A New Fast Image Encryption Scheme Based on 2D Chaotic Maps

Radu Eugen BORIGA, Ana Cristina DĂSCĂLESCU, and Adrian Viorel DIACONU

Abstract— **Chaotic cryptography has been widely studied in the last 20 years. A common issue in the design of several proposed chaos-based cryptosystems is the use of a single chaotic map in the encoding/decoding processes, fact which leads to a low level security. We present a new symmetric keystream image encryption scheme, in which three 2D chaotic maps, recently proposed by the authors, are used instead of a single chaotic map. Those maps are derived from some plans curves equations, their trigonometric forms ensuring a large key space. The proposed scheme has a bi-modular architecture, in which the pixels are shuffled via a random permutation generated by using a new efficient algorithm, and a diffusion stage, in which the pixels' values are altered using a new XOR-scheme. In order to evaluate the security of the proposed image encryption scheme, a standard analysis was carried out.**

Index Terms— **chaos-based cryptography, chaotic maps, image encryption, keystream encryption**

I. INTRODUCTION

IMAGE encryption schemes have been increasingly studied in order to ensure secure images transmission through the Internet or through other communication networks. To meet this challenge, cryptographic techniques need to be applied. Traditional symmetric ciphers, such as Data Encryption Standard (DES), are designed with good confusion and diffusion properties [10], [29], [30], [41]. These two properties can also be assured by using chaotic maps which are usually ergodic and sensitive to system parameters and initial conditions. In this sense, in the last decade, many researchers have proposed different encryption schemes based on chaotic maps [8], [11], [15], [16], [27], [30], [32], [39].

The chaos-based encryption schemes are made up of two stages: confusion and diffusion. In the diffusion stage, a combination of chaotic maps is used to alter the values of all pixels, while in the confusion stage the pixels from the plain image are shuffled. The symmetric secret key is defined by the control parameters properly chosen so as the involved maps have to be in chaotic regime.

Different chaotic systems have been utilized in image encryption schemes: Fridrich used a 3D version of the baker map [13], Pareek et al. used a generalized logistic map [27], while Lian et al. used a standard map [23]. For some of the proposed chaos based encryption schemes it was proved that an incorrect selection of the initial conditions or the use of chaotic maps with a small range of the control parameters or an uneven value distribution, lead to a weak security [1]-[3], [8], [11], [15], [17], [22], [27], [28], [36], [39].

Motivated by the extent of previous work, the present paper aims to present a new image encryption scheme based on three chaotic map derived from equations of some plan curves, previously proposed by authors in [5], [6] ,[9]. In order to increase the space of the secret key, those maps involve some trigonometric functions. Their good cryptographic properties lead to a robust image encryption scheme.

The rest of the paper is organized as follows: section 2 presents the proposed chaos-based encryption scheme, section 3 presents the performance analysis of the proposed image encryption scheme and section 4 concludes the work carried out so far.

II. DESCRIPTION OF THE PROPOSED CRYPTOSYSTEM

The large number of image encryption schemes proposed in the last decade which uses the properties of discrete chaotic maps shows that chaos theory is currently regarded as a viable way to develop safe and fast cryptographic applications. Most proposed systems have a bi-modular architecture, in which the first of the modules performs the diffusion of the information using a permutation and the second one performs the confusion by modifying pixel values using a deterministic algorithm [8], [11], [16], [27], [39]. Thus, diffusion and confusion, the two requirements postulated by Shannon as being indispensable to any encryption system in his masterpiece "*Theory of Communication Systems secrecy*", are met [31].

In most cases, the vulnerability of the chaos-based encryption systems is induced by the use of binary streams extracted from a single orbit of a chaotic map or by the use of maps which have chaotic behavior only for small ranges of control parameters' values. Moreover, the low speeds can be caused by the need for several rounds of permutation and/or substitution of the original image pixel [2], [3], [27], [39].

The proposed cryptosystem tries to improve these weaknesses by using both a new fast algorithm for generating random permutations with few fixed points in the diffusion process, in order to eliminate the need for several rounds of pixels shuffling, and three 2D discrete chaotic maps whose cryptographic properties have been demonstrated to be very good in [5], [6], [9] in the confusion process, in order to eliminate the need for several rounds of substitutions of the pixels values.

The proposed cryptosystem is a symmetric one, so the

Manuscript received February 04, 2014; revised April 15, 2014.

R.E. Boriga and A.C. Dăscălescu are with Titu Maiorescu University, 189 Văcărești Ave., 040051, Bucharest, Romania (phone/fax: +40213301083; e-mail: radu.boriga@prof.utm.ro, cristina.dascalescu@prof.utm.ro).

A.V. Diaconu is with IT & C Department, Lumina-The University of South-East Europe, 64B Colentina Street, 021187, Bucharest, Romania (e-mail: adrian.diaconu@lumina.org).

secret key is common to both the transmitter and receiver, which implies the existence of a secure communication channel through which the key will be bidirectionally transmitted.

The block diagram of the encryption process is illustrated in Fig. 1, while the block diagram of the decryption process is illustrated in Fig. 2.

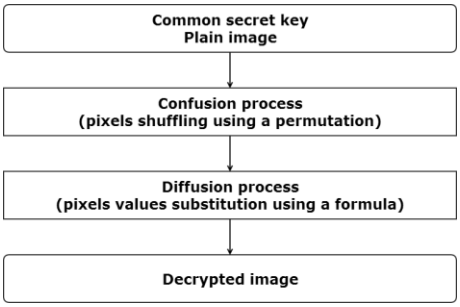

Fig. 1. The block diagram of the encryption process

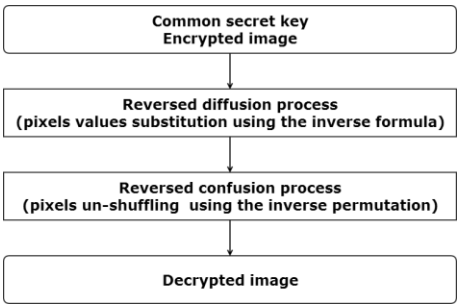

Fig. 2. The block diagram of the decryption process

Next, we describe in detail each block of the proposed cryptosystem, which uses the following 2D discrete chaotic maps proposed in [5], [6], [9]:

1) the *serpentine* map was proposed and analyzed in [6] and it's defined as follows:

$$\begin{cases} x_{n+1}^{(S)} &= \operatorname{arctg}\left(\operatorname{ctg}\left(2^{r_S} x_n^{(S)}\right)\right) \\ y_{n+1}^{(S)} &= \sin\left(2^{r_S} y_n^{(S)}\right)\cos\left(2^{r_S} y_n^{(S)}\right) \end{cases} \quad (1)$$

where $x_n^{(S)} \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right]\setminus\{0\}$, $y_n^{(S)} \in \left[-\frac{1}{2},\frac{1}{2}\right]$ and the control parameter $r_S \in \mathbb{R}^+$.

