Encryption Quality Measurement of a Proposed Cryptosystem Algorithm for the Colored Images Compared with Another Algorithm

Osama Abu Zaid[1], Nawal El-Fishawy[2], and Elsayed Nigm[1]
[1]Department of Mathematics, Zagazig University, Egypt
[2]Department of Computer Science and Engineering, Menoufia University, Egypt

Abstract: *In this paper, a proposed cryptosystem algorithm based on two different chaotic systems is presented. The proposed cryptosystem algorithm is designated as PCACH. A recently developed encryption algorithm which is designated here, as HuXia is reviewed. These two algorithms are applied to three images of different color frequencies, i.e., different types of colored-images are encrypted with each of the two encryption algorithms. Both of them are applied to the different images with two different types of encryption modes, Electronic Code Book (ECB) and Cipher Block Chaining (CBC). Visual inspection is not sufficient to assess the quality of encryption so other measuring factors are considered based on measuring the maximum deviation and the Correlation Coefficient (CC) between the original and the encrypted images. For judging the force of security, we measure the plain-text sensitivity by using Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) analysis, measuring information entropy and measuring the key sensitivity. Also, the encryption/decryption time and the throughput are measured for the two algorithms. The results suggest that PCACH is a very good algorithm and superior to HuXia.*

Keywords: *Encryption algorithms, image encryption, quality measurements, modes of encryption*.

Received April 28, 2014; accepted August 13, 2014; published online March 8, 2015

1. Introduction

We are now living in the midst of a communications revolution which necessitates multimedia transmission in a secure manner. Visual encryption is important in transferring images through communication networks to protect them against reading, alteration of their content, adding false information or deleting part of their content [7, 16].

Chaotic maps are very complicated nonlinear dynamic systems, which are applied in encryption techniques, because they are very sensitive to initial conditions and can generate good pseudorandom sequences [3, 13, 18].

Recently, a number of chaos-based encryption schemes have been proposed for securing the multimedia. Chaotic map system which is used for image encryption is two-dimensional (2D) or higher-dimensional chaotic map as the image can be considered as a 2D array of pixels [8, 9, 11].

A novel color image encryption algorithm based on chaotic maps, designated as HuXia in this paper, has been proposed to encrypt color images, Lu and Xiao [12].

This paper presents a proposed cryptosystem algorithm for colored images based on the intermixture of a 2D chaotic map system (Henon chaotic system) and a 3D chaotic map system (Chen's chaotic system). The proposed cryptosystem algorithm is designated here as PCACH. PCACH contains confusion and diffusion algorithms so it has the benefits of both of the algorithms mentioned above. A confusion (permutation) algorithm based on Chen's chaotic system is used to shuffle the locations of pixels of the plain-image. A diffusion (substitution) algorithm based on the intermixture of Chen's and Henon chaotic systems is then used to change the values of pixels of the shuffled-image which is produced from the confusion algorithm.

PCACH and HuXia are applied on three different colored-images with two modes of encryption: Electronic Code Book (ECB) mode [7] and Cipher Block Chaining (CBC) mode [7].

This paper is organized as follows: Section 2 will present an overview on the HuXia algorithm, section 3 will present the chaotic systems which are used in this work, section 4 will present an overview on modes of operations of encryption, section 5 will introduce the proposed cryptosystem algorithm PCACH, section 6 will discuss the experimental results and analysis and section 7 will discuss our final conclusions.

2. Overview on an Encryption Algorithm (HuXia)

The HuXia algorithm has been described [12] based on Chen's and Lorenz chaotic systems. In order to, increase security, the algorithm firstly integrates image information into the Lorenz map and then the image information is mixed into the Chen's map via the Lorenz map.

This algorithm utilizes two 3D chaotic maps to enhance the security. HuXia includes three phases. Firstly, the algorithm integrates image information into the Lorenz map. Secondly, exceptionally pseudo-random sequences are generated by a suitable step. Thirdly, the positions of the image pixels are shuffled by the Lorenz map and then the gray values of the permuted image are encrypted by the Chen system [12]. Theoretical analysis and simulation results demonstrate that HuXia can resist the brute-force attacks. In addition, the distribution of grey values of the encrypted image has a random-like behaviour, so the algorithm HuXia has a good ability against attacks [12].

3. The Chaotic Systems

In this section we present a brief overview of the two chaotic systems which are used to produce the proposed cryptosystem. These chaotic maps systems are the Henon chaotic system and Chen's chaotic system.

3.1. The Henon Chaotic System

The Henon chaotic system 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.

The Henon map presents a simple 2D 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 have been done. Nevertheless, the complete picture of all possible bifurcations under the change of the parameters a and b has not yet emerged. 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 [10, 15].

Formula 1 illustrates the two equations of the Henon chaotic map system.

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

3.2. Chen's Chaotic System

Chen's chaotic map system which is described in Formula 2, illustrates a set of three differential equations [4, 5, 12, 17].

$$\begin{aligned} \dot{x} &= a(y_0 - x_0) \\ \dot{y} &= (c - a) x_0 - x_0 z_0 + c y_0 \\ \dot{z} &= x_0 y_0 - b z_0 \end{aligned} \tag{2}$$

Where a>0, b>0 and c such that $2c > a$ are parameters of the system [19]. When a=35, b=3 and c=28; Chen's system has a chaotic attractor as shown in Figure 1. Recently, a study about Chen's chaotic map system has attracted the attention of many researchers.

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 [12].

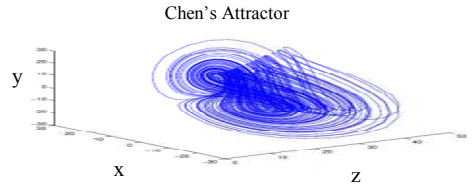


Figure 1. Chaotic behaviour of Chen's system.

4. Overview on Modes of Operations for Encryption

In this paper the colored images encryption is done with two modes of operation, the ECB mode and the CBC mode which are described in [6, 7]. The two modes are used to decide which one of them will increase the quality of encryption of the image.

