A Proposed Confusion Algorithm Based on Chen's Chaotic System for Securing Colored Images

Moussa Demba and Osama M. Abu Zaid
Dept. of Computer Science, Computer Sciences and Information College, Al- Jouf University, KSA.
Email: {bah.demba, oaabuzeid}@ju.edu.sa

***Abstract*—This paper introduces a proposed confusion algorithm based on Chen's chaotic system. Chen's chaotic system which used to obtain a proposed confusion algorithm is three dimension chaotic map system. A proposed encryption Algorithm is designated as PCACHS. It is applied on two different color's frequencies colored-images. A proposed algorithm (PCACHS) is used to shuffle the positions of pixels of the colored plain-image. PCACHS is 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 confusion algorithm (PCACHS) is a good algorithm to provide an efficient and secure method for confusing or securing colored images.**

***Index Terms*—image security, confusion, encryption, chaotic system, Chen's**

I. Introduction

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

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

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

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

This paper introduces a proposed confusion algorithm for colored images based on Chen's chaotic map system. A proposed algorithm is designated in this paper as (PCACHS). The Confusion procedure based on Chen 's chaotic system is used to shuffle the positions of pixels of the colored plain-image.

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 confusion algorithm (PCACHS). 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.

II. Chen's Chaotic System

Chen's chaotic map system as important one of the 3-D chaotic map systems, which is described by (1), as 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 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 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.

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].

Manuscript received October 10, 2013; revised December 10, 2013.

doi: 10.12720/ijsps.1.2.296-301

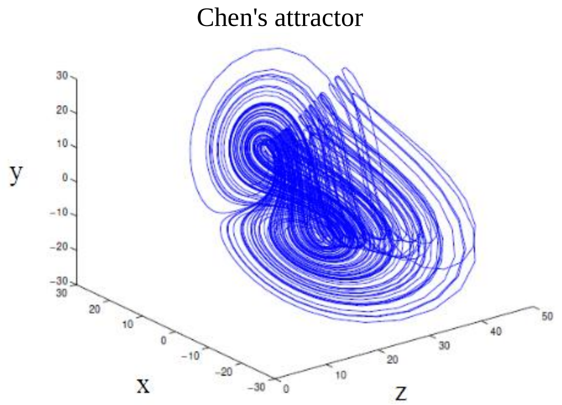


Figure 1. Chaotic behavior of Chen's system

III. PCACHS Algorithm

In this part of the paper, the proposed confusion algorithm (PCACHS) based on Chen's chaotic systems is presented. The proposed algorithm (PCACHS) consists of the confusion procedure and the re-confusion procedure. Here, the confusion procedure only is designed and discussed because the re-confusion procedure is the reversed way of the confusion procedure.

The proposed confusion algorithm (PCACHS) is designed to shuffle the positions of pixels of the image.

The proposed confusion algorithm (PCACHS) consists of five steps of operations as following:

Step 1: Obtain the *R*, *G* and *B* matrixes (the three color components Red, Green and Blue) of the color image of size $m\times n\times 3$, respectively. *R* represents $m\times n$ matrix for the red, *G* represents $m\times n$ matrix for the green, and *B* represents $m\times n$ matrix for the blue. Afterwards, each color’s matrix (including *R*, *G* and *B*) 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 (*R1*, *G1*, and *B1*) represent the plaintext which will be permuted.

Step 2: Obtain the *RR*, *GG*, and *BB* matrixes as in (2), which are generated by Chen's chaotic system at *a* =35, *b* =3, *c* =28, the initial values $x_0 = 0+v$, $y_0 = 1+v$, $z_0 = 0+v$, and $h = 0.055555$.

$$\begin{aligned} RR(i) &= mod(floor(x),256);\\ GG(i) &= mod(floor(y),256);\\ BB(i) &= mod(floor(z),256); \end{aligned} \tag{2}$$

where $\boldsymbol{i}$ is from $\boldsymbol{1}$ to $\boldsymbol{si}$. Values of $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$ are obtained from the three equations of Chen's system in formula 1. $\boldsymbol{v}$ is obtained by (3), where it is used to modify the keys in the proposed algorithm.

