CRYPTOSYSTEM ALGORITHM BASED ON CHAOTIC SYSTEMS FOR ENCRYPTING COLORED IMAGES

Osama M. Abu Zaid[1] , Nawal A. El-Fishawy[2] , and E. M. Nigm[3]

[1] Ph. D. Researcher in Computer Science, Department of Mathematics, Faculty of Sciences, Zagazig University, Egypt.

[2] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt.

[3] Department of Mathematics , Faculty of Sciences, Zagazig University, Egypt.

Abstract

In this paper, a cryptosystem algorithm based on Chen's and Henon chaotic systems will be introduced and discussed. A proposed cryptosystem algorithm will be designated as CACHS. CACHS meet the requirements of secure image transfer. It will be applied on medium color's frequencies of colored-image. CACHS contains confusion and diffusion algorithms. Confusion algorithm based on Chen's is used to shuffle the positions of pixels of the colored plain-image. Diffusion algorithm based on mixing of Henon and Chen's chaotic systems is used to change the values of pixels of the shuffled-image. CACHS will be applied on the three colors channels of the colored image with two modes of operations ECB and CBC. The results of several experimental, statistical analysis, key sensitivity tests, NPCR and UACI analysis, and information entropy analysis will show that CACHS is a well algorithm to provides an efficient and secure approach for encrypting the colored images.

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

1. Introduction

In recent years, with information and communication technologies developing, how to protect the delivered information transmission over the networks from attacking has become a vital issue [1]. This age of communications revolution which necessitates multimedia transmission in a secure manner. encryption is important in transferring image through the communication networks to protect it against reading, alteration of its content, adding false information, or deleting part of its content.

Chaotic maps are very complicated nonlinear dynamic systems, which are applied in the field of figure correspondence and encryption [2-4], 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[5].

Traditional cryptosystem algorithms such as Data Encryption Standard (DES) are designed with good confusion and diffusion properties [6]. These two properties can also be found in chaotic systems which are usually ergodic and are sensitive to system parameters and initial conditions.

Traditional image encryption algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large [7,8]. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption [9].

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 [10,11]. 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 [12-14]. The colored image consist of three 2D arrays of pixels for the color channels R, G, and B.

This paper will introduce a proposed encryption algorithm for colored images based on intermixture of 2D chaotic map system (Henon chaotic system) and 3D chaotic map system (Chen's chaotic system). A proposed encryption algorithm will be designated in this paper as (CACHS). An encryption process of the proposed algorithm (CACHS) contains permutation and substitution procedures; so it has the benefits of both of them. Permutation procedure based on Chen 's chaotic system is used to shuffle the positions of pixels of the colored plain-image. Substitution 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. CACHS will be applied on Red, Green,

and Blue channels of the colored-image with two modes of operations; Electronic Code Book (ECB) mode, and Cipher Block Chaining (CBC).

This paper is organized as follows. Section 2 presents a brief overview on the chaotic systems which are used in the work. After this, Section 3 discuss a proposed algorithm (CACHS). Section 4 discuss the experimental results and analysis. In the final, Section 5 presents the final conclusion of the paper.

2. The Chaotic Systems

In this section, a brief overview on the two chaotic systems which are used in this work is introduced. These chaotic maps systems are Henon chaotic system and Chen's chaotic system.

2.1 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.

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. [15,16]

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

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

2.2 Chen's Chaotic System

Chen's chaotic map system is described by formula 2 which illustrates a set of the three differential equations of Chen's chaotic map system. [1,7,17,18]

$$\begin{cases} x = a(y_0 - x_0) \\ y = (c - a)x_0 - x_0 z_0 + cy_0 \\ z = x_0 y_0 - bz_0 \end{cases} \quad (2)$$

where $a > 0$, $b > 0$ and c such that ($2c > a$) are parameters of the system [19]. Chen's system is chaotic when the parameters have the values; $a=35$, $b=3$ and $c \in$ [20, 28.4].

When $a=35$, $b=3$, and $c=28$. It has been experienced that Chen's chaotic system is relatively difficult to control as compared to the Lorenz system due to the prominent three-dimensional and complex dynamic property[1]. Recently, the study about Chen's chaotic map system has attracted many researchers' attention.

In [1], authors obtained on 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.

3. A Proposed Encryption Algorithm (CACHS)

In this section, the proposed encryption algorithm based on Chen's and Henon chaotic systems (CACHS) is presented. The proposed algorithm (CACHS) consists of the encryption scheme and the decryption scheme. In this part of the paper 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 [1]. The encryption scheme of the proposed algorithm (CACHS) consists of two algorithms, the first is permutation and confusion algorithm, and the second is substitution and diffusion algorithm.

