Signal Processing 93 (2013) 1328–1340

Contents lists available at SciVerse ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Image encryption process based on chaotic synchronization phenomena

Ch.K. Volos [a,*], I.M. Kyprianidis [b], I.N. Stouboulos [b]

[a] Department of Mathematics and Engineering Studies, Hellenic Army Academy, Athens GR-16673, Greece
[b] Physics Department, Aristotle University of Thessaloniki GR-54124, Greece

ARTICLE INFO

Article history:
Received 27 January 2012
Received in revised form
15 September 2012
Accepted 12 November 2012
Available online 20 November 2012

Keywords:
True random bits generator
Chaos
Complete synchronization
Inverse π-lag synchronization
Nonlinear circuit
Encryption

ABSTRACT

This paper presents a novel image encryption scheme, which uses a chaotic True Random Bits Generator (TRBG). The chaotic TRBG is based on the coexistence of two different synchronization phenomena. The first one is the well-known complete chaotic synchronization while the second one is a recently new proposed synchronization phenomenon, the inverse π-lag synchronization. This coexistence is observed in the case of two mutually coupled identical nonlinear circuits. The nonlinear circuit, which is used, produces double-scroll chaotic attractors. The initial conditions of the coupled system and the values of the circuit's parameters serve as the private key of the proposed cryptographic scheme. In order to face the challenge of using this chaotic TRBG in such cryptographic schemes, the produced bits sequence is subjected to statistical tests which are the well-known Federal Information Processing Standards-140-2. This bits sequence has then been used to encrypt and decrypt gray-scale images. Also, the security analysis of the encrypted image demonstrates the high security of the proposed encryption scheme.

1. Introduction

In recent years, confidentiality of information is an essential feature of the digital era since the communications over open networks occur more and more frequently. The rapid development of Internet technology appointed communication using multimedia techniques one of the most prevailing approaches of communication. Also, digital image information has become very important because of the vitality and visualization. Nevertheless in many cases, image data transferred in the Internet must not be public. So, reliable, fast and secure communication systems must be implemented to transmit images or photographs in many applications, such as photographs from military satellites, drawings of military establishment, images of medical systems, online personal photographs, images of electronic publishing and fingerprint images of authentication systems.

As it is known, digital images have some very characteristic features such as, strong correlation among adjacent pixels, bulk data capacity, redundancy of data, being less sensitive compared to the text data and existence of patterns and backgrounds. Therefore, because of these features, traditional ciphers like DES, AES, IDEA and RSA, are not suitable for real time image encryption as these ciphers require a large computational time and high computing power. Also, most of the conventional image encryption algorithms are based on position permutation. This process has the advantage of fast encryption speed but the security depends on the security of the algorithm, which do not satisfy the requirement of a modern encryption system.

Nowadays, there are two major approaches that are used to protect digital images from attackers. The first one

* Corresponding author. Tel: +30 210 2833507.
E-mail address: chvolos@gmail.com (Ch.K. Volos).

0165-1684/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2012.11.008

is the information hiding, such as digital watermarking of an image [1–5]. The second one is the encryption, which includes conventional encryption techniques and others such as chaotic encryption [6–11].

The rapid development of nonlinear dynamics in the last two decades and especially of chaotic dynamics makes researchers realize that chaotic systems can be used in cryptosystems [12], because of their corresponding counterparts in cryptosystems, such as the sensitivity on initial conditions and system parameters, ergodicity and topological transitivity. Also, unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptosystems rely on the complex dynamics of nonlinear systems which are deterministic.

The first, who proposed an encryption process based on chaos, was Matthews in 1989 [13]. After him, many other researchers have proposed schemes based on chaotic systems. In 2000, Yen and Guo [14] proposed a chaotic key-based algorithm for image encryption. A year later, in 2001 a fast encryption image encryption algorithm based on vector quantization was developed [15]. Also, in the last decade, image encryption schemes based on chaotic Cat maps and Baker maps were proposed [16–18].

Furthermore, in the last decade, the security of many cryptographic systems was based on random number generators. Generators that produce random sequences can be classified into three types: True Random Number Generators (TRNGs), Pseudo-Random Number Generators (PRNGs) and Hybrid Random Number Generators (HRNGs) [19]. This classification is mainly based on the source of the randomness. The first type of these generators, TRNGs take advantage of nondeterministic sources, which come from an unpredictable natural process in a physical or hardware device that can output a sequence of statistically independent data, as opposed to PRNGs that produce numbers sequences by a computer program. As sources of random numbers may be considered the elapsed time during radioactive decay [20], the thermal and shot noise [21], the frequency instability of an oscillator [22], the variations in disk drive response times [23], the integrating dark current from a metal insulator semiconductor capacitor [24], the mouse movement [25] and the environmental noise [26].

A new approach is suggested in this paper for efficient and practical chaotic image encryption scheme. The basic idea of our method is to encrypt a gray-scale image via a chaotic True Random Bits Generator (TRBG), which is based on the interaction between two mutually coupled identical chaotic circuits [27,28]. The proposed coupled system shows the phenomenon of the coexistence of two different synchronization phenomena, the well-known complete chaotic synchronization and the recently new proposed synchronization phenomenon, the inverse π-lag synchronization [27,28]. According to a binary sequence generated from the chaotic generator, the pixels of the gray-scale image XOR-ed to the predetermined keys.

The rest of the paper is organized as follows: In Section 2 basic features of chaotic systems and the synchronization phenomena, which are the base of this work, are presented. Section 3 introduces the chaotic TRBG. In Section 4 the results of the use of a well known statistical tests suite (FIPS-140-2) are presented. Section 5 demonstrates how to encrypt and decrypt the "Lenna" images via the chaotic sequences obtained from the chaotic TRBG. In Section 6 security analysis on the proposed "Lenna" image encryption scheme, is presented. Finally, conclusion remarks are drawn in the last Section.

2. Chaotic systems and synchronization phenomena

As it known, a dynamical system in order to be considered as chaotic must fulfill the three following conditions [29]:

- It must be very sensitive on initial conditions,
- its periodic orbits must be dense and
- it must be topologically mixing.

In this work the use of coupled continuous-time chaotic systems for generating true random bits sequences in image encryption process is shown. The study of the interaction between coupled chaotic systems was a landmark in the evolution of the chaotic synchronization's theory [30]. The most well-known type of synchronization is the complete or full synchronization, in which the interaction between two identical coupled chaotic systems leads to a perfect coincidence of their chaotic trajectories, i.e.

$$x_1(t) = x_2(t) \quad \text{as } t \to \infty \tag{1}$$

where x_1 and x_2 are the signals of the coupled chaotic systems.

Although, since 2010 a new synchronization phenomenon, the inverse π-lag synchronization, between two mutually coupled identical nonlinear systems, has been observed [27,28]. This new type of synchronization is observed when the coupled system is in a phase locked (periodic) state, depending on the coupling factor and it can be characterized by eliminating the sum of two relevant periodic signals (x_1 and x_2) with a time lag τ, which is equal to $T/2$, where T is the period of the signals x_1 and x_2:

$$x_1(t) = -x_2(t+\tau), \quad \tau = T/2 \tag{2}$$

Nevertheless, depending on the coupling factor and the chosen set of system's initial conditions, the inverse π-lag synchronization coexists with a complete synchronization [28]. So, the proposed TRBG, which is used for the image encryption, is based on the coexistence of these two types of synchronization, which are used as representing the states "0" and "1" in the seed generation, as it will be described in details in the next section.

3. The chaotic true random bits generator

The proposed chaotic TRBG, which is used, in this work, for the image encryption process, consists of three blocks (Fig. 1). The first of these blocks (S_1) includes the coupled nonlinear system, which is necessary in this TRBG. This system is based on a nonlinear Chua's like autonomous circuit which demonstrates the inverse π-lag synchronization [28,31].

