# Confusion Algorithm based on 3-D Chaotic Map System for Securing the Colored Images

Osama M. Abu Zaid
College of Computer Science and Information, Al-Jouf University, KSA.

Moussa Demba
College of Computer Science and Information, Al-Jouf University, KSA.

Mohamed A. Al-Refaiy
College of Computer Science and Information, Al-Jouf University, KSA.

## ABSTRACT
In this paper, confusion algorithm based on three dimension chaotic map system will be proposed and presented. Chen's chaotic system is 3-D chaotic map system, which will be used to obtain a proposed confusion algorithm. A proposed encryption algorithm will be designated as CA3DCS. It will be applied on two different color's frequencies colored-images. A proposed algorithm (CA3DCS), which Contains Confusion procedure based on Chen 's chaotic system is used to shuffle the positions of pixels of the colored plain-image. CA3DCS 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 confusion algorithm (CA3DCS) is a good algorithm to provides an efficient and secure way for confusing or encrypting the colored images.

## General Terms
Security, Confusion, Encryption, Image.

## Keywords
Security; Confusion; Image encryption; 3-D Chaotic; and Chen's chaotic 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 for 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 confusion algorithm for colored images based on the 3-D chaotic map system (Chen's chaotic system). A proposed algorithm will be designated in this paper as (CA3DCS). The Confusion procedure based on Chen 's chaotic system is used to shuffle the positions of pixels of the colored plain-image.

The proposed confusion algorithm CA3DCS will be applied on all color's channels of the image; Red, Green, and Blue.

This paper is organized as follows. Section 2, presents an overview on Chen's chaotic map system. In section 3 we will discuss the proposed confusion algorithm (CA3DCS). Section 4 will present experimental results and analysis. In section 5 we conclude the paper.

## 2. AN OVERVIEW ON CHEN'S CHAOTIC MAP SYSTEM
In this section, an overview on Chen's chaotic map system as important one of the 3-D 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 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.

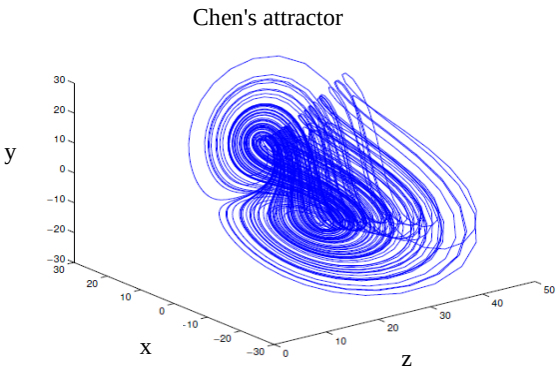


**Fig 1: Chaotic behavior of Chen's system**

Chen's chaotic map system has a good performance 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 CONFUSION ALGORITHM (CA3DCS)

In this section, the proposed confusion algorithm (CA3DCS) based on Chen's chaotic systems is presented. The proposed algorithm (CA3DCS) consists of the confusion (encryption) procedure and the re-confusion (decryption) procedure. In this part of the paper the confusion procedure only is designed and discussed because The re-confusion (decryption) procedure is the reversed technique of the confusion procedure.

The proposed confusion algorithm (CA3DCS) is designed to permute the positions of the pixels of the image, i.e. shuffling the positions of pixels of the image.

Figure 2, illustrates the data-flow diagram for a proposed confusion (permutation) algorithm. The proposed confusion algorithm (CA3DCS) consists of five steps of operations as following:

**Step1:** 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.

**Step2:** Obtain the *RR*, *GG*, and *BB* matrixes as in formula 2 which are generated by Chen's chaotic system at $a = 35$, $b = 3$, $c = 28$, the initial values $x_0 = 0+v$, $y_0 = 1+v$, $z_0 = 0+v$, and $h = 0.055555$.

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

Where ***i*** is from ***1*** to ***si***. Values of ***x***, ***y***, and ***z*** are obtained from the three equations of Chen's system in formula 1. ***v*** is obtained by formula 3, where it is used to modify the keys in the proposed algorithm.

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

Formula 4 generates values of $v1$, $v2$ and $v3$ which are used to obtain ***v***.

