A PROPOSED PERMUTATION SCHEME BASED ON 3-D CHAOTIC SYSTEM FOR ENCRYPTING THE 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 proposed permutation scheme based on three dimension chaotic map system will be presented. Chen's chaotic system is 3-D chaotic map system, which will be used to obtain the proposed permutation scheme. A proposed permutation scheme will be designated as PPS3DCS. It will be applied on two different color's frequencies colored-images. A proposed scheme (PPS3DCS), which Contains permutation procedure based on Chen's chaotic system is used to shuffle the positions of pixels of the colored plain-image. PPS3DCS will be applied on all color's channels of the image; Red, Green, and Blue. The expectant results of several experiments, statistical analysis, key sensitivity tests, and information entropy analysis will show that the proposed permutation scheme (PPS3DCS) is a good encryption scheme to provides an efficient and secure way for confusing or encrypting the colored images.

Keywords *chaotic map; permutation; Image encryption; 3-D Chaotic map system.*

1. Introduction

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.

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 will introduce a proposed permutation scheme for encrypting the colored images based on the 3-D chaotic map system (Chen's chaotic system). A proposed permutation scheme will be designated in this paper as (PPS3DCS). The permutation procedure based on Chen 's chaotic system is used to shuffle the positions of pixels of the colored plain-image.

The proposed permutation scheme PPS3DCS will be applied on all color's channels of the image; Red, Green, and Blue.

This paper is organized as follows. Section 2, will presents an overview on Chen's chaotic map system. Section 3, and its subsections 3.1,will discuss the proposed permutation scheme (PPS3DCS). Section 4, and its subsections 4.1 and 4.2 will present the experimental results and analysis by implementing statistical analysis and security analysis tests. Section 5, will discuss the final conclusion.

2. An Overview on Chen's Chaotic Systems

In this section, an overview on Chen's chaotic map system as important one of the three dimension chaotic map systems, which is used in this work.

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. [10-13]

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

where $a > 0$, $b > 0$ and c such that $(2c > a)$ are parameters of the system [14]. Chen's system i s 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 a chaotic attractor as shown in Fig.1. It has been experienced that Chen's chaotic system is relatively difficult due to the prominent three-dimensional and complex dynamic property[10]. Recently, the study about Chen's chaotic map system has attracted many researchers' attention.

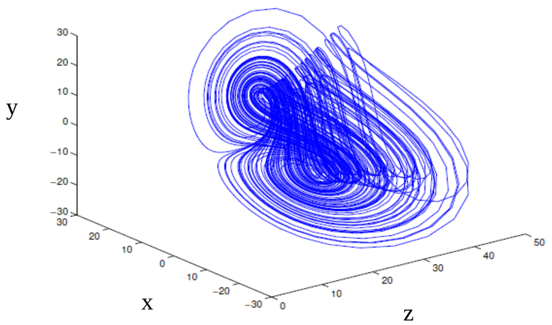

Fig. 1 Chaotic behavior of Chen's system

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].

3. A Proposed Scheme (PPS3DCS)

In this section, the proposed permutation scheme (PPS3DCS) based on Chen's chaotic systems is presented. The proposed scheme (PPS3DCS) consists of the permutation (confusion) procedure and the re-permutation (re-confusion) procedure. In this part of the paper the permutation (confusion) procedure only is designed and discussed because The re-confusion (decryption) procedure is the reversed technique of the permutation procedure.

3.1 The Permutation Procedure

The proposed permutation scheme (PPS3DCS) is designed to permute the positions of the pixels of the image, i.e. shuffling the positions of pixels of the image.

The proposed permutation scheme (PPS3DCS) 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 confused.

Step2: Obtain the sequences *XX*, *YY*, and *ZZ* (1-D matrixes) as in formula 2 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.

$$\begin{aligned} XX(i) &= floor(x)\ MOD\ 256; \\ YY(i) &= floor(y)\ MOD\ 256; \\ ZZ(i) &= floor(z)\ MOD\ 256; \end{aligned} \quad (2)$$

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 1. ***k*** is obtained by formula 3, where it is used to modify the keys in the proposed algorithm.

$$\boldsymbol{k} = (k1+k2+k3)/10\text{^}13 \quad (3)$$

Formula 4 is employed to generate the values of $k1$, $k2$ and $k3$ which are used to obtain ***k***.

$$\begin{aligned} k1 &= \sum_{i=1}^{m} \sum_{j=1}^{n} \boldsymbol{a1}(i,j) \\ k2 &= \sum_{i=1}^{m} \sum_{j=1}^{n} \boldsymbol{a2}(i,j) \\ k3 &= \sum_{i=1}^{m} \sum_{j=1}^{n} \boldsymbol{a3}(i,j) \end{aligned} \quad (4)$$

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***=[125 3 4 10 9 5 20 8 155 255], after apply the function of descending sort; the result is ***XX1***=[255 155 125 20 10 9 8 5 4 3]. In position expression; the positions [1 2 3 4 5 6 7 8 9 10] shifted to the positions [3 10 9 5 6 8 4 7 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 65 125 120 42 50 255 220 90 56].