The autonomous nonlinear circuit (Fig. 2), which has been used, is capable of producing double-scroll chaotic attractors. A great number of such systems are known, like Chua [32] or Lorenz [33], and some of them are easily implemented as electronic circuits. All these systems have the characteristic of two attractors, between which the process state will oscillate. A double-scroll oscillator needs to have at least three degrees of freedom in order to be chaotic.

The state equations of the chosen system are the following:

$$\begin{cases} \frac{dx}{dt} = y \\ \frac{dy}{dt} = z \\ \frac{dz}{dt} = -\alpha\cdot(x+y+z)+b\cdot f(x) \end{cases} \quad (3)$$

where α and b are the circuit parameters and are defined as follows:

$$\alpha = (R\cdot C)^{-1}\ b = (R_X\cdot C)^{-1} \quad (4)$$

The state parameters x, y, and z represent the voltages at the outputs of the operational amplifiers numbered as "1", "2" and "3" respectively, as shown in Fig. 2.

Also, the function $f(x)$ in system's equation (3) is a saturation function [28,31], which represents the voltage at the output of the operational amplifier numbered as "5" and is defined by the following expression:

$$f(x) = \begin{cases} 1 & \text{if} \quad x > \frac{R_2}{R_3}\cdot 1\ \text{V} \\ \frac{R_3}{R_2}\cdot x & \text{if} \quad -\frac{R_2}{R_3}\cdot 1\ \text{V} \le x \le \frac{R_2}{R_3}\cdot 1\ \text{V} \\ -1 & \text{if} \quad x < -\frac{R_2}{R_3}\cdot 1\ \text{V} \end{cases} \quad (5)$$

So, the function $f(x)$ is implemented in such a way that the saturation plateaus are ± 1 and the slope of the intermediate linear region is $k=R_3/R_2$.

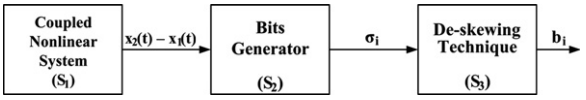

Fig. 1. The chaotic true random bits generator scheme.

In this work the values of the circuit elements were adjusted: $R=20$ kΩ, $R_1=1$ kΩ, $R_2=14.3$ kΩ, $R_3=28.6$ kΩ, $R_X=10$ kΩ and $C=1$ nF, so as to demonstrate double-scroll chaotic attractors. Consequently, $\alpha=0.5$, $b=1.0$ and $k=2.0$. Furthermore, the operational amplifiers were of the type LF411 and the voltages of the positive and negative power supplies were set ± 15 V.

The Lyapunov exponents of the proposed system (3) for the chosen set of circuit's parameters and for initial conditions ($x_0=0.4$, $y_0=0.3$, $z_0=0.2$) were calculated by employing the Wolf et al. algorithm [34] on the time-series of $y(t)$: $LE_1=0.1718$, $LE_2=0$, $LE_3=-0.9593$. So, according to the theory of nonlinear systems, the existence of one positive Lyapunov exponent confirms numerically that the double-scroll attractor of the circuit is chaotic.

As it is previously mentioned, the proposed TRBG uses a system of two mutually coupled identical double-scroll chaotic circuits of this type. The system of the two bidirectionally or mutually coupled Nonlinear Circuits (NC) is shown in Fig. 3. For this reason the coupling of the identical nonlinear circuits is achieved via a linear resistor R_C connected between the nodes A of each circuit. So, the state equations, describing the coupled system, are

$$\begin{cases} \frac{dx_1}{dt} = y_1 \\ \frac{dy_1}{dt} = z_1+\xi\cdot(y_2-y_1) \\ \frac{dz_1}{dt} = -\alpha\cdot(x_1+y_1+z_1)+b\cdot f(x_1)-p(t) \\ \frac{dx_2}{dt} = y_2 \\ \frac{dy_2}{dt} = z_2+\xi\cdot(y_1-y_2) \\ \frac{dz_2}{dt} = -\alpha\cdot(x_2+y_2+z_2)+b\cdot f(x_2) \end{cases} \quad (6)$$

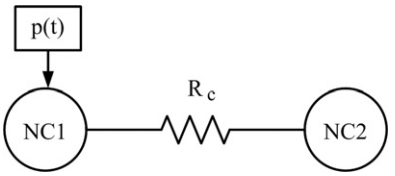

Fig. 3. The system of two bidirectionally or mutually coupled nonlinear circuits via a linear resistor.

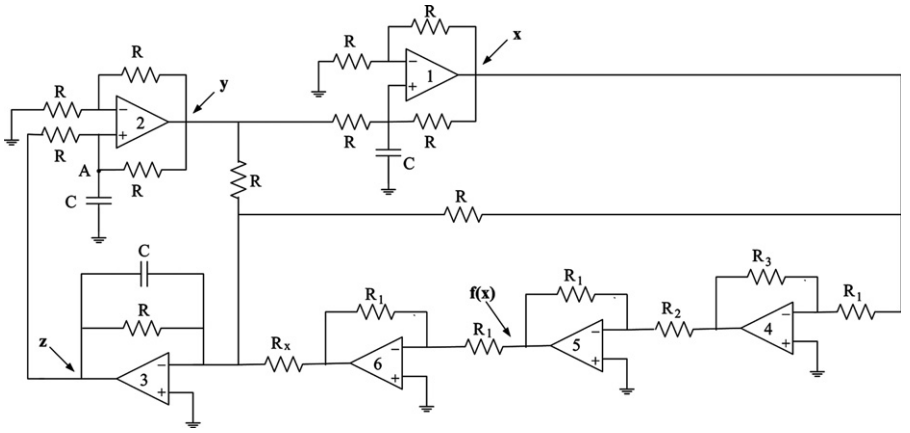

Fig. 2. The schematic of the autonomous nonlinear circuit.

The first three equations of system (6) describe the first of the two coupled identical nonlinear circuits (NC1), while the other three describe the second one (NC2). The coupling coefficient is $\xi = R/R_C$ and it is present in the equations of both circuits, since the coupling between them is bidirectional. The study of the coupled system's dynamic behavior, by using tools of nonlinear dynamics, such as bifurcation diagrams, reveals the appearance of the coexistence phenomenon of inverse π-lag synchronization with the complete synchronization from ξ greater than the value of 1.7. So, in this work the coupling coefficient (ξ) of the system is adjusted to be equal to 2.1, so that the coupled system is in the region of coexistence of the two previous mentioned synchronization phenomena. The rich dynamic behavior of the proposed coupled system and the desired chaotic behavior are presented in details in Ref. [28].

Also, $p(t)$ in the third equation of the system (6) is an external source which produces pulses that are necessary, as a perturbation, for changing the initial conditions of the system and therefore the synchronization state of the coupled system (inverse π-lag or complete synchronization). In detail, this source produces a pulse train of amplitude 0.7 V having a duty cycle of 4%. Thus, the pulse duration is 2 ms, while the period of the pulse train is 50 ms.

Consequently, the first block (S_1) of the TRBG produces the synchronization signal $[x_2(t)–x_1(t)]$ of the coupled system which varies between two states. In the first one, the signals $x_1(t)$ and $x_2(t)$ are identical because the system is in a complete synchronization mode. In Fig. 4 the phase portrait of $x_2(t)$ versus $x_1(t)$, which confirms the appearance of this type of synchronization, is shown. In the second state, the signal $x_2(t)$ is inverse of the signal $x_1(t)$ with π phase difference (Fig. 5(a)), because the system is in inverse π-lag synchronization. So, the phase portrait of $x_2(t)$ versus $x_1(t)$ is a very narrow closed loop (Fig. 5(b)).