The evolution rule of the map (1) is, for any value of the control parameter, $r_S \in \mathbb{R}^+$, given by:

$$f_S: \left[-\frac{\pi}{2},\frac{\pi}{2}\right]\setminus\{0\}\times\left[-\frac{1}{2},\frac{1}{2}\right] \to \left[-\frac{\pi}{2},\frac{\pi}{2}\right]\times\left[-\frac{1}{2},\frac{1}{2}\right], \quad (2)$$
$$f_S(x,y) = \left(\operatorname{arctg}(\operatorname{ctg}(2^r x)), \sin(2^r y)\cos(2^r y)\right)$$

The study of the long time behavior of the *serpentine* map according to the control parameter $r_S \in \mathbb{R}^+$ and to the initial condition $(x_0, y_0) \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right]\setminus\{0\}\times\left[-\frac{1}{2},\frac{1}{2}\right]$ was carried out in [6]. Using some tools from chaos theory, such as Lyapunov exponent, bifurcation diagram and stability of the fixed points, we proved theoretically and numerically, that the *serpentine* map is chaotic for $r_s > 0$ and hyperchaotic for $r_s > 8$. The theoretical results are listed below:

Theorem 1 [6]. Let f_S be the *serpentine* map, defined by the relation (2). Then, for any control parameter $r > 0$ the f_S map is chaotic.

Theorem 2 [6]. Let f_S be the *serpentine* map, defined by the relation (2). Then, for any control parameter $r > 6$ the f_S map is hyperchaotic.

In Fig. 3 the bifurcation diagram and the Lyapunov exponents of the *serpentine* map are plotted.

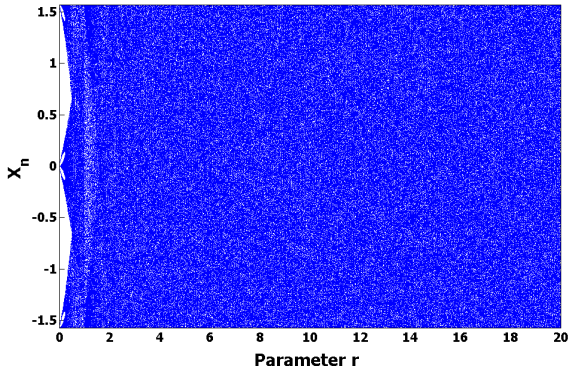

Fig. 3(a). Bifurcation diagram

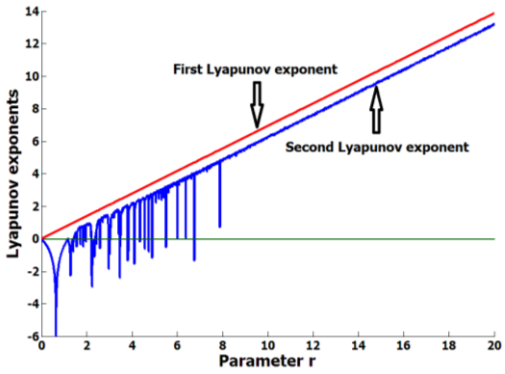

Fig. 3(b). Lyapunov exponents

Fig. 3. Analysis of the *serpentine* map's chaotic behavior

2) the *lemniscate* map was proposed and analyzed in [9] and it's defined as follows:

$$\begin{cases} x_{n+1}^{(L)} &= \dfrac{\cos\left(2^{r_L} y_n^{(L)}\right)}{1+\sin^2\left(2^{r_L} y_n^{(L)}\right)} \\ y_{n+1}^{(L)} &= \dfrac{2\sqrt{2}\sin\left(2^{r_L} x_n^{(L)}\right)\cos\left(2^{r_L} x_n^{(L)}\right)}{1+\sin^2\left(2^{r_L} x_n^{(L)}\right)} \end{cases} \quad (3)$$

where $x_n^{(L)}, y_n^{(L)} \in [-1,1]$ and the control parameter $r_L \in \mathbb{R}^+$.

The time behavior of *lemniscate* map depends on the control parameter $r_L \in \mathbb{R}^+$ and the initial condition $(x_0, y_0) \in [-1,1]\times[-1,1]$. Using some numerical methods and specific tools from chaos theory, such as Lyapunov exponent, bifurcation diagram and the fractal dimension of the attractor, we proved numerically in [9] that the *lemniscate* map is in a chaotic regime for control parameter $r_L > 0$ and for $r_L > 3$ is in a hyperchaotic regime. In Fig. 4 the bifurcation diagram and the Lyapunov exponents of the *lemniscate* map are plotted.

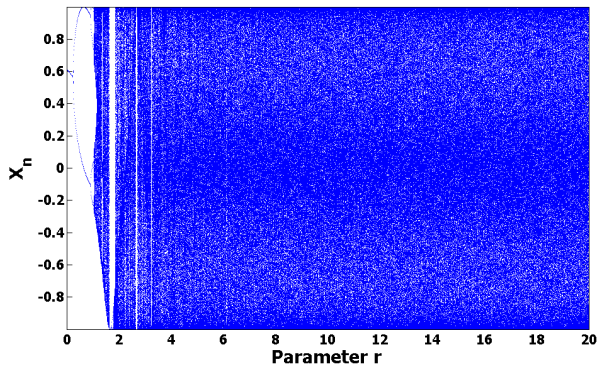

Fig. 4(a). Bifurcation diagram

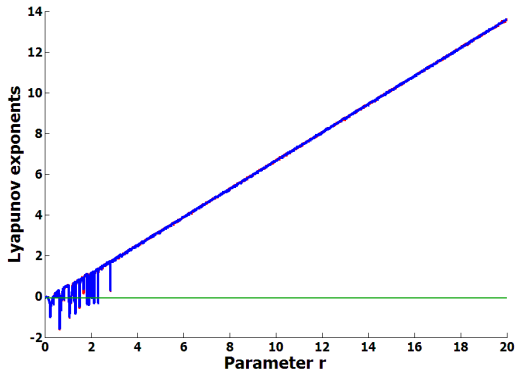

Fig. 4(b). Lyapunov exponents

Fig. 4. Analysis of the *lemniscate* map's chaotic behavior

3) the *xsin* map was proposed and analyzed in [5] and it's defined as follows:

$$\begin{cases} x_{n+1}^{(T)} = \operatorname{arctg}\left(\operatorname{ctg}\left(x_n^{(T)} + \sin\left(r_T^3 y_n^{(T)}\right)\right)\right) \\ y_{n+1}^{(T)} = x_n^{(T)} \end{cases} \quad (4)$$

where $x_n^{(T)}, y_n^{(T)} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ and the control parameter $r_T \in \mathbb{R}^+$.

The *xsin* map is derivate from the transcendental equation $x + sin\, x = 0$. Due to its complex analytical form we use some numerical methods from chaos theory, such as Lyapunov exponent, bifurcation diagram and the fractal dimension of the attractor, in order to analyze its time behavior regarding control parameter $r_T \in \mathbb{R}^+$. We proved in [5] that the *xsin* map is in a chaotic regime for control parameter $r_T > 1.35$ and in a hyperchaotic regime for $r_T > 3$. In Fig. 5 the bifurcation diagram and the Lyapunov exponents of the *xsin* map are plotted.