The ECB is the simplest mode of operation, where the file is divided into blocks of equal length and each block is encrypted with the same encryption key, as shown in Figure 2. The plaintext is divided into P_1, P_2, P_3,… of size n bits which are encrypted to C_1, C_2, C_3, ... where, the encryption algorithm is $C_j=E_K(P_j)$ and the decryption algorithm is $P_j=D_K(C_j)$, where j=1, 2, 3, … and E_K is encryption map with the key (K) and D_K is decryption map with the same key (K).

The CBC is the second mode of operation. In the CBC mode, each block of plaintext is XORed with the previous cipher text being encrypted. CBC mode uses an Initialization Vector (IV). In decryption, the same XOR operation is repeated so that, its effect is cancelled. This mechanism is shown in Figure 3.

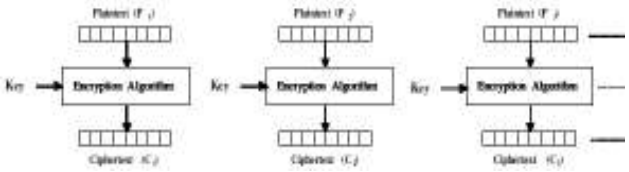


Figure 2. The construction of the ECB for encryption algorithm.

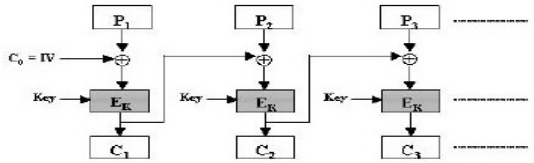


Figure 3. The construction of the CBC for encryption algorithm.

In the CBC mode, the encryption algorithm is $C_j=E_K(C_{j-1} \oplus P_j)$ and the decryption algorithm is $P_j=D_K(Cj) \oplus C_{j-1}$, where j=1, 2, 3,… and $C_0=IV$.

5. The Proposed Cryptosystem Algorithm

The proposed algorithm PCACH consists of the encryption scheme and the decryption scheme. Here, the encryption scheme only is discussed because the decryption scheme is the reverse technique of the encryption scheme.

The best case of any cryptosystem algorithm at utilization of confusion and diffusion procedures. The encryption scheme of the proposed algorithm Proposed Cryptosystem Algorithm (PCACH) consists of two algorithms, the first is confusion (permutation) algorithm and the second is diffusion (substitution) algorithm.

5.1. Confusion (Permutation) Algorithm

The confusion algorithm PPS3DCS is described in [1]. PPS3DCS is the first part of designing the encryption scheme of the proposed cryptosystem algorithm PCACH. It is designed to permute (shuffle) positions of the pixels of image. The confusion algorithm PPS3DCS produces permuted (shuffled) images, which will be used as input to the diffusion (substitution) algorithm. This algorithm PPS3DCS consists of five steps of operations has been described in [1].

5.2. Diffusion (Substitution) Algorithm

The diffusion algorithm is the second part of designing of the encryption scheme of the proposed cryptosystem algorithm PCACH. It is designed to encrypt the pixels of the image i.e., changing values of the pixels of the permuted image. Here, this algorithm is applied on the permuted-image which is produced from the confusion algorithm in section 1. This algorithm consists of seven steps as follows:

- *Step* 1: There are three sequences *XX*, *YY* and *ZZ* of size $m \times n$ which are generated by Chen's chaotic system and are used to permute the $a1$, $a2$ and $a3$ matrices of colours (*R*, *G* and *B*) of the plain-image. Also, there are *arp*, *agp* and *abp* matrices of colours of the permuted-image which were produced from the confusion algorithm.
- *Step* 2: The Henon chaotic system is converted into one dimensional chaotic system [2]. The one dimensional Henon chaotic system is defined as in Formula 3:

$$w_{i+2} = 1 - a w_{i+1}^2 + b w_i \tag{3}$$

Obtain w_2, where the initial value w_0=0.01 and the initial value w_1=0.02, values of parameters *a* and *b* are the same values of *a* and *b* for Chen's chaotic system.

- *Step* 3: The Chen's chaotic system is defined as in the following formula:

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

Obtain x_2, y_2, and z_2, where values of the parameters are a=35, b=3, c=28. Also, The three initial values are x_1=*XX*(100), y_1=*YY*(500) and z_1=*ZZ*(800) which are generated by the Chen's chaotic system.

- *Step* 4: Obtain two sequences (1-D matrix) *ARH* and *ARC* of size $si=m \times n$, where *ARH* is generated by Henon chaotic system according to the equations in Formula 5 and *ARC* is generated by Chen's chaotic system according to the equations in Formula 6. Where *i* is the variable of the counter for loop i.e., i=1,…, *si* at value of the step of the counter is three. In Formula 6, the constant is adopted equal to 10^{14}.

$$\begin{aligned} ARH(i) &= floor(w_0 * z_1) \; MOD \; 256 \\ ARH(+1) &= floor(w_1 * x_1) \; MOD \; 256 \\ ARH(i+2) &= floor(w_2 * y_1) \; MOD \; 256 \end{aligned} \tag{5}$$

$$\begin{aligned} ARC(i) &= floor((abs(x_2) * ARH(i) - floor(abs(x_2))) * constant \; MOD \; 256 \\ ARC(i+1) &= floor((abs(y_2) * ARH(i+1) - floor(abs(y_2))) * constant \; MOD \; 256) \\ ARC(i+2) &= floor((abs(z_2) * ARH(i+2) - floor(abs(z_2))) * constant \; MOD \; 256) \end{aligned} \tag{6}$$

At the end of each loop of the counter, the initial values w_0, w_1, x_1, y_1 and z_1 are changed according to the following formula.

$$\begin{aligned} x_1 &= x_2 * w_0 \\ y_1 &= y_2 * w_1 \\ z_1 &= z_2 * w_2 \\ w_0 &= w_1 \\ w_1 &= w_2 \end{aligned} \tag{6}$$