In the second block (S_2) of the proposed TRBG, the two different levels of the output signal $[x_2(t)–x_1(t)]$ are quantized to "0" and "1" according to the following equation:

$$\sigma_i = \begin{cases} 0 & \text{if } x_2(t)-x_1(t) < 1 \text{ V} \\ 1 & \text{if } x_2(t)-x_1(t) > 1 \text{ V} \end{cases} \quad (7)$$

Therefore, if the system is in a complete synchronization state a bit "0" is produced, while if the system is in an inverse π-lag synchronization state a bit "1" is produced. The block S_2 may be implemented by using a comparator for Eq. (7) and a "sample and hold" circuit, which samples the output voltage $[x_2(t)–x_1(t)]$ of the first block (S_1). The sampling period equals the period of the pulse train ($T=50$ ms) and the sampling occurs at the middle of each pulse. The results of the above procedure of the proposed chaotic TRBG are shown in Fig. 6. More precisely, the pulse train which is used in the system is shown in Fig. 6(a). Also, the time-series of the difference signal $[x_2(t)–x_1(t)]$ and the produced bits sequence by the chaotic TRBG, are shown in Fig. 6(b) and (c) respectively.

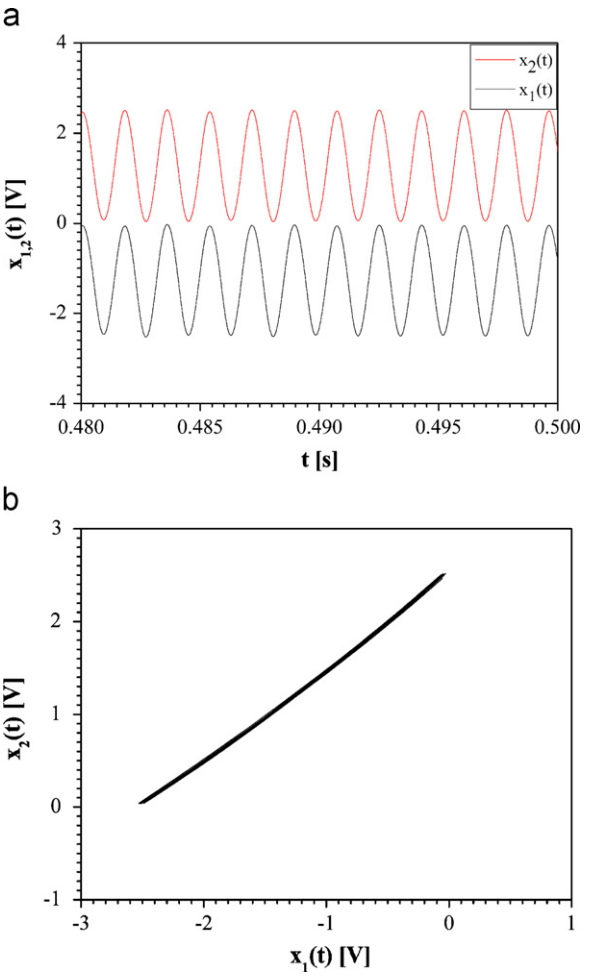

Fig. 5. In the case of inverse π-lag synchronization: (a) Time-series of $x_1(t)$ (black line) and $x_2(t)$ (red line) of both coupled circuits and (b) the synchronization phase portrait of $x_2(t)$ versus $x_1(t)$. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this article.)

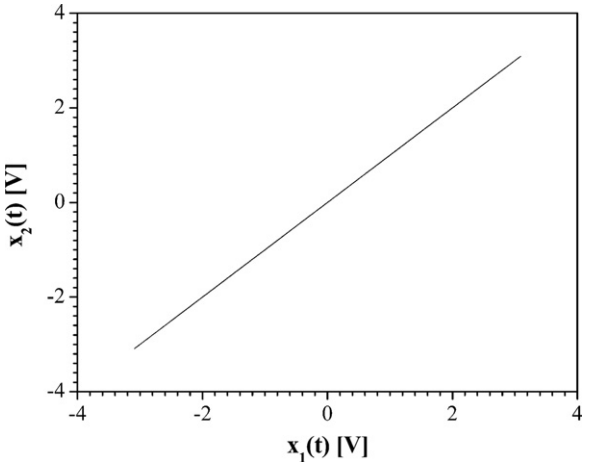

Fig. 4. The synchronization phase portrait of $x_2(t)$ versus $x_1(t)$ in the case of complete synchronization.

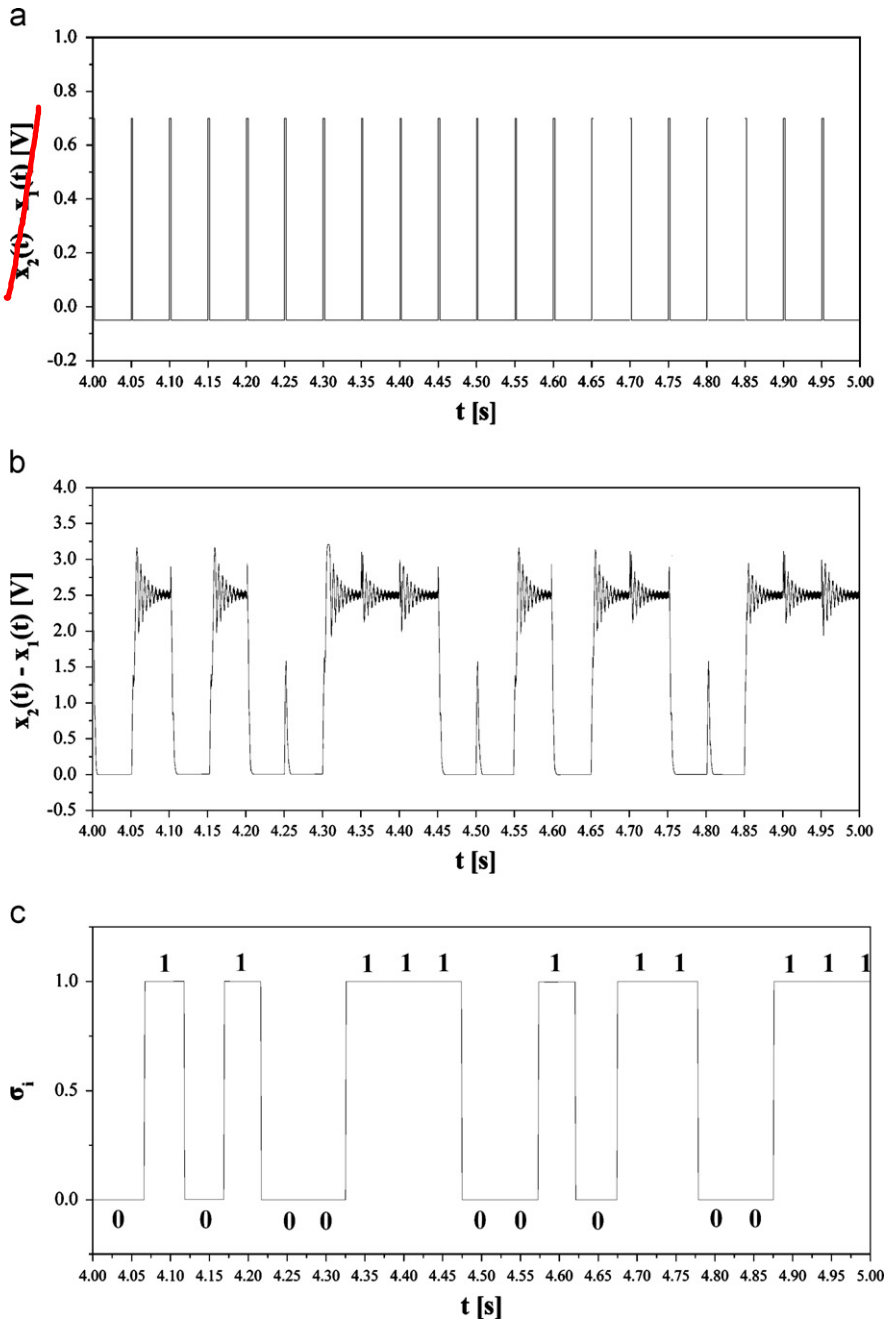

Fig. 6. Time-series of (a) pulses $p(t)$, (b) difference signal $[x_2(t)–x_1(t)]$ and (c) the produced bits sequence, with the proposed technique.

