Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 123-149
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

# Image Encryption Scheme Based on Coupled Chaotic Systems

**Christos K. Volos**[1]

## Abstract

Nowadays, military operations require security in the transmission of information, which provides a significant strategic advantage. In addition, nonlinear systems which show chaotic behavior are governed by some useful features including among others random-like and complex dynamics, high sensitivity on initial conditions and system's parameters. So, in this paper, an image encryption scheme based on a chaotic true random bits generator is proposed. The chaotic generator consists of a system of two mutually coupled identical nonlinear circuits each of which produces double scroll chaotic attractors. The values of the system's parameters and initial conditions are the keys of the cryptographic scheme. Since the dynamic behavior of the coupled system is so unpredictable, a coexistence of two different types of synchronization (complete and inverse $\pi$-lag synchronization) are used for representing the states "0" and "1" respectively. A well-known statistical suite FIPS-140-2 is adopted to test the distribution of the bits sequence. The produced bits sequence is used to encrypt and decrypt images. Finally, the

[1] Department of Mathematics and Engineering Studies, Hellenic Army Academy, Athens, GR-16673, Greece, e-mail: chvolos@gmail.com

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
*Published online* : March 30, 2013

security analysis of the encrypted image demonstrates the high security of the proposed scheme.

**Mathematics Subject Classification:** 94A60
**Keywords:** True random bits generator; chaos; complete synchronization; inverse $\pi$-lag synchronization; nonlinear circuit; image encryption

# 1 Introduction

In the last decades, the confidentiality of digital image information is an essential feature of the digital era especially after the rapid development of Internet technology. Nevertheless in many cases, image data, such as online personal photographs, images of medical systems, images of electronic publishing and fingerprint images from authentication systems must not be public. Also, images for military use such as drawings of military establishment, photographs which are produced by satellites or from military missions, must be also kept private for enemy's attacks. Therefore, reliable, fast and secure communication systems are needed in order to transmit digital images or photographs.

Digital images, as it is known from the bibliography, have some very important features such as, bulk data capacity, strong correlation among adjacent pixels, redundancy of data, being less sensitive compared to the text data and existence of patterns and backgrounds. So, concerning the above mentioned 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. Nowadays, the position permutation, which is used in a great number of conventional image encryption algorithms, has the advantage of fast encryption speed. However, the security of these methods depends on the security of the algorithm, which does not satisfy the basic requirement of a modern encryption scheme.

So, for overcoming the previous mentioned problem, many research groups have proposed two major approaches that are used to protect digital images from attackers. The first one is the information hiding, such as digital watermarking of an image [1-3], while the second one is the encryption, which includes conventional encryption techniques and others such as chaotic encryption [4-7].

Additionally, the rapid development of nonlinear dynamics and especially of chaotic systems leads many researchers to realize, that chaotic systems can be used in cryptosystems [8]. This happens because cryptography and chaos have some very important common features such as the ergodicity, the topological transitivity and the sensitivity on initial conditions and system's parameters. However, despite the similarities conventional cryptographic algorithms and chaos-based cryptosystems have a major difference. Chaotic cryptosystems which are relied on the complex dynamics of nonlinear systems are deterministic.

Until now, many image encryption schemes based on chaotic systems have been proposed [9-14]. The most of these were chaotic key-based algorithms based on various types of known chaotic maps, like Cat or Baker map.

Additionally in the last decade a great number of random number generators used for the security of cryptographic systems have been designed. As it is known, random number generators can be classified into three types: True Random Number Generators (TRNGs), Pseudo-Random Number Generators (PRNGs) and Hybrid Random Number Generators (HRNGs) [15]. This classification is mainly based on the source of randomness. The TRNGs, which are the most interesting case of random number generators, take advantage of nondeterministic sources, that come from an unpredictable natural process in a physical or hardware device that can output a sequence of statistically independent data [16-22].

In this paper, a new scheme of efficient and practical chaotic image encryption process is proposed. In details, this work presents the encryption of a gray-scale image via a new proposed chaotic TRBG, which is based on the interaction between two mutually coupled identical nonlinear circuits [23,24]. As it has been reported, in some cases of coupled systems the phenomenon of the coexistence of two different synchronization phenomena, the well-known complete chaotic synchronization and the inverse $\pi$-lag synchronization was observed. The binary sequence, which is generated from the proposed chaotic TRBG, is applied to encrypt the gray-scale image by using the XOR function.

So, in Section 2 the definition of a chaotic system and the synchronization phenomena, which are used, are presented in details. Section 3 introduces the chaotic TRBG. In Section 4 the results of the use, in the proposed chaotic TRBG, of the well known statistical tests suite (FIPS-140-2), are presented. Section 5 demonstrates the encryption and decryption process of gray-scale images such as satellite photographs for military use via the chaotic sequence obtained from the proposed TRBG. In Section 6 the necessary security analysis of the proposed chaotic image encryption scheme, is presented. Finally, conclusion remarks are drawn in the last Section.

## 2 Chaotic Systems

The basic component of the proposed encryption scheme is a chaotic system. So, a dynamical system in order to be considered as chaotic must fulfil the three following conditions [25]:

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

Firstly, the term topologically mixing means that the chaotic trajectory at the phase space will move over time so that each designated area of this trajectory will eventually cover part of any particular region. The second feature of chaotic systems is that its periodic orbits have to be dense, which means that, the trajectory of a dynamical system is dense, if it comes arbitrarily close to any point in the domain. Finally, the third and probably the most important feature of chaotic systems, is the sensitivity on initial conditions. This means that a small variation on a system's initial conditions will produce a totally different chaotic trajectory.

As it is mentioned, this paper presents the use of coupled continuous-time chaotic systems for generating true random bits sequences in image encryption process. The phenomenon of interaction between coupled chaotic systems was a landmark in the evolution of the chaotic synchronization's theory [26]. Regardless of the fact that many synchronization types have been proposed until now, the most well-studied 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.

