New Chaotic Permutation Methods for Image Encryption

Abir Awad[1] , Abdelhakim Saadane[2]

***Abstract*— Since two decades, and in order to reach higher performance, more and more studies look to combine the conventional encryption methods and the complex behaviour of chaotic signals. To quantify the expected improvement induced by such a mix, this paper aims to compare the performance of two well known chaotic maps, namely, Logistic and piecewise linear chaotic map with their performance when they are perturbed by a new technique. These four chaotic maps are then used to control three bit permutation methods: Grp, Cross and Socek, known to have good inherent cryptographic properties. When applied to images, the common measures like NPCR, UACI, intra and inter-components correlation coefficients, histogram and distribution of two adjacent pixels lead to two main results. First, Socek permutation method remains better than Grp and Cross whatever the used chaotic map. Second, the proposed chaotic permutation methods controlled by the perturbed maps present higher performance and is more secure and suitable for chaotic image encryption schemes.**

***Index Terms*—Image encryption, Chaotic map, Perturbation technique, Random permutation method.**

I. INTRODUCTION

The security of transmitted digital information through a channel, against passive or active attacks, becomes more and more important. Since 1990s, chaos has been widely studied in secure communications. The idea of taking advantage of digital chaotic systems to construct cryptosystems has been extensively investigated and attracts more and more attention [1-3]. Researchers are especially interested in enhancing the chaotic generators and the diffusion stage of the cryptosystems. In order to be used in every application, chaotic sequences must seem absolutely random and have good cryptographic properties. Many studies on chaotic maps are conducted [4], [5] and [6]. The logistic map, which is widely used in the encryption domain, is discussed in [7] and [8]. In [9] and [10], we studied and improved the Piece Wise Linear Chaotic Map (PWLCM). The improved chaotic maps generate chaotic signals with desired statistical properties and in compliance with NIST statistical tests.

Manuscript received November 12, 2010.

[1]Abir Awad was with the Operational Cryptology and Virology Laboratory (C +V)^O, ESIEA-OUEST, Drs Calmette and Guérin street, 53003 Laval, Cedex, France. And currently, she is with LIFO, University of Orléans, Léonard de Vinci street, 45000 Orléans, France (phone: + 33-2-38417288; e-mail: abir.awad@gmail.com).

[2]Abdelhakim Saadane is with XLIM – SIC Laboratory, University of Nantes, Christian Pauc street BP 50609 Nantes Cedex 3, France (phone: + 33-2-40683046; e-mail: abdelhakim.saadane@univ-nantes.fr).

To obtain better properties and to avoid the dynamical degradation caused by the digital chaotic system working in a finite state, a perturbation technique is used. In this paper, chaotic output signals, which present random statistical properties, are used for the diffusion operation in a cryptosystem.

Diffusion spreads the redundant information in the plain text over the cipher text. As a primary method to achieve diffusion, permutation is widely used in cryptographic algorithms. Bit level permutations particularly, are the core of any encryption algorithm.

Based on such bit level permutation, several methods have been proposed in the literature. Few of them however, have performed comparative study between chaos based permutations [11]. This paper proposes to extend this comparative study by comparing the performance of three well attractive bit level permutations when they are controlled by four different chaotic signals.

The first two bit level permutations called Grp and Cross are detailed in [12-14]. These permutations are in fact, permutation instructions developed to efficiently implement arbitrary n-bit permutation in any programmable processors, whether they are general purpose microprocessors or application-specific cryptography processors. The third one, called hereafter Socek permutation, has been developed by Socek and al. and is well described in [8]. Proposed to enhance a previous algorithm, this permutation uses a 1-D piecewise linear chaotic map (PWLCM) instead of the original 1-D chaotic Logistic map thereby improving the statistical properties of the generated secret bits.

In what follows, we propose to control theses methods with perturbed chaotic generators. In order to be used in all applications, chaotic sequences must seem absolutely random. To this end, the perturbing orbit technique presented in [9] is used. Designed to generate chaotic signals with desired statistical properties and verifying NIST statistical tests, this technique has already been used in [10] to control a cryptographic algorithm.

Digital images are used to test the proposed approaches. Indeed, it is well known that images are different from texts in many aspects, such as high redundancy and correlation. The main obstacle in designing effective image encryption algorithms is that it is rather difficult to diffuse such image data. In most of the natural images, the value of any given pixel can be reasonably predicted from the values of its neighbours. By using measures like the Number of Pixels Change Rate (NPCR), the Unified Average Changing Intensity (UACI), the correlation coefficients, the distribution of two adjacent pixels and the entropy analysis, we prove that the proposed chaotic permutation methods can be used in

order to dissipate the high correlation among pixels and increase the entropy value.

This paper is organized as follows. Section 2 presents the chaotic maps and describes the perturbation technique. Section 3 details the chaotic permutation techniques. The simulation results are presented in section 4 while section 5 is devoted to the conclusion.