Also, it is known that a natural source of random bits may not give unbiased bits as direct output. Although, many interesting applications, especially in cryptography, rely on sequences of unbiased bits. So, there are various techniques in the literature which are used to extract unbiased bits from a defective generator with unknown bias. These are called de-skewing techniques (block S_3) [35]. These techniques also eliminate the correlation in the output of the natural sources of random bits. Von Neumann [36] has probably been the first author to state this problem. He proposed a digital post-processing that balances the distribution of bits. Post-processing converts non-overlapping pairs of bits into output bits by converting the bit pair "01" into an output "0", converting "10" into an output "1", while the pairs "11" and "00" are discarded. In this work, Von Neumann's technique is used because it can easily be integrated into the hardware and it does not decrease the bit rate too much, compared with the other proposed methods. However, this technique decreases throughput because of generating approximately 1 bit from 4 bit.

4. Statistical tests

In this section the "randomness" of the produced bits sequence, by the used chaotic TRBG, is examined. Thus, one of the most important statistical test suites, the FIPS (Federal Information Processing Standards) [37] of the National Institute of Standards and Technology (NIST), is used. So, the results of the use of the statistical tests, Monobit test, Poker test, Runs test, and Long run test, which are part of the FIPS-140-2 are presented in details.

The chaotic TRBG produces a bitstream, $s=s_0, s_1, s_2, \ldots, s_{n-1}$, of length n (at least 20,000 bits). According to FIPS-140-2, the random bits sequence which is produced by the specific TRBG must satisfy the following standards.

Monobit test: The number n_1 of 1's in the bitstream must be $9725 < n_1 < 10275$.
Poker test: This test determines whether the sequences of length n ($n=4$) show approximately the same number of times in the bitstream. The bounds of this statistic are then $2.16 < x_3 < 46.17$.
Runs test: This test determines whether the number of 0's (Gap) and 1's (Block) of various lengths in the bitstream are as expected for a random sequence (Table 1).
Long run test: This test is passed if there are no runs longer than 26 bits.

As it is known from information theory the noise has maximum entropy. So, the system's parameters ($\alpha=0.5$, $b=1.0$ and $k=2.0$) and initial conditions ($x_{01}=0.40$, $y_{01}=0.30$, $z_{01}=0.20$, $x_{02}=-0.50$, $y_{02}=-0.40$, $z_{02}=-0.1$) are chosen so as the measured entropy of the TRBG is maximal. Thus, the measure-theoretic entropy [38] of the proposed chaotic TRBG with respect to system's parameters and initial conditions is calculated, by using Eq.(8), to be $H_n=0.69185$ for $n=3$ and $H_n=0.69189$ for $n=4$, where n is the length of the n-word sequences.

$$H_n = \lim_{n\to\infty}\left(-\sum_{B^n} P(B^n)\ln P(B^n)/n\right) \tag{8}$$

In Eq.(8) $P(B^n)$ is the probability of occurrence of a binary subsequence B of length n.

Therefore, with the previous mentioned procedure, bits sequence of length 20 000 bits has been obtained from the output of the proposed chaotic TRBG calculated via the numerical integration of Eq.(6). Then this bits sequence is subjected to the four tests of FIPS-140-2 test suite. As a result, it has been numerically verified that the bits sequence passed the test suite of FIPS-140-2 (Table 2).

Table 1
Required intervals for length of runs test.

Length of run	Required interval
1	2315–2685
2	1114–1386
3	527–723
4	240–384
5	103–209
6	103–209

Table 2
Results of FIPS-140-2 test, for the chaotic TRBG.

Monobit test	Poker test	Runs test	Long run test
$n_1=10078$ (50.39%)	39.178	$B_1=2592$ $B_2=1305$ $B_3=643$ $B_4=310$ $B_5=118$ $B_6=130$	No
Passed	**Passed**	**Passed**	**Passed**

5. The encryption scheme

The proposed encryption scheme of gray-scale images, which for the aim of this work has been implemented in MATLAB, is based on XOR function. This scheme includes the following steps.

Step 1: The scheme finds the pixel size $M \times N$ of the image, where M and N represent row and column of the image. The pixels are arranged by order from left to right and top to bottom. Then an image data set, in which each element is the decimal gray-scale value of the pixel (0–255), is produced. Finally each decimal value is converted to a binary equivalent number and in the end a one-dimensional matrix B is produced.
Step 2: The matrix A which is a binary sequence produced by the chaotic TRBG, with the procedure that is described in Section 3, and the above mentioned matrix B produces a third one-dimensional matrix C by using the XOR function: $C=A\oplus B$.
Step 3: The produced in the previous step matrix C is converted to the encrypted image by the inverse process of step 1.

If somebody wants to decrypt the image the XOR function must be applied again ($C\oplus B=A$). In Fig. 7 the plain gray-scale image of "Lenna" (size 131×131), the encrypted and the decrypted image which are produced with the above scheme is shown.

6. Security analysis

As it known a good encryption scheme should be robust against all kinds of statistical, cryptanalytic and brute-force attacks. Thus, in this work security analysis on the proposed image encryption scheme, such as histogram analysis, correlation of two adjacent pixels, differential analysis and information entropy, is presented.

6.1. Histogram analysis

In 1949 Shannon [39] suggested two methods in order to prevent the statistical attacks, the diffusion and confusion. The histograms of the plain (Lenna) and the encrypted images, which are obtained by the proposed method, are shown in Fig. 8. Comparing the histograms we can see a uniform distribution of gray-scale values of the encrypted image, which testify the toughness of the method over any

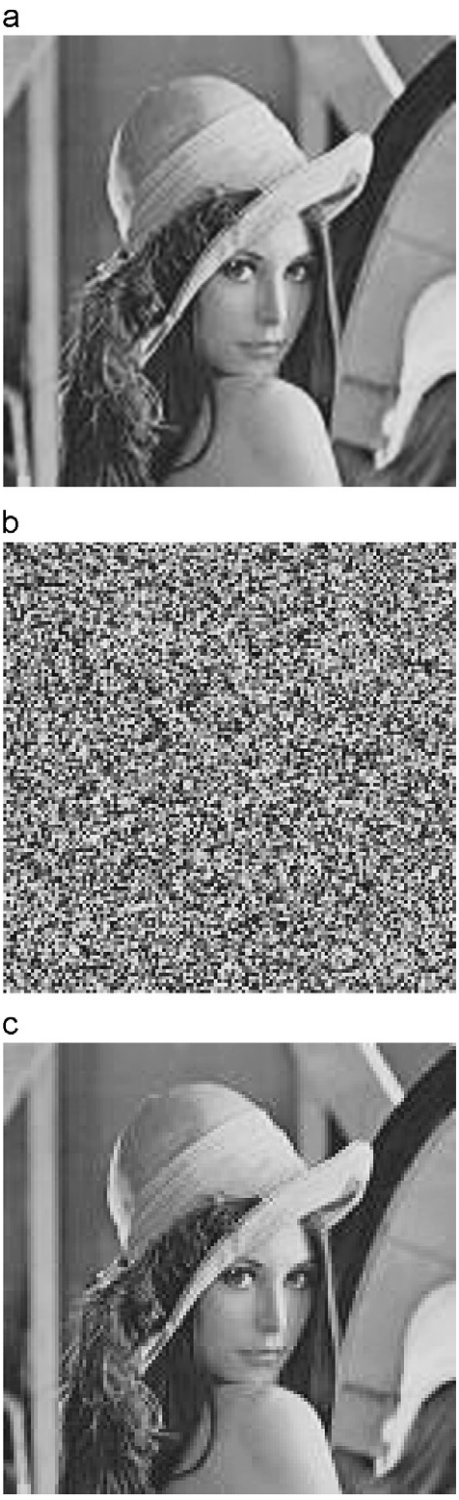

Fig. 7. (a) The plain image, (b) the encrypted image and (c) the decrypted image.