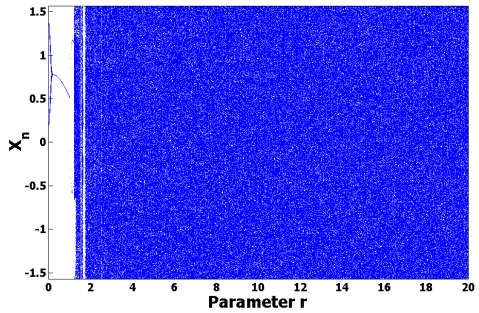

Fig. 5(a). Bifurcation diagram

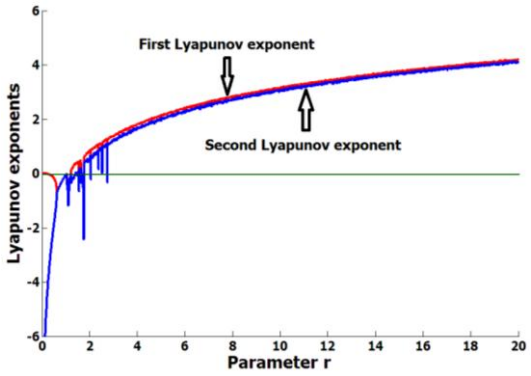

Fig. 5(b). Lyapunov exponents

Fig. 5. Analysis of the *xsin* map's chaotic behavior

A. *The secret key*

The secret key of the cryptosystem is formed from the initial conditions of the maps (1), (3) and (4), chosen so that each map have to be in a chaotic regime. In order to achieve a chaotic regime, all three chaotic maps are pre-iterated. Practically, the secret key consists of 9 real numbers and 3 unsigned integers, which must be chosen so as to satisfy simultaneously the following restrictions [5], [6], [9]:

- $x_0^{(S)} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \setminus \{0\}$, $y_0^{(S)} \in \left[-\frac{1}{2}, \frac{1}{2}\right]$ and $r_S \in [10{,}110]$;
- $x_0^{(L)} \in [-1{,}1]$, $y_0^{(L)} \in [-1{,}1]$ and $r_L \in [250{,}350]$;
- $x_0^{(T)} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, $y_0^{(T)} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ and $r_T \in [10{,}100]$;
- $m_S, m_L, m_T \geq 1000$ (number of maps pre-iterations).

The keystreams used in this cryptosystem are obtained discretizing the real values generated by the chaotic maps. So, a real value x is discretized to the unsigned integer $floor(10^{15} \times |x|)$, where $floor(a)$ represents the nearest integer less than or equal to a.

Since a chaotic map has a high sensitivity even to infinitesimal changes in the initial conditions, it's recommended to implement the cryptosystem using a real data type with high precision, such as the double data type defined in *IEEE Standard 754-2008* [18].

B. *The confusion process*

In an image encryption scheme, the confusion process usually consists of the pixels' permutation from the plain image, in order to hide the correlations among the plain image, the encrypted image and encryption key [11], [16], [19], [24], [25], [30], [32], [34], [37], [40]. In this sense, we propose a fast and efficient algorithm for generating random permutations suitable for image shuffling.

The proposed algorithm combines the use of random values, generated by the branches of the serpentine map (1), with the use of deterministic ones. So, a permutation $q = (q_1, q_2, \ldots, q_n)$ of degree n is constructed element by element, as follows: a random unsigned integer value, obtained by discretizing and scaling the real values generated alternatively by one of the two branches of the *serpentine* map (1), is checked if it was previously used or not. If true, the maximum unused value is assigned to the current element of the permutation, otherwise the random value generated by the *serpentine* map is used.

The algorithm for generating a random permutation $q = (q_1, q_2, \dots, q_n)$ of degree n is the following:

Algorithm 1

INPUT: $n \in \mathbb{N}^*$, $\left(x_0^{(S)}, y_0^{(S)}\right) \in \left[-\frac{1}{2}, \frac{1}{2}\right] \times \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \setminus \{0\}$, $m_S \geq 1000$ and $r_S \in [10,110]$
OUTPUT: random permutation $q = (q_1, q_2, \dots, q_n)$

$x \leftarrow x_0^{(S)}$; $y \leftarrow y_0^{(S)}$
// the *serpentine* map is pre-iterated for m_S times
for i **from** 1 **to** m_S **do**
    $x \leftarrow \text{arctg}(\text{ctg}(2^{r_S} x))$
    $y \leftarrow \sin(2^{r_S} y)\cos(2^{r_S} y)$
endfor

// L is a labeling array of dimension n (i.e. L_i is equal to 1 if
// a value $i \in \{1,2,\dots,n\}$ is used in permutation q, otherwise
// L_i is equal to 0), so all values from 1 to n are initially //unused
for i **from** 1 **to** n **do**
    $L[i] \leftarrow 0$
endfor

// variable max stores the maximum unused value between
// 1 and n and variable b stores the current branch of the //*serpentine* map
$max \leftarrow n + 1$; $b \leftarrow 0$
for i **from** 1 **to** n **do**
    // the discretized and scaled real value of the current branch of the *serpentine* map
    // is assigned to the current element of the permutation q
    if $b = 0$ **then**
        $q[i] \leftarrow 1 + floor\left(10^{15} \times \left|x_n^{(S)}\right|\right) \bmod n$
    else
        $q[i] \leftarrow 1 + floor\left(10^{15} \times \left|y_n^{(S)}\right|\right) \bmod n$
    endif

    // if the value of the permutation's current element //q was previously used, it is replaced by the maximum //unused value between 1 and n
    if $L[q[i]] = 1$ **then**
        $j \leftarrow max - 1$
        while $j \geq 1$ **and** $L[j] = 1$ **do**
            $j \leftarrow j - 1$
        endwhile
        $max \leftarrow j$; $q[i] \leftarrow max$
    endif

    // the final value of the current element is labeled as //used and the other branch of the serpentine map //becomes the current branch
    $L[q[i]] \leftarrow 1$; $b \leftarrow (b + 1) \bmod n$

    //the *serpentine* map is iterated one time
    $x \leftarrow \text{arctg}(\text{ctg}(2^{r_S} x))$
    $y \leftarrow \sin(2^{r_S} y)\cos(2^{r_S} y)$
endfor

The proposed algorithm has a maximum complexity of $\mathcal{O}(n^2)$, but, if a chaotic and ergodic map is used, its average complexity will be close to $\mathcal{O}(n)$. Moreover, the generated random permutations have a very small number of fixed points, proved by the fact that in the case of 1000000 generated permutations, with lengths between 10000 and 10000000, the maximum percent of fixed points was 0.01%.

In the encryption process, the pixels from the plain image are shuffled using the permutation q, while in the decryption process the pixels are un-shuffled using the inverse permutation q^{-1}, which can be easily determined with an algorithm with an $\mathcal{O}(n)$ complexity, so the complexity of the proposed algorithm remains the same.