II. CHAOTIC MAPS AND PERTURBATION TECHNIQUE

The first step in designing a block encryption algorithm is to choose a chaotic map. Choosing maps for encryption algorithms is not an easy task and one should consider only maps with good cryptographic properties, like a large cycle length and the uniformity distribution. In this section, we present two well known chaotic maps: Logistic map and PWLCM map. Then, we discuss the perturbation technique that enhancing the dynamical degradation of the chaotic map in a digital space.

A. Logistic map

The Logistic map defines one of the simplest forms of a chaotic process. Because of its mathematical simplicity, this model continues to be useful test bed for new ideas in chaos theory as well as application of chaos in cryptography [15]. It is defined by the following equation:

$$x(n) = \lambda x(n-1)(1 - x(n-1)) \tag{1}$$

Where $x(n)$ is a state variable, which lies in the interval [0,1] and λ is the control parameter and belongs to interval (0; 4]. λ should be greater than the accumulation point 3.569945672 in order to maintain the highly chaotic state.

B. PWLCM map

Due to the poor dynamical behavior of the logistic map [8], [16] some implementations use the following Zhou's map with better balance property [17]. A piecewise linear chaotic map (PWLCM) is a map composed of multiple linear segments.

$$x(n) = F[x(n-1)] = \begin{cases} x(n-1)x\dfrac{1}{p} & if\ 0 \le x(n-1) < p \\ [x(n-1)-p]x\dfrac{1}{0.5-p} & if\ p \le x(n-1) < 0.5 \\ F[1-x(n-1)] & if\ 0.5 \le x(n-1) < 1 \end{cases} \tag{2}$$

where the positive control parameter and the initial condition are respectively $p \in (0; 0.5]$ and $x(i) \in [0; 1]$.

Compared to the Logistic map situation, we have a wider range of control parameter choices when using the PWLCM because the Logistic map is ergodic in [0, 1] only when r approaches 4. The PWLCM has a better balance property and uniform invariant density function.

C. Perturbation technique

Since digital chaotic iterations are constrained in a discrete space with 2^N elements, it is obvious that every chaotic orbit will eventually be periodic and will finally go to a cycle with limited length not greater than 2^N. Generally, each digital chaotic orbit includes two connected parts:

$x_1, x_2, \ldots x_l$, and $x_l, x_{l+1}, \ldots x_{l+n}$, which are respectively called "transient branch" and "cycle". Accordingly, l and $n+1$ are respectively called "transient length" and "cycle period", and $l+n$ is called "orbit length".

To improve the dynamical degradation, a perturbation based algorithm is used [18]. The cycle length is expanded and so good statistical properties are reached.

Here, for computing precision N, each x can be described as:

$$x(n) = 0.x_1(n)x_2(n)\ldots x_i(n)\ldots x_N(n) \qquad x_i(n) \in \{0,1\},\ i = 1,2,\ldots,N \tag{3}$$

A suitable candidate for the perturbing signal generator is the maximal length LFSR because its generated sequences have the following advantages: 1) definite cycle length (2^k-1) (k is the degree); 2) uniform distribution; 3) delta like autocorrelation function; 4) easy implementation; 5) controllable maximum signal magnitude given by $2^{-N}(2^k-1)$ when used in N-precision system.

The perturbing bit sequence can be generated every n clock as follows:

$$Q_{k-1}^{+}(n) = Q_k(n) = g_0 Q_0(n) \oplus g_1 Q_1(n) \oplus \ldots \oplus g_{k-1} Q_{k-1}(n) \quad with\ n = 0,1,2,\ldots \tag{4}$$

$\oplus$ represents 'exclusive or', $g = [g_0\ g_1 \ldots g_{k-1}]$ is the tap sequence of the primitive polynomial generator, and $Q_0, Q_1, \ldots, Q_{k-1}$ are the initial register values of which at least one is non zero.

The perturbation begins at $n = 0$, and the next ones occur periodically every Δ iterations (Δ is a positive integer), with $n = l \times \Delta$, $l = 1,2,\ldots$, The perturbed sequence is given by the equation (5):

$$x_i(n) = \begin{cases} F[x_i(n-1)] & 1 \le i \le N-k \\ F[x_i(n-1)] \oplus Q_{N-i}(n) & N-k+1 \le i \le N \end{cases} \tag{5}$$

Where $F[x_i(n)]$ represents the ith bit of $F[x(n)]$.

The perturbation is applied on the last k bits of $F[x(n)]$.

When $n \neq l \times \Delta$, no perturbation occurs, so $x(n) = F[x(n-1)]$.

The system cycle length is given by the following relation

$$T = \sigma \times \Delta \times \left(2^k - 1\right), \tag{6}$$

where σ is a positive integer. The lower bound of the system cycle length is

$$T_{\min} = \Delta \times \left(2^k - 1\right). \tag{7}$$

III. CHAOTIC PERMUTATION TECHNIQUES

In this section, we present the studied permutation methods: Grp, Cross and Socek. This paper compares these methods when they are controlled by four chaotic maps. The chaotic value $x(i)$ is in the interval [0, 1[. Then, a discretization method is applied to transform it to unsigned integer on 32 bits using the following formulas:

$$y(i) = round(x(i).2^{32}), \quad (8)$$

where *x(i)* is a chaotic real value and *y(i)* is the discretized one. *round* function (instead of *floor* and *ceil*) insures the minimal degradation of the chaotic map. The advantage of this function is discussed in [19].