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

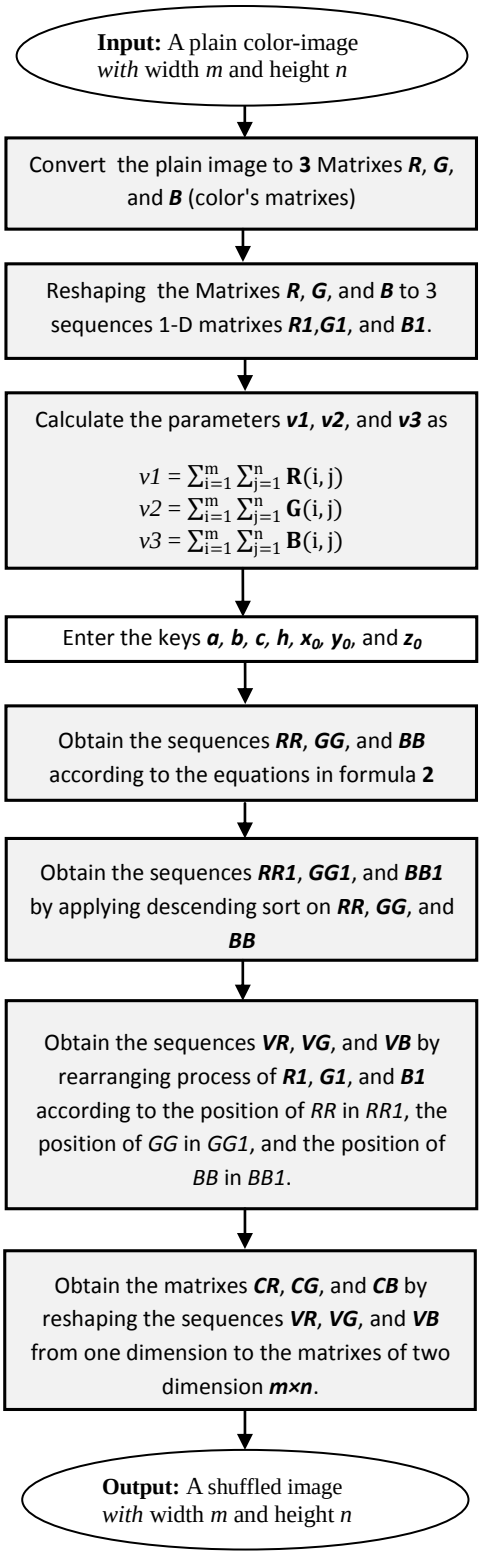


**Fig 2: The Data-Flow diagram for a confusion (permutation) algorithm (CA3DCS)**

**Step3:** 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].

**Step4:** 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].

**Step5:** obtain the ***CR***, ***CG***, and ***CB*** matrixes (the confused (permuted) 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×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.

# 4. EXPERIMENTAL RESULTS AND ANALYSIS

In this paper, a practical programs of a proposed confusion algorithm (CA3DCS) 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 *fruit.bmp*) as a plain-images of the size *120×120* pixels, which are shown in Fig. 3(a) and Fig. 4(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 permuted-images.

### *4.1.1 Histogram Analysis*

The plain colored-images (*flower.bmp* and *fruit.bmp*) of the size *120×120* pixels are shown in Fig.3(a) and Fig.4(a) respectively, and the histogram for *R*, *G*, *B* of these images is shown in Fig.3(b, c, d) and Fig.4(b, c, d) respectively.

Figure 5(a) and Fig.6(a) show the shuffled-images for *flower.bmp* and *fruit.bmp* which are produced from applying the proposed confusion algorithm (CA3DCS). The histogram for *R*, *G*, *B* of these images is shown in Fig.5(b, c, d) and Fig.6(b, c, d), respectively.

Figures 5 and 6 show that the histograms of the confused (shuffled)-images are the same histogram of the plain-images.

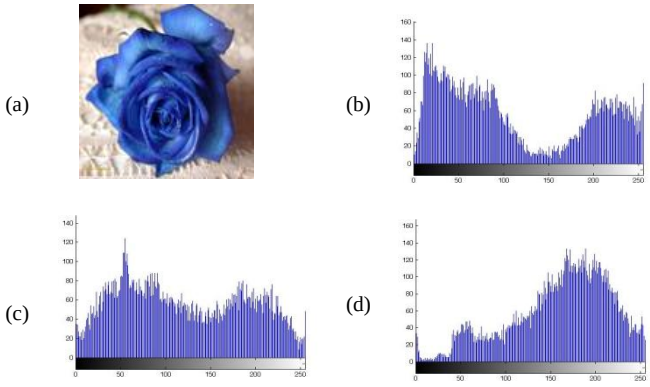


**Fig 3: The first plain-image and its histogram: (a) the image (*flower.bmp*); (b) histogram of R; (c) histogram of G; (d) histogram of B.**