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

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

In 2010 a new synchronization phenomenon has been presented [23,24]. This new type of synchronization, which is called *inverse $\pi$-lag synchronization*, is observed between two mutually coupled identical chaotic systems, with a specific type of symmetry. In this type of synchronization each one of the coupled chaotic systems has symmetry under the transformation,

$$S : (x, y, z) \quad \to \quad (-x, -y, -z). \tag{2}$$

Also in this type of synchronization 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 $x_2$ of each coupled system) with a time lag $\tau$, which is equal to $T/2$, where $T$ is the period of the signals $x_1$ and $x_2$.

$$x_1(t) = -x_2(t + \tau), \quad \tau = T/2 \tag{3}$$

So, in this type of chaotic systems the inverse $\pi$-lag synchronization coexists with a complete synchronization depending on the coupling factor and the chosen set of system's initial conditions [24]. Therefore, the proposed chaotic 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 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 basically of three blocks (Figure 1). The first of these blocks ($S_1$) includes the mutually coupled chaotic system, which are necessary in this TRBG. This system is based on a nonlinear chaotic circuit which demonstrates the phenomenon of inverse $\pi$-lag synchronization [24, 27]. So, in this work the most well-known nonlinear circuit, the Chua oscillator (Figure 2(a)), is chosen.

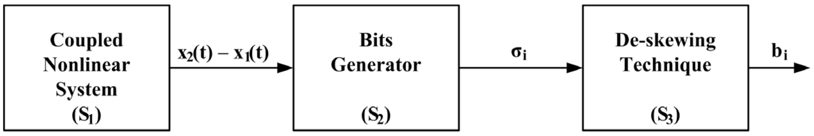
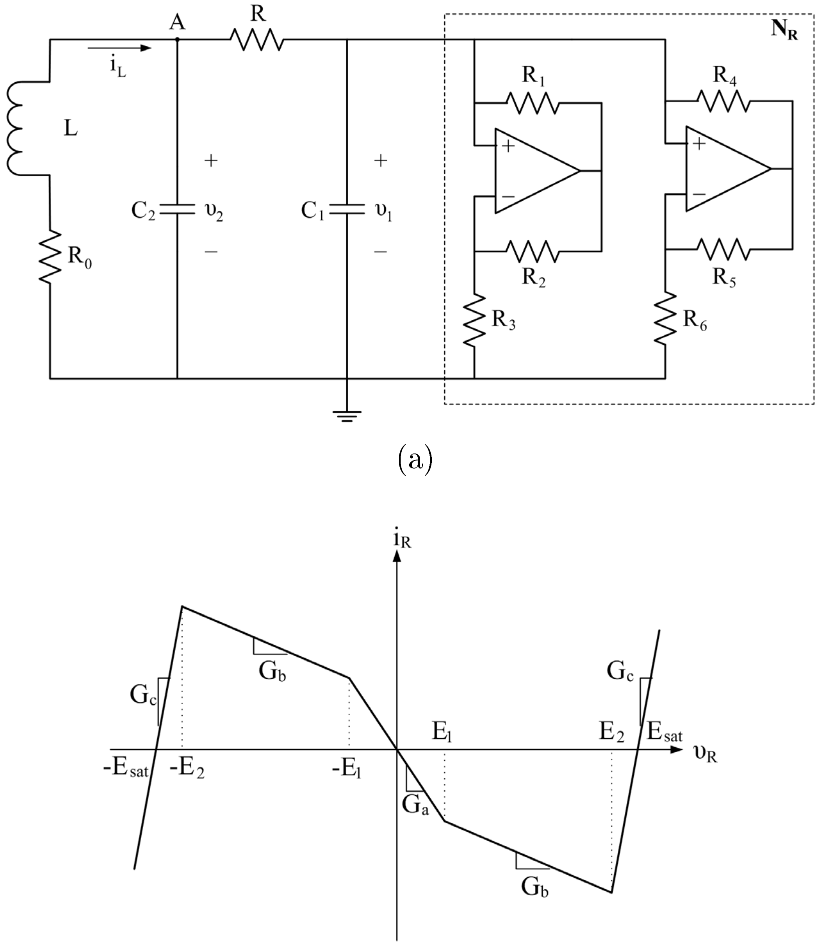


Figure 1: The chaotic true random bits generator scheme



(a)

(b)

Figure 2: (a) Scheme of the circuit of Chua's oscillator and (b) the five segment picewise linear i - $\upsilon$ characteristic

Chua oscillator, which has been used, compines its simple structure with the appearance of a great number of chaotic and non-chaotic attractors. This makes the circuit of Chua oscillator, a system often used to demonstrate experimentally, theoretically and numerically many properties and phenomena proper for chaotic oscillators, such as the appearance of double-scroll chaotic attractors. As it known, a great number of systems, which produce double-scroll chaotic attractors, such as Chua's [28] or Lorenz's [29] have been studied. The common characteristic of all these systems is the existence 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.

As it is mentioned, the first block ($S_1$) of the proposed TRBG includes a system of two mutually coupled identical Chua oscillators. The mutual coupling, between these two identical Nonlinear Circuits (NC), is achieved via a linear resistor $R_C$ connected between the nodes A of each circuit (Figure 3). The dimensionless differential equations (4)-(9) that describe the coupled system dynamics are [30,31]:

$$\begin{aligned}
\frac{dx_1}{d\tau} &= \alpha\left[y_1 - x_1 - f(x_1)\right] && (4)\\
\frac{dy_1}{d\tau} &= x_1 - y_1 + z_1 + \xi\left(y_2 - y_1\right) && (5)\\
\frac{dz_1}{d\tau} &= -\beta y_1 - \gamma z_1 - p && (6)\\
\frac{dx_2}{d\tau} &= \alpha\left[y_2 - x_2 - f(x_2)\right] && (7)\\
\frac{dy_2}{d\tau} &= x_2 - y_2 + z_2 + \xi\left(y_1 - y_2\right) && (8)\\
\frac{dz_2}{d\tau} &= -\beta y_2 - \gamma z_2 && (9)
\end{aligned}$$

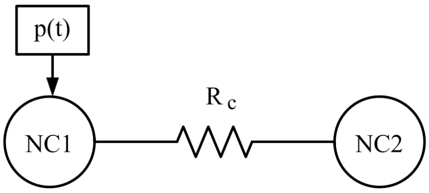


Figure 3: The system of two mutually coupled nonlinear circuits via a linear resistor

In this system, the first three equations describe the first of the two coupled Chua oscillators (NC1), while the other three describe the second one (NC2). The state parameters $x_{1,2} = v_1/E_1$ and $y_{1,2} = v_2/E_2$ represent the voltages at the capacitors $C_1$ and $C_2$ while $z_{1,2} = i_L R/E_1$ is the current through the inductor $L$, as shown in Figure 2(a). The dimensionless time $\tau$ is $\tau = t/RC_2$ and the normalized parameters $\alpha$, $\beta$ and $\gamma$ are: $\alpha = C_2/C_1$, $\beta = R^2C_2/L$ and $\gamma = RR_0C_2/L$ respectively.