The proposed perturbation technique is then applied on the digital chaotic value *y(i)* that is subsequently used to control the following three permutation methods.

A. Grp permutation

The Grp permutation method [12-14] is defined as follows:

R3=Grp(R1, R2)

R1 is the source array or the original block, *R2* is the configuration array and *R3* is the destination array for the permuted bits.

As we said, we propose to control this method by chaotic values. Then, in each iteration, the control array *R2* is filled by a chaotic binary suite (8 bits). But, the digital chaotic value *y(i)* is on 32 bits. Consequently, we need to generate the chaotic value once every four iterations. Then, the 32 chaotic bits are divided into four parts. Thus, each chaotic byte can be used to control the permutation of a byte from the image (bits of *R1*).

The basic idea of the Grp instruction is to divide the bits in the source *R1* into two groups according to the bits in *R2*. For each bit in *R1*, we check the corresponding bit in *R2*. If the bit in *R2* is 0, we move this bit from *R1* into the first group. Otherwise, we put this bit into the second group (see Fig.1).

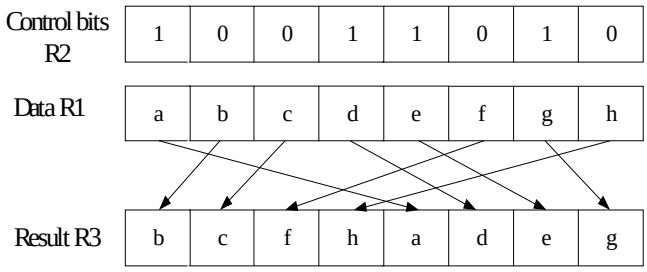


Fig. 1. The Grp permutation method performed on 8 bits

B. Cross permutation

The Cross method is based on the Benes network, which is formed by connecting two butterfly networks of the same size back-to-back [13]. Cross instruction is defined as follows:

R3=Cross(m1, m2, R1, R2)

R1 is the source array which contains the bits to be permuted, *R2* is the configuration array and *R3* is the destination array for the permuted bits. Cross instruction performs two basic operations on the source according to the contents of the configuration array *R2* and the values of *m1* and *m2*. Fig. 2 shows an example of Cross instruction working on 8-bit systems. Similarly to Grp technique explained above, we propose to fill the control array *R2* by chaotic bits to enhance the security of the permuted images.

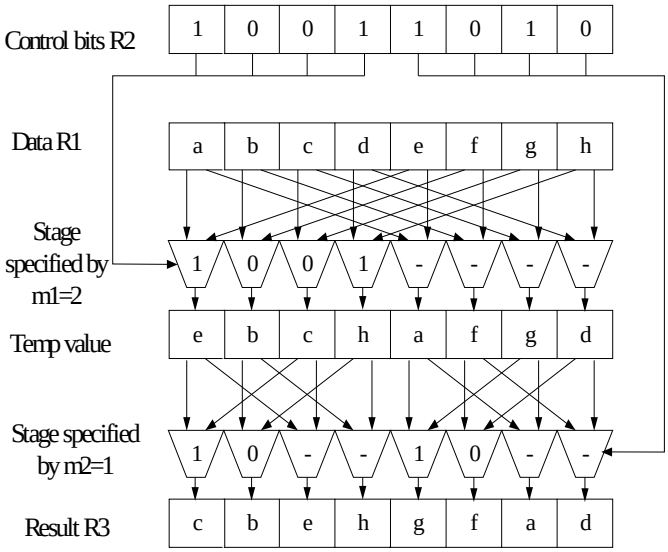


Fig. 2. The Cross permutation method performed on 8-bit

C. Socek permutation

The permutation method proposed by Socek [8] is a computational approach of degree 8. It permutes the indices of bits of each pixel using the chaotic value. These indices are placed in an array *p= [1, 2, 3, 4, 5, 6, 7, 8]* and we have then to permute the elements of this array using the chaotic value. Then, the bits are rearranged according to the permuted indices of the new array *q*. Fig. 3 presents an example of Socek method applied on 8 bits. In this case, the obtained new array of indices is *q=[4, 6, 7, 1, 3, 8, 2, 5]*.

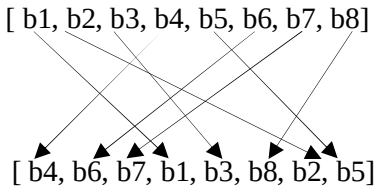


Fig. 3. Socek method applied on 8 bits

In this method, a transformation to binary format is not needed. We just use the perturbed digital chaotic value limited by 8! (permutation of 8 bits) to perform the permutation of each original block (byte). In the original method, Socek used PWLCM as control map instead of logistic map. In this paper, we compare the performance of his proposition and the permutation method controlled by the perturbed Logistic and PWLCM maps.

