using the following formulas [11,12]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\,,\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (12)$$

$$cov(x,y) = E\big(x - E(x)\big)\big(y - E(y)\big) \quad (13)$$

$$C_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \quad (14)$$

Where x and y denote two adjacent pixels, and N is the total number of duplets (x, y) obtained from the image. Tables 3, 4 illustrate the results of CAH, and CAV analysis for the plain-images *flower.bmp* and *fruit.bmp* respectively.

Table 3: Results of CAH, and CAV analysis for the plain-image *flower.bmp*.

	The plain image (*flower.bmp*)		
	R	***G***	***B***
CAH	0.9664	0.9670	0.9749
CAV	0.9709	0.9613	0.9479

Table 4: Results of CAH, and CAV analysis for the plain-image *fruit.bmp*.

	The plain image (*fruit.bmp*)		
	R	***G***	***B***
CAH	0.9367	0.9433	0.9287
CAV	0.9827	0.9812	0.9719

According to Tables 3, 4 anyone can observe, the results of CAH, and CAV analysis of two adjacent pixels for the plain-images are approach to 1, implying that high correlation exists among pixels.

Table 5, 6 illustrate the results of CAH, and CAV analysis for the two encrypted-images, which have been produced by applying the proposed cryptosystem (PCA2CS) on two plain-images *flower.bmp* and *fruit.bmp* respectively, with the two modes ECB and CFB.

Table 5: Results of CAH, and CAV analysis for the encrypted images of *flower.bmp* by applying PCA2CS with the modes.

		The encrypted image of (*flower.bmp*)		
		R	***G***	***B***
CAH	**ECB**	0.0014	-0.0141	0.0009
	CFB	-0.0105	-0.0024	0.0646
CAV	**ECB**	-0.0065	-0.0019	0.0044
	CFB	0.0004	0.0010	0.0427

Table 6: Results of CAH, and CAV analysis for the encrypted images of *fruit.bmp* by applying PCA2CS with the modes.

		The encrypted image of (*fruit.bmp*)		
		R	***G***	***B***
CAH	**ECB**	0.0026	0.0272	0.00059
	CFB	-0.0066	0.0062	-0.0751
CAV	**ECB**	-0.00007	-0.0031	-0.0068
	CFB	-0.0396	-0.00042	0.0039

According to Tables 5, 6, the results of CAH and CAV for the correlation analysis of two adjacent pixels for the encrypted-images with both of two modes are approach to 0, implying that no detectable correlation exists among pixels. Therefore the proposed cryptosystem (PCA2CS) can protect the encrypted-images from statistical attacks. Also, from Table 5, 6, the results sometimes better with ECB than CFB and other sometimes the converse is actualize, but the results for the two modes are better with the high frequencies colors image than the other.

5.2 Security Analysis

A good cryptosystem should resist most kinds of known attacks, also it must be achieves sensitive to any little change in the plain-text or secret keys to make brute-force attacks infeasible, and a good values for the information entropy analysis.

In the proposed cryptosystem (PCA2CS), the parameters a, b, c, and h, the initial values x_0, y_0, z_0, u_0, u_1, x_1, y_1, and z_1 are used as a secret keys.

5.2.1 NPCR and UACI Analysis

A very vital relationship between the plain-image and the encrypted-image may be revealed [11]. If a significant change in the encrypted-image can be caused

by a trivial change in the plain-image by means of diffusion and confusion, then the algorithm would make differential attacks practically useless. In order to test the influence of a one pixel change on the plain-images encrypted by the proposed cryptosystem (PCA2CS), *NPCR* (Number of Pixels Change Rate) and *UACI* (Unified Average Changing Intensity) are used. *NPCR* and *UACI* are computed by the following formulas [11,15]:

$$\mathbf{NPCR} = \frac{\sum_{i,j} \boldsymbol{d(i,j)}}{\boldsymbol{m \times n}} \times \mathbf{100\%} \quad (15)$$

$$\mathbf{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{|\boldsymbol{EI1(i,j) - EI2(i,j)}|}{255} \times 100\% \quad (16)$$

$$\textbf{Where } d(i,j) = \begin{cases} \mathbf{0}, & EI1(i,j) = EI2(i,j) \\ \mathbf{1}, & EI1(i,j) \neq EI2(i,j) \end{cases}$$

In This tests, we need two plain-images: the plain-image and the other image obtained by changing one pixel value of the plain-image. the two images are encrypted by a proposed cryptosystem (PCA2CS) with the same keys to generate the corresponding encrypted-images *EI1* and *EI2*. Where the grey values of the pixel at position (*i, j*) of *EI1* and *EI2* are denoted as *EI1*(*i, j*) and *EI2*(*i, j*) respectively; *m* and *n* are width and height of the encrypted-image. *d*(*i, j*) is determined by *EI1*(*i, j*) and *EI2*(*i, j*).