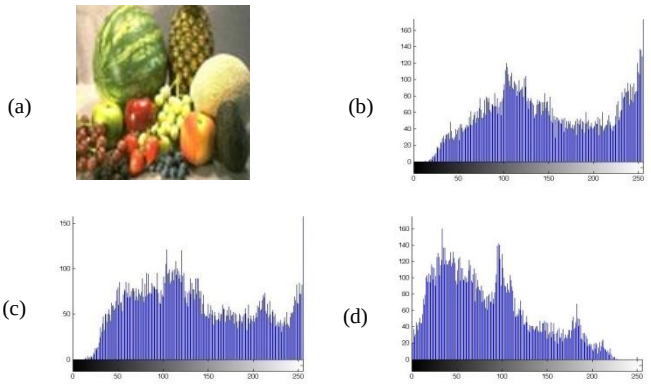


**Fig 4: The second plain-image and its histogram:(a) the image (*fruit.bmp*); (b) histogram of R; (c) histogram of G; (d) histogram of B.**

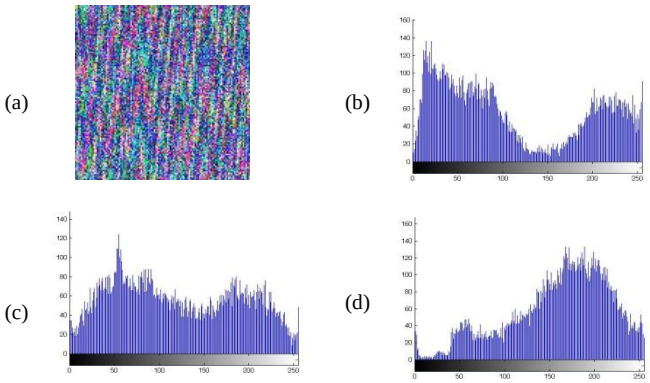


**Fig 5: The shuffled-image for *flower.bmp* and its histogram: (a) the shuffled-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.**

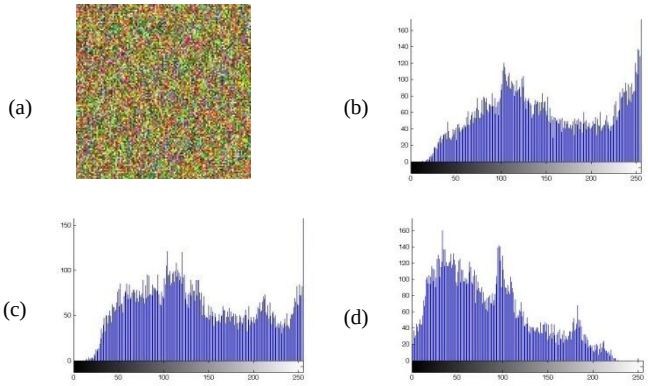

**Fig 6: The shuffled-image for *fruit.bmp* and its histogram: (a) the shuffled-image; (b) histogram of R; (c) histogram of G; (d) histogram of B.**

From all previous figures of confused (permuted) images and its histograms, as anyone can see, The proposed confusion algorithm (CA3DCS) 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 (CA3DCS) is qualification for encrypting both the low frequencies colored-image (*flower.bmp*) and the high frequencies colored-image (*fruit.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 *fruit.bmp* by CA3DCS.**

| | CC analysis results | | |
|---|---|---|---|
| | *R* | *G* | *B* |
| *Flower.bmp* | 0.0127 | -0.0113 | 0.0160 |
| *Fruit.bmp* | 0.0013 | -0.0101 | 0.0058 |

Table 1, illustrates that the proposed confusion algorithm (CA3DCS) achieves small values (very far from one and near to zero) of CC for the two images, so a CA3DCS is a complicated and a good algorithm for encrypting the images.

The results of CC is better with the high frequencies colors image than the other image.

### *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]:

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

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

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

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 illustrates the results of HC and VC analysis for the two permuted-images, which are produced by applying the proposed confusion algorithm (CA3DCS) on the plain-images.

