Research Article

Multimedia Security Application of a Ten-Term Chaotic System without Equilibrium

Xiong Wang,1 Akif Akgul,2 Sezgin Kacar,2 and Viet-Thanh Pham3

1Institute for Advanced Study, Shenzhen University, Shenzhen, Guangdong 518060, China
2Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University, Serdivan, Turkey
3Modeling Evolutionary Algorithms Simulation and Artificial Intelligent, Faculty of Electrical & Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam

Correspondence should be addressed to Viet-Thanh Pham; phamvietthanh@tdt.edu.vn

Received 19 July 2017; Revised 4 October 2017; Accepted 31 October 2017; Published 15 November 2017

Academic Editor: Dimitri Volchenkov

Copyright © 2017 Xiong Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A system without equilibrium has been proposed in this work. Although there is an absence of equilibrium points, the system displays chaos, which has been confirmed by phase portraits and Lyapunov exponents. The system is realized on an electronic card, which exhibits chaotic signals. Furthermore, chaotic property of the system is applied in multimedia security such as image encryption and sound steganography.

1. Introduction

Recently, there is an increased interest in multimedia communication, which is vital in various areas ranging from entertainment industries, economics, and medical applications to militaries [1, 2]. Several attempts have been made to provide confidentiality, identity, and integrity. A considerable amount of studies about multimedia security has been introduced, for example, data encryption, steganographic messages, watermarking, or multimedia authentication [1–6].

Extensive researches have shown that the use of chaos for multimedia communication is a potential application [7–11]. Because of the similar characteristics between chaotic systems and cryptographic primitives, chaotic cryptography is a major area of interest [12]. Liu et al. presented the audio encryption scheme with confusion and diffusion [13]. They based on a multiscroll chaotic system and one-time keys [13]. By using complex hyperchaotic systems, color image encryption was proposed [14]. Chaos maps with Markov properties were applied to construct a new encryption algorithm [15]. In addition, Ghebleh and Kanso introduced a robust chaos scheme to image steganography [16]. In order to generate message authentication codes, suitability of chaos functions was studied in [17].

In this work, we study a ten-term chaotic system without equilibrium and its multimedia security application. The chaotic attractors in this system are “hidden attractors” because the basin of attraction for a hidden attractor is not connected with any unstable fixed point [18–21]. It is noted that the concept of hidden attractors has been suggested in connection with the occurrence of unpredictable attractors in multistable systems [21]. Researchers have shown that multistability is connected with the occurrence of unpredictable attractors [21–30]. Recently, hidden attractor has been investigated in numerous systems such as Chua system [19], drilling system [31], Lorenz-like system [32], Goodwin oscillator [33], electromechanical systems [34], two-dimensional maps [35], phase-locked loop circuits [36], and Rabinovich–Fabrikant system [37].

2. A System without Equilibrium and Its Implementation

2.1. A System without Equilibrium. Chaotic systems without equilibrium attract have been attracting a lot of interest [38–42]. When mentioning a chaotic system without equilibrium, it means that there is no real equilibrium in such a system.
In this work, we study a general three-dimensional form described by
\[\begin{align*}
\dot{x} &= a_1 y, \\
\dot{y} &= a_2 x + a_3 y + a_4 z + a_5 x z, \\
\dot{z} &= a_6 x + a_7 z + a_8 x y + a_9 x z + a_{10},
\end{align*}\] (1)
where \(a_i (i = 1, \ldots, 10)\) are parameters and \(a_i \neq 0\).