3.1 Permutation and Confusion Algorithm

Permutation and confusion algorithm is the first part of designing of the encryption scheme of the proposed algorithm (CACHS). It is designed to permute the positions of the pixels of the image, i.e. shuffling the positions of pixels of the image. This algorithm consists of five steps of operations as following:

Step1: Obtain the ***a1***, ***a2*** and ***a3*** matrixes (the three color components Red, Green and Blue) of the color image of size $m \times n \times 3$, respectively. ***a1*** represents $m \times n$ matrix for the red, ***a2*** represents $m \times n$ matrix for the green, and ***a3*** represents $m \times n$ matrix for the blue. Afterwards, each color's matrix (including ***a1***, ***a2*** and ***a3***) is reshaped by Matlab into one dimension matrix (vector) of integers within {0, 1… 255}, wherein length of the vector is ***si*** = $m \times n$. Then, the so obtained three vectors (***aa1***, ***aa2***, and ***aa3***) represent the plaintext which will be permuted and encrypted.

Step2: Obtain the sequences *XX*, *YY*, and *ZZ* (1-D matrixes) as in formula 3 which are generated by Chen's chaotic system at a =35, b =3, c =28, the initial values $x_0 = 0+k$, $y_0 = 1+k$, $z_0 = 0+k$, and $h = 0.055555$.

$$\begin{aligned} XX(i) &= floor(x)\ MOD\ 256; \\ YY(i) &= floor(y)\ MOD\ 256; \\ ZZ(i) &= floor(z)\ MOD\ 256; \end{aligned} \quad (3)$$

Where ***i*** is from ***1*** to ***si***. Values of ***x***, ***y***, and ***z*** are obtained from the three equations of Chen's chaotic system in formula 2. ***k*** is obtained by formula 4, where it is used to modify the keys in the proposed algorithm.

$$\boldsymbol{k} = (k1+k2+k3)/10\text{^}13 \quad (4)$$

Formula 5 is employed to generate the values of $k1$, $k2$ and $k3$ which are used to obtain ***k***.

$$\begin{aligned} k1 &= \sum_{i=1}^{m}\sum_{j=1}^{n} \boldsymbol{a1}(i,j) \\ k2 &= \sum_{i=1}^{m}\sum_{j=1}^{n} \boldsymbol{a2}(i,j) \\ k3 &= \sum_{i=1}^{m}\sum_{j=1}^{n} \boldsymbol{a3}(i,j) \end{aligned} \quad (5)$$

Step3: The matrixes *XX*, *YY*, and *ZZ* are sorted in descending sort by using Matlab function (sort). The Matrixes *XX1*, *YY1*, and *ZZ1* are produced from sorting of the matrixes *XX*, *YY*, and *ZZ* respectively.

For example, let suppose ***XX***=[1 3 4 10 9 5 2 8 155 255], after apply the function of descending sort; the result is ***XX1***=[255 155 10 9 8 5 4 3 2 1]. In position expression; the positions [1 2 3 4 5 6 7 8 9 10] shifted to the positions [10 8 7 3 4 6 9 5 2 1].

Step4: The reshaped matrixes ***aa1***, ***aa2*** and ***aa3*** are rearranged respectively according to the position of *XX* in *XX1*, the position of *YY* in *YY1*, and the position of *ZZ* in *ZZ1*. The sequences ***ar***, ***ag***, and ***ab*** which are obtained from rearranging process of ***aa1***, ***aa2***, and ***aa3*** respectively.

For example, let suppose ***aa1***=[125 56 90 42 50 220 120 255 65 35], according to the position of XX in XX1 as in example of step3; the result is ***ar*** = [35 65 42 50 255 220 90 56 120 125].

Step5: Obtain the matrixes ***arp***, ***agp***, and ***abp*** (the permuted matrixes of the color's matrixes ***a1***, ***a2***, and ***a3***), which are produced respectively by reshaping the sequences ***ar***, ***ag***, and ***ab*** from one dimension to the matrixes of two dimension $m \times n$.

According to the confusion algorithm, the position of any pixel in ***a1***, ***a2***, *or* ***a3*** is different with its position in ***arp***, ***agp***, or ***abp*** respectively, which will lead to be strong for the attacks.

3.2 Substitution and Diffusion Algorithm

Substitution and diffusion algorithm is the second part of designing of the encryption scheme of the proposed algorithm (CACHS). It is designed to encrypt the pixels of the image, i.e. changing values of the pixels of the image. Here this algorithm is applied on the permuted image which is produced from the permutation and confusion algorithm in the previous section. This algorithm consists of seven steps of operations as following:

Step1: There are three sequences *XX*, *YY* and *ZZ* of size $\boldsymbol{m \times n}$ which are generated by Chen's chaotic system and are used to permute the ***a1***, ***a2*** and ***a3*** matrixes of the plain-image. Also, there are ***arp***, ***agp***, and ***abp*** matrixes of colors of the permuted image which is produced from the permutation procedure according to steps of the previous section.

Step2: The Henon chaotic system is converted into one dimensional chaotic system [30]. The one dimensional Henon chaotic system is defined as in formula 6:

$$w_{i+2} = 1 - aw_{i+1}^2 + bw_i \quad (6)$$

Obtain $\boldsymbol{w_2}$, where the initial value $\boldsymbol{w_0}$ = 0.01, and the initial value $\boldsymbol{w_1}$ = 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:

$$\begin{aligned} x_2 &= a(y_1 - x_1) \\ y_2 &= (c-a)x_1 - x_1z_1 + cy_1 \\ z_2 &= x_1y_1 - bz_1 \end{aligned} \quad (7)$$

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 $\boldsymbol{x_1}$= *XX* (100), $\boldsymbol{y_1}$= *YY* (500) and $\boldsymbol{z_1}$= *ZZ* (800) which are generated by the Chen's chaotic system.