statistical attack, instead of the histogram of the plain image, which has a discrete form. So, the encrypted image is secure with this encryption scheme from any statistical attack.

6.2. Correlation of two adjacent pixels

Each pixel of any image has a high correlation with its adjacent pixels either in horizontal, vertical or diagonal directions. For testing the correlation in a plain and encrypted image respectively, the correlation coefficient γ [16] of each pair of pixels by using the following formulas was calculated:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2 \tag{10}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)] \tag{11}$$

$$\gamma(x,y) = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{12}$$

In Eqs. (9)–(12) x and y are the gray values of two adjacent pixels in the image and N is the total number of adjacent pairs of pixels. Figs. 9–11 show the correlations of two horizontal, vertical and diagonal pixels in the plain and the encrypted image respectively. Also, Table 3 presents the correlation coefficient of the encrypted image, which has been decreased significantly, in regard to the correlation coefficient of the plain image. It is obvious that the correlation coefficient of the encrypted image in any direction is approximately equal to zero, so the correlated relationship is very low.

6.3. Differential analysis

The differential attack is one of the most famous attacks in the encrypted image. This method is based on a slightly change (modify one pixel) in the encrypted image and the result is observed. With this technique somebody can find a relationship between the encrypted and plain image. So, if a minor change in the plain image can cause a significant change in the encrypted image, then the differential attack would become practically useless.

The strength of the proposed encryption method against the differential attach is examined by changing one pixel in the plain image and two common numbers: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) [17], are calculated. Therefore, if $A(i, j)$ and $B(i, j)$ are the pixels in row-i and column-j of the encrypted images A and B, with only one pixel difference between the respective plain images, then the NPCR is calculated by the following formula:

$$NPCR(A,B) = \frac{\sum_{i,j} D(i,j)}{N}\cdot 100\% \tag{13}$$

where N is the total number of pixels and $D(i, j)$ is the matrix produced by the formula:

$$D(i,j) = \begin{cases} 1 & \text{if } A(i,j) \neq B(i,j) \\ 0 & \text{if } A(i,j) = B(i,j) \end{cases} \tag{14}$$

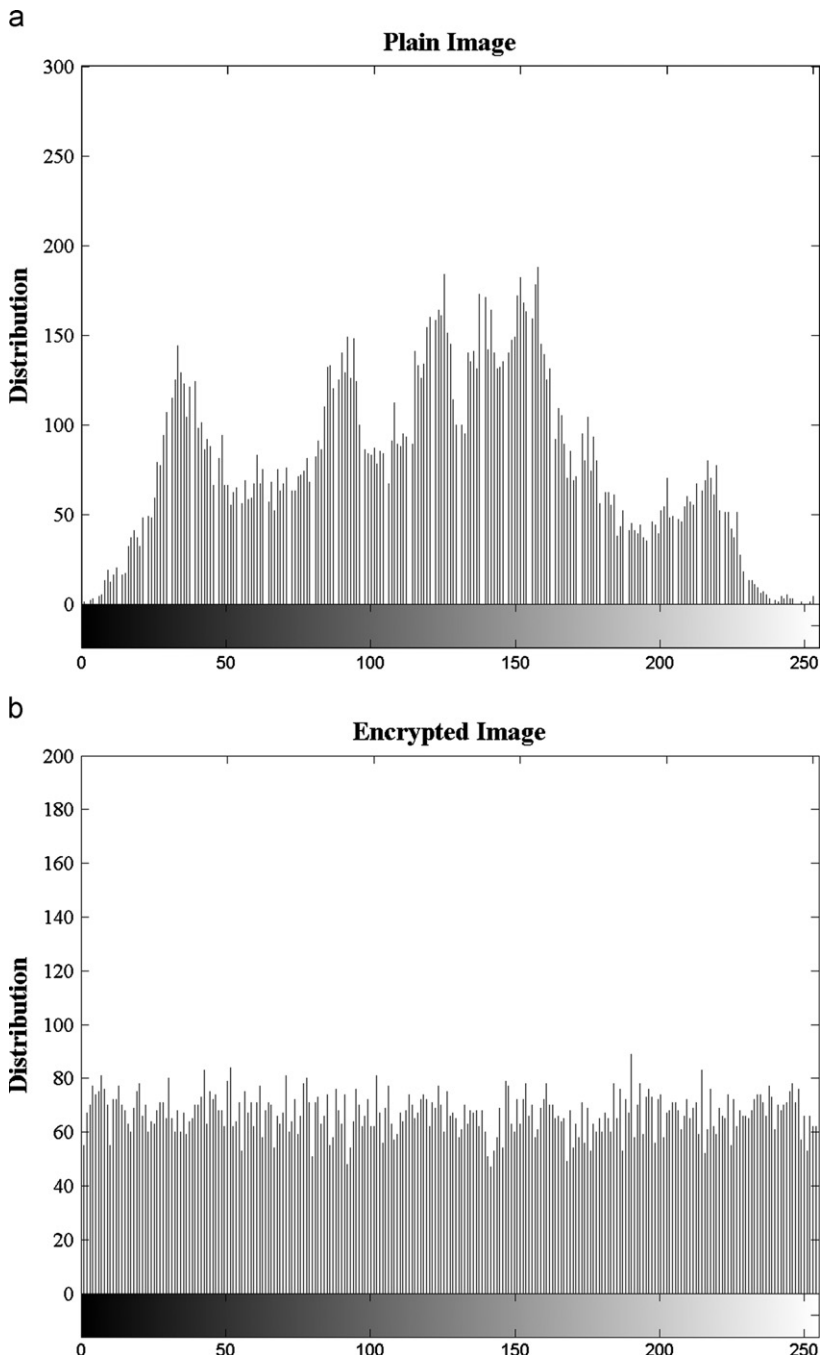

Fig. 8. Histograms of (a) the plain and (b) the encrypted image.

For two random selected images the NPCR is $NPCR = (1-2^L)\times 100\%$, where L is the number of bits used for representing the pixels of an image. So, for a gray-scale image (8 bit/pixel), the NPCR is equal to 99.6093785%.

The second number (UACI) measures the average intensity of differences between the plain image and the encrypted image, calculated by the following formula:

$$UACI(A,B) = \frac{1}{N}\left(\sum_{i,j}\frac{|A(i,j)-B(i,j)|}{2^L-1}\right)\cdot 100\% \tag{15}$$

The expected value of UACI for two random selected images is

$$UACI = \frac{\sum_{i-1}^{2^L-1} i\cdot(i+1)}{2^L\cdot\left(2^L-1\right)} \tag{16}$$

So, for a gray scale image the UACL is equal to 33.46354%.