IV. SIMULATION RESULTS

Experimental results are given in this section to demonstrate the efficiency of the proposed chaotic permutation methods. They extend a previous investigation [11] performed on Mandrill image (Fig. 4(a)) by using three permutation methods: Grp, Cross and Socek. In this study, the same permutation methods are controlled by four chaotic maps: the Logistic map, the perturbed logistic map, the PWLCM map and the perturbed PWLCM map. Barbara (Fig. 4(b)) color image of size 512*512*3 is used as the plain image. Grp, Cross and Socek permutation methods, Logistic and PWLCM maps and their perturbed versions, are implemented in Matlab.

The standard chaotic maps, Logistic and PWLCM, are first used to determine the best permutation method. The selected method is then controlled by the perturbed maps and the performances are, in both cases, compared through several indicators.

(a) (b)

Fig. 4. (a) Mandrill image, (b) Barbara image

A. Comparison between the permutation methods

In this section, the Grp, Cross and Socek methods are controlled by the PWLCM and Logistic maps. Their efficiency is compared using the number of Pixels Change Rate (NPCR), the Unified Average Changing Intensity (UACI), the correlation coefficients, the distribution of two adjacent pixels and the entropy analysis.

Difference between the original and the permuted images

Common measures like *NPCR* (Number of Pixels Change Rate) and *UACI* (Unified Average Changing Intensity) are used to test the difference between the original image *P1* and the permuted one *C1*.

NPCR stands for the number of pixel change rate. Then, if *D* is a matrix with the same size as images *P1* and *C1*, *D (i,j)* is determined as follows:

$$D(i,j)=\begin{cases}1 & if\ P_1(i,j)\neq C_1(i,j)\\ 0 & else\end{cases} \qquad (9)$$

NPCR is defined by the following formula:

$$NPCR=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}D(i,j)}{M\times N}\times 100 \qquad (10)$$

where *M* and *N* are the width and height of P_1 and C_1.

The *UACI* measures the normalized mean difference rate between the plain image and the permuted one.

UACI is defined by the following formula:

$$UACI=\frac{1}{MxN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{\left|P_1(i,j)-C_1(i,j)\right|}{255}x100\ . \qquad (11)$$

Table I and II summarize the mean values of NPCR and UACI obtained between the original image Barbara and the permuted one using the PWLCM and the Logistic maps respectively. The three color components are considered.

Table I. Mean values of NPCR and UACI between the original image Barabra and the permuted one, using PWLCM as control map.

	PWLCM		
	Grp	Cross	Socek
NPCR	49.2780	87.7043	99.9596
UACI	13.6973	21.5096	28.8622

Table II. Mean values of NPCR and UACI between the original image Barbara and the permuted one, using Logistic as control map.

	Logistic		
	Grp	Cross	Socek
NPCR	70.9935	86.4111	96.7238
UACI	18.1053	18.2042	24.0471

First, the comparison of NPCR mean values shows that Socek method is better than Cross and Grp methods whatever the used chaotic map. The comparison of UACI mean values leads to the same conclusion. Similar results are obtained for Mandrill image.

Correlation coefficients of intra and inter - color - components

To quantify the dependence between two images, Pearson's correlation coefficient is commonly used. Given by eq. 15, this coefficient is obtained by dividing the covariance between the two images (eq. 14) by the product of their standard deviations (eq. 13 and eq. 12). E in eq.12 is the expected value operator. $P_1(i,j)$ and $C_1(i,j)$ are respectively the pixels gray values of the first and the second images.

$$E(x)=\frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}P_1(i,j) \qquad (12)$$

$$D(P_1) = \frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}[P_1(i,j) - E(P_1(i,j))]^2 \quad (13)$$

$$\mathrm{cov}(P_1,C_1) = \frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}[P_1(i,j) - E(P_1(i,j))][C_1(i,j) - E(C_1(i,j))] \quad (14)$$

$$r_{P_1C_1} = \frac{\mathrm{cov}(P_1,C_1)}{\sqrt{D(P_1)}\sqrt{D(C_1)}} \quad (15)$$

Tables III, IV, V and VI give the correlation coefficients of intra and inter–color-components of original image Barbara and permuted images using respectively the PWLCM and the Logistic as control map.

Table III. Mean values of the correlation coefficients of intra-component of the original Barbara and the permuted images, using PWLCM as control map.

Correlation	Barbara image	Permuted image using PWLCM to control		
		Grp	Cross	Socek
Red (R) component Correlation	0.1502	0.0276	0.0194	0.0121
Green (G) component Correlation	0.0954	0.0154	0.0129	0.0087
Blue (B) component Correlation	0.0753	0.0156	0.0126	0.0071
Mean value	0.1070	0.0195	0.0150	0.0093

Table IV. Mean values of the correlation coefficients of intra-component of the original Barbara and the permuted images, using Logistic as control map.