$$\boldsymbol{v} = (v1+v2+v3)/10\text{^}13 \tag{3}$$

Equation (4), is employed to generate the values of *v*1, *v*2 and *v*3 which are used to obtain $\boldsymbol{v}$.

$$\begin{aligned} v1 &= \textstyle\sum_{i=1}^{m}\sum_{j=1}^{n}\boldsymbol{R}(i,j)\\ v2 &= \textstyle\sum_{i=1}^{m}\sum_{j=1}^{n}\boldsymbol{G}(i,j)\\ v3 &= \textstyle\sum_{i=1}^{m}\sum_{j=1}^{n}\boldsymbol{B}(i,j) \end{aligned} \tag{4}$$

Step 3: The matrixes *RR*, *GG*, and *BB* are sorted in descending sort by using MatLab function (sort). The Matrixes *RR1*, *GG1*, and *BB1* are produced from sorting of the matrixes *RR*, *GG*, and *BB* respectively.

For example, let suppose *RR*=[125 3 4 10 9 5 20 8 155 255], after apply the function of descending sort; the result is *RR1*=[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].

Step 4: The reshaped matrixes *R1*, *G1* and *B1* are rearranged respectively according to the position of *RR* in *RR1*, the position of *GG* in *GG1*, and the position of *BB* in *BB1*. *VR*, *VG*, and *VB* are the vectors, which are obtained from rearranging process of *R1*, *G1*, and *B1* respectively.

For example, let suppose *R1*=[125 56 90 42 50 220 120 255 65 35], according to the position of *RR* in *RR1* as in example of step3; the result is *VR* = [35 65 42 50 255 220 90 56 120 125].

Step 5: obtain the *CR*, *CG*, and *CB* matrixes (the confused matrixes of the color's matrixes *R*, *G*, and *B*), which are produced respectively by reshaping the vectors *VR*, *VG*, and *VB* from one dimension to the matrixes of two dimension $m\times n$.

According to the confusion algorithm, the position of any pixel in *R*, *G*, *or B* is different with its position in *CR*, *CG*, or *CB* respectively, which will lead to be strong for the attacks.

IV. Implementation Results and Analysis

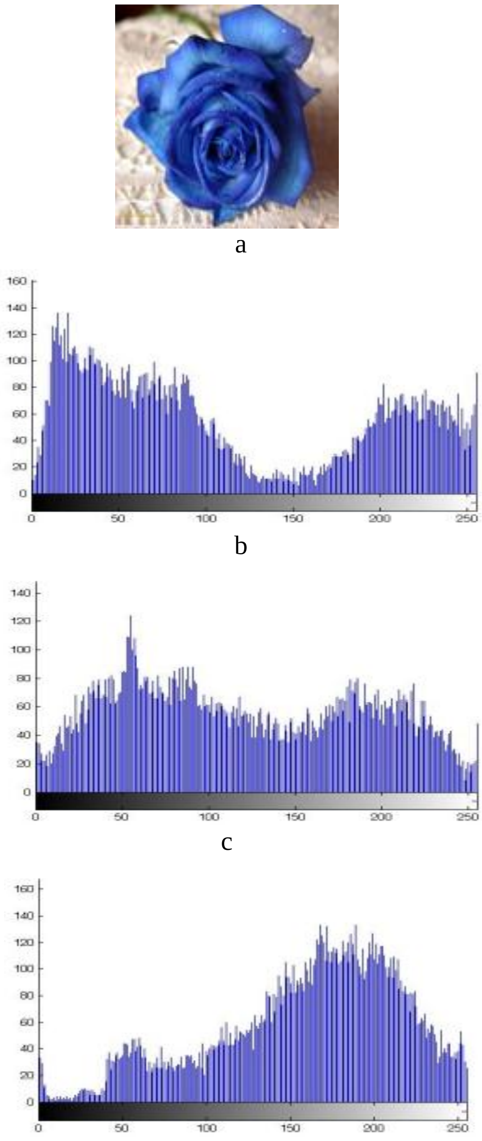
In this paper, an implementation program of a proposed confusion algorithm (PCACHS) and a practical programs of all experimental and security analysis tests are designed by MATLAB 7.0 on windows 7 system on Laptop computer with Intel CORE I_3 Processor, 3.0 GB RAM. All programs have been applied on two different 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.