The dimensionless form of the nonlinear function $f(x)$ (Figure 2(b)) is given by the following equation:

$$\begin{aligned} f(x) &= m_c x + 0.5\,(m_a - m_b)\,(|x+1| - |x-1|) + \\ &\quad +0.5\,(m_b - m_c)\,(|x + E_2/E_1| - |x - E_2/E_1|) \end{aligned} \tag{10}$$

where, $m_a = RG_a$, $m_b = RG_b$ and $m_c = RG_c$. Also, the slopes $G_a$, $G_b$, $G_c$ and the breakpoints $E_{1,2}$ of the five segment nonlinearity are given by:

$$G_a = -\frac{1}{R_3} - \frac{1}{R_6} \tag{11}$$

$$G_b = \frac{1}{R_1} - \frac{1}{R_6} \tag{12}$$

$$G_c = \frac{1}{R_1} + \frac{1}{R_4} \tag{13}$$

$$E_1 = \frac{R_3}{R_2 + R_3} E_{sat} \tag{14}$$

$$E_2 = \frac{R_6}{R_5 + R_6} E_{sat} \tag{15}$$

The values of the coupled Chua's oscillators parameters are chosen so that each coupled circuit demonstrates double-scroll chaotic attractors: $L = 18mH$, $C_1 = 10nF$, $C_2 = 100nF$, $G = 1/R = 555\mu S$, $R_0 = 12.5\Omega$, $R_1 = R_2 = 22k\Omega$, $R_3 = 3.3k\Omega$, $R_4 = R_5 = 220\Omega$, $R_6 = 2.2k\Omega$. Consequently, $\alpha = 10$, $\beta = 18$ and $\gamma = 0.125$. Also, the operational amplifiers were of the type LF411 and the voltages of the positive and negative power supplies were set $\pm 15V$.

In system's equations $\xi$ is the coupling coefficient, where $\xi = R/R_C$ and it is present in the equations of both circuits, since the coupling between them is bidirectional. In order to show the coexistence of the two previous mentioned synchronization phenomena (complete synchronization and inverse $\pi$-lag synchronization) the coupling coefficient $\xi$ of the system is adjusted to be equal to 14.

Furthermore, the necessary perturbation for changing the system's initial conditions and consequently the synchronization state of the coupled system is the function $p$ in the third equation of the dimensionless system, which is an external source that produces a pulse train of amplitude 1V and having a duty cycle of 4%. So, the pulse duration is 2ms, while the period of the pulse train is 50ms.

The operation of the first block ($S_1$) of the proposed TRBG is described in detail below: This block produces the synchronization signal $[x_2(t) - x_1(t)]$ of the coupled system which varies between the two synchronization modes (complete synchronization and inverse $\pi$-lag synchronization) depending of the coupled system's initial conditions. In the complete synchronization mode, the signals $x_1(t)$ and $x_2(t)$ are identical and the synchronization signal $[x_2(t)-x_1(t)]$ is equal to zero. As a result, in the synchronization phase portrait of $x_2(t)$ versus $x_1(t)$ the trajectories remain strictly on the diagonal (Figure 4).

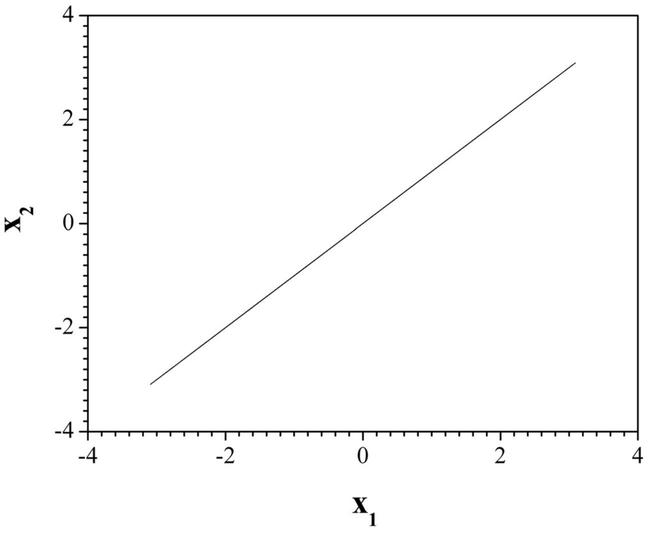


Figure 4: The phase portrait of $x_2(t)$ versus $x_1(t)$ in the case of complete synchronization

In the inverse $\pi$-lag synchronization mode, the signals $x_1(t)$ and $x_2(t)$ are inverse with a $\pi$ phase difference. So, the phase portrait of $x_2(t)$ versus $x_1(t)$ is a narrow closed loop (Figure 5).