Step4: 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 8, and *ARC* is generated by Chen's chaotic system according to the equations in formula 9. 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. And in formula 9 the constant is adopted equal to $\boldsymbol{10^{14}}$.

$$\begin{aligned} ARH(i) &= floor(w_0 * z_1)\ MOD\ 256; \\ ARH(i+1) &= floor(w_1 * x_1)\ MOD\ 256; \\ ARH(i+2) &= floor(w_2 * y_1)\ MOD\ 256; \end{aligned} \quad (8)$$

$$\begin{aligned} ARC(i) &= floor((abs(x_2)*ARH(i)-floor(abs(x_2)))* \\ &\quad constant\ \ MOD\ 256); \\ ARC(i+1) &= floor((abs(y_2)*ARH(i+1)-floor(abs(y_2)))* \\ &\quad constant\ \ MOD\ 256); \\ ARC(i+2) &= floor((abs(z_2)*ARH(i+2)-floor(abs(z_2)))* \\ &\quad constant\ \ MOD\ 256); \end{aligned} \quad (9)$$

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:

$$\begin{aligned} x_1 &= x_2 * w_0; \\ y_1 &= y_2 * w_1; \\ z_1 &= z_2 * w_2; \\ w_0 &= w_1; \\ w_1 &= w_2; \end{aligned} \quad (10)$$

Step5: Obtain three sequences (1-D matrixes) *XXC*, *YYC*, and *ZZC* of size $si = m \times n$, where these sequences based on the sequence *ARC* which is produced in step4 and the values of *k1*, *k2*, and *k3* which are produced in step2 of the previous subsection. *XXC*, *YYC*, and *ZZC* are generated according to the equations in formula 11.

$$\begin{aligned} XXC(i) &= ((k1+k2)*ARC(i))\ MOD\ 256; \\ YYC(i) &= ((k2+k3)*ARC(i))\ MOD\ 256; \\ ZZC(i) &= ((k3+k1)*ARC(i))\ MOD\ 256; \end{aligned} \quad (11)$$

Step6: *XXC*, *YYC* and *ZZC* are changed based on exclusive OR operation for themselves with the sequence *ARH* which is produced in step4. A new sequences *XXC*, *YYC*, and *ZZC* are generated according to the equations in formula 12.

$$\begin{aligned} XXC(i) &= XXC(i) \oplus ARH(i); \\ YYC(i) &= YYC(i) \oplus ARH(i); \\ ZZC(i) &= ZZC(i) \oplus ARH(i); \end{aligned} \quad (12)$$

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

$$\begin{aligned} EIMR(i,j) &= arp(i,j) \oplus XXC(t); \\ EIMG(i,j) &= agp(i,j) \oplus YYC(t); \\ EIMB(i,j) &= abp(i,j) \oplus ZZC(t); \end{aligned} \quad (13)$$

Where ***arp***, ***agp***, and ***abp*** are the color's matrixes of the permuted-image which are generated in step5 of the previous subsection. 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 $si = m \times n$.

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 taken full advantages. These features strengthen the proposed encryption algorithm security.