We can solve the following three equations to find the system's equilibrium:
\[a_1 y = 0,\]
\[a_2 x + a_3 y + a_4 z + a_5 x z = 0,\] (2)
\[a_6 x + a_7 z + a_8 x y + a_9 x z + a_{10} = 0.\]

From (2), we have
\[A x^2 + B x + C = 0,\] (3)
in which
\[\begin{align*}
A &= a_2 a_3 a_6 - a_3^2 a_6, \\
B &= a_2 a_3 a_7 - a_3 a_6 a_8 - a_3^2 a_{10}, \\
C &= -a_2 a_7 a_{10},
\end{align*}\] (4)
for
\[a_3 a_7 - a_4 a_6 \neq 0.\] (5)

As a result, there is no equilibrium in general form (1) for
\[
\Delta = B^2 - 4AC < 0.\] (6)

Based on conditions (5) and (6) and \(a_i \neq 0\), we have applied a search procedure [40] to find the set of parameters for which general form (1) does not have equilibrium. A set of parameters has been found as follows:
\[\begin{align*}
a_1 &= a, \\
a_2 &= a_7 = a_8 = -1, \\
a_3 &= b, \\
a_4 &= c, \\
a_5 &= a_6 = a_{10} = 1, \\
a_6 &= d,
\end{align*}\] (7)
where \(a, b, c, d > 0\). General form (1) is rewritten by
\[\begin{align*}
\dot{x} &= a y, \\
\dot{y} &= -x + by + cz + xz, \\
\dot{z} &= x - z - xy + d x z + 1.
\end{align*}\] (8)

It is simple to see that system (8) has no equilibrium for \(a = 2, b = 0.1, c = 2.5,\) and \(d = 0.3\). However, it displays chaos as shown in Figure 1. In this case, calculated Lyapunov exponents of the system are illustrated in Figure 2. Lyapunov exponents are \(L_1 = 0.2563, L_2 = 0,\) and \(L_3 = -0.5762\) for \(t = 10,000\). Positive Lyapunov exponent \(L_1 = 0.2563\) verifies the chaotic behavior of system (8). Attractors of system (8) are hidden attractors according to the introduced definition in [21]. It is noted that the hidden attractors are observed in systems without equilibria, with no unstable fixed points or with one stable fixed point [21].

### 2.2. Electronic Circuit Implementation of the Chaotic System without Equilibrium

Electronic implementation of a chaotic model is useful for confirming the model's feasibility as well as realizing applications [43–45]. The main aim of this section is to design a circuit to realize the system without equilibrium by using electronic elements [46–51]. The chaotic system must be rescaled for electronic circuit implementation. The amplitude values of system (\(x, y,\) and \(z\)) are in the interval of \((-80, 60)\). They are higher than the interval of \((-15, 15)\) which are electronic materials limitations. For scale process, let \(X/2 = x, Y/6 = y,\) and \(Z = z/4\) and then adjust the original state variables \(x, y, z\) instead of the variables \(X, Y, Z\).

As a result, the scaled system finally becomes of the following form:
\[\begin{align*}
\dot{X} &= 3aY, \\
\dot{Y} &= -\frac{1}{3}X + bY + \frac{2}{3}Z + \frac{4}{3}XZ, \\
\dot{Z} &= \frac{1}{2}X - Z - 3XY + 2dXZ + \frac{1}{4}.
\end{align*}\] (9)

An electronic circuit is designed for the scaled system as shown in Figure 3.

As can be seen in Figure 3, we selected \(C1 = C2 = C3 = 1\ \text{nF}, R1 = 66\ \text{kQ}, R2 = R3 = R8 = R9 = R15 = R16 = 100\ \text{kQ}, R4 = 1200\ \text{kQ}, R5 = 4000\ \text{kQ}, R6 = 240\ \text{kQ}, R7 = 30\ \text{kQ}, R10 = 800\ \text{kQ}, R11 = 400\ \text{kQ}, R12 = 24000\ \text{kQ}, R13 = 67\ \text{kQ},\) and \(R14 = 14\ \text{kQ}\). The scaled chaotic system was done on the electronic card (see Figure 4). All phase portraits on the oscilloscope are shown in Figure 5, which illustrate the feasibility of the system.

### 3. Image Encryption and Sound Steganography Applications of the System without Equilibrium

After considering the circuit implementation of the system, in this section, image encryption and hiding of encrypted image data in a sound file have been implemented to show that the no-equilibrium chaotic system can be used in multimedia security applications. In order to realize these applications, firstly random number generator design has been done.