Therefore, the values of these two numbers show that the encryption scheme is very weak to a differential attack. To improve this weakness of the proposed scheme

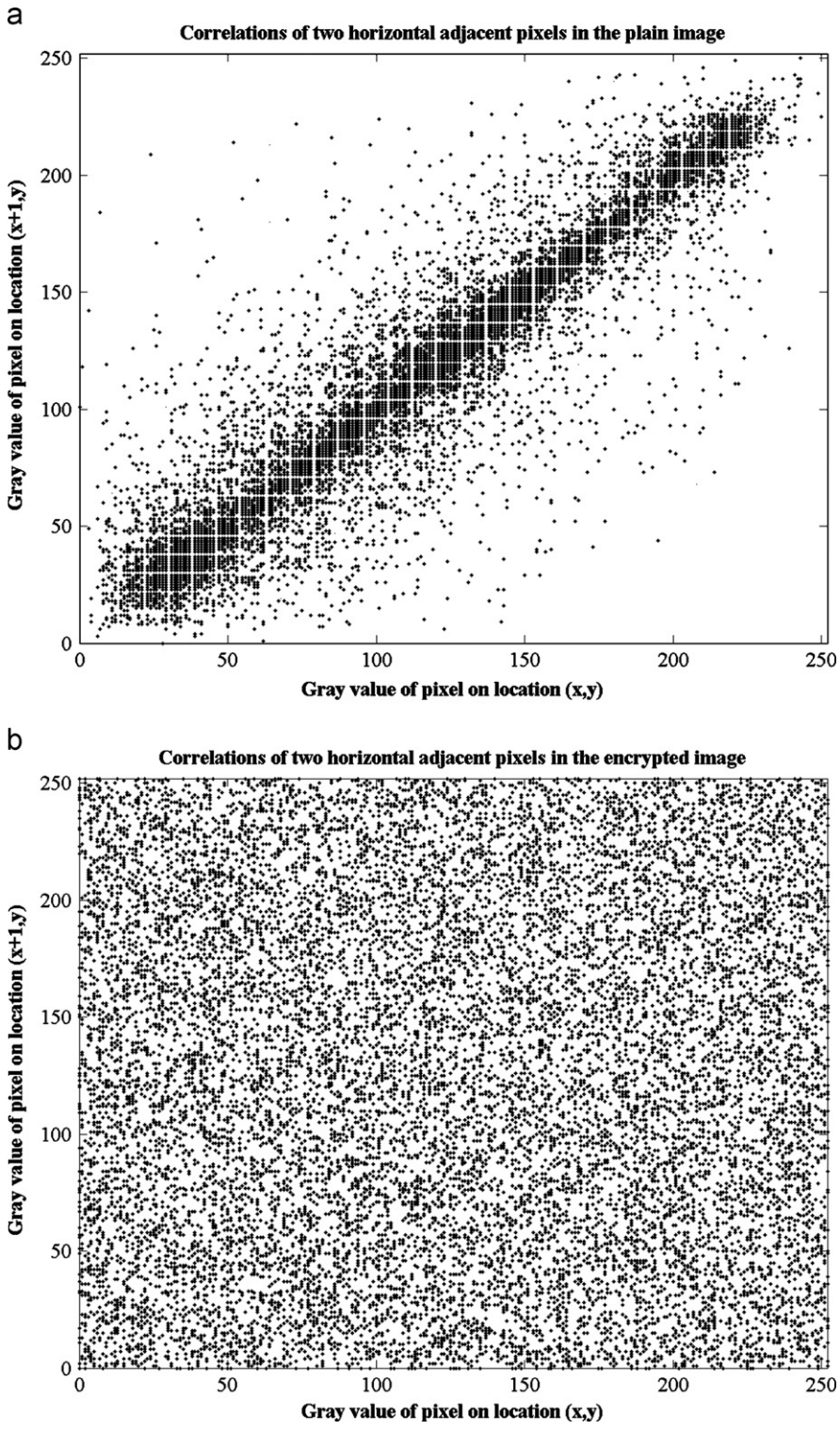

Fig. 9. Correlation analysis of two horizontal adjacent pixels (a) in the plain and (b) the encrypted image.

the encryption process in more than one round is evaluated. The NPCR and UACI at two different rounds of encryption process are calculated and listed in Table 4. In each round the bitstream is shifted only one bit. Table 4 shows that the performance is very satisfactory after only two rounds of encryption while the values of NPCR and UACI have the tendency to be equal to the calculated values of random selected images.

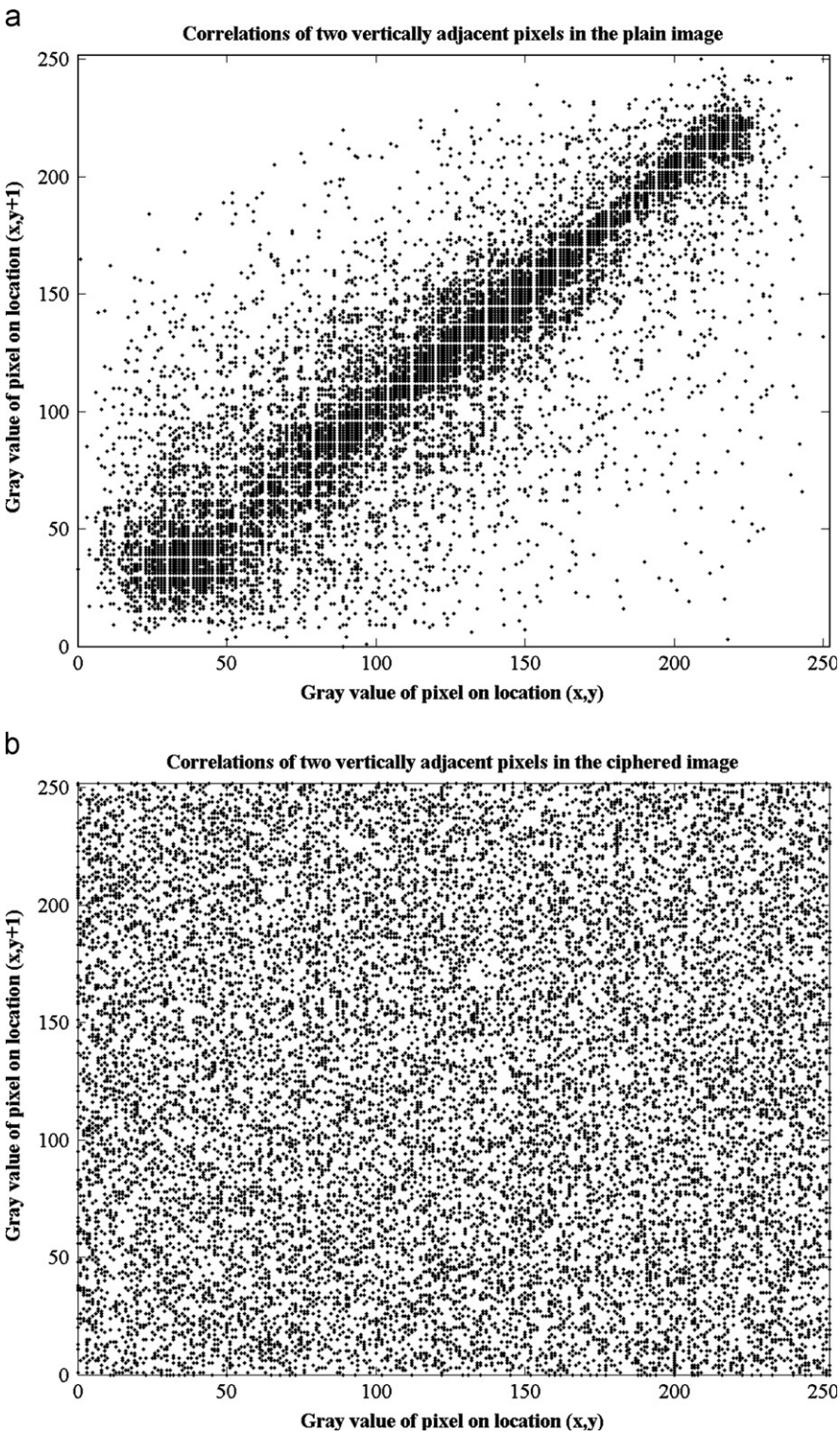

Fig. 10. Correlation analysis of two vertical adjacent pixels (a) in the plain and (b) the encrypted image.