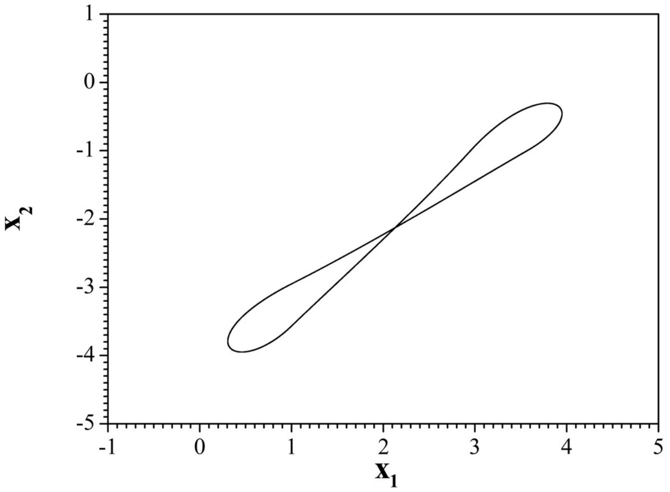
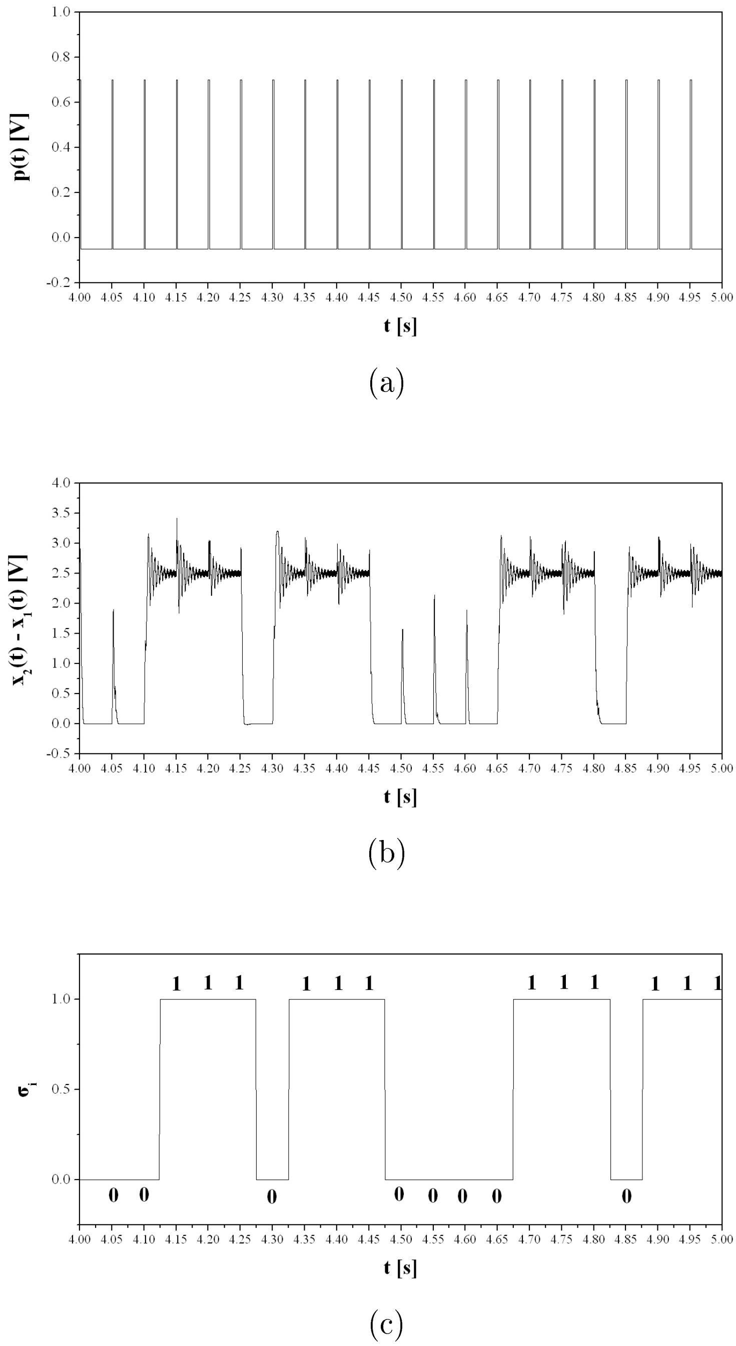


Figure 5: The phase portrait of $x_2(t)$ versus $x_1(t)$ in the case of inverse $\pi$-lag synchronization

The second block ($S_2$) of the proposed TRBG is responsible for the quantization of the two different levels of the synchronization signal $[x_2(t) - x_1(t)]$ into "0" and "1" according to the following procedure: $\sigma_i = 0$ if $x_2 - x_1 < 1V$ or $\sigma_i = 1$ if $x_2 - x_1 \geq 1V$.

This method is very easily implemented by using a comparator and a "sample and hold" circuit, which samples the synchronization signal $[x_2(t) - x_1(t)]$ produced by the first block ($S_1$). The sampling period equals the period of the pulse train ($T = 50ms$) and the sampling occurs at the middle of each pulse. Therefore, if the coupled system is in an inverse $\pi$-lag synchronization state a bit "1" is produced, while if the system is in a complete synchronization state a bit "0" is produced respectively. In Figure 6 the way of producing the chaotic bits sequence by the proposed TRBG is shown. In more details, Figure 6(a) shows the pulse train which is used in the proposed system. Also, the time-series of the synchronization signal $[x_2(t) - x_1(t)]$ and the produced bits sequence by the chaotic TRBG, are shown in Figures 6(b) and 6(c) respectively.



(a)

(b)

(c)

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

Furthermore, various techniques for the extraction of unbiased bits from a defective generator with unknown bias have been proposed. All these techniques are called de-skewing techniques, which their objective is to eliminate the correlation in the output of the natural sources of random bits. The first author who stated this problem was Von Neumann [32]. He proposed a digital post-processing that balances the distribution of bits by converting non-overlapping pairs of bits into output bits. This occurs by converting the bit pair "01"into an output "0", the bit pair "10" into an output "1", while the pairs "11" and "00" are discarded [32]. 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 (block $S_3$). However, this technique decreases throughput because of generating approximately 1 bit from 4 bits.

# 4 Statistical Tests of the TRBG

In this section one of the most important statistical test suites is used to check the "randomness" of the produced, by the proposed chaotic TRBG, bits sequence. This is FIPS (Federal Information Processing Standards) [33] of the National Institute of Standards and Technology (NIST). The results of the use of the four statistical tests, Monobit test, Poker test, Runs test, and Long run test, which are part of the FIPS-140-2 are presented in details. As it is known, according to FIPS statistical tests, the examined TRBG will produce a bitstream, $b_i = b_0, b_1, b_2, ..., b_{n-1}$, of length $n$ (at least 20000 bits), which 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.