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 permutation (confusion) scheme, 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.

4. Experimental Results and Analysis

In this paper, a practical programs of a proposed permutation scheme (PPS3DCS) 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. All programs have been applied on two different color's frequencies colored-image (*flower.bmp* and *pepper.bmp*) as a plain-images of the size *120×120* pixels, which are shown in Fig. 2(a) and Fig. 3(a) respectively.

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 permuted-image, the correlation analysis of two adjacent pixels with the directions horizontal (HC), and vertical (VC) for all color's channels *R*, *G*, *B* of the encrypted-image.

4.1.1 Histogram Analysis

The plain colored-images (*flower.bmp* and *pepper.bmp*) of the size *120×120* pixels are shown in Fig.2(a) and Fig.3(a) respectively, and the histogram for *R*, *G*, *B* of these images is shown in Fig.2(b, c, d) and Fig.3(b, c, d) respectively.

Figure 4(a) and Fig.5(a) show the shuffled-images for *flower.bmp* and *pepper.bmp* which are produced from applying the proposed permutation scheme (PPS3DCS). The histogram for *R*, *G*, *B* of these images is shown in Fig.4(b, c, d) and Fig.5(b, c, d) respectively.

Figures 4 and 5 show that the histograms of the permuted (shuffled)-images are the same of the plain-images.

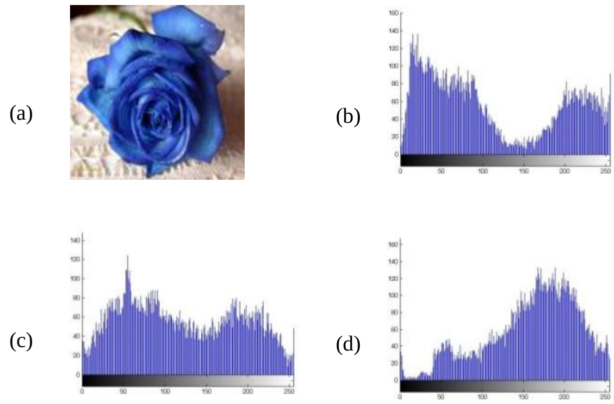

Fig. 2 The first plain-image and its histogram: (a) the image (*flower.bmp*); (b) histogram of R; (c) histogram of G; (d) histogram of B.

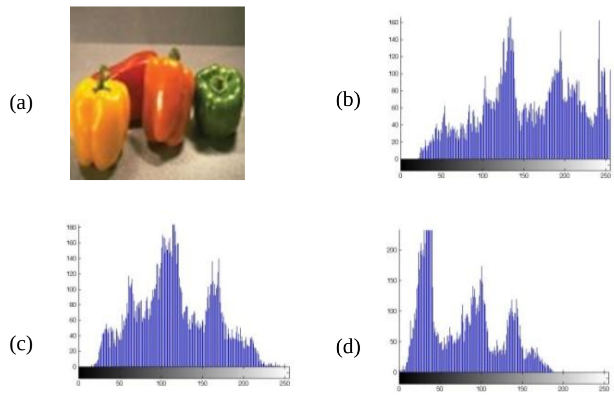

Fig. 3 The second plain-image and its histogram:(a) the image (*pepper.bmp*); (b) histogram of R; (c) histogram of G; (d) histogram of B.