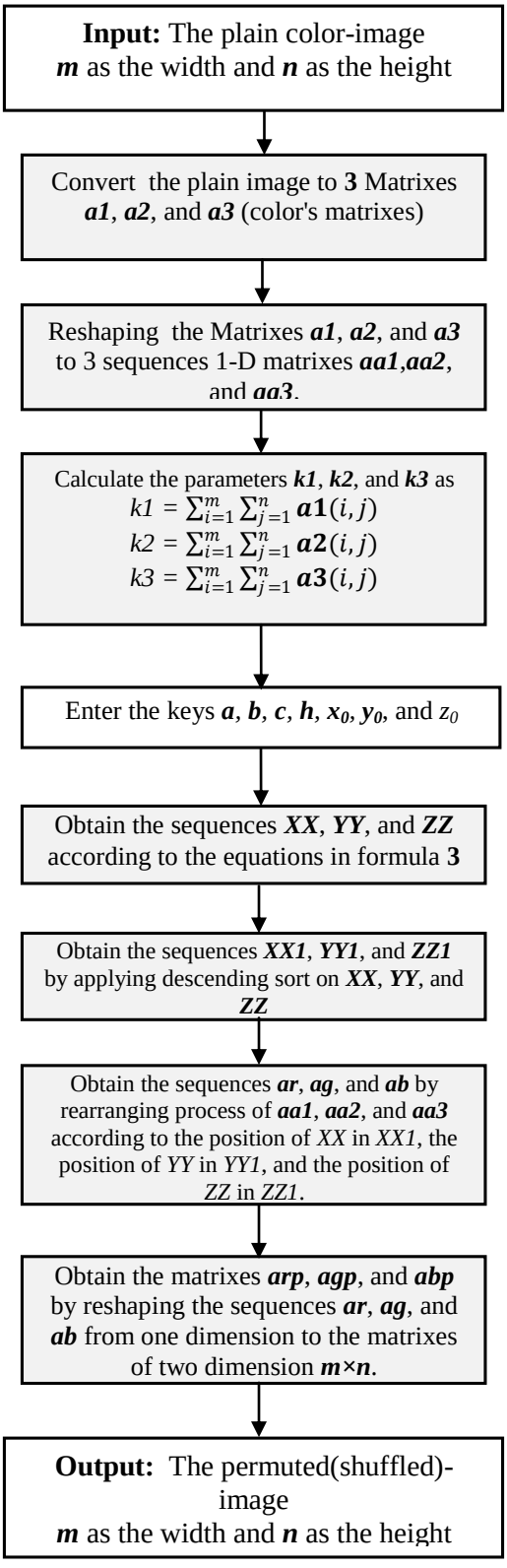

Fig. 1 The Data-Flow diagram for a permutation (Confusion) algorithm of encryption scheme of CACHS

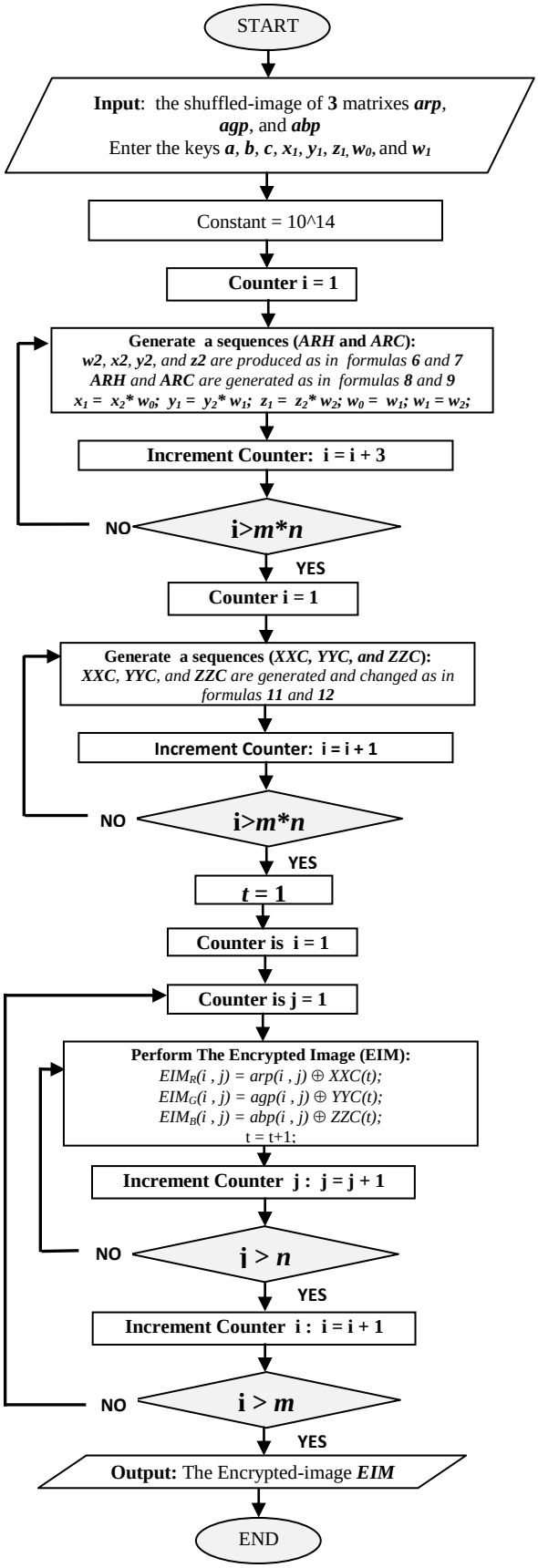

Fig. 2 The Flow-Chart for a substitution (Diffusion) algorithm of encryption scheme of CACHS

4. Experimental Results and Analysis

In this paper, a practical programs of a proposed encryption algorithm (CACHS) 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 Laptop computer with Intel CORE I_3 Processor, 3.0 GB RAM, and 320 GB Hard Disk. All programs have been applied on the colored-image which have high frequency of colors (*fruit.bmp*) as a plain-image of the size *120×120* pixels, which are shown in Fig. 3(a).

4.1 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 (CC) 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 (HC), vertical (VC), and diagonal (DC) for all color's channels *R*, *G*, *B* of the encrypted-image.

4.1.1 Histogram Analysis

The plain colored-image (*fruit.bmp*) of the size *120×120* pixels are shown in Fig.3(a), and the histogram for *R*, *G*, *B* of this image is shown in Fig.3(b, c, d).
The application of the proposed algorithm (CACHS) on this image has two sequent steps; first is permutation (confusion) algorithm and second is substitution (diffusion) algorithm.

Figure 4(a) show the shuffled-image for *fruit.bmp* which are produced from applying the permutation (confusion) algorithm. The histogram for *R*, *G*, *B* of this image is shown in Fig.4(b, c, d) which are the same histograms of the plain-image.