- *Step 5*: Obtain three sequences (1-D matrices) *XXC*, *YYC* and *ZZC* of size $si=m \times n$, where these sequences based on the sequence *ARC* which is produced in step 4 and the values of $k1$, $k2$ and $k3$ which are produced from the confusion algorithm PPS3DCS [1]. *XXC*, *YYC* and *ZZC* are generated according to the equations in Formula 8.

$$\begin{aligned} XXC(i) &= ((k1 + k2) * ARC(i)) \; MOD \; 256 \\ YYC(i) &= ((k2 + k3) * ARC(i)) \; MOD \; 256 \\ ZZC(i) &= ((k3 + k1) * ARC(i)) \; MOD \; 256 \end{aligned} \tag{7}$$

- *Step 6*: *XXC*, *YYC* and *ZZC* are changed based on exclusive OR operation for themselves with the sequence *ARH* which is produced in step 4. A new sequences *XXC*, *YYC* and *ZZC* are generated according to the equations in Formula 9.

$$\begin{aligned} XXC(i) &= XXC(i) \oplus ARH(i) \\ YYC(i) &= YYC(i) \oplus ARH(i) \\ ZZC(i) &= ZZC(i) \oplus ARH(i) \end{aligned} \tag{8}$$

- *Step 7*: Then, the matrices of colors of the encrypted image can be obtained by the following formula:

$$\begin{aligned} EIM_R(i,j) &= arp(i,j) \oplus XXC(t) \\ EIM_G(i,j) &= agp(i,j) \oplus YYC(t) \\ EIM_B(i,j) &= abp(i,j) \oplus ZZC(t) \end{aligned} \tag{9}$$

Where *arp*, *agp* and *abp* are the colour's matrices of the permuted-image which are generated from steps of the confusion algorithm PPS3DCS [1]. Also, *i* is the first dimension of the matrices where i=1, ..., *m* and *j* is the second dimension of the matrices where j=1, ..., *n*. Also, t=1, ..., *si* , where $si = m \times n$.

According to all previous steps, it is clear that the generation of the key streams depends on the plaintext through all the color components and every pixel value of the Encryption Matrix (EIM) includes the

information of all the color components, i.e., the diffusion has been maximized.

Figure 4 illustrates the flow-chart diagram for the diffusion algorithm of the encryption scheme of PCACH which produces EIM.

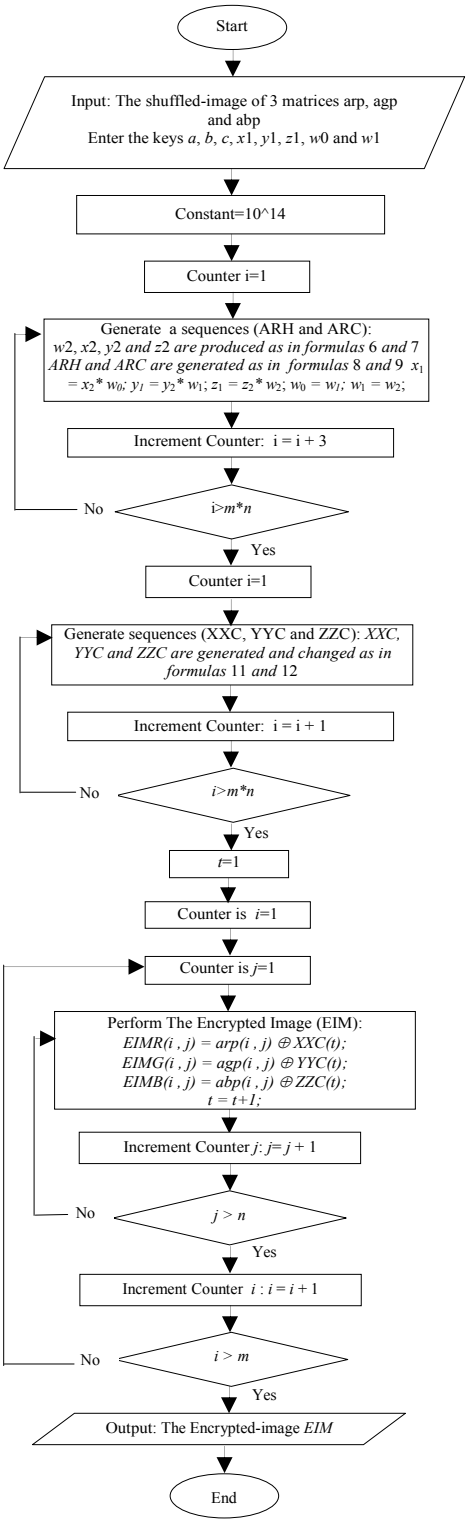
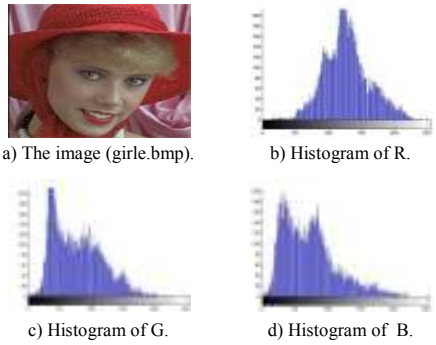


Figure 4. The Flow-Chart for a substitution (Diffusion) algorithm of encryption scheme of PCACH.