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 |

Using the fact from the information theory that the noise has maximum entropy, the system's parameters ($\alpha = 10$, $\beta = 18$ and $\gamma = 0.125$) and initial conditions ($x_{01}$ = 0.8, $y_{01}$ = -0.2, $z_{01}$ = 0.4, $x_{02}$ = -0.5, $y_{02}$ = 0.1, $z_{02}$ = 0.2) are chosen such that the measured entropy of the TRBG is maximal.

For the above values of system's parameters and initial conditions the measure-theoretic entropy [34] of the proposed chaotic TRBG is calculated to be $H_n = 0.69307$ for $n = 3$ and $H_n = 0.69293$ for $n = 4$, where $n$ is the length of the $n$-word sequences. The measure-theoretic entropy is calculated by using the following equation.

$$H_n = \lim_{n \to \infty} \left( - \sum_{B^n} P(B^n)(lnP(B^n) \right) /n \tag{16}$$

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

By using the proposed chaotic TRBG, bits sequence of length 20000 bits has been obtained via a numerical integration of Eqs.(4)-(9), which is subjected to the four tests of FIPS-140-2 test suite. Table 2 presents the results, which verifies that the produced bits sequence passed the test suite of FIPS-140-2. It must be highlighted that the proposed approach with Chua oscillator presents better results concerning this test suite in regard to previous similar chaotic TRBG [35]. Specifically, the increase in measure-theoretic entropy, compared to other works, is due to use of a higher order nonlinear system, while the improvement of the results of FIPS-140-2 test suite are a consequence of the proposed chaotic TRBG's design and the appropriate choice of system's initial conditions and parameters.

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

| Monobit Test | Poker Test | Runs Test | Long Run Test |
|---|---|---|---|
| $N_1 = 10001$<br>50.005% | 2.2172 | $B_1 = 2568$<br>$B_2 = 1251$<br>$B_3 = 607$<br>$B_4 = 317$<br>$B_5 = 148$<br>$B_6 = 152$ | No |

## 5 The Encryption Scheme

For the aim of this work the proposed encryption scheme of gray-scale images, which has been implemented in MATLAB, is presented in details in this section. This encryption process is mainly based on XOR function as many other relative works. The encryption 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 Figure 7 the plain gray-scale image of a photograph which has been taken from a satellite (size $500 \times 308$), the encrypted and the decrypted image which are produced with the above scheme are shown.

# 6 Security Analysis

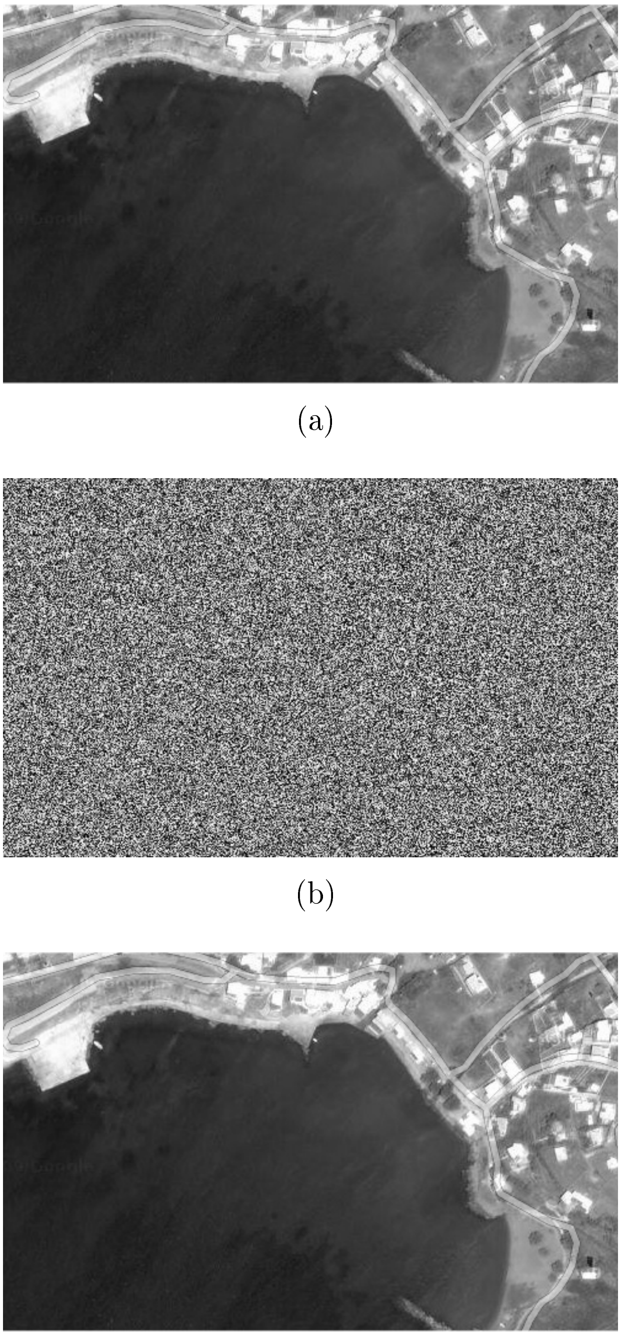
As it known a good encryption scheme should be robust against all kinds of statistical, cryptanalytic and brute-force attacks. Thus, in this work security analysis on the proposed image encryption scheme, such as histogram analysis, correlation of two adjacent pixels, differential analysis and information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

## 6.1 Histogram Analysis

In 1949 Shannon [36] suggested two methods in order to prevent the statistical attacks, the diffusion and confusion. The histograms of the plain and encrypted images, which are obtained by the proposed method, are shown in Figure 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 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 $\gamma$ [12] of each pair of pixels by using the following formulas was calculated.