A. 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 permuted-images.

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.



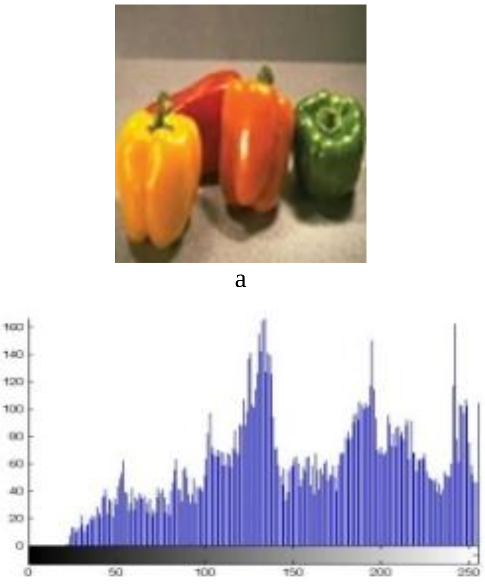
a

b

c

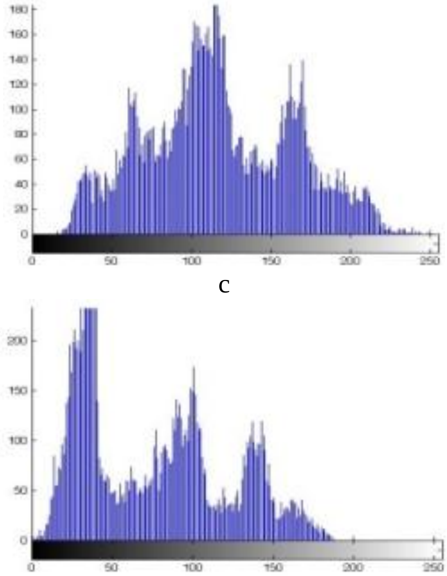
d

Figure 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.



a

b



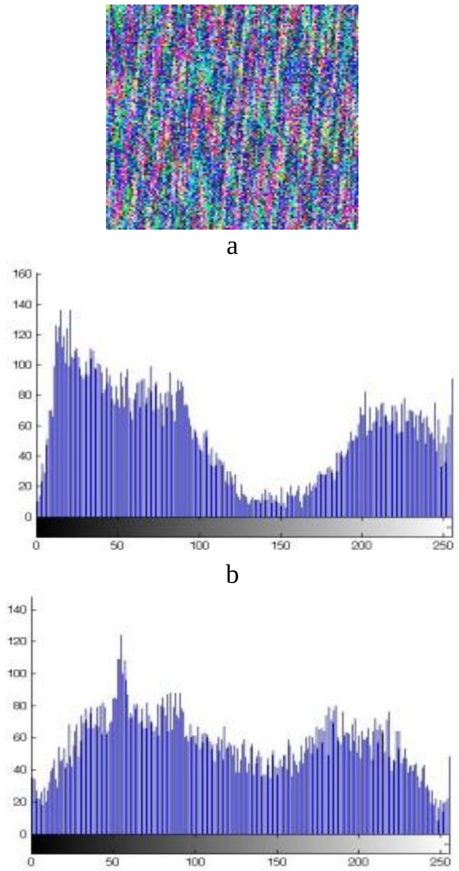
c

d

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

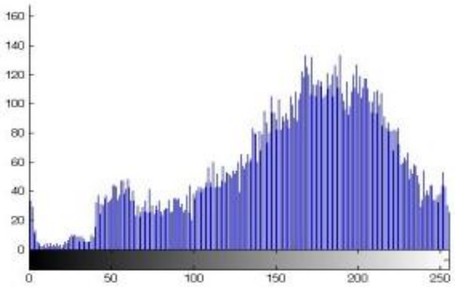
Fig. 4 and Fig. 5 show that the histograms of the confused (shuffled)-images are the same of the plain-images.