#### 3.1. Random Number Generator (RNG) Design

One of the most basic structures used in chaos-based encryption and steganography applications is RNG. In this study, before the security applications, a RNG design has been implemented.
Figure 1: Projections of attractors without equilibrium in (a) $x - y$ plane, (b) $x - z$ plane, and (c) $y - z$ plane for $a = 2$, $b = 0.1$, $c = 2.5$, and $d = 0.3$ and initial conditions $(x(0), y(0), z(0)) = (1, 1, 1)$. The attractor of system (8) is “hidden” according to the definition introduced in [21].

for use in these applications. In RNG design, $mod(256)$ operation has been performed by taking 13, 14, and 15 digits after the point of state variables obtained by using Runge–Kutta 4 (RK4) algorithm. In this case, 8 bits of each state variable are obtained in each iteration of the RK4 algorithm. Finally, each 8-bit sequence obtained from 3 state variables $(x, y, z)$ has been XORed at each iteration to obtain a random bit sequence of RNG. In Table 1, the statistical NIST-800-22 test results of the random number sequence of 1,000,000 bits obtained from the designed RNG are shown.

The statistical NIST-800-22 test is known as the internationally accepted best random test. The NIST test is a comprehensive test consisting of 15 different tests. In order to be able to speak of a complete randomness, obtained $P$ values from the all of 15 tests must be provided with the condition of $1 > P$ value $> 0.01$. When the values in Table 1 are examined, it is seen that the RNG based on the new system is successful in all tests.

3.2. Image Encryption Application. In this application, image encryption is performed using RNG obtained in Section 3.1. In the application $128 \times 128$ pixel size image with gray scale (“pepper”) is used. All pixels of the original image have converted to binary and all binary bits have been subjected to XOR processing with a random bit sequence obtained from the RNG to perform encryption. The decryption process is also performed by applying the reverse of the encryption process. Figure 6 shows the original, encrypted, and decrypted images. As seen in the figure, the encrypted image is not understood. So, the encryption is visually very successful. Correlation, histogram, entropy, and differential attack analyses were also performed to analyze the performance of the
### Table 1: NIST-800-22 test results of the new chaotic system based RNG.

<table>
<thead>
<tr>
<th>Statistical tests</th>
<th>P value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (Monobit) Test</td>
<td>0.4556674150378</td>
<td>Successful</td>
</tr>
<tr>
<td>Block-Frequency Test</td>
<td>0.31273896039824</td>
<td>Successful</td>
</tr>
<tr>
<td>Cumulative-Sums Test</td>
<td>0.5441395972238</td>
<td>Successful</td>
</tr>
<tr>
<td>Runs Test</td>
<td>0.11747875093071</td>
<td>Successful</td>
</tr>
<tr>
<td>Longest-Run Test</td>
<td>0.8863602631487</td>
<td>Successful</td>
</tr>
<tr>
<td>Binary Matrix Rank Test</td>
<td>0.79420619304231</td>
<td>Successful</td>
</tr>
<tr>
<td>Discrete Fourier Transform Test</td>
<td>0.47830862437369</td>
<td>Successful</td>
</tr>
<tr>
<td>Binary Matrix Rank Test</td>
<td>0.058644145317821</td>
<td>Successful</td>
</tr>
<tr>
<td>Overlapping Templates Test</td>
<td>0.86831417679646</td>
<td>Successful</td>
</tr>
<tr>
<td>Maurer’s Universal Statistical Test</td>
<td>0.432931702138117</td>
<td>Successful</td>
</tr>
<tr>
<td>Approximate Entropy Test</td>
<td>0.0419351614775444</td>
<td>Successful</td>
</tr>
<tr>
<td>Random-Excursions Test (x = −4)</td>
<td>0.746783846542712</td>
<td>Successful</td>
</tr>
<tr>
<td>Random-Excursions Variant Test (x = −9)</td>
<td>0.841074242469133</td>
<td>Successful</td>
</tr>
<tr>
<td>Serial Test-1</td>
<td>0.366073450623053</td>
<td>Successful</td>
</tr>
<tr>
<td>Serial Test-2</td>
<td>0.333453364381209</td>
<td>Successful</td>
</tr>
<tr>
<td>Linear-Complexity Test</td>
<td>0.99265609183689</td>
<td>Successful</td>
</tr>
</tbody>
</table>