Correlation	Permuted image using Logistic to control		
	Grp	Cross	Socek
Red (R) component Correlation	0.0762	0.0223	0.0171
Green (G) component Correlation	0.0235	0.0137	0.0086
Blue (B) component Correlation	0.0316	0.0127	0.0095
Mean value	0.0437	0.0162	0.0117

From Tables III and IV, it can be seen that both maps reduce significantly the intra-component correlation coefficients. The reduction is higher for PWLCM map and Socek method remains better than Grp and Cross methods in all cases.

Table V. Inter-components correlation coefficients of the original image Barbara and the permuted images, using PWLCM as control map.

Correlation	Barbara image	Permuted image using PWLCM to control		
		Grp	Cross	Socek
Correlation between R and G	0.8368	0.1481	0.1093	0.0511
Correlation between G and B	0.9379	0.1775	0.1417	0.0676
Correlation between B and R	0.7290	0.1373	0.1086	0.0505

Table VI. Inter-components correlation coefficients of the original image Barbara and the permuted images, using Logistic as control map.

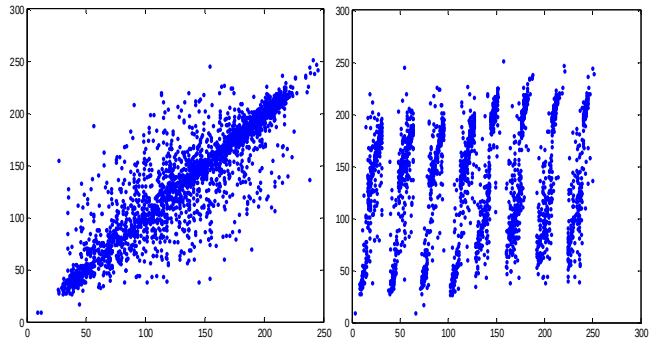
Correlation	Permuted image using Logistic to control		
	Grp	Cross	Socek
Correlation between R and G	0.3678	0.2141	0.0958
Correlation between G and B	0.6042	0.3196	0.2341
Correlation between B and R	0.3080	0.2001	0.0482

The analysis of results given in Tables V and VI shows a similar behavior for the inter-components correlation coefficients. The best results are reached when PWLCM map is used to control Socek permutation method. The mean reduction of correlation coefficient in this case is about 14.9 (9.3 for Logistic map and Socek method).

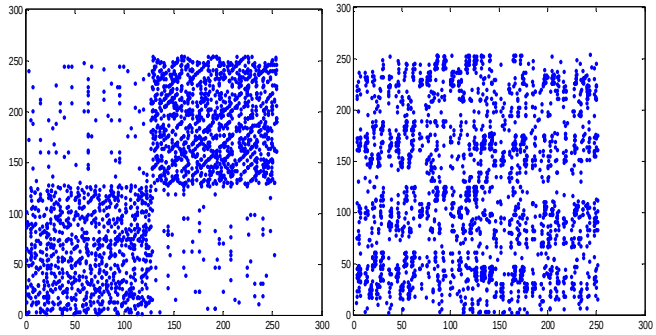
Distribution of two adjacent pixels

Statistical analysis on large amounts of images shows that on average, 8 to 16 adjacent pixels are correlated.
In this section, some simulations are carried out to test the correlation distribution between two horizontally, vertically and diagonally adjacent pixels, in the original and permuted images. Fig. 5 shows the correlation distribution of two vertically adjacent pixels in the first component of the original image and the permuted images when Grp, Cross and Socek methods are controlled by the PWLCM map. Similar results are obtained when the permutation methods are controlled by the logistic map.

Firstly, 250000 pairs of two adjacent pixels from the image are randomly selected. Then, we plot the pixel value on location *(x, y+1)* over the pixel value on location *(x, y)*.



(a) (b)



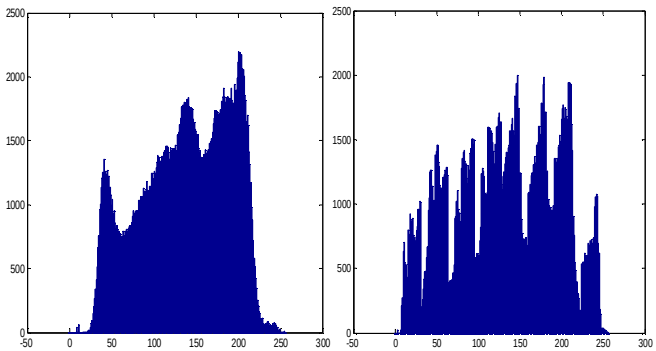
(c) (d)

Fig. 5. Distribution of two vertically adjacent pixels in (a) the original image Barbara and in the permuted images: using (b) Grp method , (c) Cross method and (d) Socek permutation method.