6. Experimental Results and Discussion

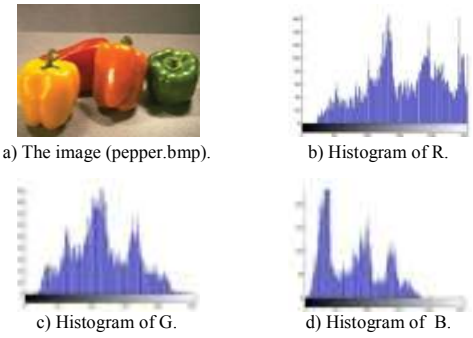
In this work, a practical program of the algorithm HuXia, the proposed cryptosystem algorithm (PCACH) with the modes of operations and a practical programs of all quality of encryption measuring factors are designed by MATLAB 7.01 on windows 7 system with Intel CORE I_3 Processor and 3.0 GB RAM. All programs were applied on three different colored-images (girl.bmp, pepper.bmp and fruit.bmp) as a plain-images of the size 120×120 pixels, which are shown in Figures 5-a, 6-a and 7-a respectively. Also, the histograms of R, G and B for the three plain-images are shown in Figures 5-b, c, d, 6-b, c, d and 7-b, c, d, respectively.



a) The image (girle.bmp). b) Histogram of R.

c) Histogram of G. d) Histogram of B.

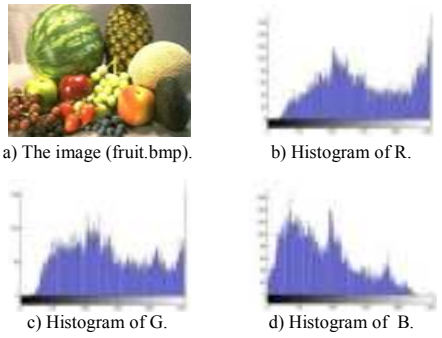
Figure 5. The first plain-image and its histogram.



a) The image (pepper.bmp). b) Histogram of R.

c) Histogram of G. d) Histogram of B.

Figure 6. The first plain-image and its histogram.



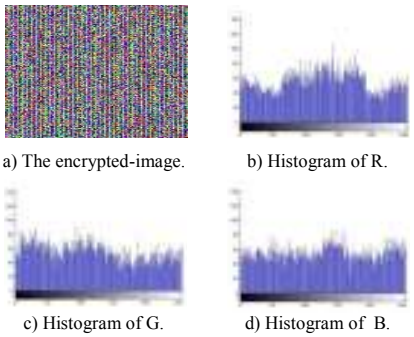
a) The image (fruit.bmp). b) Histogram of R.

c) Histogram of G. d) Histogram of B.

Figure 7. The third plain-image and its histogram.

As a sample, the encrypted images which are produced by applying the HuXia algorithm on *girl.bmp* with ECB mode and fruit.bmp with CBC mode are shown in Figures 8-a and 9-a respectively. Also, their histograms are shown in Figures 8-b, c, d and 9-b, c, d respectively.

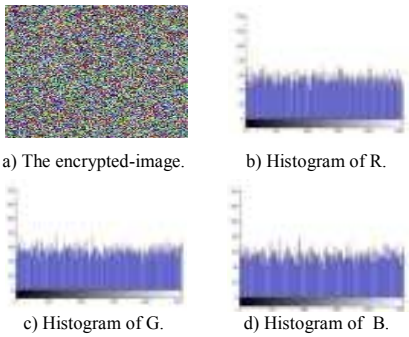
Also, the encrypted images which are produced by applying PCACH algorithm on girl.bmp with ECB mode and fruit.bmp with CBC mode are shown in Figures 10-a and 11-a respectively. Also, their histograms are shown in Figure 10-b, c, d and 11-b, c, d respectively.



a) The encrypted-image. b) Histogram of R.

c) Histogram of G. d) Histogram of B.

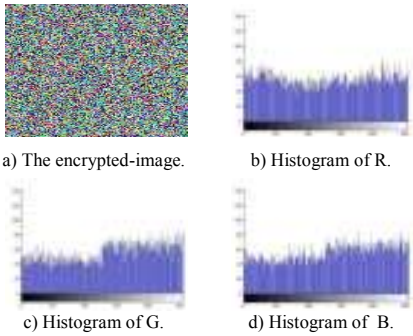
Figure 8. The encrypted-image for girl.bmp which is produced by applying HuXia with ECB mode.



a) The encrypted-image. b) Histogram of R.

c) Histogram of G. d) Histogram of B.

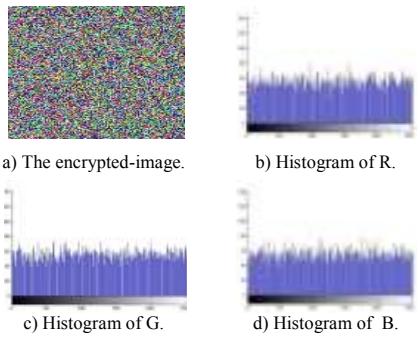
Figure 9. The encrypted-image for fruit.bmp which is produced by applying HuXia with CBC mode.



a) The encrypted-image. b) Histogram of R.

c) Histogram of G. d) Histogram of B.

Figure 10. The encrypted-image for girl.bmp which is produced by applying PCACH with ECB mode.



a) The encrypted-image. b) Histogram of R.

c) Histogram of G. d) Histogram of B.

Figure 11. The encrypted-image for fruit.bmp which are produced by applying PCACH with CBC mode.

6.1. Quality of Encryption Measuring Factors

One of the important factors in examining the encrypted image is visual inspection where the higher the disappeared features of the image the better the encryption algorithm, but in most instances, all features of the image are completely disappeared for the two algorithms, so visual inspection only is not sufficient to identify the best algorithm. So, other measuring techniques are considered to evaluate the degree of encryption quantitatively, and to compare HuXia and PCACH.

6.1.1. The Maximum Deviation Measuring Factor

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [2, 7, 21]. The steps of this measure are done as follows:

1. Count the number of pixels of each grayscale value in the range from 0 to 255 and present the results graphically (in the form of curves) for both original and encrypted images (i.e., get their histogram distributions).
2. Compute the absolute difference or deviation between the two curves and present it graphically.
3. Compute the area under the absolute difference curve, which is the sum of deviations *MD* and this represents the encryption quality. Is given by the following equation:

$$MD = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \quad (10)$$

Where h_i is the amplitude of the absolute difference curve at value i. At the higher the value of *MD*, then the encrypted image is more deviated from the original image.