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

| | ( *flower.bmp*) | | | (*fruit.bmp*) | | |
|---|---|---|---|---|---|---|
| | *R* | *G* | *B* | *R* | *G* | *B* |
| HC | 0.9664 | 0.9670 | 0.9749 | 0.9367 | 0.9433 | 0.9287 |
| VC | 0.9709 | 0.9613 | 0.9479 | 0.9827 | 0.9812 | 0.9719 |

**Table 3. Results of HC and VC analysis for the permuted images of *flower.bmp* and *fruit.bmp* by applying the CA3DCS.**

| | ( *flower.bmp*) | | | (*fruit.bmp*) | | |
|---|---|---|---|---|---|---|
| | *R* | *G* | *B* | *R* | *G* | *B* |
| HC | 0.1069 | -0.0091 | -0.0032 | -0.0203 | 0.0034 | -0.0007 |
| VC | 0.2798 | 0.3087 | 0.1598 | 0.0920 | 0.0376 | 0.0785 |

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, the results of HC and VC for the correlation analysis of two adjacent pixels for both the two confused (permuted)-images with the modes are approach to 0, implying that no detectable correlation exists among pixels. Therefore the proposed confusion algorithm (CA3DCS) can protect the confused-image from statistical attacks.

Also, from the results of HC and VC in Table 3, the results of a CA3DCS 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 confusion algorithm (CA3DCS), 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 algorithm (CA3DCS) is very sensitive to the secret keys mismatch. The decrypted images by using CA3DCS are the same of the original images, where are decrypted by using CA3DCS 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 CA3DCS on *fruit.bmp* demonstrate that the proposed algorithm (CA3DCS) is very sensitive to the secret keys ***a*** mismatch ($10^{-14}$), ***b*** mismatch ($10^{-15}$), ***c*** mismatch ($10^{-14}$), ***h*** mismatch ($10^{-16}$), $\boldsymbol{x_0}$ mismatch ($10^{-16}$), $\boldsymbol{y_0}$ mismatch ($10^{-15}$), and $\boldsymbol{z_0}$ mismatch ($10^{-14}$).

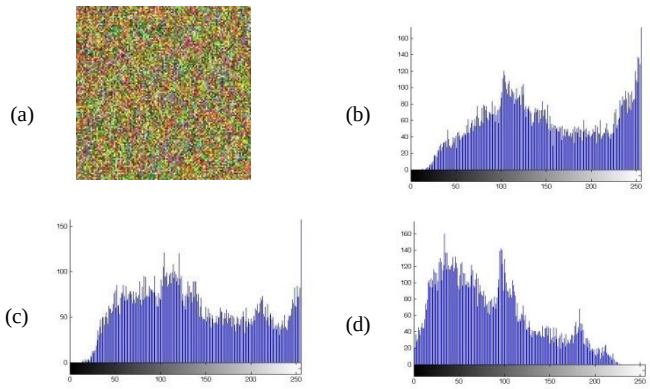


**Fig.7 The sensitivity to the secret key *b* of CA3DCS for decrypting the confused-image of *fruit.bmp*: (a) the decrypted image, which is produced at *b = 3.000000000000001*; (b) histogram of R; (c) histogram of G; (d) histogram of B.**

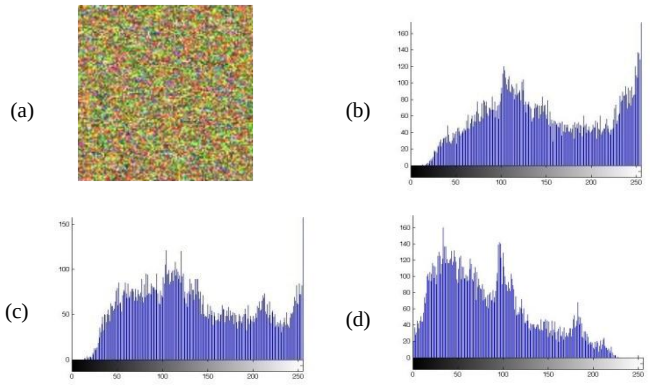


**Fig.8 The sensitivity to the secret key *b* of CA3DCS for decrypting the confused-image of *fruit.bmp*: (a) the decrypted image, which is produced at $x_0 = 0.0000000000000001+v$; (b) histogram of R; (c) histogram of G; (d) histogram of B.**

For example, Fig.7 illustrates the sensitivity of the proposed confusion algorithm (CA3DCS) with the secret key ***b***, where as the permuted-image which is shown in Fig. 6(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 (*fruit.bmp*).