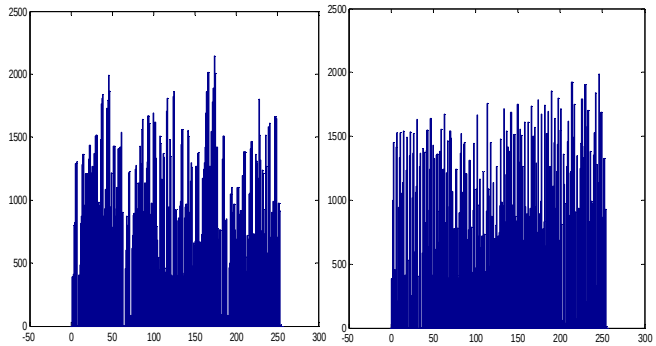
The strong correlation between the adjacent pixels in the original image Barbara (Fig. 5(a)) is reduced in the permuted images. One can see that the best distribution is obtained using the Socek permutation technique Fig. 5(d). Similar behavior is observed when the permutation methods are controlled by Logistic map.

Histogram analysis

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the permuted images as well as the original color image. Fig. 6 shows the histogram of the Red component of the original image Barbara and the permuted images by Grp, Cross and Socek methods using PWLCM map.



(a) (b)



(c) (d)

Fig. 6. Histogram of the first component of (a) Barbara image and the permuted images: using (b) Grp method, (c) Cross method and (d) Socek method.

As we can see, the histograms of the permuted images are significantly different from that of the original image. Better results are obtained with Socek method as the different gray levels of the image are almost equally distributed over pixels.

Similar results are obtained when Logistic map is used to control the same permutation methods.

Information entropy analysis

Entropy is a statistical measure of randomness that can be used to characterize the texture of an image. It is well known that the entropy $H(m)$ of a message source m can be calculated as :

$$H(m)=\sum_{i=0}^{2^N-1} p(m_i)\log_2\frac{1}{p(m_i)} \qquad (15)$$

Where $p(m_i)$ represents the probability of message m_i.

When an image is encrypted, its entropy should ideally be 8. If it is less than this value, there exists a certain degree of predictability which threatens its security.

Tables VII and VIII list the mean entropy values obtained for the original image and the permuted ones when the three color components of Barbara image are considered.

The obtained results are very close to the theoretical value. This means that information leakage in the permutation process is negligible.

Table VII. Entropy value for the original image Barbara and the permuted ones using PWLCM as a control map.

	Original Image	PWLCM		
		Grp	Cross	Socek
Entropy	7.6517	7.8118	7.8845	7.9515

Table VIII. Entropy value for the permuted images of Barbara using Logistic as a control map.

	Logistic		
	Grp	Cross	Socek
Entropy	7.7723	7.8333	7.8472

B. Comparison between the chaotic maps and the perturbed versions

This section presents an experimental comparison between the original chaotic maps (PWLCM and Logistic map) and their perturbed versions. Both perturbed chaotic maps are used to control the Socek bit-permutation method. Then, we use the same indicators used above to prove the efficiency of the perturbation technique and to compare the four chaotic maps. To do this test, we used the original colored images of Mandrill Fig. 4(a) and Barbara Fig. 4(b).

Difference between the original and the permuted images

Table IX gives NPCR and UACI between the original image Barbara and the permuted images when Socek method is controlled by the perturbed PWLCM and the perturbed Logistic map.

Table IX. Mean values of NPCR and UACI between the origin al image Barbara and the permuted images, using the perturbed PWLCM and the perturbed Logistic map.

	Socek method controlled by	
	Perturbed PWLCM	Perturbed Logistic
NPCR	98.7439	97.1354
UACI	27.1276	24.8613

The comparison between NPCR and UACI in tables I, II, and IX shows that the chaotic maps performance remains similar even if an error rate slightly higher is observed with the original PWLCM.
Same results are obtained for Mandrill image (see table X).

Table X. Mean values of NPCR and UACI between the Mandrill image and the permuted one, using Logistic map, PWLCM map and their perturbed versions.

	Socek method controlled by			
	PWLCM	Perturbed PWLCM	Logistic	Perturbed Logistic
NPCR	99.569	98.520	96.6427	97.1082
UACI	29.106	27.139	23.9389	24.7024

Correlation coefficients of intra and inter - color - components

Tables XI and XII present intra and inter components correlation coefficients for the permuted images of Barbara when Socek permutation is controlled respectively by the perturbed PWLCM and the perturbed Logistic map.

One can easily notice that the intra-component correlation coefficients of perturbed PWLCM map are lower than those of perturbed Logistic map. The comparison with results of Tables III and IV shows that the chaotic maps further reduce the correlation coefficients.

Same conclusion can be formulated for the inter-components correlation coefficients where the mean reduction of correlation coefficients is about 20 (against 14.9 for non perturbed PWLCM).

Same behavior is observed with Mandrill image (see table XIII and XIV).

Table XI. Mean values of the correlation coefficients of intra-component of original and permuted images of Barbara, using the perturbed Logistic map and the perturbed PWLCM map.

Correlation	Permuted image using Socek method controlled by	
	Perturbed PWLCM	Perturbed Logistic
Red (R) component Correlation	0.0111	0.0137
Green (G) component Correlation	0.0080	0.0081
Blue (B) component Correlation	0.0062	0.0076
Mean value	0.0084	0.0098

Table XII. Inter-components correlation coefficients of original and permuted images of Barbara, using the perturbed Logistic map and the perturbed PWLCM map.