Table 1 illustrates the results of *MD* measuring factor for encrypted-images which are produced from applying HuXia with the two modes ECB and CBC.

Table 1. Results of MD measuring factor for encrypted-images which are produced from applying HuXia with the two modes ECB and CBC.

		R	G	B
girl.bmp	**ECB**	11468	11869	13493
	CBC	12443	13123	13197
pepper.bmp	**ECB**	6737	10411	12796
	CBC	7135	9618	12735
fruit.bmp	**ECB**	6259	5196	7766
	CBC	6093	5246	9205

Table 2 illustrates the results of MD measuring factor for encrypted-images which are produced from applying the proposed cryptosystem algorithm PCACH with the two modes ECB and CBC.

Table 2. Results of MD measuring factor for encrypted-images which are produced from applying PCACH with the two modes ECB and CBC.

		R	G	B
girl.bmp	**ECB**	14071	15326	14748
	CBC	13202	13249	13291
pepper.bmp	**ECB**	7943	10625	13748
	CBC	7210	9680	12819
fruit.bmp	**ECB**	6506	5652	11257
	CBC	6206	5395	9403

Tables 1, 2 and Figure 12 illustrate all results of MD for the proposed cryptosystem algorithm PCACH more than all results for the algorithm HuXia with every one of modes ECB or CBC. Also, the results with algorithm HuXia is appeared irregularly, i.e., sometimes results for ECB better than results for CBC and sometimes vice versa, but the results of PCACH for ECB better than the results for CBC. Then,

PCACH satisfy quality of encryption better than the quality of HuXia.

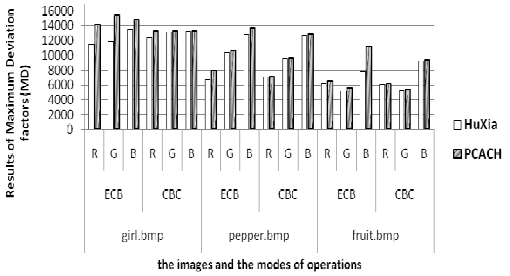


Figure 12. Results of MD measuring factor for encrypting the three image by the two algorithms HuXia and PCACH with the two modes ECB and CBC .

6.1.2. Correlation Coefficient Measuring Factor

The Correlation Coefficient (CC) between plain-image and encrypted-image equals one if they are highly dependent, i.e., the encryption process failed in encrypting the plain-image.

If the *CC* equals zero, then the plain-image and its encrypted-image are totally different. So, success of the encryption process means smaller values (near to zero) of the *CC* [2, 7]. The *CC* is measured by the following formula:

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

Where $E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i$, x and y are gray-scale pixel values of the plain and encrypted images.

Figure 13 is obtained by taking the Absolute values for the results of *CC*, which is shown in Tables 3, 4. All results of *CC* for the proposed cryptosystem algorithm PCACH are very close to zero and less than all results for the algorithm HuXia with every one of modes ECB or CBC. Also, sometimes results for ECB better than results for CBC and sometimes vice versa. Then, PCACH gives results for *CC* better than results of HuXia, so PCACH satisfy quality of encryption better than the quality of HuXia.

Table 3. Results of CC measuring factor for encrypted-images which are produced from applying HuXia with the two modes ECB and CBC.

		R	G	B
girl.bmp	**ECB**	-0.0079	0.0093	-0.036
	CBC	-0.0089	0.0027	-0.0088
pepper.bmp	**ECB**	-0.0038	-0.0090	-0.0075
	CBC	-0.0072	0.0092	-0.0140
fruit.bmp	**ECB**	-0.0074	-0.0032	-0.0100
	CBC	0.0370	0.0032	0.0065

Table 4. Results of CC measuring factor for encrypted-images which are produced from applying PCACH with the two modes ECB and CBC.

		R	G	B
girl.bmp	**ECB**	-0.0078	0.0019	0.0175
	CBC	0.0079	-0.0020	0.0029
pepper.bmp	**ECB**	-0.0035	-0.0013	-0.0044
	CBC	-0.0015	-0.0035	-0.0034
fruit.bmp	**ECB**	0.0012	-0.0029	-0.0069
	CBC	0.0147	-0.0020	0.00095

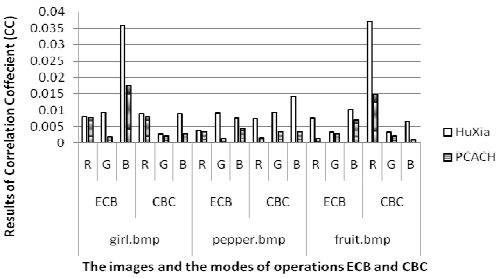


Figure 13. Results of CC measuring factor for encrypting the three image by the two algorithms HuXia and PCACH with the two modes ECB and CBC.

6.2. Security Measuring Factors

A good encryption cryptosystem algorithm must be sensitive to any little change in the plain-text or secret keys and good values for the information entropy analysis.

6.2.1. The Plain-Image Sensitivity Measuring Factor

If a significant change in the encrypted-image can be caused by a trivial change in the plain-image by the use of diffusion and confusion, then the algorithm would make differential attacks practically useless. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to test the influence of a one pixel change on the plain-image which is encrypted by using HuXia and PCACH. NPCR and UACI are computed by the following formulas [2, 12]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (12)$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|E1(i,j) - E2(i,j)|}{255} \times 100\% \quad (13)$$

Where $D(i,j) = \begin{cases} 0, & E1(i,j) = E2(i,j) \\ 1, & E1(i,j) \neq E2(i,j) \end{cases}$ This test needs two plain-images: The plain-image and a second image which is obtained by changing the value of one pixel of the plain-image. The two images are encrypted by the encryption algorithm to generate the corresponding encrypted-images $E1$ and $E2$, where M and N are width and height of the encrypted-images. $D(i, j)$ is determined by $E1(i, j)$ and $E2(i, j)$.