C. The diffusion process

In an image encryption scheme, a good diffusion process ensures that a minor change of one pixel from the plain image leads to great modifications over the whole encrypted image. Usually, this can be achieved by pixels values substitutions in a deterministic way [11], [16], [19], [24], [25], [30], [32], [34], [37], [40].

We assume that, from now on, the plain image of size $m \times n$ is denoted by $P = \left(p_{i,j}\right)_{\substack{0 \leq i < m \\ 0 \leq j < n}}$ and the encrypted image, of the same size, by $C = \left(c_{i,j}\right)_{\substack{0 \leq i < m \\ 0 \leq j < n}}$.

Thus, the diffusion in the encryption process is achieved by applying the following formula for each pixel of the plain image (i.e. for each $i = \overline{0, m-1}$ and each $j = \overline{0, n-1}$) in order to obtain the value of the corresponding pixel from the encrypted image:

$$c_{i,j} = p_{i,j} \oplus xsin_{i*n+j+1}^{(1)} \oplus p_{r,c} \quad (5)$$

where by $xsin_k^{(1)}$ we denote the value x_k generated by the *xsin* map (4), initialized by using the values r_T, $x_0^{(T)}$ and $y_0^{(T)}$, and the pixel $p_{r,c}$ is given by:

$$p_{r,c} = \begin{cases} p_{m-1,n-1}, \text{ if } i = 0, j = 0 \\ p_{0, l_{j+1}^{(2)} \bmod j}, \text{ if } i = 0, j \neq 0 \\ p_{l_{i*n+1}^{(1)} \bmod i, l_{i*n+1}^{(2)} \bmod n}, \text{ if } i \neq 0, j = 0 \\ p_{l_{i*n+j+1}^{(1)} \bmod i, l_{i*n+j+1}^{(2)} \bmod j}, \text{ if } i \neq 0, j \neq 0 \end{cases} \quad (6)$$

where by $l_k^{(1)}$ and $l_k^{(2)}$ denote the values x_k and y_k generated by the *lemniscate* map (3), initialized by using the values r_L, $x_0^{(L)}$ and $y_0^{(L)}$. By mod we denote the modulo operation.

In the decryption process, the plain image is obtained from the encrypted image by applying in a similar way the following formula, complementary of the formula (5) from the encryption process:

$$p_{i,j} = c_{i,j} \oplus xsin_{i*n+j+1}^{(1)} \oplus p_{r,c} \quad (7)$$

Note that in the substitution formulas (5) and (6) for the value of a pixel, we used the value of another pixel from the original image, fact that leads to a high quality of the diffusion process, because the encrypted image will be more sensitive to minor changes in the plain image.

III. Performance Analysis of the Proposed Cryptosystem

The security of the proposed cryptosystem was analyzed using a standard methodology in the area of image encryption [14], [16], [37], [40]. Thus, there were performed several specific statistical tests, such as image pixels distribution, the correlation between adjacent pixels of the encrypted image, Shannon entropy and the correlation between original image and the encrypted one. The resistance of the proposed cryptosystem against differential attacks was proved using two standard indicators, NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity), while resistance against a brute force attack was analyzed through the size of the secret key space.

In the testing process we used 100 heterogeneous images in uncompressed BMP format, with the color depth equal to 24 and standard dimensions (e.g. 256×256, 512×512, 720×576, 1024×1024 and 3000×4000) [20], [35]. All tests were performed for each of the three RGB color channels, in order to achieve a rigorous analysis of proposed cryptosystem performance.

Next, we will present the analysis' results only for the following 10 standard test images from USC-SIPI Image Database (Miscellaneous and Aerials sets) [35]: Girl (4.1.01), House (4.1.05), Mandrill (4.2.03), Lena (4.2.04), Peppers (4.2.07), Man (5.3.01), Airport (5.3.02), San Diego (2.2.03), Stockton (2.2.11), Washington, D.C. (infra-red) (wash-ir).

A. *Pixels' distribution analysis*

Pixels' distribution analysis claims to estimate the resistance of a cryptosystem against cryptanalytic attacks of statistical type, such as ciphertext-only attack or plaintext-ciphertext attack. Regardless of the encryption key used, a cryptosystem with high security needs to produce encrypted images with a uniform distribution of pixel values in each color channel, so that it hides the uneven distribution of the original image.

Most often used visual analysis tool in the study of the distribution of pixel values is the color histogram, in which the pixel values frequencies are plotted separately for each color channel.

Fig. 6 contains a pair of plain/encrypted image, along with the associated color histograms.

Fig. 6(a). Lena image

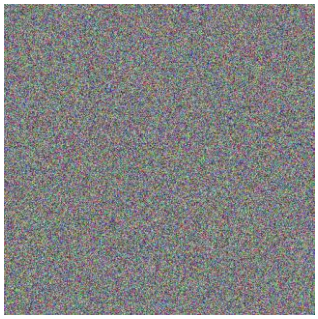

Fig. 6(b). Lena encrypted image

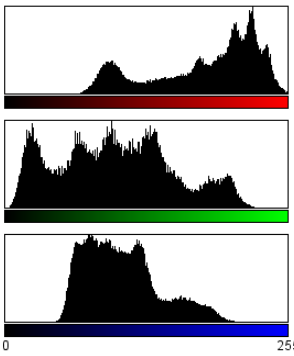

Fig. 6(c). Histogram of the Lena image

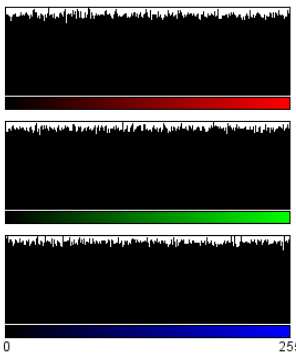

Fig. 6(d). Histogram of the encrypted Lena image

Fig. 6. Pixels distribution analysis of the standard image Lena

Note that after the encryption of Lena image, which has a strong color uneven distribution (Fig. 6(c)), it was obtained an image with a uniform distribution of pixel values (Fig. 6(d)) for each RGB channel, so an attacker can not extract statistical information about the original image or the keystream/secret key.

To analyze the distribution of pixel values for a large number of encrypted images, we used the χ^2 −test. The value of the χ^2 −test for an encrypted image of dimension $m \times n$ is given by the following formula [26]:

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0} \tag{8}$$

where v_i is the observed frequency of a pixel value i ($0 \leq i \leq 255$) and v_0 is the expected frequency of a pixel value i, so $v_0 = \frac{m \times n}{256}$.

The results obtained by applying the χ^2 test on 100 encrypted images can be summarized as it follows: in 96% of the tests, the values obtained were lower than the critical value $\chi^2_{255,0.05} = 293.25$ and only in 4% of the tests, the values obtained were lying in the interval [294.68,322.35], very close to the critical value $\chi^2_{255,0.05} = 293.25$.

Table I shows the results obtained by applying the χ^2 − test for 10 pairs of plain/encrypted test images.