Table 7: Results of NPCR and UACI analysis for the encrypted images of *flower.bmp* by applying PCA2CS with the modes.

		For The Encrypted images of (*flower.bmp)*			
		R	***G***	***B***	**Median**
NPCR %	**ECB**	99.632	99.611	99.604	99.616
	CFB	99.535	99.708	99.590	99.611
UACI %	**ECB**	32.994	33.923	33.582	33.499
	CFB	33.270	33.347	33.570	33.396

Table 8: Results of NPCR and UACI analysis for the encrypted images of *fruit.bmp* by applying PCA2CS with the modes.

		For The Encrypted images of (*fruit.bmp)*			
		R	***G***	***B***	**Median**
NPCR %	**ECB**	99.604	99.660	99.611	99.625
	CFB	99.611	99.611	99.604	99.609
UACI %	**ECB**	33.653	33.778	33.352	33.594
	CFB	33.712	33.143	33.479	33.445

From Tables 7, 8, the results of NPCR and UACI for the two encrypted images with two plain-images respectively with both of modes (ECB, and CFB) are very close to the ideal values (*NPCR*=99.609% and *UACI*=33.4635%)[11], i.e. with the proposed cryptosystem (PCA2CS), a very little change of the plain-image pixel values (one pixel) will lead to a significant change of the encrypted-image.

From Tables 7, 8, the result of NPCR analysis of the high frequency colors image (*fruit.bmp*) with the mode ECB is better than the other results. Also the results for both *flower.bmp* and *fruit.bmp* with the CFB mode are convergent.

From Tables 7, 8, the result of UACI analysis of the high frequency colors image (*fruit.bmp*) with the mode ECB is better than the other results. Also the results of UACI for *fruit.bmp* are better than the results for *flower.bmp* with both ECB and CFB mode.

5.2.2 Key Sensitivity Analysis

The experimental results demonstrate that the proposed cryptosystem (PCA2CS) is very sensitive to the secret keys mismatch. The decrypted image by using PCA2CS are the same of the original image, where are decrypted by using PCA2CS with *a=35*, *b=3*, *c*=28, h=0.055555, $x_0=0+v$, $y_0=1+v$, $z_0=0+v$, $u_0=0.01$, $u_1=0.02$, $x_1=XX(100)$, $y_1=YY(500)$, *and* $z_1=ZZ(800)$ to produce the original image.

The experimental results for applying PCA2CS on *fruit.bmp* with both of modes demonstrate that the proposed cryptosystem (PCA2CS) is very sensitive to the secret keys $\boldsymbol{a}$ mismatch (10^{-14}), $\boldsymbol{b}$ mismatch (10^{-15}), $\boldsymbol{c}$ mismatch (10^{-14}), $\boldsymbol{h}$ mismatch (10^{-16}), $\boldsymbol{x_0}$ mismatch (10^{-16}), $\boldsymbol{y_0}$ mismatch (10^{-15}), $\boldsymbol{z_0}$ mismatch (10^{-14}), $\boldsymbol{u_0}$ mismatch (10^{-17}), $\boldsymbol{u_1}$ mismatch (10^{-17}), $\boldsymbol{x_1}$ mismatch (10^{-13}), $\boldsymbol{y_1}$ mismatch (10^{-14}),and $\boldsymbol{z_1}$ mismatch (10^{-14}).

For example, Fig.6 illustrates the sensitivity of the proposed algorithm (PCA2CS) with the secret key $\boldsymbol{u_1}$, where as the encrypted-image which is shown in Fig.4(a) decrypted using $\boldsymbol{u_1}$= 0.02000000000000001, and the remains secret keys as the same as in the normal case. As can be seen that, even the secret key $\boldsymbol{u_1}$ is changed a little (10^{-17}), the decrypted image is absolutely different from the original image (*fruit.bmp*).