a

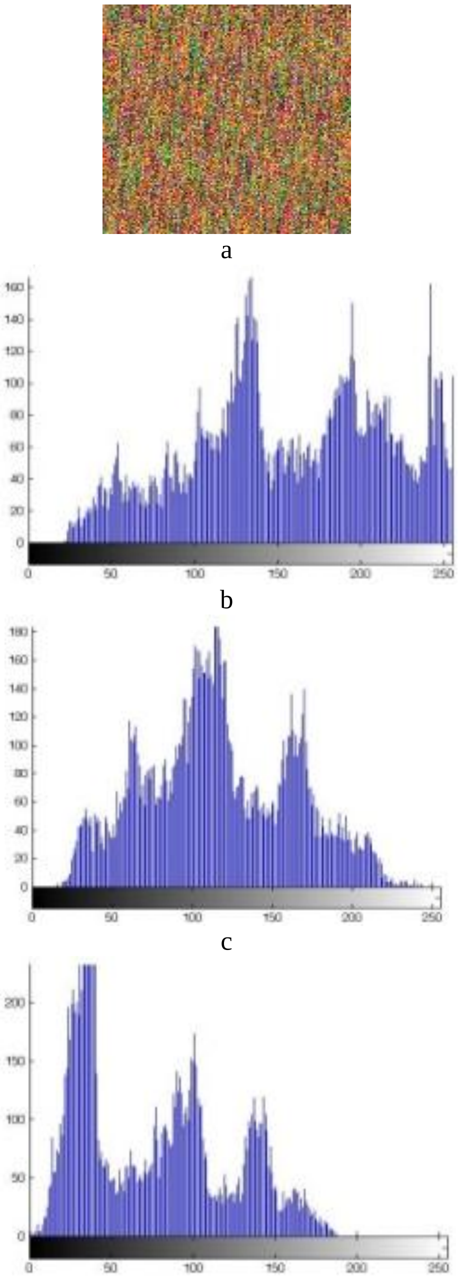
b

c



d

Figure 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.



d

Figure 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 confused (shuffled) images and its histograms, as anyone can see, The proposed confusion algorithm (PCACHS) is a complicated and very good procedure for disguise any countenance of the image without changing its histogram. Also, anyone can observe, the proposed algorithm (PCACHS) is qualification for encrypting both the low frequencies colored-image (*flower.bmp*) and the high frequencies colored-image (*pepper.bmp*).

2) Correlation coefficient analysis (CC)

The correlation coefficient for two images 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 confused are totally different. So, success of the confusion process means smaller values of the CC [15]. The CC is measured by (5):

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

where $\boldsymbol{E}(\boldsymbol{x}) = \frac{1}{N}\sum_{i=1}^{N} x_i$ (5)

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 I. RESULTS OF CC ANALYSIS FOR ENCRYPTING FLOWER.BMP AND PEPPER.BMP BY PCACHS.

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

Table I and Fig. 6, illustrate that the proposed confusion algorithm (PCACHS) achieves small values (very far from one and near to zero) of CC for the two images, so a PCACHS 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.

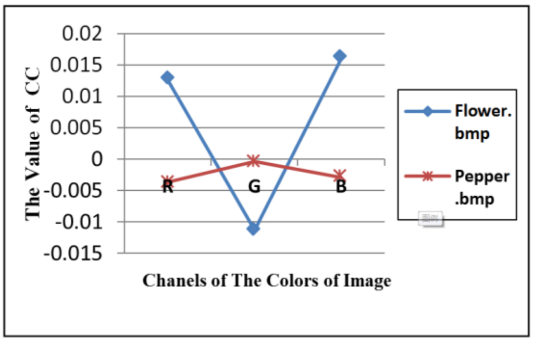


Figure 6. Values of CC analysis for confused images of flower.bmp and pepper.bmp

3) Correlation analysis of two vertically adjacent pixels (CAV)