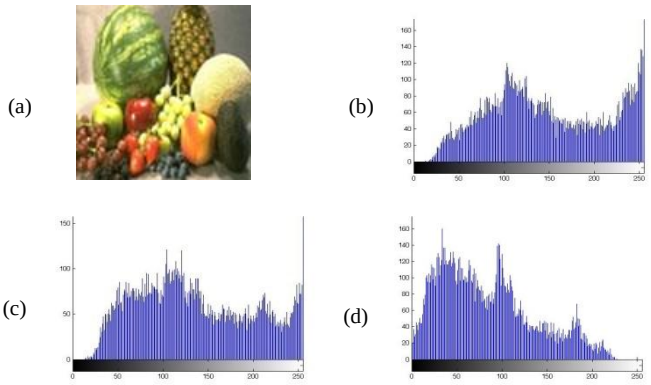

Fig. 3 The plain colored-image and its histogram: (a) the image (fruit.bmp); (b) histogram of R; (c) histogram of G; (d) histogram of B.

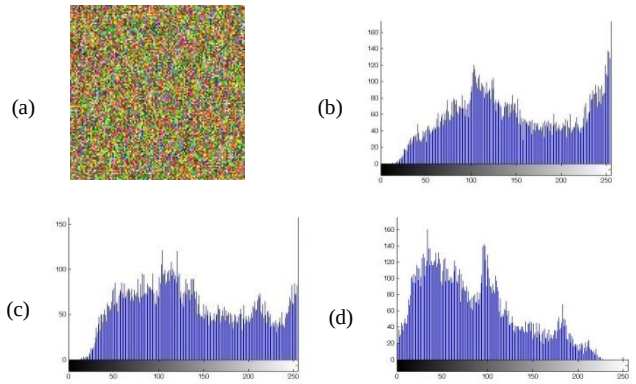

Fig. 4 The shuffled-image for fruit.bmp and its histogram: (a) the shuffled-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

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

Figure 6(a) illustrates the encrypted-image for *fruit.bmp* which is produced from applying the proposed cryptosystem algorithm (CACHS) with CBC mode. The histogram for *R*, *G*, *B* of the encrypted-image is shown in Fig. 6(b, c, d).

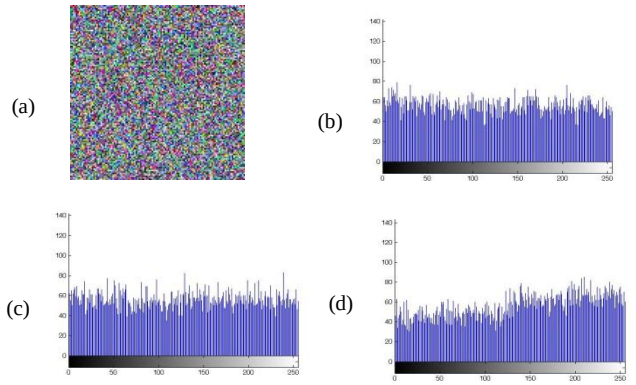

Fig. 5 The encrypted-image for fruit.bmp which are produced by applying CACHS with ECB mode: (a)the encrypted-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

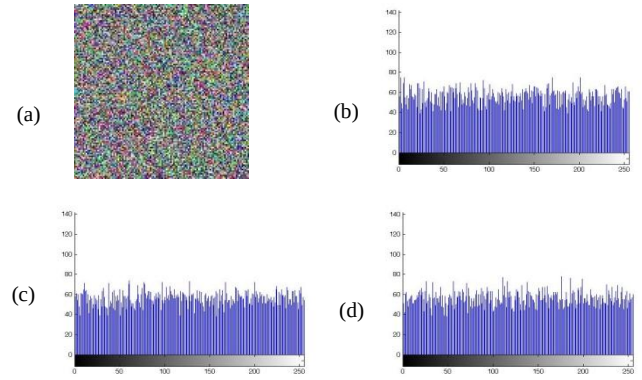

Fig. 6 The encrypted-image for fruit.bmp which are produced by applying CACHS with CBC mode: (a)the encrypted-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

From all previous figures of histograms, as anyone can see, the histogram of the encrypted-image is fairly uniform and is significantly different from that of the plain-image. The proposed algorithm (CACHS) is a complicated and very good procedure for disguise any countenance of the image. Also, anyone can observe, the proposed algorithm (CACHS) is qualification for encrypting the colored-images.

4.1.2 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 CC [20]. The CC is measured by formula 14:

$$\mathbf{CC} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \qquad (14)$$

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

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

Tables 1, illustrates that the proposed cryptosystem algorithm (CACHS) achieves very small values (near to zero) of CC with all modes of operations for the colored-image, so a CACHS is a complicated and a good algorithm for encrypting the images. Also, the results of CC for CBC mode is better than the results for ECB mode.

Table 1: Results of CC analysis for encrypting *fruit.bmp* by CACHS with the modes.