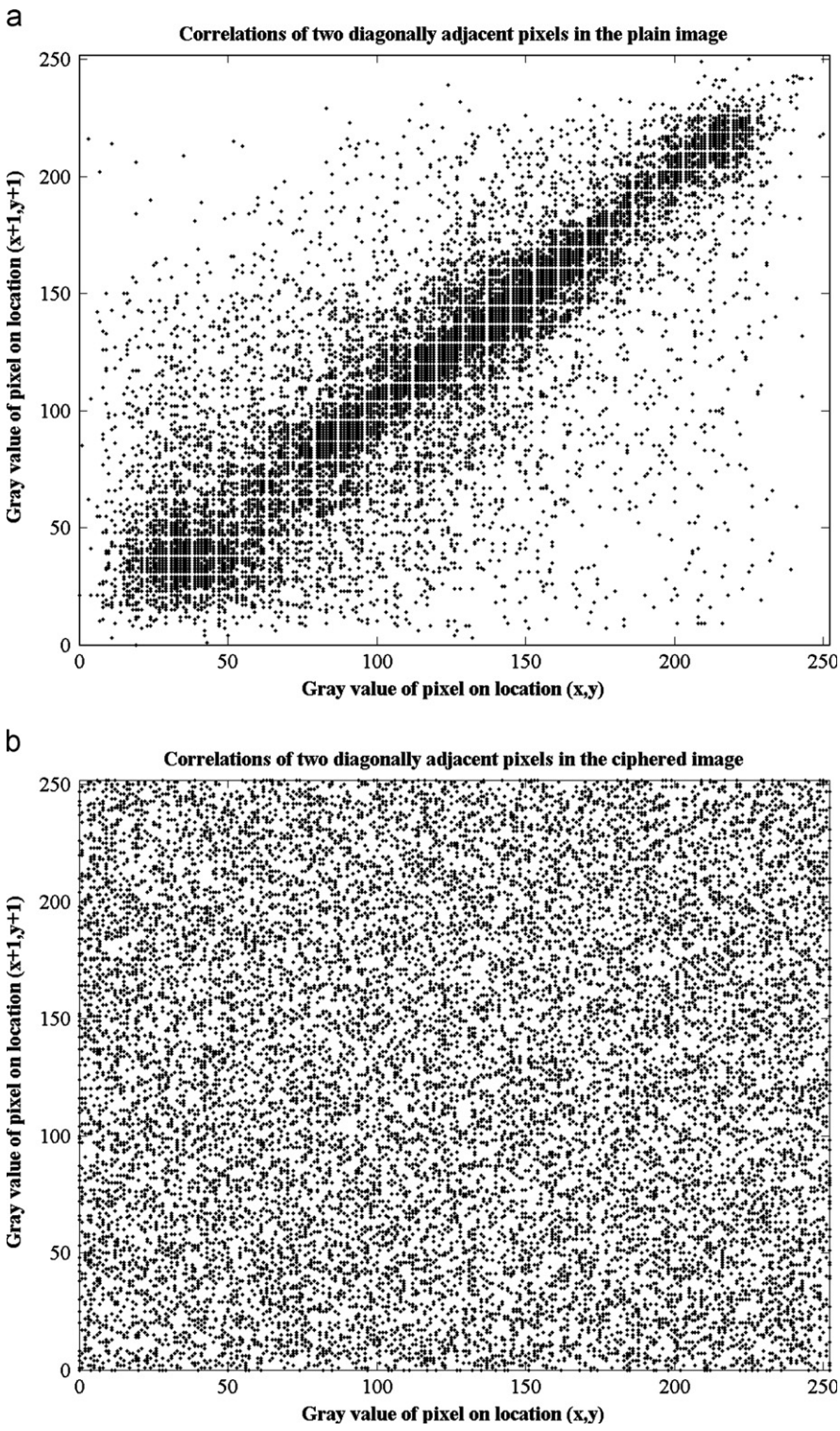

Fig. 11. Correlation analysis of two diagonal adjacent pixels (a) in the plain and (b) the encrypted image.

Table 3
Correlation coefficients of two adjacent pixels in the plain and encrypted image.

	Plain image	Encrypted image
Horizontal	0.9376	0.0047
Vertical	0.8714	−0.0016
Diagonal	0.8359	−0.0069

Table 4
NPCR and UACI of two encrypted plain images at two different rounds.

Round	**1**	**2**
NPCR (%)	0.0117	99.5863
UACI (%)	0.0021	33.4035

6.4. Information entropy

The entropy of a source is calculated by the formula:

$$H(S) = -\sum_{i=0}^{N-1} p(s_i)\cdot \log_2 p(s_i) \quad (17)$$

where $p(s_i)$ is the possibility of appearance of the symbol s_i.

The information entropy of an image presents the distribution of the gray-scale values (0–255). As much uniform the distribution is so much bigger the information entropy is. Our calculations shown that the information entropy of the plain image is equal to 7.4620, while the information entropy of the encrypted image is higher, 7.9612. Due to the fact that the information entropy of the encrypted image is increased, we have come to the conclusion that the proposed encryption method is safe from an entropy attack.

7. Conclusion

In this work a novel encryption scheme based on a true random bits generator was presented. The main element of this TRBG was two mutually coupled identical nonlinear circuits which show the phenomenon of coexistence of two different synchronization phenomena. The first of these was the complete chaotic synchronization while the second one was the inverse π-lag synchronization. The private keys of the proposed cryptographic scheme were the initial conditions of the coupled system and the values of the circuit's parameters.

The bitstream, which is produced by the proposed TRBG, is used to encrypt a gray-scale image by using the XOR function. Statistical analysis confirmed the robustness of the encryption process against various known statistical attacks.

So, in this paper the great sensitivity of nonlinear systems on the initial conditions and the variations of the parameters were used to encrypt an image. For this reason an intruder, who does not know the nonlinear system, or system's variables, or initial values of the system, is not in the position to achieve the encryption for recovering the original plain image. In order to show this characteristic, the set of the initial conditions of the proposed TRBG, ($x01=0.4$, $y01=0.3$ and $z01=0.2$, $x02=0.2$, $y02=0.4$ and $z02=0.1$) has been changed and the failure of recovering the plain image by the intruder is presented in Fig. 12.

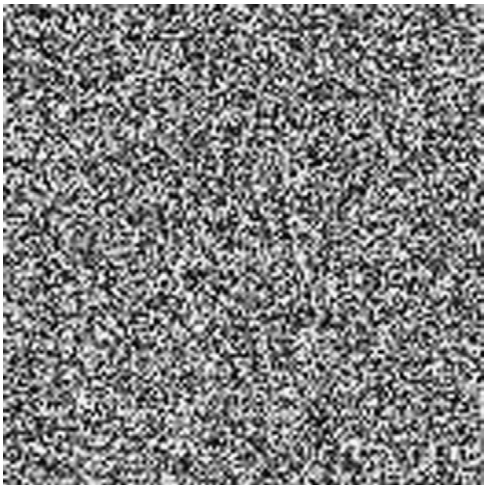

Fig. 12. The recovered image by an intruder.