It is well known that the adjacent pixels of an image have very high correlation coefficients in vertical directions. The following formulas is employed to test the correlation analysis between two vertically adjacent pixels (designed as CAV), in plain images and confused 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 equations [10], [11]:

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

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

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

where x and y denote two adjacent pixels, and N is the total number of duplets (x, y) obtained from the image. Table II illustrates the results of CAV analysis for the two plain colored-images. Table III illustrates the results of CAV analysis for the two confused-images, which are produced by applying the proposed confusion algorithm (PCACHS) on the plain-images.

According to Table II, anyone can observe, the results of CAV 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.

TABLE II. RESULTS OF CAV ANALYSIS FOR THE PLAIN IMAGES FLOWER. BMP AND PEPPER. BMP.

	CAV analysis results		
	R	G	B
Flower.bmp	0.9709	0.9613	0.9479
Pepper.bmp	0.9822	0.9739	0.9772

TABLE III. RESULTS OF CAV ANALYSIS FOR THE CONFUSED IMAGES OF FLOWER. BMP AND PEPPER. BMP BY APPLYING THE PCACHS

	CAV analysis results		
	R	G	B
Flower.bmp	0.2798	0.3087	0.1598
Pepper.bmp	0.0725	0.0254	0.0549

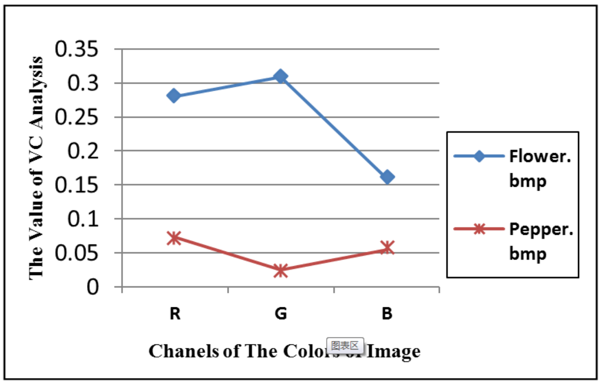


Figure 7. Values of CAV analysis for confused images of flower.bmp and pepper.bmp

According to Table III and Fig. 7, the results of CAV for the correlation analysis of two adjacent pixels for both the two confused (shuffled)-images with the modes are approach to 0, implying that no detectable correlation exists among pixels. Therefore the proposed confusion algorithm (PCACHS) can protect the confused-image from statistical attacks.

Also, from the results of CAV in Table III and Fig. 7, the results of a PCACHS is better with the high frequencies colors image (*pepper.bmp*) than the other image.

B. 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 confusion algorithm (PCACHS), the parameters a, b, c, and h, the initial values x_0, y_0, *and* z_0 are used as secret keys.

1) The key sensitivity analysis

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

The experimental results for applying PCACHS on *fruit.bmp* demonstrate that the proposed algorithm (PCACHS) 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}).

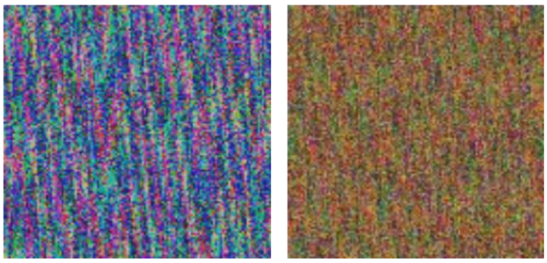


Figure 8. The sensitivity to the secret key *b* of PCACHS for decrypting the confused-images of *flower.bmp* and *pepper.bmp*: (a) the decrypted image of *flower.bmp*, which is produced at *b = 3.000000000000001*; (b) the decrypted image of *pepper.bmp*, which is produced at *b = 3.000000000000001*

For example, Fig. 8 illustrates the sensitivity of the proposed confusion algorithm (PCACHS) with the secret key b, where as the confused-images which are shown in Fig. 4(a) and 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 images are absolutely different from the plain images (*flower.bmp* and *pepper.bmp*).