Modes	**CC for encrypting *fruit.bmp***		
	R	***G***	***B***
ECB	0.0012	-0.0029	-0.0069
CBC	0.0014	-0.0020	0.00095

4.1.3 Correlation Analysis of Two Adjacent Pixels

It is well known that the adjacent pixels of an image have very high correlation coefficients in horizontal, vertical and diagonal directions. The following formulas is employed to test the correlation between two horizontally adjacent pixels (designed as **HC**), two vertically adjacent pixels (designed as **VC**), and two diagonally adjacent pixels (designed as **DC**), 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 r_{xy} of each pair by using the following formulas [1,7]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\,,\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (15)$$

$$cov(x,y) = E\big(x - E(x)\big)\big(y - E(y)\big) \quad (16)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \quad (17)$$

Where x and y denote two adjacent pixels, and N is the total number of duplets (x, y) obtained from the image. Table 2 illustrates the results of HC, VC, and DC analysis for the plain colored-image (*fruit.bmp*).

Table 3 illustrates the results of HC, VC, and DC analysis for the two encrypted-images, which are produced by applying the proposed cryptosystem algorithm (CACHS) on the plain-image with the two modes ECB and CBC.

Table 2: Results of HC, VC, and DC analysis for the plain colored-image *fruit.bmp*.

	The plain image (*fruit.bmp*)		
	R	***G***	***B***
HC	0.9367	0.9433	0.9287
VC	0.9827	0.9812	0.9719
DC	0.9153	0.9010	0.9000

Table 3: Results of HC, VC, and DC analysis for the encrypted images of *fruit.bmp* by applying the CACHS with the modes.

		The encrypted image of (*fruit.bmp*)		
		R	***G***	***B***
HC	**ECB**	0.0026	0.0272	0.00059
	CBC	-0.0066	0.0062	-0.0751
VC	**ECB**	-0.00007	-0.0031	-0.0068
	CBC	-0.0396	-0.00042	0.0039
DC	**ECB**	-0.0024	0.0089	-0.0185
	CBC	-0.0614	0.0069	-0.0371

According to Table 2, anyone can observe, the results of HC, VC, and DC for the correlation analysis of two adjacent pixels for the plain colored-image are approach to 1, implying that high correlation exists among pixels.

According to Table 3, the results of HC, VC, and DC for the correlation analysis of two adjacent pixels for the encrypted-image with both of two modes are approach to 0, implying that no detectable correlation exists among pixels. Therefore the proposed cryptosystem algorithm (CACHS) can protect the encrypted-image from statistical attacks. Also, from Table 3, the results sometimes better with ECB than CBC and other sometimes the converse is actualize.

4.2 Security Analysis

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

In the proposed cryptosystem algorithm (CACHS), the parameters a, b, c, and h, the initial values x_0, y_0, z_0, w_0, w_1, x_1, y_1, and z_1 are used as a secret keys. The key space is large enough to resist all kinds of brute-force attacks.

4.2.1 The Plain-text Sensitivity Analysis

A very vital relationship between the plain-image and the encrypted-image may be revealed [1]. 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 algorithm (CACHS), *NPCR* (Number of Pixels Change Rate) and *UACI* (Unified Average Changing Intensity) are used. *NPCR* and *UACI* are computed by the following formulas [1, 20]:

$$\mathbf{NPCR} = \frac{\sum_{i,j} \boldsymbol{D(i,j)}}{\boldsymbol{M \times N}} \times \mathbf{100\%} \quad (18)$$

$$\mathbf{UACI} = \frac{1}{M \times N}\sum_{i,j} \frac{|\boldsymbol{E1(i,j) - E2(i,j)}|}{255} \times 100\% \quad (19)$$

$$\textbf{Where } D(i,j) = \begin{cases} \mathbf{0}, & E1(i,j) = E2(i,j) \\ \mathbf{1}, & E1(i,j) \neq E2(i,j) \end{cases}$$

This test needs 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 algorithm (CACHS) with the same keys to generate the corresponding encrypted-images *E1* and *E2*. Where the grey values of the pixel at position (i, j) of *E1* and *E2* are denoted as *E1*(i, j) and *E2*(i, j) respectively; M and N are width and height of the encrypted-image. $D(i, j)$ is determined by *E1*(i, j) and *E2*(i, j).

Table 4: Results of NPCR and UACI analysis for the encrypted images of *pepper.bmp* by applying the CACHS with the modes.

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

From Table 4, anyone can observe that the results of NPCR and UACI for the two encrypted images with both of modes (ECB, and CBC) are very close to the ideal values (*NPCR*=99.609% and *UACI*=33.4635%)[1], i.e. with the proposed cryptosystem algorithm, A very little change of the plain-image pixel values (one pixel) will lead to a significant change of the encrypted-image.

4.2.2 The Key Sensitivity Analysis

The experimental results demonstrate that the proposed cryptosystem algorithm (CACHS) is very sensitive to the secret keys mismatch. The decrypted image by using CACHS are the same of the original image, where are decrypted by using CACHS with $a=35$, $b=3$, $c=28$, h=0.055555, $x_0=0+k$, $y_0=1+k$, $z_0=0+k$, $w_0=0.01$, $w_1=0.02$, $x_1=XX(100)$, $y_1=XX(500)$, *and* $z_1=XX(800)$ to produce the original image.