TABLE I
Results of the χ^2- test

Test image	χ^2 − test	
	Plain image	Encrypted image
Girl	161648.19	248.19
House	317258.15	293.56
Mandrill	101863.46	259.34
Lena	237534.11	262.74
Peppers	340999.44	274.78
Man	709340.68	257.41
Airport	1974776.14	267.07
San Diego	6187844.74	256.06
Stockton	4219744.87	245.47
Washington, D.C.	5355559.26	239.38

Thus, we conclude that the distribution of pixel values is uniform in the encrypted images, which demonstrates that the proposed cryptosystem is able to resist against cryptanalytic attacks of statistical type.

B. Global and local entropy

Information theory is the mathematical theory of data communication and storage, founded in 1949 by Shannon [31], [33]. Modern information theory is concerned with error-correction, cryptography, communications systems, and related topics. It is well known that the global entropy $H(S)$ of an image source S can be calculated as:

$$H(S) = -\sum_{i=0}^{255} P(i)\log_2 P(i) \tag{9}$$

where $P(i)$ represents the probability of a pixel value i $(0 \le i \le 255)$ and the global entropy is expressed in bits. Actually, given that a real information source seldom generates random messages, in general its global entropy value is much smaller than the ideal one equal to 8, so there exists a certain degree of predictability, which threatens its security.

In order to analyze the statistical independence of an encrypted image vs. plain image/keystream, we calculated the global entropy of the 100 pairs of plain-encrypted images. The plain images used in the testing process had entropy values between 4.762235 and 7.838074, and through the encryption process images with entropies between 7.999218 and 7.999831 were obtained. The global entropies obtained for 10 pairs of plain/encrypted test images are shown in Table II:

TABLE II
RESULTS OF GLOBAL ENTROPY TEST

Test image	Entropy	
	Plain image	Encrypted image
Girl	6.415479	7.999817
House	6.400674	7.999615
Mandrill	7.644440	7.999282
Lena	7.271856	7.999246
Peppers	7.297795	7.999216
Man	7.523737	7.999826
Airport	6.830330	7.999816
San Diego	5.662656	7.999821
Stockton	6.070791	7.999823
Washington, D.C.	7.222260	7.999827

The values obtained are very close to the maximum theoretical value of 8, which means that information leakage in the encryption process is negligible and the encryption system is secure against the entropy attack.

In [38] was proposed a new measure for randomness of an image, using Shannon entropy over local image blocks. Even the encrypted image has a very flat histogram and high Shannon entropy over the whole image, a randomness test, using the block entropy test, should not be omitted in evaluating the quality of the encryption process. If an image contains some image blocks with low Shannon entropy, then it is not a ideally encrypted, no matter how high its global Shannon entropy is [38].

The (k, T_B)–local Shannon entropy over image blocks is in [38] define by:

$$\overline{H_{(k,T_B)}}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{10}$$

where $S_1, S_2, \dots, S_k$ are randomly selected non–overlapping blocks image with T_B pixels within a test image S of L intensity scales and $H(S_i)$ are computed using Shannon entropy (9) for $\forall\, i \in \{1,2,\dots,k\}$.

In our test, the local Shannon entropy measure is evaluated for the 10 encrypted test images. From each encrypted image, we randomly selected $k = 30$ non-overlapping image blocks with $T_B = 1936$ pixels. In [38] it was proven that the observed value of $(30,1936)$-local Shannon entropy should lie in the confidence interval $[7.901901305, 7.903037329]$, with respect to α-level confidence equal to 0.05. Table III shows the image pixel randomness measured by local Shannon entropy for the 10 encrypted images.

TABLE III
LOCAL SHANNON ENTROPY TEST FOR ENCRYPTED IMAGES
$(k = 30, T_B = 1936, \alpha = 0.05)$

File name	Local Shannon entropy of the encrypted images	Result
Girl	7.9022	SUCCESS
House	7.9024	SUCCESS
Mandrill	7.9018	SUCCESS
Lena	7.9024	SUCCESS
Peppers	7.9021	SUCCESS
Man	7.9025	SUCCESS
Airport	7.9026	SUCCESS
San Diego	7.9028	SUCCESS
Stockton	7.9020	SUCCESS
Washington, D.C.	7.9021	SUCCESS
Mean ± Std.	7.9022 ± 0.0003	
Number of images passing the α–level test	10	

Thus, the results obtained both for local and global entropies show that the proposed scheme provides random-like encrypted images.

C. Pixels' correlation analysis

In order to analyze the encryption quality of the proposed algorithm, the correlation coefficient was used to evaluate both the correlations between the plain image and the encrypted image and the correlations between adjacent pixels of the encrypted image.

Numbering the pixels from a color channel X of a plain image $P = (p_{i,j})_{\substack{0\le i<m\\ 0\le j<n}}$ with $P_X = (p_{i,j}^X)_{\substack{0\le i<m\\ 0\le j<n}}$ and the ones from a color channel Y of the corresponding encrypted image $C = (c_{i,j})_{\substack{0\le i<m\\ 0\le j<n}}$ with $C_Y = (c_{i,j}^Y)_{\substack{0\le i<m\\ 0\le j<n}}$, we could see that the correlation coefficient between the pixels from two color channels X and Y, viewed as random variables, is given by:

$$\rho_{X,Y}(P,C) = \frac{cov(P_X, C_Y)}{\sqrt{D(P_X)}\sqrt{D(C_Y)}} \tag{11}$$

where $D(\cdot)$ is the variance of a random variable and $cov(\cdot,\cdot)$ is the covariance of two random variables [26].

To determine possible correlations between the plain images and the corresponding encrypted ones, we calculated the correlation coefficient for 100 pairs of plain/encrypted images. Table IV shows the values of the correlation coefficient obtained for 10 pairs of plain/encrypted images.

TABLE IV
CORRELATION COEFFICIENTS BETWEEN THE PLAIN AND THE ENCRYPTED IMAGES

Test image	Correlation coefficient
Girl	0.00338
House	-0.00205
Mandrill	0.00407
Lena	-0.00355
Peppers	0.00621
Man	-0.00168
Airport	0.00022
San Diego	0.00662
Stockton	0.00683
Washington, D.C.	-0.00313

In all the 100 performed tests, the values obtained ranged from -0.00575 and 0.00662, so very close to 0, which confirms there are no significant correlations between the pixels of the plain images and the encrypted corresponding ones, so the cryptosystem is secure against the chosen plaintext attack and plaintext-ciphertext attack.

Another important aspect in assessing the security of an image encryption system to the statistical cryptanalytic attacks is to verify if there are no significant correlations between adjacent pixels of the encrypted image. Thus, we chose 100 pairs of plain/encrypted images and for each pair of images we chose a set of 1000 pixels adjacent horizontally, vertically or diagonally.

In Fig. 7(a) we plotted the value of the pixel at the position (x, y) versus the value of the pixel at the position $(x + 1, y)$ in the Lena image, while in Fig. 7(b) we plotted them from the encrypted Lena image. We repeated the same plotting for vertically adjacent pixels (Fig. 7(c) - 7(d)) and for diagonally adjacent pixels (Fig. 7(e) - 7(f)).