Table 5. Results of NPCR, and UACI analysis for all encrypted-images which are produced by HuXia with ECB and CBC.

			R	G	B	Avg.
Girl	**ECB**	NPCR	99.450	99.538	99.536	99.508
		UACI	32.279	32.890	32.322	32.497
	CBC	NPCR	99.583	99.602	99.620	99.602
		UACI	33.411	33.540	33.182	33.378
Pepper	**ECB**	NPCR	99.519	99.530	99.478	99.509
		UACI	33.556	33.695	33.366	33.539
	CBC	NPCR	99.604	99.562	99.549	99.572
		UACI	33.265	33.430	33.580	33.425
Fruit	**ECB**	NPCR	99.528	99.581	99.521	99.543
		UACI	32.822	33.128	33.458	33.136
	CBC	NPCR	99.639	99.581	99.620	99.613
		UACI	33.476	33.435	33.109	33.340

Table 5 above illustrates the results of NPCR% and UACI% for the images which are produced by applying the HuXia algorithm with the modes ECB

and CBC. Table 6 below illustrates the results of NPCR% and UACI% for the images which are produced by applying the PCACH algorithm with the same modes.

Table 6. Results of NPCR and UACI analysis for all encrypted-images which are produced by PCACH with ECB and CBC.

			R	G	B	Avg.
Girl	ECB	NPCR	99.520	99.665	99.684	99.623
		UACI	33.475	33.545	33.648	33.556
	CBC	NPCR	99.590	99.611	99.688	99.630
		UACI	33.429	33.642	33.257	33.442
Pepper	ECB	NPCR	99.618	99.625	99.653	99.632
		UACI	33.866	33.996	33.451	33.771
	CBC	NPCR	99.611	99.576	99.646	99.611
		UACI	33.285	33.467	33.585	33.446
Fruit	ECB	NPCR	99.667	99.611	99.604	99.628
		UACI	33.741	33.961	33.646	33.783
	CBC	NPCR	99.701	99.604	99.639	99.648
		UACI	33.694	33.537	33.138	33.456

Figure 14, illustrates the results of NPCR% for all images with the modes ECB and CBC. But Figure 15 illustrates the results of UACI% for all images with the modes ECB and CBC.

Tables 5, 6 and Figures 14, 15 show that, all results of NPCR% and UACI% for the proposed cryptosystem algorithm PCACH are greater than all results for the algorithm HuXia with every one of modes ECB or CBC. Also, in general, the results for CBC are better than the results for ECB. PCACH's results for NPCR% and UACI% are better than the results of HuXia so it appears that PCACH satisfies high security concerns better than HuXia.

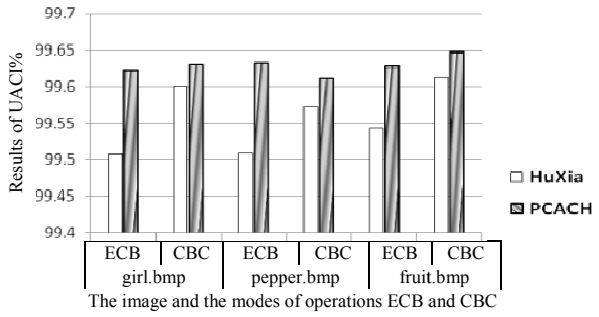


Figure 14. Results of NPCR% for the three images by using HuXia and PCACH with the two modes ECB and CBC.

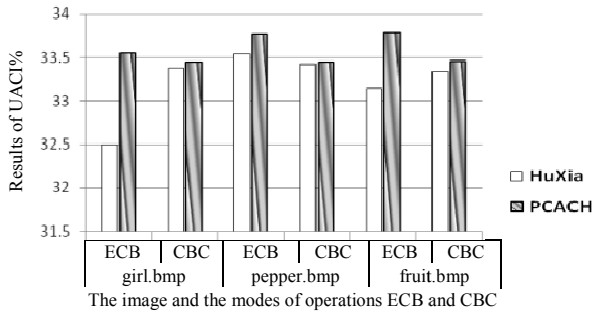


Figure 15. Results of UACI% for the three images by using HuXia and PCACH with the two modes ECB and CBC.

6.2.2. The Key Sensitivity Measuring Factor

The experimental results demonstrate that, both HuXia and PCACH are very sensitive to the secret keys mismatch. The key sensitivity results for applying HuXia and PCACH are shown in Table 7.

Table 7. Results of key sensitivity measuring factor for HuXia and PCACH algorithms.

Name and Precision for HuXia						
h	x_0	y_0	z_0	x_1	y_1	z_1
10^{-16}	10^{-15}	10^{-14}	10^{-14}	10^{-14}	10^{-14}	10^{-14}
Name and Precision for PCACH						
h	x_0	y_0	z_0	x_1	y_1	z_1
10^{-16}	10^{-16}	10^{-15}	10^{-14}	10^{-14}	10^{-14}	10^{-14}
w_0	w_1	a	b	c		
10^{-17}	10^{-17}	10^{-14}	10^{-15}	10^{-14}		

From Table 7, we can see the PCACH algorithm has larger keys space than the HuXia algorithm. Also, any one of keys with little movement (e.g., w0 is changed 10-17) will produce an incorrect decrypted image. Therefore, both HuXia and PCACH are very sensitive to keys and they can also resist various attacks based on sensibility.

Table 7 illustrates the results of precision of the keys for the proposed algorithm PCACH are better than the results of the HuXia algorithm and sometimes are very convergent. Therefore, PCACH satisfies high quality of security better than HuXia.

6.2.3. Information Entropy Measuring Factor

Information entropy [12, 14, 20] is a common criterion that shows the randomness of the data. Information entropy is illustrated in the following formula [12].

$$IE(x) = -\sum_{i=0}^{N-1} P(x_i)\, Lb(P(x_i)) \quad (14)$$

That N is the number of gray level in the color's channel of the image, x is the total number of symbols, $xi \in x$, where $P(xi)$ represents the probability of occurrence of xi 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 entropy tends to the ideal value 8 [14].