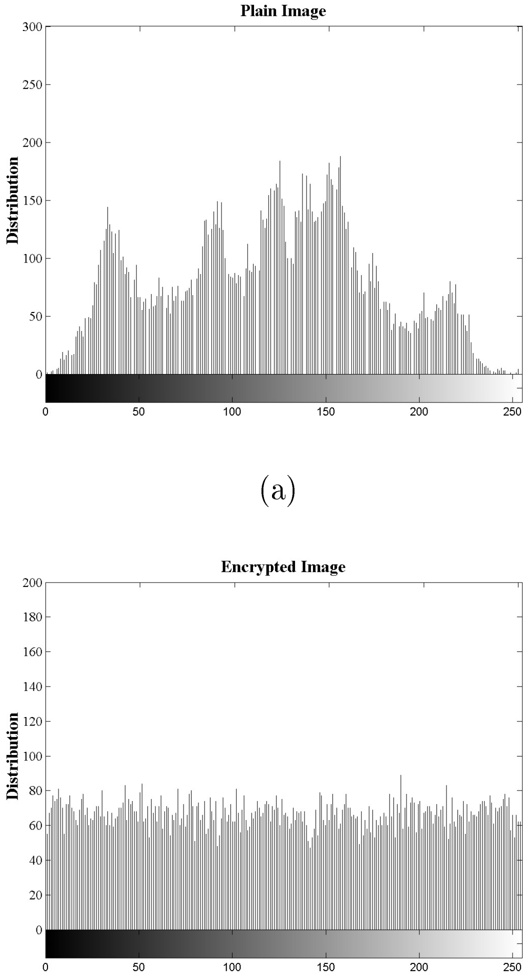


(a)

(b)

(c)

Figure 7: (a) The plain image, (b) the encrypted image and (c) the decrypted image



(a)

(b)

Figure 8: Histograms of (a) the plain and (b) the encrypted image

$$
\begin{aligned}
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i && (17)\\
D(x) &= \frac{1}{N}\sum_{i=1}^{N} \left[x_i - E(x)\right]^2 && (18)\\
cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N} \left[x_i - E(x)\right]\left[y_i - E(y)\right] && (19)\\
\gamma(x,y) &= \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} && (20)
\end{aligned}
$$

In equations (17)-(20) $x$ and $y$ are the gray values of two adjacent pixels in the image and $N$ is the total number of adjacent pairs of pixels. Figures 9, 10 and 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.

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

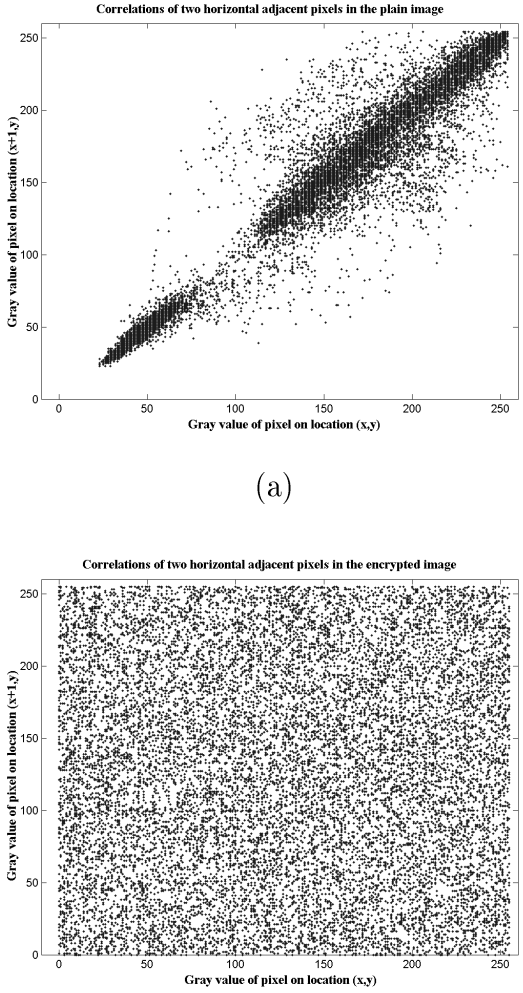
| | Plain Image | Encrypted Image |
|---|---|---|
| Horizontal | 0.9727 | 0.0103 |
| Vertical | 0.9865 | 0.0065 |
| Diagonal | 0.9616 | 0.0075 |

## 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 attack 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) [13], 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:

$$NPCR(A,B) = 100\% \left( \sum_{i,j} D(i,j) \right) /N \tag{21}$$



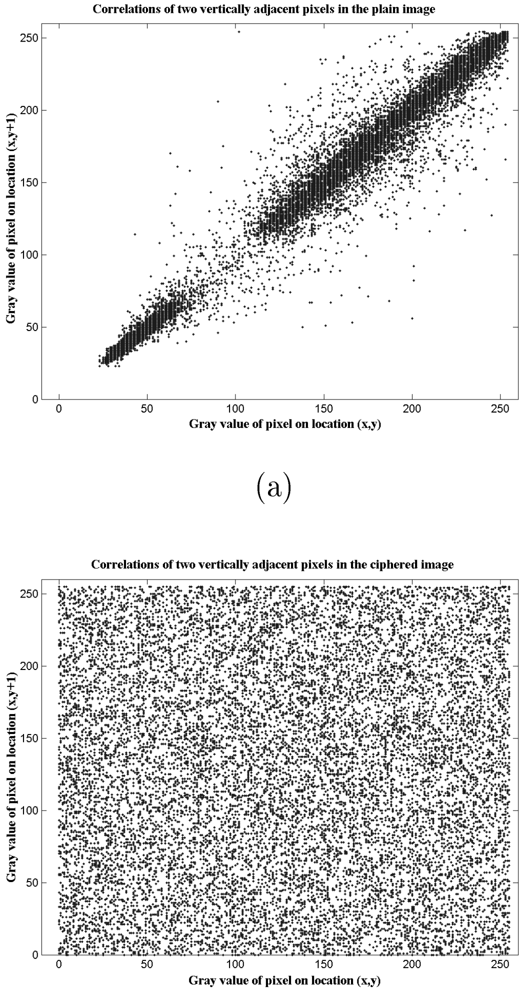
(a)

(b)

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

where $N$ is the total number of pixels and $D(i,j)$ is produced by the following way: $D(i,j) = 1$ if $A(i,j) \neq B(i,j)$ or $D(i,j) = 0$ if $A(i,j) = B(i,j)$.