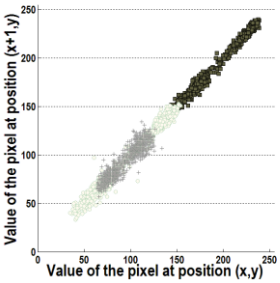

Fig. 7(a). Correlation of horizontally adjacent pixels in the plain image

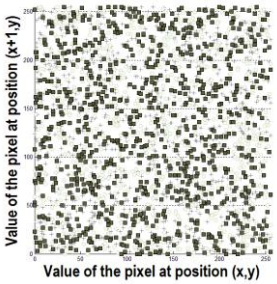

Fig. 7(b). Correlation of horizontally adjacent pixels in the encrypted image

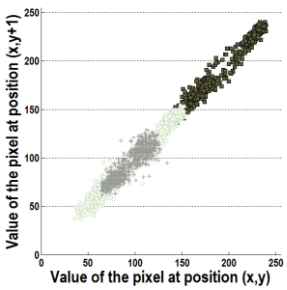

Fig. 7(c). Correlation of vertically adjacent pixels in the original image

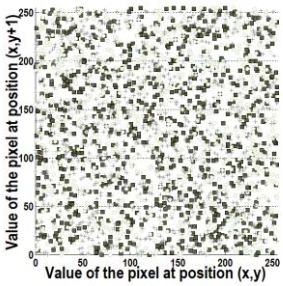

Fig. 7(d). Correlation of vertically adjacent pixels in the encrypted image

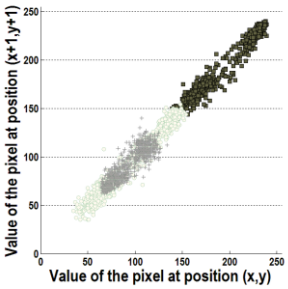

Fig. 7(e). Correlation of vertically adjacent pixels in the original image

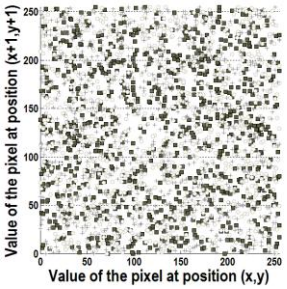

Fig. 7(f). Correlation of vertically adjacent pixels in the encrypted image

Fig. 7. Correlation coefficient of adjacent pixels from Lena plain/encrypted image

In Table V we listed the values of the correlation coefficient of the adjacent pixels obtained for 10 pairs of plain/encrypted images.

TABLE V
CORRELATION COEFFICIENTS OF ADJACENT PIXELS IN THE PLAIN AND THE ENCRYPTED IMAGES

Test image	Adjacency direction	Correlation coefficient	
		Plain image	Encrypted image
Girl	Horizontal	0.83818	-0.00569
	Vertical	0.87524	0.00253
	Diagonal	0.81132	0.00383
House	Horizontal	0.89832	-0.00304
	Vertical	0.92206	0.00502
	Diagonal	0.83605	-0.00531
Mandrill	Horizontal	0.64423	0.00128
	Vertical	0.71606	0.00513
	Diagonal	0.62313	-0.00982
Lena	Horizontal	0.96055	-0.00057
	Vertical	0.94182	0.00404
	Diagonal	0.94381	0.00261
Peppers	Horizontal	0.97405	-0.00142
	Vertical	0.98003	-0.00182
	Diagonal	0.95771	0.00323
Man	Horizontal	0.96842	-0.00154
	Vertical	0.96961	-0.00291
	Diagonal	0.98736	-0.00106
Airport	Horizontal	0.92763	0.00021
	Vertical	0.94185	-0.00564
	Diagonal	0.84168	0.00895
San Diego	Horizontal	0.82204	-0.00713
	Vertical	0.84371	0.00066
	Diagonal	0.77358	-0.00665
Stockton	Horizontal	0.68103	0.00021
	Vertical	0.72579	-0.00836
	Diagonal	0.63613	-0.00186
Washington, D.C.	Horizontal	0.90102	-0.00261
	Vertical	0.93587	0.00131
	Diagonal	0.88402	0.00333

In all the 100 performed tests, the values obtained ranged from -0.00982 and 0.00923, so very close to 0, which confirms that through the encryption process the inherent strong correlation existing in plain images were almost eliminated. This fact proves, once again, that the proposed system will resist against cryptanalytic attacks of statistical type.

D. Key space analysis

The secret key of a cryptosystem must be chosen to achieve a satisfactory compromise between the inconvenience of a large key length, such as lower speed of

encryption and decryption processes, and the inconvenience produced by a small one, respectively the possibility of guessing it in a short time using the simplest cryptanalytic attack, the brute force attack.

The secret key of the proposed cryptosystem contains, along with 3 unsigned integers, 9 real numbers which must be stored and transmitted using a real data type with high precision in order to prevent negative effects caused by the discretization of real numbers. If the implementation is done using a programming language that complies with *IEEE Standard 754-2008*, then it is recommended to use the double data type, which stores real numbers on 8 bytes with an accurate of 15 decimals. Thus, the length of the secret key will be of 672 bits, which means that the size of the secret key space will be equal to 2^{672}, a value large enough to avoid guessing secret key by exhaustive search in a reasonable time.

E. Key Sensitivity Analysis

A good cryptosystem should be sensitive to any small change in the secret key, so that the using in the decrypting process of a secret key which differs very little from the original one leads to a completely different image from the initial plain image. Our proposed encryption algorithm is very sensitive to a little change in the secret key. If we change only by 10^{-12}, any component of the secret key, then the decrypted image will be totally different from the plain-image. Fig. 8 shows 3 images obtained by decrypting the encrypted Lena image using 3 secret keys which have only one component, different by 10^{-12} from the original secret key. It is obvious that all images are totally different from the plain-image Lena and, moreover, the decrypted images seem to be a noise.

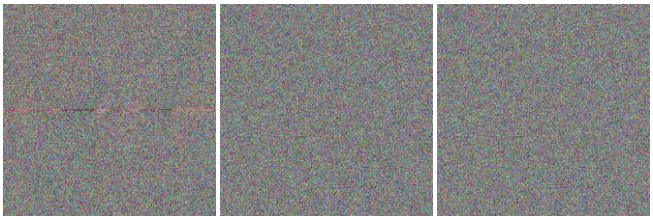

Fig. 8(a). Decrypted image using a secret key with x_L altered by 10^{-12}

Fig. 8(b). Decrypted image using a secret key with r_S altered by 10^{-12}

Fig. 8(c). Decrypted image using a secret key with y_T altered by 10^{-12}

Fig. 8. Decrypted Lena image using an altered initial secret key

Testing 900 pairs of images obtained after considering 100 plain images and all the 9 corresponding decrypted images resulted by using a secret key with only one real component different by 10^{-12} from the initial secret key, we obtained in 99.8% of cases values of the correlation coefficient very close to 0 and very large values of the mean square error, which entitles us to say that the proposed cryptosystem is very sensitive to changes of the secret key, thus enhancing its security against of brute force attacks.