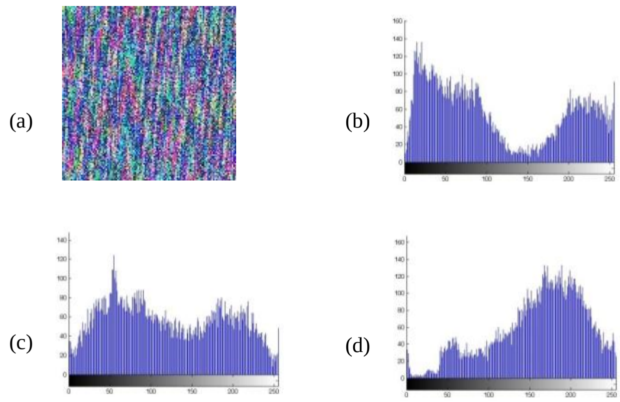

Fig. 4 The shuffled-image for *flower.bmp* and its histogram: (a) the shuffled-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

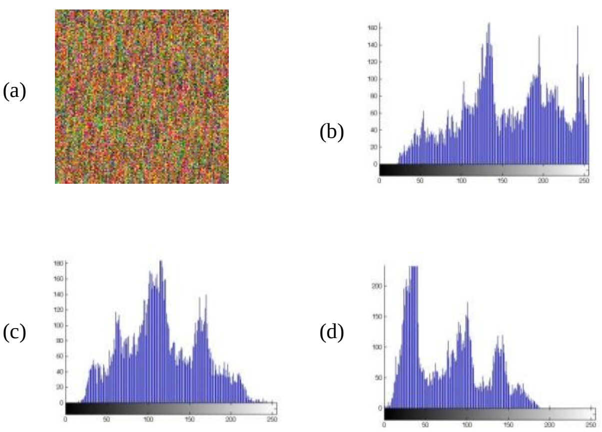

Fig. 5 The shuffled-image for *pepper.bmp* and its histogram: (a) the shuffled-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.

From all previous figures of permuted -images and its histograms, as anyone can see, The proposed permutation scheme (PPS3DCS) is a complicated and very good procedure for disguise any countenance of the image without changing its histogram. Also, anyone can observe, the proposed scheme (PPS3DCS) is qualification for encrypting both the low frequencies colored-image (*flower.bmp*) and the high frequencies colored-image (*pepper.bmp*).

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 [15]. The CC is measured by formula 5:

$$\mathbf{CC} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (5)$$

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

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.

Table 1: Results of CC analysis for encrypting *flower.bmp* and *pepper.bmp* by PPS3DCS.

Modes	**CC analysis results**		
	R	***G***	***B***
Flower.bmp	0.0127	-0.0113	0.0160
pepper.bmp	-0.0037	-0.00038	-0.0029

Table 1 and Fig. 6, illustrate that the proposed permutation scheme (PPS3DCS) achieves small values (very far from one and near to zero) of CC for the two images, so a PPS3DCS is a complicated and a good algorithm for encrypting the images. Also, the results of CC is better with the high frequencies colors image than the other image.

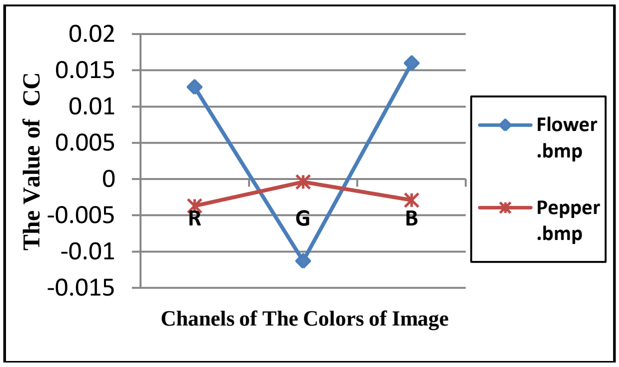

Fig. 6 Values of CC analysis for permuted images of flower.bmp and pepper.bmp

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 and vertical directions. The following formulas is employed to test the correlation between two horizontally adjacent pixels (designed as **HC**) and two vertically adjacent pixels (designed as **VC**) respectively, in plain images and permuted images, the following procedure was carried out. First, select 900 pairs of two adjacent pixels from an image. Then, calculate the correlation coefficient $\boldsymbol{r_{xy}}$ of each pair by using the following formulas [10,11]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \,, \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (6)$$

$$cov(x,y) = E\big(x - E(x)\big)\,\big(y - E(y)\big) \quad (7)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\,\sqrt{D(y)}} \quad (8)$$

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 and VC analysis for the two plain colored-images.

Table 3, Fig. 7, and Fig. 8 illustrate the results of HC and VC analysis for the two permuted-images, which are produced by applying the proposed permutation scheme (PPS3DCS) on the plain-images.

Table 2: Results of HC and VC analysis for the plain images *flower.bmp* and *pepper.bmp*.

	(***flower.bmp)***			***(pepper.bmp)***		
	R	***G***	***B***	***R***	***G***	***B***
HC	0.9664	0.9670	0.9749	0.9980	0.9968	0.9964
VC	0.9709	0.9613	0.9479	0.9822	0.9739	0.9772

Table 3: Results of HC and VC analysis for the permuted images of *flower.bmp* and *pepper.bmp* by applying the PPS3DCS.