Finally, the great advantage of this encryption scheme, in comparison to other similar works, is the use of a sixth order nonlinear dynamical system in the design of a chaotic TRBG. For the first time such a high order dynamical system, which is also very easy to be implemented in hardware, is used with very satisfactory results. Furthermore, the circuit's implementation of this system and the confirmation of the encryption process's results are the future challenges.

References

[1] M.M. Yeung, S. Pankanti, Verification cryptosystems: issues and challenges, Journal of Electronic Imaging 9 (2000) 468–476.
[2] V. Fotopoulos, M.L. Stavrinou, A.N. Skodras, Medical image authentication and self-correction through an adaptive reversible watermarking technique, in: Eighth IEEE International Conference on Bioinformatics and Bioengineering, vols. 1–2, 2008, pp. 910–914.
[3] I. Kostopoulos, S.A.M. Gilani, A.N. Skodras, Colour image authentication based on a self-embedding technique, in: Fourteenth International Conference on Digital Signal Processing, vol. 2, 2002, pp. 733–736.
[4] C. Deng, X. Gao, X. Li, D. Tao, Local histogram based geometric invariant image watermarking, Signal Processing 90 (2010) 3256–3264.
[5] S. Rawat, B. Raman, A Blind, Watermarking algorithm based on fractional Fourier transform and visual cryptography, Signal Processing 92 (2012) 1480–1491.
[6] L. Zhang, X. Liao, X. Wang, An image encryption approach based on chaotic maps, Chaos, Solitons & Fractals 24 (2005) 759–765.
[7] S.M. Seyedzadeh, S. Mirzakuchaki, A. Fast, Color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Processing 92 (2012) 1202–1215.
[8] X. Tong, M. Cui, Image encryption scheme based on 3d baker with dynamical compound chaotic sequence cipher generator, Signal Processing 89 (2009) 480–491.
[9] X. Wang, L. Teng, X. Qin, A Novel, Colour image encryption algorithm based on chaos, Signal Processing 92 (2012) 1101–1108.
[10] X. Liao, S. Lai, Q. Zhou, A Novel Image, Encryption algorithm based on self-adaptive wave transmission, Signal Processing 90 (2010) 2714–2722.
[11] T.-H. Chen, C.-S. Wu, Efficient multi-secret image sharing based on Boolean operations, Signal Processing 91 (2011) 90–97.

[12] L. Kocarev, G. Jakimoski, T. Stojanovski, U. and Parlitz, From chaotic maps to encryption schemes, in: IEEE International Symposium on Circuits and Systems, Monterey, 1998.
[13] R. Matthews, One the derivation of a chaotic encryption algorithm, Cryptologia 8 (1989) 29–42.
[14] J.C. Yen, J.I. Guo, A New Key-based Design for image encryption and decryption, in: IEEE Conference on Circuits and Systems, vol. 4, 2000, pp. 49–52.
[15] C.C. Chang, M.S. Hwang, T.S. Chen, A New, Encryption algorithm for image cryptosystems, Journal of Systems and Software 58 (2001) 83–91.
[16] G.R. Chen, Y. Mao, C. Chui, A symmetric image encryption scheme based on 3d chaotic cat map, Chaos, Solitons & Fractals 21 (2004) 749–761.
[17] G.R. Chen, Y. Mao, C Chui, A Symmetric image encryption scheme based on chaotic maps with finite precision representation, Chaos, Solitons & Fractals 32 (2007) 1518–1529.
[18] Y. Mao, G. Chen, S. Lian, A Novel Fast, Image encryption scheme based on 3D chaotic baker maps, International Journal of Bifurcation and Chaos in Applied Sciences and Engineering 14 (2004) 3613–3624.
[19] T. Shu, Uniform Random Numbers: Theory and Practice, Kluwer Academic Publishers, 1995.
[20] M. Guide, Concept for a high-performance random number generator based on physical random phenomena, Frequenz 39 (1985) 187–190.
[21] W.T. Holman, J.S. Connelly, A.B. Downlatabadi, An integrated analog-digital random noise source, IEEE Transactions on Circuits and Systems I 44 (1997) 521–528.
[22] R.C. Fairfield, R.L. Mortenson, K.B. Coulthart, An LSI random number generator (RNG), in: Advances in Cryptology, Lecture Notes in Computer Science, vol. 0196, Springer-Verlag, 1987, pp. 203–230.
[23] D. Davis, R. Ihaka, P. Fenstermacher, Cryptographic randomness from air turbulence in disk drives, in: Advances in Cryptology, Lecture Notes in Computer Science, vol. 0839, Springer-Verlag, 1994, pp.114–120.
[24] G.B. Agnew, Random sources from cryptographic systems, in: Advances in Cryptology-CRYPTO'85, Springer-Verlag, New York, 1986, pp.77–81.
[25] Y. Hu, X. Liao, K. Wong, Q. Zhou, A True, Random number generator based on mouse movement and chaotic cryptography,, Chaos Soliton & Fractals 40 (2009) 2286–2293.
[26] N.G. Bardis, A.P. Markovskyi, N. Doukas, N.V. Karadimas, True random number generation based on environmental noise measurements for military applications, in: 8th WSEAS International Conference on Signal Processing, Robotics and Automation, Cambridge, UK, 2009, pp. 68–73.
[27] Ch.K. Volos, I.M. Kyprianidis, I.N. Stouboulos, Anti-phase and inverse π-lag synchronization in coupled duffing-type circuits, International Journal of Bifurcation and Chaos 21 (2011) 2357–2368.
[28] K. Ch., I.M. Volos, I.N. Kyprianidis, Stouboulos, various synchronization phenomena in bidirectionally coupled double scroll circuits, Communications in Nonlinear Science and Numerical Simulation 16 (2011) 3356–3366.
[29] B Hasselblatt, A. Katok, A First Course , in Dynamics: With a Panorama of Recent Developments, University Press, Cambridge, 2003.
[30] L.M Pecora, T.L. Carroll, Synchronization in chaotic systems, Physical Review Letters 64 (1990) 821–824.
[31] K. Ch, I.M. Volos, I.N. Kyprianidis, A.N. Stouboulos, Anagnostopoulos, experimental study of the dynamic behavior of a double scroll circuit, Journal of Applied Functional Analysis 4 (2009) 703–711.
[32] L. Pivka, C.W. Wu, A. Huang, Chua's oscillator: a compendium of chaotic phenomena, Journal of the Franklin Institute 331 (1994) 705–741.
[33] Y.H. Ku, X. Sun, On Nonlinear Systems–Chaos, Journal of the Franklin Institute 326 (1989) 93–107.
[34] A. Wolf, J. Swift, H. Swinney, J. Vastano, Determining Lyapunov exponents from a time series, Physica D-Nonlinear Phenomena 16 (1985) 285–317.
[35] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
[36] J. Von Neumann, Various techniques used in connection with random digits, in: G.E. Forsythe (Eds.), Applied Mathematics Series, National Bureau of Standards, vol. 12, 1951, pp. 36–38.
[37] NIST, Security Requirements for Cryptographic Modules, FIPS PUB 140-2, 2001, 〈http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf〉.
[38] A.M. Fraser, Information and entropy in strange attractors, IEEE Transactions on Information Theory 35 (1989) 245–262.
[39] C.E. Shannon, Communication theory of secrecy system, Journal of Bell Systems Technology 28 (1949) 656–715.