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

2) Entropy analysis

Information entropy [10], [16] 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 (9).

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

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

TABLE IV. RESULTS OF INFORMATION ENTROPY ANALYSIS (IE) FOR THE CONFUSED IMAGES OF FLOWER.BMP AND PEPPER.BMP BY APPLYING THE PCACHS.

The Information Entropy IE(x)			
	R	G	B
Flower.bmp	7.7531	7.9175	7.6624
Pepper.bmp	7.6704	7.4326	7.4170

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].

From Table IV, all the results of information entropy *IE(x)* for both the images, which are confused (shuffled) by PCACHS are very close to the ideal value. So these results mean that the confused-images are close to a random source and the proposed algorithm (PCACHS) is secure against entropy attack. Also from Table IV, the information entropy analysis *IE(x)* illustrates the results for the low frequencies colors image (*flower.bmp)* better than the results for the other image.

V. CONCOLUSION

This paper was introduces an efficient and secure way for the colored-image encryption, this way is a proposed confusion algorithm (PCACHS) which is based on Chen's chaotic system. PCACHS is the confusion algorithm for shuffling the locations of pixels of the images. PCACHS was applied on two different colored-image. The experimental results and analysis show that PCACHS is very good algorithm and has high security, where as it 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 confusion algorithm (PCACHS) has high encryption quality, and it is suitable to provide good method for securing multimedia.

ACKNOWLEDGMENT

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

REFERENCES

[1] D. Xiao, X. F. Liao, and P. C. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons and Fractals*, vol. 40, no. 5, pp. 2191-2199, 2009.

[2] X. Ma, C. Fu, W. M. Lei, and S. Li, "A novel chaos-based image encryption scheme with an improved permutation process," *IJACT*, vol. 3, no. 5, pp. 223-233, 2011.

[3] D. M. Chen and Y. P. Chang, "A novel image encryption algorithm based on Logistic maps," *AISS*, vol. 3, no. 7, pp. 364-372, 2011.

[4] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759–765, 2005.

[5] K. W. Wong, "A fast chaotic cryptography scheme with dynamic look-up table," *Phys Lett. A*, vol. 298, no. 4, pp. 238-242, 2002.

[6] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys Lett A*, vol. 309, no. 1-2, pp. 75-82, 2003.

[7] Z. H. Guan, F. J. Huang, and W. J. Guan, "Chaos-based image encryption algorithm," *Phys Lett A*, vol. 346, no. 1-3, pp. 153-157, 2005.

[8] S. G. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of chaotic standard map," *Chaos, Solitons and Fractals*, vol. 26, no. 1, pp. 117-129, 2005.

[9] Y. Feng, L. J. Li, and F. Huang, "A symmetric image encryption approach based on line Maps," in *Proc. ISSCAA*, Jan 2006, pp. 1362-1367.

[10] H. B. Lu and X. Xiao, "A Novel color image encryption algorithm based on chaotic maps," *Advances in Information Sciences and Service Sciences*, vol. 3, no. 11, 2011.

[11] G. R. Chen, Y. B. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, pp. 749–761, 2004.

[12] X. D. Wang, L. X. Tian, and L. Q. Yu, "Linear feedback controlling and synchronization of the Chen's chaotic system," *International Journal of Nonlinear Science*, vol. 2, no. 1, pp. 43-49, 2006.

[13] C. Cokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Elsevier Physics Letters A*, vol. 373, pp. 1357–1360, 2009.

[14] T. S. Zhou, Y. Tang, and G. R. Chen, "Chen's attractor exists," *International Journal of Bifurcation and Chaos*, vol. 14, no. 9, pp. 3167-3177, 2004.

[15] O. M. A. Zaid, N. A. El-fishawy, E. M. Nigm, and O. S. Faragallah, "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.

[16] M. K. Sabery and M. Yaghoobi, "A New approach for image encryption using chaotic logistic map," in *Proc. International Conference on Advanced Computer Theory and Engineering*, 2008, pp. 585-590.

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

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.