Also, Fig.8 illustrates the sensitivity of the proposed confusion algorithm (CA3DCS) with the secret key $\boldsymbol{x_0}$, where as the permuted-image which is shown in Fig. 6(a) decrypted using $\boldsymbol{x_0} = 0.0000000000000001+v$, and the remains secret keys as the same as in the normal case. As can be seen that, even the secret key $\boldsymbol{x_0}$ is changed a little ($10^{-16}$), the decrypted image is absolutely different from the original image (*fruit.bmp*).

Therefore anyone can conclude that the proposed confusion algorithm (CA3DCS) 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.

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

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.

**Table 4. Results of Information Entropy analysis for the confused images of *flower.bmp* and *fruit.bmp* by applying the CA3DCS.**

| **The Information Entropy *H(x)*** | | | |
|---|---|---|---|
| | *R* | *G* | *B* |
| *Flower.bmp* | 7.7531 | 7.9175 | 7.6624 |
| *Fruit.bmp* | 7.6927 | 7.7697 | 7.5346 |

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 4, all the results of information entropy *H(x)* for both the images, which are confused (permuted) by CA3DCS 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 (CA3DCS) is secure against entropy attack.

Also from Table 4, 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.

## 5. CONCLUSION

In this paper, confusion algorithm (CA3DCS) is proposed for colored-images encryption based on Chen's chaotic system. CA3DCS is the confusion algorithm for shuffling the locations of pixels of the images. The proposed confusion algorithm (CA3DCS) is applied on two different colored-image. The experimental results and analysis show that the proposed algorithm (CA3DCS) is very good algorithm and has high

security, where as the proposed confusion algorithm (CA3DCS) 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 (CA3DCS) has high encryption quality, and it is suitable to provides an efficient and secure way for the colored-image encryption.

## 6. ACKNOWLEDGMENTS

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.

## 7. REFERENCES

[1] Di X, Xiaofeng L, Pengcheng W. 2009. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons and Fractals, Vol.40, No.5, pp. 2191-2199.

[2] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li. 2011. A novel chaos-based image encryption scheme with an improved permutation process. IJACT,Vol.3, No.5, pp.223-233.

[3] Dongming Chen, Yunpeng Chang. 2011. A novel image encryption algorithm based on Logistic maps. AISS, Vol. 3, No.7, pp.364-372.

[4] Zhang LH, Liao XF, Wang XB. 2005 An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals, Vol. 24, pp. 759–765.

[5] Wong KW. 2002. A fast chaotic cryptography scheme with dynamic look-up table. Phys Lett A , Vol. 298, pp. 238-242.

[6] Pareek NK, Patidar V, Sud KK. 2003.Discrete chaotic cryptography using external key. Phys Lett A, Vol. 309, pp.75-82.

[7] Guan ZH, Huang FJ, Guan WJ. 2005. Chaos-based image encryption algorithm. Phys Lett A, Vol. 346, pp.153-157.

[8] Lian SG, Sun J, Wang Z. 2005. A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals, Vol. 26, No. 1, pp.117-129.

[9] Feng Y, Li LJ, Huang F. Jan 2006. A symmetric image encryption approach based on line Maps. In: Proc ISSCAA2006, p. 1362-67.

[10] Huibin Lu, Xia Xiao. 2011.A Novel Color Image Encryption Algorithm Based on Chaotic Maps. Advances in information Sciences and Service Sciences (AISS), Vol. 3, No. 11.

[11] Guanrong Chen, Yaobin Mao, Charles K. Chui. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, Vol. 21, pp. 749–761.

[12] Xuedi Wang, Lixin Tian, Liqin Yu. 2006. Linear Feedback Controlling and Synchronization of the Chen's Chaotic System. International Journal of Nonlinear Science, Vol.2, No.1, pp. 43-49.

[13] Cahit Cokal, Ercan Solak. 2009. Cryptanalysis of a chaos-based image encryption algorithm. Elsevier Physics Letters A, Vol. 373, pp. 1357–1360.

[14] Tianshou Zhou, Yun Tang, And Guanrong Chen. 2004. Chen's Attractor Exists. International Journal of Bifurcation and Chaos, Vol. 14, No. 9, pp. 3167-3177.

[15] Osama M. Abu Zaid, Nawal A El-fishawy, E M Nigm and Osama S Faragallah. 2013. A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security. International Journal of Computer Applications, USA, Vol. 61, No. 5, pp. 29-39.

[16] M. Sabery.K, M. Yaghoobi. 2008. A New Approach for Image Encryption Using Chaotic Logistic Map. IEEE Computer Society, ICACTE, pp. 585-590.

[17] Zhiliang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu. 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences,Vol.181, No.6, pp.1171-1186.