Table 8 and Figure 16, illustrate the average of information entropy results for the algorithms HuXia and PCACH with the modes ECB and CBC.

Table 8 and Figure 16, illustrate the results of IE with ECB for PCACH are better than the results for HuXia with ECB but the results for both of them with CBC are similar. Also, for both of them the results of IE with CBC are better than the others.

Table 8. Results of information entropy for encrypted-images which are produced from HuXia and PCACH algorithms with modes ECB and CBC.

			Average of IE(x)
girl.bmp	HuXia	ECB	7.965
		CBC	7.988
	PCACH	ECB	7.973
		CBC	7.988
pepper.bmp	HuXia	ECB	7.976
		CBC	7.987
	PCACH	ECB	7.979
		CBC	7.987
fruit.bmp	HuXia	ECB	7.964
		CBC	7.988
	PCACH	ECB	7.980
		CBC	7.988

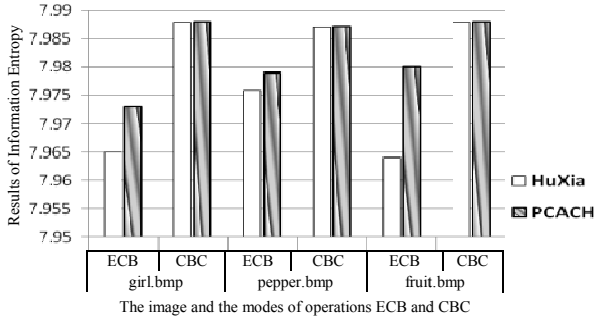


Figure 16. Results of information entropy for the three images by using HuXia and PCACH with the two modes ECB and CBC.

6.3. Time and Throughput Measuring Factors

To measure the encryption/decryption time and the throughput, the girl.bmp and pepper.bmp images are taken as a case study. The encryption time and decryption time of the images when applying the two algorithms HuXia and PCACH with the two modes of operation are shown in Table 9 and Figure 17. The throughput is defined as the amount of encrypted data per unit time (Kbps). Table 10 and Figure 18 indicate the throughput values of the two algorithms with the two modes.

Table 9. Results of encryption/decryption Time for HuXia and PCACH algorithms with modes ECB and CBC.

			Enc. time	Dec. time
girl.bmp	HuXia	ECB	0.2360	0.2175
		CBC	0.6500	0.6250
	PCACH	ECB	0.0750	0.0735
		CBC	0.3660	0.3420
pepper.bmp	HuXia	ECB	0.2500	0.2350
		CBC	0.7645	0.7430
	PCACH	ECB	0.0780	0.0750
		CBC	0.4525	0.4220

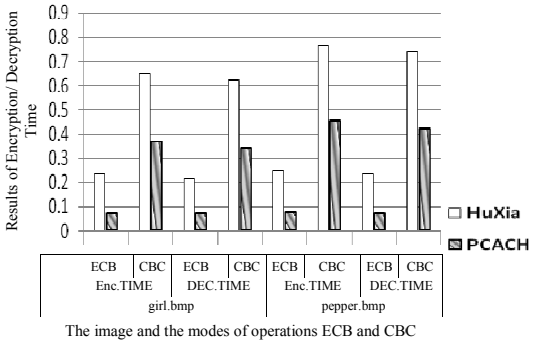


Figure 17. Results of encryption/ decryption time for applying HuXia and PCACH with the two modes ECB and CBC.

From Table 9 and Figure 17, it is clear that PCACH with the two modes achieves the smallest encryption and decryption time, i.e., the PCACH algorithm is faster than the HuXia algorithm. For both of them, the encryption and decryption time with ECB mode is smaller than the time with CBC mode.

Table 10. Results of the throughput (Kbps) for HuXia and PCACH algorithms with modes ECB and CBC.

			The Throughput
girl.bmp	HuXia	ECB	1430.51
		CBC	519.38
	PCACH	ECB	4501.33
		CBC	922.40
pepper.bmp	HuXia	ECB	1350.4
		CBC	441.60
	PCACH	ECB	4328.21
		CBC	746.08

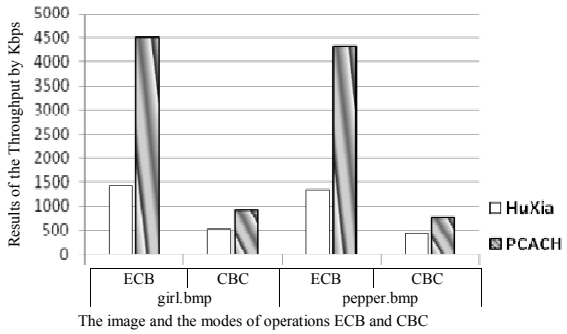


Figure 18. Results of the throughput by Kbps for applying HuXia and PCACH with the two modes ECB and CBC.

From Table 10 and Figure 18, it is clear that PCACH with the ECB mode has the highest throughput while HuXia with CBC has the smallest throughput value. The PCACH algorithm achieves throughput bigger than the throughput of the HuXia algorithm i.e., the PCACH algorithm is better than the HuXia algorithm.

7. Conclusions

This paper inspected two encryption algorithms, HuXia and PCACH, on encrypting two images of different construction with two modes of operation for encryption. Two evaluating measuring factors for quality of encryption, three evaluating measuring factors for security analysis, encryption/decryption time and the throughput were considered.

From the results of the factors for quality of encryption, PCACH satisfies quality of encryption better than HuXia, where PCACH with CC factor gives results better than HuXia. PCACH with factors NPCR% and UACI% gives results better than HuXia with every one of the modes of ECB and CBC. The results of precision of the keys sensitivity for PCACH are better than the results of HuXia, and sometimes are very convergent. The results of information entropy with ECB for PCACH are better than the results for HuXia with ECB. Our results suggest PCACH satisfies high quality of security better than HuXia. Also, PCACH achieves less time and high throughput as compared to HuXia. We conclude that PCACH has a high quality of encryption and provides an efficient and secure way for colored-image encryption.