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 99.60938%. The second number (UACI), measures the average intensity of differences between



(a)

(b)

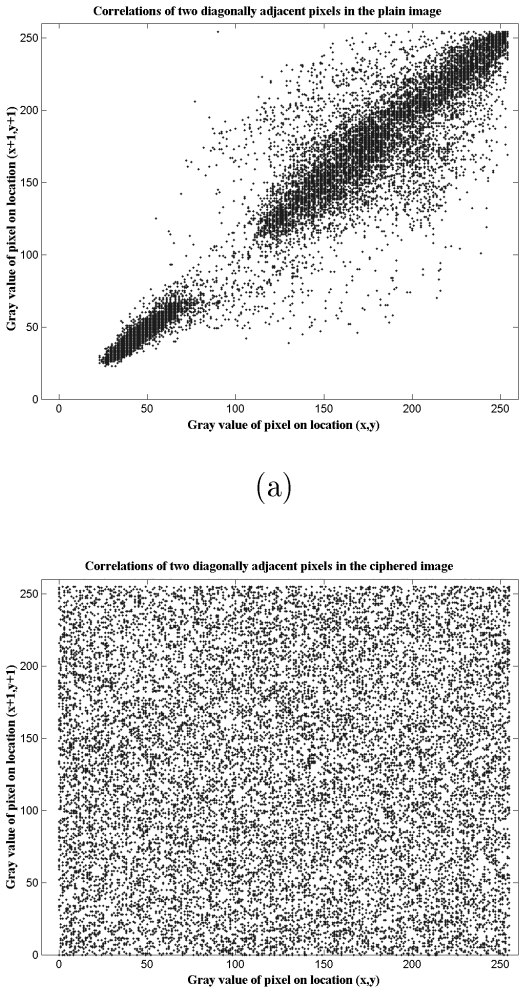
Figure 10: Correlation analysis of two vertically adjacent pixels (a) in the plain and (b) the encrypted image

the plain image and the encrypted image, calculated by the following formula:

$$UACI(A,B) = \frac{1}{N}\left(\sum_{i,j}\frac{|A(i,j)-B(i,j)|}{2^L-1}\right)100\% \tag{22}$$

The expected value of UACI for two random selected images is:

$$UACI = \left(\sum_{i-1}^{2^L-1} i(i-1)\right)/2^L(2^L-1) \tag{23}$$



(a)

(b)

Figure 11: Correlation analysis of two diagonally adjacent pixels (a) in the plain and (b) the encrypted image

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 the encryption process in more than one round is evaluated. The NPCR and UACI at 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.

Table 4: NPCR and UACI of two encrypted plain images at two encryption rounds

| Round | 1 | 2 |
|---|---|---|
| NPCR | 0.0165% | 99.5239% |
| UACI | 0.0032% | 33.3972% |

### 6.4 Information Entropy

The entropy of a source is calculated by the formula:

$$H(s) = -\sum_{i=0}^{N-1} p(s_i) log_2 p(s_i) \tag{24}$$

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 has shown that the information entropy of the plain image is equal to 7.2872, while the information entropy of the encrypted image is higher, 7.9672. 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 an image encryption scheme based on a chaotic true random bits generator was presented. The main element of this TRBG was two mutually coupled identical Chua's oscillator 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 $\pi$-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 chaotic bitstream, which is produced by the proposed TRBG, was used to encrypt a gray-scale image from a satellite by using the XOR function. The statistical analysis of the plain and encrypted images confirmed the robustness of the encryption process against various known statistical attacks. Therefore, 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 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 ($x_{01} = 0.5$, $y_{01} = 0.1$, $z_{01} = 0.3$, $x_{02} = 0.3$, $y_{02} = 0.2$, $z_{02} = 0.2$) has been changed and the failure of recovering the plain image by the intruder is presented in Figure 12. Finally, a comparison of existing methods used for satellite transmission for military use with the proposed image encryption scheme would enhance the value and acceptability of this scheme.

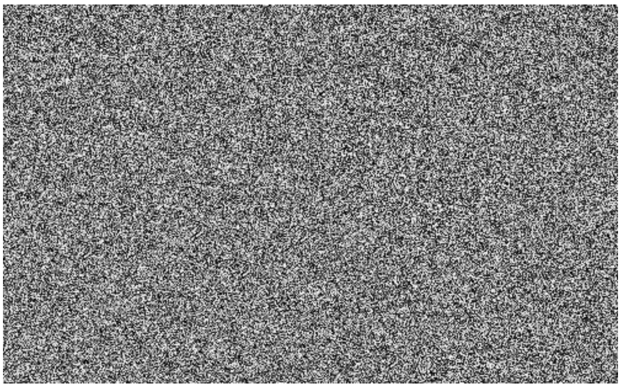


Figure 12: The recovered image by an intruder

## References

[1] M.M. Yeung and S. Pankanti, Verification Cryptosystems: Issues and Challenges, *J. Electron. Imaging*, **9**, (2000), 468–476.

[2] S. Rawat and B. Raman, A Blind Watermarking Algorithm Based on Fractional Fourier Transform and Visual Cryptography, *Signal Process.*, **92**, (2012), 1480–1491.

[3] V. Fotopoulos, M.L. Stavrinou and A.N. Skodras, Medical Image Authentication and Self-Correction through an Adaptive Reversible Watermarking Technique, *Proceedings of the 8th IEEE International Conference on Bioinformatics and Bioengineering*, **1 - 2**, (2008), 910–914.

[4] X. Liao, S. Lai and Q. Zhou, A Novel Image Encryption Algorithm Based on Self-adaptive Wave Transmission, *Signal Process.*, **90**, (2010), 2714–2722.

[5] T.-H. Chen and C.-S. Wu, Efficient Multi-secret Image Sharing Based on Boolean Operations, *Signal Process.*, **91**, (2011), 90–97.