F. Resistance against differential attacks

To test the security of the proposed cryptosystem against differential attacks it is necessary to evaluate how a minor change in the plain image is reflected in the encrypted image. For this purpose we consider two plain images $P_1 = \left(p_{i,j}^{(1)}\right)_{\substack{0\le i<m\\0\le j<n}}$ and $P_2 = \left(p_{i,j}^{(2)}\right)_{\substack{0\le i<m\\0\le j<n}}$ which differ by the value of a single pixel and their corresponding encrypted images $C_1 = \left(c_{i,j}^{(1)}\right)_{\substack{0\le i<m\\0\le j<n}}$ and $C_2 = \left(c_{i,j}^{(2)}\right)_{\substack{0\le i<m\\0\le j<n}}$.

To test the influence of one-pixel change in the plain image on the whole encrypted image using the proposed cryptosystem, two common measures are used: *Number of Pixels Change Rate* (NPCR) and *Unified Average Changing Intensity* (UACI).

The NPCR indicator measures the percentage of different pixel numbers between the encrypted images C_1 and C_2 and it's defined as follows:

$$NPCR = \left(\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} d_{i,j}\right)\times 100\% \tag{12}$$

where the matrix $D = \left(d_{i,j}\right)_{\substack{0\le i<m\\0\le j<n}}$ is given by:

$$d_{i,j} = \begin{cases} 0, & \text{if} \quad c_{i,j}^{(1)} = c_{i,j}^{(2)} \\ 1, & \text{if} \quad c_{i,j}^{(1)} \neq c_{i,j}^{(2)} \end{cases} \tag{13}$$

The UACI indicator measures the percentage average intensity of differences between the encrypted images C_1 and C_2 and it's defined as follows:

$$UACI = \left(\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\frac{\left|c_{i,j}^{(1)} - c_{i,j}^{(2)}\right|}{255}\right)\times 100\% \tag{14}$$

In [21] the theoretical maximum values of 99.609375% for NPCR and 33.463541% for UACI are stated.

In Table VI we listed the values of the NPCR and UACI indicators obtained for the 10 test images.

TABLE VI
RESULTS OF THE DIFFERENTIAL ATTACK TESTS

Test image	NPCR (%)	UACI (%)
Girl	99.24	33.10
House	98.87	32.16
Mandrill	99.12	33.11
Lena	99.22	33.12
Peppers	99.15	33.14
Man	99.16	33.18
Airport	99.18	33.11
San Diego	99.14	32.84
Stockton	99.21	33.15
Washington, D.C.	99.19	32.17

Using the proposed cryptosystem, 100 tests were performed, achieving values of the NPCR indicator between 98.87% and 99.23% and between 32.17% and 33.18% for the UACI indicator, which are very close to the theoretical maximum ones, fact which confirms that the proposed cryptosystem will withstand to the differential attacks.

G. Quality of the Decryption Process

Performance evaluation of a cryptosystem should

consider the quality of the decryption process, verifying that the image obtained after decryption is the same with the plain one. In this sense, we evaluated the *Mean Squared Error* (MSE) between a plain image $P = (p_{i,j})_{\substack{0\le i<m\\0\le j<n}}$ and the corresponding decrypted one $= (d_{i,j})_{\substack{0\le i<m\\0\le j<n}}$, using the following formula [26]:

$$MSE(P,D) = \left(\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(p_{i,j} - d_{i,j} \right)^2 \right) \qquad (15)$$

A value close to 0 of MSE shows a good quality of the decryption process, while a greater value indicates the occurrence of some errors.

Fig. 9 presents the results of the decryption process for Lena test image, using the correct secret key and an altered secret key by 10^{-15} on r_L component. Similar results were obtained altering others components of the secret key by 10^{-15} for the real values or by 1 bit for the unsigned integer ones.

Fig. 9(a). Lena image

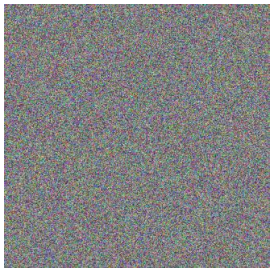

Fig. 9(b). Encrypted Lena image

Fig. 9(c). Decrypted Lena image using correct secret key

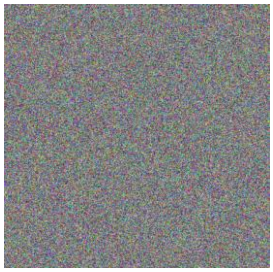

Fig. 9(d). Decrypted Lena image using a secret key changed by 10^{-15} on r_L component

Fig. 9. Results of the decryption process

In all the 100 tests performed, the value of MSE between the plain image and the corresponding encrypted one was 0, which shows that decryption is carried out without loss of information.

H. Speed performance

An important factor to consider when analyzing the efficiency of a cryptosystem is its speed. Accordingly, we ran the proposed algorithm implemented in C language (MinGW compiler) under Windows 7, using a PC with Intel(R) Core(TM) i3 @2.53GHz CPU and 3GB RAM. We used 100 standard test bitmaps (256×256) with sizes of 256×256, 512×512, 720×576, 1024×1024 and 3000×4000 [20], [35]. The mean speeds obtained are summarized in Table VII:

TABLE VII
AVERAGE SPEEDS OF THE ENCRYPTION/DECRYPTION PROCESSES

Image size (pixels)	Image size (MB)	Mean time (s)	Mean speed (MB/s)
256×256	0.19	*0.045*	*4.222*
512×512	0.75	*0.195*	*3.846*
720×576	1.19	*0.297*	*4.007*
1024×1024	3.00	*0.762*	*3.937*
3000×4000	34.33	*8.575*	*4.003*

Analyzing the mean speeds from Table VII, we can see that the proposed scheme has a mean encryption/decryption speed about 4 MB/s, so the proposed algorithm is faster than the ones presented in [16], [30], [32], thus being suitable for real time image encryption.

I. Performances' comparison with other image encryption schemes

Next, we will present a comparison of performances, taking into account some of the most recent works [16], [30], [32]. Table VIII summarizes the mean values obtained for correlation coefficient of adjacent pixels (CCAP), NPCR, UACI and speed.

TABLE VIII
PERFORMANCES' COMPARISON WITH OTHER IMAGE ENCRYPTION SCHEMES

Indicator		Sivakumar et al. [32]	Saraswathi et al. [30]	Ghebleh et al. [16]	Ours scheme
NPCR		99.48	99.85	99.61	99.24
UACI		30.87	33.58	33.72	33.13
CCAP	Horizontal	0.342	0.01776	-0.0043	0.0039
	Vertical	0.352	0.04912	0.0049	0.0059
	Diagonal	0.298	0.00348	0.0057	0.0004
Speed (MB/s)		1.65	0.45	2.4	3

Taking into consideration the results from Table VIII, it we can see that the proposed image encryption scheme has similar or better results than other recent proposed schemes [16], [30], [32].