References

[1] Abu Zaid O., El-Fishawy N., and Nigm E., "A Proposed Permutation Scheme Based on 3-D Chaotic System For Encrypting The Colored Images," *IJCSI International Journal of Computer Science*, vol. 10, no. 2, pp. 208-214, 2013.

[2] Abu Zaid O., El-Fishawy N., Nigm E., and Faragallah O., "A Proposed Encryption Scheme Based on Henon Chaotic System (PESH) for Image Security," *International Journal of*

Computer Applications, vol. 61, no. 5, pp. 29-39, 2013.

[3] Chen D. and Chang Y., "A Novel Image Encryption Algorithm Based on Logistic Maps," *Advances in Information Sciences and Service Sciences*, vol. 3, no. 7, pp. 364-72, 2011.

[4] Chen G., Mao Y., and Chui C., "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, 2004.

[5] Cokal C. and Solak E., "Cryptanalysis of A Chaos-Based Image Encryption Algorithm," *Elsevier, Physics Letters A*, vol. 373, no. 15, pp. 1357-1360, 2009.

[6] Electronic Code Book-Encyclopedia Article About Electronic Code Book., available at: http://encyclopedia.thefreedictionary.com/Electronic+code+book, last visited 2015.

[7] El-Fishawy N. and Abu Zaid O., "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block Cipher Algorithms," *International Journal of Network Security*, vol. 5, no. 3, pp. 241-251, 2007.

[8] Feng Y., Li L., and Huang F., "A Symmetric Image Encryption Approach Based on Line Maps," *in Proceedings of the 1st International Symposium Systems and Control in Aerospace and Astronautics*, Harbin, pp. 1362-67, 2006.

[9] Guan Z., Huang F., and Guan W., "Chaos-Based Image Encryption Algorithm," *Physics Letters A*, vol. 346, no. 1-3, pp. 153-157, 2005.

[10] Kumar R., Sampath A., and Indumathi P., "Enhancement and Analysis of Chaotic Image Encryption Algorithms," available at: http://airccj.org/CSCP/vol1/csit1215.pdf, last visited 2011.

[11] Lian S., Sun J., and Wang Z., "A Block Cipher Based on A Suitable Use of Chaotic Standard Map," *Chaos, Solitons and Fractals*, vol. 26, no. 1, pp. 117-29, 2005.

[12] Lu H. and Xiao X., "A Novel Color Image Encryption Algorithm Based on Chaotic Maps," *Advances in Information Sciences and Service Sciences*, vol. 3, no. 11, pp. 28-35, 2011.

[13] Ma X., Fu C., Lei W., and Li S., "A Novel Chaos-Based Image Encryption Scheme with An Improved Permutation Process," *International Journal of Advanced Computer Technology*, vol. 3, no. 5, pp. 223-33, 2011.

[14] Sabery M. and Yaghoobi M., "A New Approach for Image Encryption using Chaotic Logistic Map," *in Proceedings of International Conference on Advanced Computer Theory and Engineering*, Phuket, pp. 585-90, 2008.

[15] Sonis M., "Once More on Henon Map: Analysis of Bifurcations," *Chaos, Sotilons and Fractals*, vol. 7, no. 12, pp. 2215-34, 1996.

[16] Tedmori S. and Al-Najdawi N., "Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform," *the International Arab Journal of Information Technology*, vol. 9, no. 5, pp. 471-478, 2012.

[17] Wang X., Tian L., and Yu L., "Linear Feedback Controlling and Synchronization of the Chen's Chaotic System," *International Journal of Nonlinear Science*, vol. 2, no. 1, pp. 43-9, 2006.

[18] Xiao D., Liao X., and Wei P., "Analysis and Improvement of A Chaos-Based Image Encryption Algorithm," *Chaos, Solitons and Fractals*, vol. 40, no. 5, pp. 2191-2199, 2009.

[19] Zhou T., Tang Y., and Chen G., "Chen's Attractor Exists," *International Journal of Bifurcation and Chaos*, vol. 14, no. 9, pp. 3167-77, 2004.

[20] Zhu Z., Zhang W., Wong K., and Yu H., "A Chaos-Based Symmetric Image Encryption Scheme Using A Bit-Level Permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171-86, 2011.

[21] Ziedan I., Fouad M., and Salem D., "Application of Data Encryption Standard to Bitmap and JPEG Images," *in Proceedings 20th National Radio Science Conference*, Egypt, pp. 1-8, 2003.

Osama Abu Zaid received BSc from the Faculty Of Science, Menoufia University, Egypt in 2000. He is working as a network manager in Sadat City University. He received the MSc 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 PhD. He is interested in multimedia security over computer networks, and he registered the PhD in Faculty of sciences, Zagazig University, Egypt.

Nawal El-Fishawy received the PhD degree in mobile communications the faculty of Electronic Eng., Menoufia University, Egypt, in collaboration with Southampton University in 1991. Now, she is the head of Computer Science and Engineering Dept., Faculty of Electronic Eng. Her research interest includes computer communication networks. Now, she directed her research interests to the developments of security over wireless communications networks, and encryption algorithms. She has served as a reviewer for many national and international journals and conferences. Also she participated in many technical program committees of major international conferences in wireless communications.

Elsayed Nigm is a professor of mathematics, Department of Mathematics, Zagazig University, Egypt. He obtained his BSc in mathematics, statistics and computer sciences, Zagazig University, Faculty of Science, Egypt. He obtained his MSc degree in mathematics (functional analysis), Zagazig University, Faculty of Science, Egypt. He obtained his PhD degree mathematical statistics also, from Zagazig University, Faculty of Science, Egypt in 1990. He honors awards prize of the National Committee of Mathematics, by Egyptian Academy of Sciences and Technologies, Egypt in 2000. He has published more than 51 papers in international journals, international conferences, local Journals and Local Conferences.