Correlation	Permuted image using Socek method controlled by	
	Perturbed PWLCM	Perturbed Logistic
Correlation between R and G	0.0382	0.0669
Correlation between G and B	0.0648	0.1557
Correlation between B and R	0.0406	0.0469

Table XIII. Mean values of the correlation coefficients of intra-component of original and permuted images of Mandrill, using Logistic map, PWLCM map and their perturbed versions.

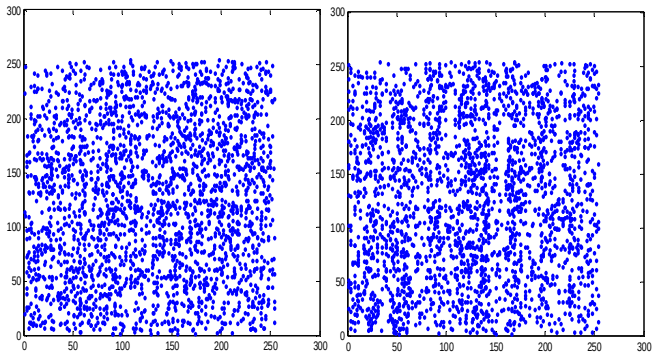
Correlation	Mandrill image	Permuted image using Socek method controlled by			
		PWLCM	Perturbed PWLCM	Logistic	Perturbed Logistic
Red (R) component Correlation	0.1911	0.0171	0.0155	0.0178	0.0162
Green (G) component Correlation	0.0883	0.0066	0.0055	0.0066	0.0058
Blue (B) component Correlation	0.0948	0.0152	0.0138	0.0159	0.0141
Mean value	0,1247	0.0130	0.0116	0.0134	0.0120

Table XIV. Inter-components correlation coefficients of original and permuted images of Mandrill, using Logistic map, PWLCM map and their perturbed versions.

Correlation	Mandrill image	Permuted image using Socek method controlled by			
		PWLCM	Perturbed PWLCM	Logistic	Perturbed Logistic
Correlation between R and G	0.3565	0.1280	0.0703	0.1410	0.0722
Correlation between G and B	0.8074	0.0684	0.0591	0.0750	0.0621
Correlation between B and R	0.1237	0.0161	0.0088	-0.0175	-0.0093

Distribution of two adjacent pixels

Fig. 7 shows the correlation distribution of two vertically adjacent pixels in the first component of the permuted images by Socek permutation method controlled by the perturbed PWLCM map and the perturbed Logistic map. Similar results are obtained when the permutation methods are applied on the Mandrill image.



(a) (b)

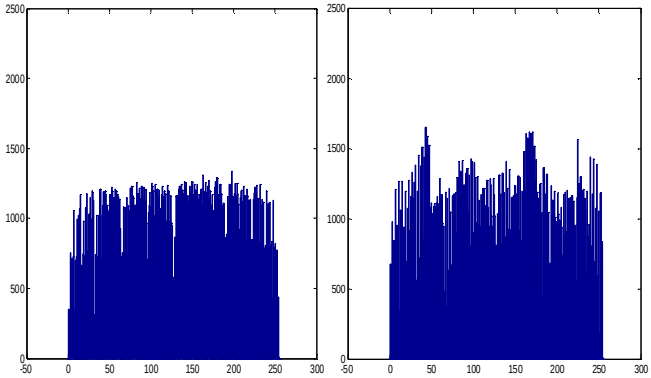
Fig. 7. Distribution of two vertically adjacent pixels in the permuted images of Barbara: using Socek permutation method controlled by (a) the perturbed PWLCM map and (b) the perturbed Logistic map.

It is clear from Fig. 7 that there is a negligible correlation between the two adjacent pixels in the images permuted with Socek method controlled by the perturbed maps.

Histogram analysis

Fig. 8 shows the histogram of the Red component of the permuted images of Barbara using Socek method controlled by the perturbed PWLCM map and the perturbed Logistic map.

Compared to histograms of Fig. 6(a) and 6(d), one can observe that gray levels of Fig. 8 are better distributed over pixels. The second point to outline is that a better uniformity is observed in the histogram of the perturbed PWLCM map. Similar results are obtained for the Mandrill image.



(a) (b)

Fig. 8. Histogram of the first component of the permuted images of Barbara: using Socek permutation method controlled by (a) the perturbed PWLCM map and (b) the perturbed Logistic map.

Information entropy analysis

Table XV shows the entropy value of the permuted images of Barbara using Socek permutation method associated with the perturbed PWLCM map and the perturbed Logistic map. The obtained values also prove the efficiency of the proposed perturbation technique. The same test is done using the Mandrill image (see Table XVI) and the same conclusions can be drawn.

Table XV. Entropy value of the permuted images of Barbara, using Socek permutation method controlled by the perturbed Logistic map and the perturbed PWLCM map.

	Permuted image using Socek method controlled by	
	Perturbed PWLCM	Perturbed Logistic
Entropy	7.9526	7.9275

Table XVI. Entropy value of the original and the permuted images of Mandrill, using Socek permutation method controlled by Logistic map, PWLCM map and their perturbed versions.