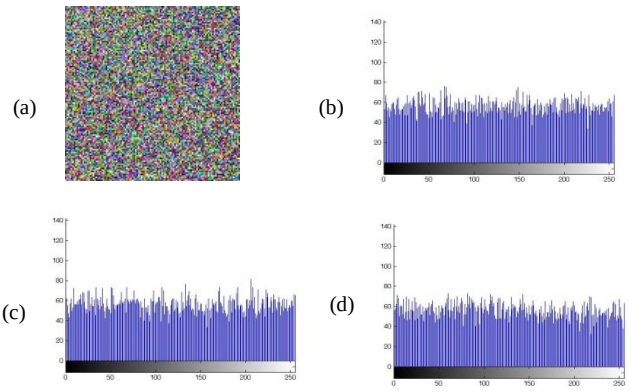

Fig. 6 The sensitivity to the secret key $\boldsymbol{u_1}$ of PCA2CS with ECB, for decrypting the encrypted-image of *fruit.bmp*: (a) the decrypted image, which is produced at $\boldsymbol{u_1}$ *=0.02000000000000001*; (b) histogram of R; (c) histogram of G; (d) histogram of B.

Therefore anyone can conclude that PCA2CS is very sensitive to all members of the secret keys, and it can also resist the various attacks based on sensibility.

5.2.3 Entropy Analysis

Information entropy [11,18,19] is a common criterion that shows the randomness of the data. Also, entropy and information theory introduced by Robert M. Gray at 2009. One of the most famous formulas of the information entropy is illustrated in following formula.

$$\boldsymbol{IE(x)} = -\sum_{i=0}^{N-1} P(x_i) Lb(P(x_i)) \qquad (17)$$

That **N** is the number of gray level in the color's channel of the image, $\boldsymbol{x}$ is the total number of symbols, $\boldsymbol{x_i} \in \boldsymbol{x}$, where $P(x_i)$ represents the probability of occurrence of $\boldsymbol{x_i}$, and ***Lb*** denotes the base 2 logarithm.

For an ideal random image, the value of information entropy is 8. The predictability of the method decreases when the information entropy tends to the ideal value (8) [18].

Table 9: Results of Information Entropy analysis for the encrypted image of *flower.bmp* and *fruit.bmp* by applying the PCA2CS with the modes.

		The Information Entropy *IE(x)*		
		R	***G***	***B***
flower.bmp	**ECB**	7.986	7.987	7.979
	CFB	7.987	7.987	7.987
fruit.bmp	**ECB**	7.986	7.984	7.970
	CFB	7.986	7.988	7.987

From Table 9, all the results of information entropy *IE(x)* for the images, which are encrypted by applying PCA2CS with both of the modes are very close to the ideal value. So these results mean that the encrypted-images are close to a random source and the proposed cryptosystem (PCA2CS) is secure against entropy attack.

Also from Table 9, the information entropy analysis *IE(x)* illustrates the results of these different images with both of modes ECB and CFB are convergent, but the results are better with CFB mode than with ECB mode.

6. Conclusion

The proposed cryptosystem algorithm (PCA2CS) based on two different chaotic maps systems. PCA2CS contains the confusion algorithm for shuffling the locations of pixels of the images, and the diffusion algorithm for encrypting the shuffled-images by changing the values of pixels of the images. The proposed cryptosystem (PCA2CS) is applied on the colored-image with two modes of operations ECB and CFB. The results and analysis show that PCA2CS is very good encryption cryptosystem and has high security, where as it has the merits: 1) its results with all tests of statistical analysis are excellent. 2) it is very sensitive to the secret keys. 3) its results of NPCR and UACI tests are excellent. 4) its results of information entropy analysis tests are excellent, because these are very closed to the ideal value 8. The proposed cryptosystem algorithm (PCA2CS) has high encryption quality, and it is suitable to provides an efficient and secure method for encrypting various colored-images.

7. Acknowledgement

We are thankful to Al Jouf University for providing financial support to this work (grant 33/88). We also thank Dr. Nawal El-Fishawy for some helpful comments.