[6] L. Zhang, X. Liao and X. Wang, An Image Encryption Approach Based on Chaotic Maps, *Chaos Soliton. Fract.*, **24**, (2005), 759–765.

[7] X. Wang, L. Teng and X. Qin, A Novel Colour Image Encryption Algorithm Based on Chaos, *Signal Process.*, **92**, (2012), 1101–1108.

[8] L. Kocarev, G. Jakimoski, T. Stojanovski and U. Parlitz, From Chaotic Maps to Encryption Schemes, *Proceedings of the IEEE International Symposium on Circuits and Systems*, (1998).

[9] R. Matthews, One the Derivation of a Chaotic Encryption Algorithm, *Cryptologia*, **8**, (1989), 29–42.

[10] J.C. Yen and J.I. Guo, A New Key-based Design for Image Encryption and Decryption, *Proceedings of the IEEE Conference on Circuits and Systems*, **4**, (2000), 49–52.

[11] C.C. Chang, M.S. Hwang and T.S. Chen, A New Encryption Algorithm for Image Cryptosystems, *J. Syst. Software*, **58**, (2001), 83–91.

[12] G.R. Chen, Y. Mao and C. Chui, A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Map, *Chaos Soliton. Fract.*, **21**, (2004), 749–761.

[13] G.R. Chen, Y. Mao and C. Chui, A Symmetric Image Encryption Scheme Based on Chaotic Maps with Finite Precision Representation, *Chaos Soliton. Fract.*, **32**, (2007), 1518–1529.

[14] Y. Mao, G. Chen and S. Lian, A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps, *Int. J. Bifurcat. Chaos*, **14**, (2004), 3613–3624.

[15] T. Shu, *Uniform Random Numbers: Theory and Practice*, Kluwer Academic Publishers, 1995.

[16] M. Guide, Concept for a High-performance Random Number Generator Based on Physical Random Phenomena, *Frequenz*, **39**, (1985), 187–190.

[17] W.T. Holman, J.S. Connelly and A.B. Downlatabadi, An Integrated Analog-digital Random Noise Source, *IEEE Trans. Circuits Syst. I*, **44**, (1997), 521–528.

[18] R.C. Fairfield, R.L. Mortenson and K.B. Coulthart, *An LSI Random Number Generator (RNG)*, Springer-Verlag (eds.), Advances in Cryptology, LNCS, **0196**, pp. 203–230, 1987.

[19] D. Davis, R. Ihaka and P. Fenstermacher, *Cryptographic Randomness from Air Turbulence in Disk Drives*, Springer-Verlag (eds.), Advances in Cryptology, LNCS, **0839**, pp. 114–120, 1994.

[20] G.B. Agnew, *Random Sources from Cryptographic Systems*, Springer-Verlag (eds.), Advances in Cryptology, LNCS, pp. 77–81, 1986.

[21] Y. Hu, X. Liao, K. Wong and Q. Zhou, A True Random Number Generator Based on Mouse Movement and Chaotic Cryptography, *Chaos Soliton. Fract.*, **40**, (2009), 2286–2293.

[22] N.G. Bardis, A.P. Markovskyi, N. Doukas and N.V. Karadimas, True Random Number Generation Based on Environmental Noise Measurements

for Military Applications, *Proceedings of the 8th WSEAS International Conference on Signal Processing, Robotics and Automation*, (2009).

[23] Ch.K. Volos, I.M. Kyprianidis and I.N. Stouboulos, Anti-phase and Inverse -Lag Synchronization in Coupled Duffing-type Circuits, *Int. J. Bifurc. Chaos*, **21**, (2011), 2357–2368.

[24] Ch.K. Volos, I.M. Kyprianidis and I.N. Stouboulos, Various Synchronization Phenomena in Bidirectionally Coupled Double Scroll Circuits, *Commun. Nonlinear Sci. Numer. Simulat.*, **16**, (2011), 3356–3366.

[25] B.Hasselblatt and A. Katok *A First Course in Dynamics: With a Panorama of Recent Developments*, University Press, Cambridge, 2003.

[26] L.M. Pecora and T.L. Carroll, Synchronization in Chaotic Systems, *Phys. Rev. Lett.*, **64**, (1990), 821–824.

[27] Ch.K. Volos, I.M. Kyprianidis, I.N. Stouboulos and A.N. Anagnostopoulos, Experimental Study of the Dynamic Behavior of a Double Scroll Circuit, *Applied Functional Analysis*, **4**, (2009), 703–711.

[28] L. Pivka, C.W. Wu and A. Huang, Chua's Oscillator: A Compendium of Chaotic Phenomena, *J. Franklin I.*, **331**, (1994), 705–741.

[29] Y.H. Ku and X. Sun, On Nonlinear Systems - Chaos, *J. Franklin I.*, **326**, (1989), 93–107.

[30] L.O. Chua, C.W. Wu, A. Huang and G.-Q. Zhong, A universal circuit for studying and generating chaos - Part i: Routes to Chaos, *IEEE Trans. Circuits Syst.*, **CAS-40**, (1993), 732–744.

[31] C.W. Wu and L. Pivka, *From Chua's circuit to Chua's oscillator: A picture book of Attractors*, A.C. Davies and W. Schwartz, World Scientific (eds.), Nonlinear Dynamics of Electronic Systems, pp. 15–79, 1994.

[32] J. Von Neumann, *Various Techniques Used in Connection with Random Digits*, G.E. Forsythe (eds.), Applied Mathematics Series, National Bureau of Standards, **12**, pp. 36–38, 1951.

[33] NIST, *Security Requirements for Cryptographic Modules*, FIPS PUB 140-2, 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[34] A.M. Fraser, Information and Entropy in Strange Attractors, *IEEE Trans. Inf. Theory*, **35**, (1989), 245–262.

[35] M.E. Yalcin, A.K. Suykens, J. Vanderwalle, True random bit generation from a double-scroll attractor, *IEEE Trans. Circ. Syst. I*, **51**, (2004), 1395–1404.

[36] C.E. Shannon, Communication Theory of Secrecy System, *Journal of Bell Systems Technology*, **28**, (1949), 656–715.