	(***flower.bmp)***			***(pepper.bmp)***		
	R	***G***	***B***	***R***	***G***	***B***
HC	0.1069	-0.0091	-0.0032	-0.0214	0.0041	-0.0010
VC	0.2798	0.3087	0.1598	0.0725	0.0254	0.0549

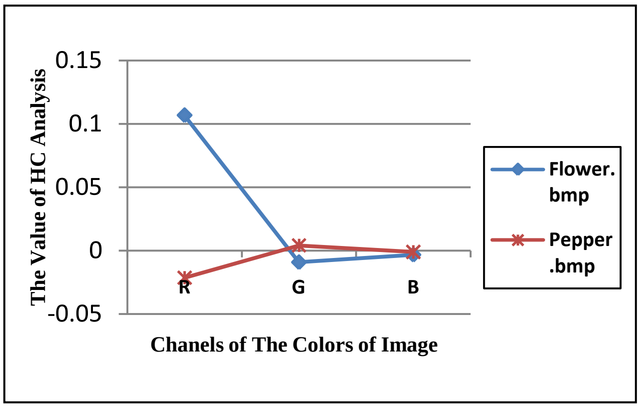

Fig. 7 Values of HC analysis for permuted images of flower.bmp and pepper.bmp

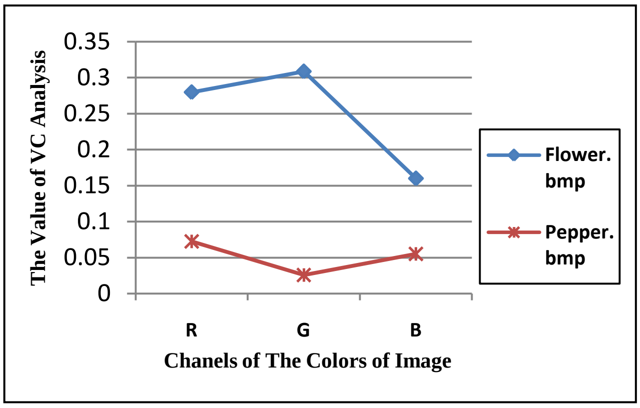

Fig. 8 Values of VC analysis for permuted images of flower.bmp and pepper.bmp

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

According to Table 3, Fig. 7, and Fig. 8, the results of HC and VC for the correlation analysis of two adjacent pixels for both the two permuted-images with the modes are approach to 0, implying that no detectable correlation exists among pixels. Therefore the proposed permutation scheme (PPS3DCS) can protect the permuted-image from statistical attacks.

Also, According to Table 3, Fig. 7, and Fig. 8, the results of HC and VC is better with the high frequencies colors image than the other image.

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 secret keys and a good values for the information entropy analysis.

In the proposed permutation scheme (PPS3DCS), the parameters *a*, *b*, *c*, and *h*, the initial values x_0, y_0, *and* z_0 are used as a secret keys.

4.2.1 The Key Sensitivity Analysis

The experimental results demonstrate that the proposed scheme (PPS3DCS) is very sensitive to the secret keys mismatch. The decrypted images by using PPS3DCS are the same of the original images, where are decrypted by using PPS3DCS with $a=35$, $b=3$, $c=28$, h=0.055555, $x_0=0+k$, $y_0=1+k$, *and* $z_0=0+k$ to produce the original image.

The experimental results for applying PPS3DCS on *pepper.bmp* demonstrate that the proposed scheme (PPS3DCS) is very sensitive to the secret keys ***a*** mismatch (10^{-14}), ***b*** mismatch (10^{-15}), ***c*** mismatch (10^{-14}), ***h*** mismatch (10^{-16}), x_0 mismatch (10^{-16}), y_0 mismatch (10^{-15}), and z_0 mismatch (10^{-14}).

(a) (b) (c) (d)

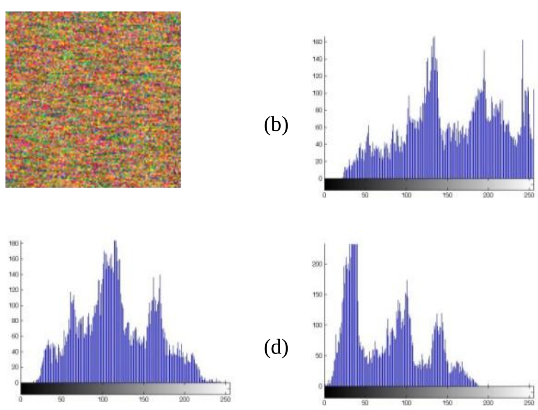

Fig. 9 The sensitivity to the secret key *b* of PPS3DCS for decrypting the confused-image of *pepper.bmp*: (a) the decrypted image, which is produced at $b = 3.000000000000001$; (b) histogram of R; (c) histogram of G; (d) histogram of B.