References

[1] Di X, Xiaofeng L, Pengcheng W, "Analysis and improvement of a chaos-based image encryption algorithm," Chaos, Solitons and Fractals, Vol.40, No.5, 2009, pp. 2191-2199.
[2] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li, "A novel chaos-based image encryption scheme with an improved permutation process, " IJACT, Vol.3, No.5, 2011, pp.223-233.
[3] Dongming Chen, Yunpeng Chang, "A novel image encryption algorithm based on Logistic maps," AISS, Vol. 3, No.7, 2011, pp.364-372.
[4] Zhang LH, Liao XF, Wang XB, "An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, Vol. 24, 2005; pp. 759–765.
[5] Wong KW, "A fast chaotic cryptography scheme with dynamic look-up table," Phys Lett A , Vol. 298,2002, pp. 238-242.
[6] Pareek NK, Patidar V, Sud KK, "Discrete chaotic cryptography using external key," Phys Lett A, Vol. 309,2003, pp.75-82.
[7] Guan ZH, Huang FJ, Guan WJ, "Chaos-based image encryption algorithm," Phys Lett A, Vol. 346,2005, pp.153-157.
[8] Lian SG, Sun J, Wang Z, "A block cipher based on a suitable use of chaotic standard map," Chaos, Solitons and Fractals, Vol. 26, No. 1,2005, pp.117-129.
[9] Feng Y, Li LJ, Huang F, "A symmetric image encryption approach based on line Maps," In: Proc ISSCAA2006, Jan 2006, p. 1362-67.
[10] Osama M. Abu Zaid, Moussa Demba, and Mohamed A. Al-Refaiy. " Confusion Algorithm Based on 3-D Chaotic Map System for Securing the Colored Images," *International Journal of Computer Applications*, USA, Vol. 72, No. 10, pp. 37-42, June 2013.
[11] Huibin Lu, Xia Xiao, "A Novel Color Image Encryption Algorithm Based on Chaotic Maps," Advances in information Sciences and Service Sciences (AISS),Vol. 3, No. 11, December 2011.
[12] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic

cat maps," Chaos, Solitons & Fractals Vol. 21, 2004, pp. 749–761.
[13] Xuedi Wang, Lixin Tian, Liqin Yu, "Linear Feedback Controlling and Synchronization of the Chen's Chaotic System," International Journal of Nonlinear Science,Vol.2, No.1, 2006, pp. 43-49.
[14] Cahit Cokal, Ercan Solak, "Cryptanalysis of a chaos-based image encryption algorithm," Elsevier, Physics Letters A, Vol. 373, 2009, pp. 1357–1360.
[15] Osama Abu M Zaid, Nawal A El-fishawy, E M Nigm and Osama S Faragallah, "A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security," International Journal of Computer Applications, USA, Vol. 61, No. 5, 2013, pp. 29-39.
[16] R.Raja Kumar, A.Sampath, P.Indumathi, "Enhancement and Analysis of Chaotic Image Encryption Algorithms," CCSEA 2011, CS & IT 02, 2011,pp. 143–153.
[17] M, Sonls, "Once more on Henon map: analysis of bifurations," Chaos, Sotilons Fractals, Vol. 7, No. 12, 1996, pp. 2215-2234.
[18] M. Sabery.K, M. Yaghoobi, "A New Approach for Image Encryption Using Chaotic Logistic Map," IEEE Computer Society, ICACTE, 2008, pp. 585-590.
[19] Zhiliang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu, "A chaos-based sysmetric image encryption scheme using a bit-level permutation," Information Sciences, Vol.181, No.6, 2011, pp.1171-1186.

Osama M. Abu Zaid ***(The Corresponding Author)*** received

B.Sc. from the faculty of science, Menoufia University, Egypt in 2000. He is working as a network manager in Menoufia University. He received the M.Sc. degree in data security from Faculty of sciences, Menoufia university, Egypt, in 2005. Now he is lecturer in Faculty of computer sciences and information, Al-Jouf university, KSA. He is working for his Ph.D. He is interested in multimedia security over wired and wireless networks, and he registered the Ph.D. in Faculty of sciences, Zagazig university, Egypt.

Moussa Demba graduated from theTunis El Manar University

in 1998. In 2006, he received a Ph.D. degree from the Tunis El Manar University in Tunisia for his research on Formal methods. His areas of interest are Program verification, Artificial intelligence and Database. Currently, he is working as an assistant professor at Aljouf University, Kingdom of Saudi Arabia.