The experimental results for applying CACHS on *fruit.bmp* with both of modes demonstrate that the proposed cryptosystem algorithm (CACHS) 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}), $\boldsymbol{w_0}$ mismatch (10^{-17}), $\boldsymbol{w_1}$ 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.7 illustrates the sensitivity of the proposed algorithm (CACHS) with the secret key $\boldsymbol{w_0}$, where as the encrypted-image which is shown in Fig.3(a) decrypted using $\boldsymbol{w_0}$= 0.01000000000000001, and the remains secret keys as the same as in the normal case. As can be seen that, even the secret key $\boldsymbol{w_0}$ is changed a little (10^{-17}), the decrypted image is absolutely different from the original image (*fruit.bmp*).

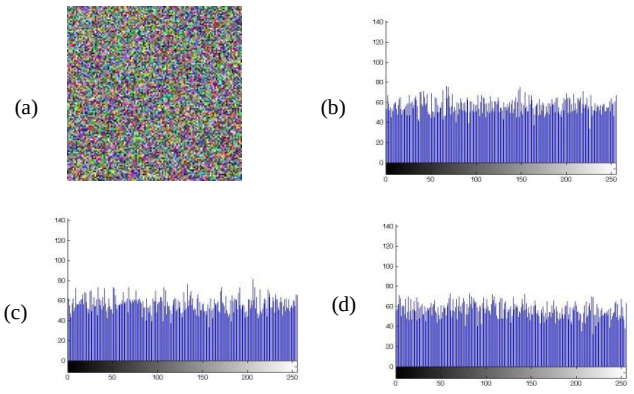

Fig. 7 The sensitivity to the secret key w_0 of CACHS with ECB, for decrypting the encrypted-image of *fruit.bmp*: (a) the decrypted image, which is produced at w_0 =*0.01000000000000001*; (b) histogram of R; (c) histogram of G; (d) histogram of B.

Another for example, Fig.8 illustrates the sensitivity of the proposed algorithm (CACHS) with the secret key $\boldsymbol{b}$, where as the encrypted-image which is shown in Fig.3(a) decrypted using $\boldsymbol{b}$= 3.000000000000001, and the remains secret keys as the same as in the normal case. As can be seen that, even the secret key $\boldsymbol{b}$ is changed a little (10^{-15}), the decrypted image is absolutely different from the original image (*fruit.bmp*).

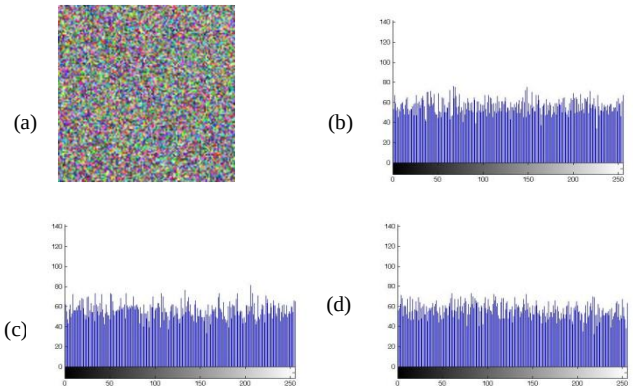

Fig. 8 The sensitivity to the secret key w_0 of CACHS with ECB, for decrypting the encrypted-image of *fruit.bmp*: (a) the decrypted image, which is produced at b = *3.000000000000001*; (b) histogram of R; (c) histogram of G; (d) histogram of B.

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

4.2.3 Information Entropy Analysis

Information entropy [1,21,22] is a common criterion that shows the randomness of the data. Also, entropy and information theory introduced by Robert M. Gray at 2009. two of the most famous formulas of the information entropy are illustrated in formulas 20 and 21 from [1] and [21] respectively.

$$\boldsymbol{H(x)} = -\sum_{i=0}^{N-1} P(x_i) Lb(P(x_i)) \quad (20)$$

or

$$\boldsymbol{H(x)} = \sum_{i=0}^{N-1} P(x_i) Log(\frac{1}{P(x_i)}) \quad (21)$$

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 $\boldsymbol{Lb}$ denotes the base 2 logarithm.

Table 5: Results of Information Entropy analysis for the encrypted image of *fruit.bmp* by applying the CACHS with the modes.

		The Information Entropy *H(x)*		
		R	***G***	***B***
fruit.bmp	**ECB**	7.986	7.984	7.970
	CBC	7.986	7.988	7.987

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)

[21]. From Table 5, all the results of information entropy *H(x)* for the image, which is encrypted by CACHS with both of the modes are very close to the ideal value. So these results mean that the encrypted-image are close to a random source and the proposed cryptosystem algorithm (CACHS) is secure against entropy attack.

Also from Table 5 and Fig. 9, the information entropy analysis *H(x)* illustrates the results with both of modes ECB and CBC are convergent, but are better with CBC mode than with ECB mode.