For example, Fig.9 illustrates the sensitivity of the proposed permutation scheme (PPS3DCS) with the secret key ***b***, where as the permuted-image which is shown in Fig.5(a) decrypted using ***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 ***b*** is changed a little (10^{-15}), the decrypted image is absolutely different from the original image (*pepper.bmp*).

Therefore anyone can conclude that the proposed permutation scheme (PPS3DCS) is very sensitive to all members of the secret keys, and it can also resist the various attacks based on sensibility.

4.2.2 Information Entropy Analysis

Information entropy [10,16,17] 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 formula 9.

$$\boldsymbol{H}(\boldsymbol{x}) = -\sum_{i=0}^{N-1} P(x_i) Lb(P(x_i)) \qquad (9)$$

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) [16].

Table 4: Results of Information Entropy analysis for the permuted images of *flower.bmp* and *pepper.bmp* by applying the PPS3DCS .

	The Information Entropy *H(x)*		
	R	***G***	***B***
Flower.bmp	7.7531	7.9175	7.6624
pepper.bmp	7.6704	7.4326	7.4170

From Table 4 and Fig. 10, all the results of information entropy *H(x)* for both the images, which are permuted (confused) by PPS3DCS are very close to the ideal value. So these results mean that the permuted-images are close to a random source and the proposed permutation scheme (PPS3DCS) is secure against entropy attack.

Also, from Table 4 and Fig. 10 , the information entropy analysis *H(x)* illustrates the results for the low frequencies colors image (*flower.bmp)* better than the results for the other image.

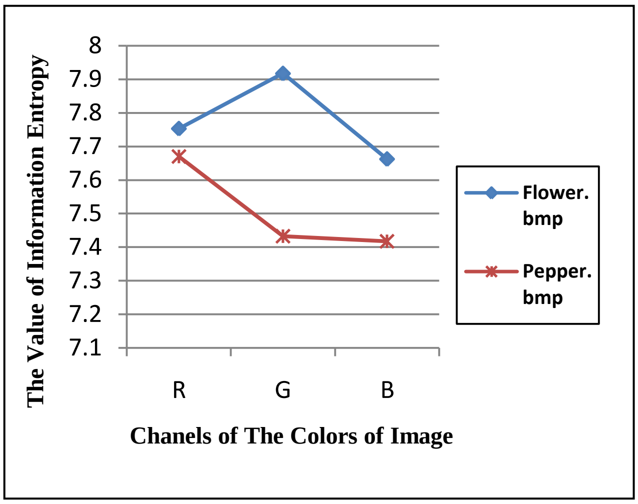

Fig. 10 Values of information entropy analysis for permuted images of flower.bmp and pepper.bmp

5. Conclusion

In this paper, a new permutation scheme (PPS3DCS) is proposed for colored-images encryption based on Chen's chaotic system. PPS3DCS is the permutation algorithm for shuffling the locations of pixels of the images. The proposed permutation scheme (PPS3DCS) is applied on two different colored-image. The experimental results and analysis show that the proposed scheme (PPS3DCS) is very good algorithm and has high security, where as the proposed permutation scheme (PPS3DCS) has merits: 1) its results with all tests of statistical analysis are excellent. 2) it is very sensitive to all members of the secret keys. 3) its results of information entropy analysis tests are excellent, because these are very closed to the ideal value. As demonstrated in the simulation and its results, the proposed permutation scheme (PPS3DCS) has high encryption quality, and it is suitable to provides an efficient and secure way for the colored-image encryption.

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, 2006, pp. 1362-67.
[10] 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, 2011.
[11] 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.
[12] 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.
[13] Cahit Cokal, Ercan Solak. Cryptanalysis of a chaos-based image encryption algorithm. Elsevier Physics Letters A, Vol. 373, 2009, pp. 1357–1360.
[14] 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.
[15] Osama M. Abu 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] M. Sabery.K, M. Yaghoobi. A New Approach for Image Encryption Using Chaotic Logistic Map. IEEE Computer Society, ICACTE, 2008, pp. 585-590.
[17] Zhiliang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu. A chaos-based symmetric 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.