IV. CONCLUSIONS

In this paper, we proposed a new chaos-based encryption scheme based on three 2D chaotic maps. The proposed scheme has a classic bi-modular architecture: a confusion stage, in which the pixels are shuffled via a random permutation generated by using a new efficient algorithm, and a diffusion stage, in which the pixels' values are altered using a new XOR-scheme. The high security of the proposed encryption scheme was proved through an extensive analysis, performed following the latest methodology in this field. Moreover, its high speed of

4MB/s, suggests that the proposed encryption scheme is suitable for real-time image encryption applications.

REFERENCES

[1] G. Alvarez, F. Montoya, M. Romera and G. Pastor, "Cryptanalysis of an ergodic chaotic cipher", *Physics Letters A*, vol. 311, no. 2-3, pp. 172–179, 2003.

[2] D. Arroyo, G. Alvarez, S. Li, C. Li and J. Nunez, "Cryptanalysis of a discrete-time synchronous chaotic encryption", *Physics Letters A*, vol. 372, no. 7, pp. 1034–1039, 2008.

[3] A. Awad, S. El Assad, W. Qianxue, C. Vlădeanu, and 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.

[4] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", *Optics and Lasers in Engineering*, vol. 51, pp. 665-673, 2013.

[5] R. Boriga and A.C. Dăscălescu, "A novel pseudo-random bit generator based on some transcendental chaotic systems", *Annals of Ovidius University - Economics Sciences Series*, vol. 11, pp. 208-212, 2011.

[6] R. Boriga, A.C. Dăscălescu and I. Priescu, "A new hyperchaotic map and its application in an image encryption scheme", *Signal Processing: Image Communication*, vol. 29, no. 8, pp. 887-901, 2014.

[7] A. Cheddad, J. Condell, K. Curran and P. McKevitt, "A hash-based image encryption algorithm", *Optics Communications*, vol. 283, no. 6, pp. 879-893, 2010.

[8] G. Chen, Y. 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.

[9] A.C. Dăscălescu and R. Boriga, "A novel pseudo-random bit generator based on a new couple of chaotic systems", *Annals of Ovidius University - Economics Sciences Series*, vol. 11, no. 1, pp. 553-558, 2011.

[10] S. Dey, "SD-AEI: An advanced encryption technique for images", in *Proceedings of Digital Information Processing and Communications (ICDIPC), Second International Conference*, Klaipeda, Lithuania, 2012 July 10-12, pp. 68-73.

[11] A.V. Diaconu and K. Loukhaoukha, "An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher", *Mathematical Problems in Engineering*, vol. 2013, article ID 848392, 2013.

[12] A.A. El-Latif, L. Li, N. Wang, Q. Han and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces", *Signal Processing*, vol. 93, pp. 2986-3000, 2013.

[13] J. Fridrich, "Image encryption based on chaotic maps", *IEEE International Conference on Systems, Man, and Cybernetics (ICSMC-97)*, Hyatt Orlando, USA, 1997 October 12-15, vol. 1, pp. 1105–1110.

[14] B. Furht and D. Kirovski, *Multimedia Security Handbook*. Boca Raton: CRC Press, Boca Raton, 2004.

[15] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos", *Physics Letters A*, vol. 372, pp. 394–400, 2008.

[16] M. Ghebleh, A. Kanso and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps", *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618-627, 2014.

[17] C.K. Huang, C.W. Liao, S.L. Hsu and Y.C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", *Telecommunication Systems*, vol. 52, no. 2, pp. 563-571, 2013.

[18] *IEEE Standard for Floating-Point Arithmetic*, IEEE Standard 754, 2008.

[19] L. Kocarev, G. Jakimoski, T. Stojanovski and U. Parlitz, "From chaotic maps to encryption schemes", in *Proceedings of the 1998 IEEE International Symposium on Circuits and Systems (ISCAS '98)*, Monterey, USA, 1998 May 31 – June 03, vol. 4, pp. 514–517.

[20] *Kodak Digital Camera Sample Pictures*, http://www.kodak.com/digitalImaging/samples/classic.shtml, last accessed 01 February 2014.

[21] H.S. Kwok and W.K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", *Chaos, Solitons & Fractals*, vol. 32, no. 4, pp. 1518-1529, 2007.

[22] C. Li, L.Y. Zhang, R. Ou, K.W. Wong and S. Shu, "Breaking a novel colour image encryption algorithm based on chaos", *Nonlinear Dynamics.*, vol. 70, no. 4, pp. 2383-2388, 2012.

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

[24] A.J. Menezes, P.C. Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997.

[25] O. Mirzaei, M. Yaghoobi and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos", *Nonlinear Dynamics*, vol. 67, no. 1, pp. 557-566, 2012.

[26] A. Papoulis, *Probability, Random Variables and Stochastic Processes*, New York: McGraw-Hill, 1965.

[27] N.K. Pareek, V. Patidar and K.K Sud, "Image encryption using chaotic logistic map", *Image and Vision Computing*, vol. 24, no. 9, pp. 926-934, 2006.

[28] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos", *Physics Letters A*, vol. 372, pp. 5973–5978, 2008.

[29] F. Riaz, S. Hameed, I. Shafi, R. Kausar and A. Ahmed, "Enhanced image encryption techniques using modified advanced encryption standard", *Communications in Computer and Information Science*, vol. 281, pp. 385-396, 2012.

[30] P.V. Saraswathi and M. Venkatesulu, "A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal", *Journal of Computer Science*, vol. 8, no. 9, pp. 1541-1546, 2012.

[31] C. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[32] T. Sivakumar and R. Venkatesan, "A novel approach for image encryption using dynamic SCAN pattern", *IAENG International Journal of Computer Science*, vol. 41, no. 2, pp. 91-101, 2014.

[33] A. Şerbănescu and C.I. Rîncu, *Systemes et signaux face au chaos. Applications aux communications*. Bucharest: Military Technical Academy Press, 2008.

[34] X.J. Tong and M.G. Cui, "Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation", *Science in China Series F: Information Sciences*, vol. 53, no. 1, pp. 191-202, 2010.

[35] *USC-SIPI Image Database*, http://sipi.usc.edu/database/database.php, last accessed: 01 February 2014.

[36] J. Wang, G. Jiang and B. Lin, "Cryptanalysis of an image encryption scheme with a pseudorandom permutation and its improved version", *Journal of Electronics (China)*, vol. 29, no. 1-2, pp. 82-93, 2012.

[37] X. Wang and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme", *Optics Communications*, vol. 284, no. 24, pp. 5804–5807, 2011.

[38] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness", *Information Sciences*, vol. 222, pp. 323-342, 2013.

[39] H. Yang, X. Lia, K.W. Wong, W. Zhang and P. Wei, "A new cryptosystem based on chaotic map and operations algebraic", *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2520–2531, 2009.

[40] G. Ye and K.W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map", *Nonlinear Dynamics*, vol. 69, no. 4, pp. 2079-2087, 2012.

[41] M.A.B. Younes and A. Jantan, "Image encryption using block-based transformation algorithm", *IAENG International Journal of Computer Science*, vol. 35, no. 1, pp. 15-23, 2008.