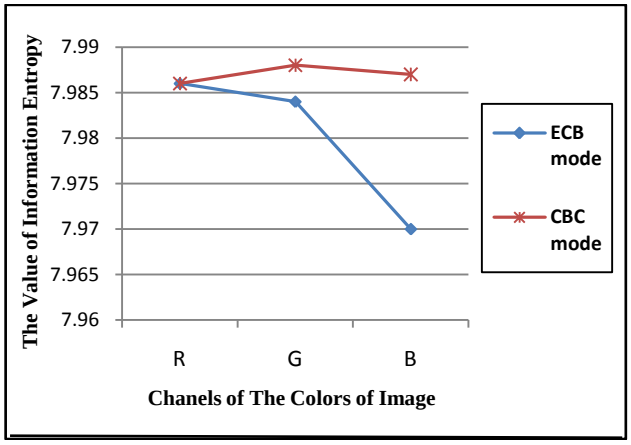

Fig. 9 Values of information entropy analysis for encrypted image of fruit.bmp with the two modes ECB and CBC

5. Conclusion

In this paper, a new cryptosystem algorithm (CACHS) is proposed for colored-images encryption based on Henon chaotic system and Chen's chaotic system. CACHS 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 algorithm (CACHS) is applied on the colored-image with two modes of operations ECB and CBC. The experimental results and analysis show that the proposed cryptosystem algorithm (CACHS) is very good encryption Algorithm and has high security, where as the proposed cryptosystem algorithm (CACHS) has merits: 1) its results with all tests of statistical analysis are excellent. 2) it has a large enough key space to resist most kinds of brute force attacks. 3) it is very sensitive to all members of the secret keys. 4) its results of NPCR and UACI tests are excellent, because these are very closed to the ideal values. 5) its results of information entropy analysis tests are excellent, because these are very closed to the ideal value 8. As demonstrated in the simulation and its results, the proposed cryptosystem algorithm (CACHS) has high encryption quality, and it is suitable to provides an efficient and secure way for the colored-image encryption.

References

[1] 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.
[2] 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.
[3] 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.
[4] Dongming Chen, Yunpeng Chang, "A novel image encryption algorithm based on Logistic maps," AISS, Vol. 3, No.7, 2011, pp.364-372.
[5] Zhang LH, Liao XF, Wang XB, "An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, Vol. 24, 2005; pp. 759–765.
[6] Schneier B. Cryptography: Theory and Practice. Boca Raton: CRC Press; 1995.
[7] 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.
[8] Chiaraluce F, Ciccarelli L, et al. "A new chaotic algorithm for video encryption". IEEE Trans Consume Electron, Vol. 48, 2002, pp. 838–843.
[9] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li, "A new chaotic algorithm for image encryption," Chaos, Solitons and Fractals , Vol.29 , 2006, pp. 393–399.
[10] Wong KW, "A fast chaotic cryptography scheme with dynamic look-up table," Phys Lett A , Vol. 298,2002, pp. 238-242.
[11] Pareek NK, Patidar V, Sud KK, "Discrete chaotic cryptography using external key," Phys Lett A, Vol. 309,2003, pp.75-82.
[12] Guan ZH, Huang FJ, Guan WJ, "Chaos-based image encryption algorithm," Phys Lett A, Vol. 346,2005, pp.153-157.
[13] 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.
[14] Feng Y, Li LJ, Huang F, "A symmetric image encryption approach based on line Maps," In: Proc ISSCAA2006, Jan 2006, p. 1362-67.
[15] R.Raja Kumar, A.Sampath, P.Indumathi, "Enhancement and Analysis of Chaotic Image Encryption Algorithms," CCSEA 2011, CS & IT 02, 2011,pp. 143–153.
[16] M, Sonls, "Once more on Henon map: analysis of bifurations," Chaos, Sotilons Fractals, Vol. 7, No. 12, 1996, pp. 2215-2234.
[17] 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.
[18] Cahit Cokal, Ercan Solak, "Cryptanalysis of a chaos-based image encryption algorithm," Elsevier, Physics Letters A, Vol. 373, 2009, pp. 1357–1360.
[19] Tianshou Zhou, Yun Tang, And Guanrong Chen, "Chen's Attractor Exists," International Journal of Bifurcation and Chaos, Vol. 14, No. 9, 2004, pp. 3167-3177.
[20] 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.
[21] M. Sabery.K, M. Yaghoobi, "A New Approach for Image Encryption Using Chaotic Logistic Map," IEEE Computer Society, ICACTE, 2008, pp. 585-590.
[22] 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 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 .

Nawal A. El-Fishawy received the Ph.D. degree in mobile communications the faculty of Electronic Eng., Menoufia university, Menouf, 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.

E. M. Nigm received the Ph.D. degree in Mathematical Statistics, Mathematics Dept., the faculty of sciences, Zagazig university, zagazig, Egypt, in 1990. Now he is professor in the mathematics Dept., Faculty of sciences, Zagazig university. His research interest includes Mathematical Statistics and computer sciences. Now he directed her research interests to the developments of security algorithms. he has served as a reviewer for many national and international journals and conferences.