	Original Image	Permuted image using PWLCM to control			
		PWLCM	Perturbed PWLCM	Logistic	Perturbed Logistic
Entropy	7.762	7.888	7.950	7.8666	7.9376

V. CONCLUSION

Novel chaotic permutation techniques are presented in this paper. They use previous chaotic maps (PWLCM and Logistic) and are designed to reach a higher security level. To test their efficiency, the performances of three well known bit-permutation methods controlled by previous chaotic maps are compared with their performances when the new chaotic maps are used. In terms of NPCR and UACI, similar behavior is observed between the previous and the proposed chaotic maps even if an error rate slightly higher is observed with the original PWLCM. When correlation coefficients are considered, the proposed chaotic maps present higher performance with lower intra and inter-components correlation coefficients. However, with an entropy value which is also improved, the proposed permutation techniques are more secure and suitable for chaotic image encryption schemes. Finally, this study allows choosing an efficient permutation method to construct a chaotic cryptosystem with good cryptographic properties.

REFERENCES

[1] G. Millérioux, J. M. Amigo, J. Daafouz, “A connection between chaotic and conventional cryptography,” IEEE Trans. Circuits and Systems, vol. 55, no. 6, pp. 1695-1703, Jul. 2008.

[2] G. Alvarez, S. Li, “Some Basic Cryptographic Requirements for Chaos Based Cryptosystems,” International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.

[3] S. E. Borujeni, M. Eshghi1, “Chaotic Image Encryption Design Using Tompkins-Paige Algorithm,” Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 762652, 22 pages, 2009.

[4] S. El Assad, C.Vladeanu, “Digital chaotic codec for DS-CDMA Communication Systems,” Lebanese Science Journal, vol. 7, No. 2, 2006.

[5] L. Kocarev, J. Szczepanski, J. M. Amigo, I. Tomovski, “Discrete Chaos —I: Theory,” IEEE Trans. Circuits and Systems Magazine, vol. 53, no. 6, pp. 1300-1309, June 2006.

[6] S. Behnia, A. Akshani, S. Ahadpour, H. Mahmodi, A. Akhavan, “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,” Physics Letters A, pp. 391-396, 2007.

[7] C. Li, S. Li, G. Alvarez, G. Chen and K. T. Lo. “Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations”. Physics Letters A, 2007.

[8] D. Socek, S. Li, S. S. Magliveras, B. Furht, “Enhanced 1-D Chaotic Key Based Algorithm for Image Encryption,” IEEE, Security and Privacy for Emerging Areas in Communications Networks, 2005.

[9] A. Awad, S. E. Assad, Q. Wang, C. Vlădeanu, B. Bakhache, “Comparative Study of 1-D Chaotic Generators for Digital Data Encryption,” IAENG International Journal of Computer Science, vol. 35, no. 4, pp. 483-488, 2008.

[10] A. Awad, S. E. Assad, D. Carragata, “A Robust Cryptosystem Based Chaos for Secure Data,” IEEE, Image/Video Communications over fixed and mobile networks, Bilbao Spain, 2008.

[11] A. Awad, A. Saadane, “Efficient Chaotic Permutations for Image Encryption Algorithms,” Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2010, WCE 2010, 30 June - 2 July, 2010, London, U.K., pp 748-753.

[12] Z. Shi, R. Lee, "Bit Permutation Instructions for Accelerating Software Cryptography," IEEE, Application-specific Systems, Architectures and Processors, pp. 138-148, 2000.

[13] R. B. Lee, Z. Shi, X. Yang, “Efficient Permutation Instructions for Fast Software Cryptography,” IEEE Micro, vol. 21, no. 6, pp. 56-69, 2001.

[14] Y. Hilewitz, Z. J. Shi, R. B. Lee, “Comparing Fast Implementations of Bit Permutation Instruction,” IEEE, Signals Systems and Computers, vol.2, 1856 – 1863, 2004.

[15] V. Patidar, K.K. Sud, “A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing,”informatica, vol. 33, pp. 441-452, 2009.

[16] T. Xiang, X.F. Liao, K.W. Wong, “An Improved Particle Swarm Optimization Algorithm Combined with Piecewise Linear Chaotic Map,” Applied Mathematics and Computation, vol. 190, no. 2, pp. 1637-1645, 2007.

[17] H. Zhou, “A Design Methodology of Chaotic Stream Ciphers and the Realization Problems in Finite Precision,” phd thesis, department of electrical Engineering, Fudan university, Shanghai China, 1996.

[18] T. Yang, C. W. Wu, L. O. Chua, “Cryptography Based on Chaotic Systems,” IEEE Trans. Circuits and Systems, vol. 44, no. 5, pp. 469–472, 1997.

[19] G. Chen, X. Mou, S. Li, "On the Dynamical Degradation of Digital Piecewise Linear Choatic Maps," International Journal of Bifurcation and Chaos, vol. 15, no 10, pp. 3119-3151, 2005.