### 3.3. Sound Steganography Application

In this section, the 128 × 128 encrypted picture obtained in Section 3.2 has been hidden in the original sound as in Figure 9. In this hiding process, firstly, the pixel values of the encrypted picture are converted into binary numbers. Secondly, the float values obtained from the sound data are converted to 32-bit binary numbers. Finally, all the bits belonging to the encrypted image are hidden by placing them in the LSB bits of the 32-bit binary numbers of the selected sound data using the RNG obtained in Section 3.1. As a result, the sound data in which the encrypted image is hidden is shown in Figure 9. There is no visual difference...
Figure 3: The circuit schematic of the scaled system.
between the original and embedded sound data seen in Figure 9. This shows that the steganography application has a good performance. Since it is not enough that there is no difference visually between the original and embedded sounds, analyses of correlation, histogram, entropy, mean square error (MSE), maximum absolute error (MAXERR), and the energy ratio (L2RAT) were also performed. As seen in Figures 10 and 11, correlation distributions and histograms of the original and embedded sounds are the same. In addition, the results of the analyses in Table 4 indicate that there is no difference between the original and embedded sounds. This means that the sound steganography application based on the chaotic system without equilibrium has a good performance.

**Table 4: Security analysis of the steganography process.**

<table>
<thead>
<tr>
<th>Analysis</th>
<th>Original sound</th>
<th>Embedded sound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlation</td>
<td>0.9994</td>
<td>0.9994</td>
</tr>
<tr>
<td>Entropy</td>
<td>13.4926</td>
<td>13.4926</td>
</tr>
<tr>
<td>MSE</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAXERR</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L2RAT</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**4. Conclusions**

This paper introduces a 3D system without equilibrium, which exhibits chaotic behavior. The system includes ten...
terms and has been implemented easily by an electronic circuit. The findings of this work add to a growing list of systems with hidden attractors. This work enhances our understanding of practical applications using systems with hidden attractors. We have used the system without equilibrium for image encryption and sound steganography. According to our knowledge, this is the first time that the 128 kbit data can be encrypted and hidden in sound files. Therefore the findings of this work have important implications for future practice. Other chaotic systems without equilibrium will be discovered in our future researches.

**Conflicts of Interest**

The authors declare that there are no conflicts of interest regarding the publication of this paper.

**Acknowledgments**

The authors acknowledge Professor GuanRong Chen, Department of Electronic Engineering, City University of Hong Kong, for suggesting many helpful references. The author Xiong Wang was supported by the National Natural
Figure 9: Original and embedded sound.

Figure 10: Correlation distributions of original and embedded sounds.

Figure 11: Histograms of original and embedded sounds.
References


A. Buscarino, L. Fortuna, M. Frasca, and G. Sciuto, “Design
of time-delay chaotic electronic circuits,” IEEE Transactions on
Circuits and Systems I: Regular Papers, vol. 58, no. 8, pp. 1888–
1896, 2011.

Weng, “Dynamics analysis and circuit implementation of a new
three-dimensional chaotic system,” Optik, vol. 126, no. 7-8,

Q. Lai and L. Wang, “Chaos, bifurcation, coexisting attrac-
tors and circuit design of a three-dimensional continuous
autonomous system,” Optik, vol. 127, no. 13, pp. 5400–5406,
2016.

A. Akgul, I. Moroz, I. Pehlivan, and S. Vaidyanathan, “A new
four-scroll chaotic attractor and its engineering applications,”

A. Akgul, S. Hussain, and I. Pehlivan, “A new three-dimen-
sional chaotic system, its dynamical analysis and electronic circuit

B. Yao, T. Jiang, Q. Xu, M. Chen, H. Wu, and Y. Hu, “Coexis-
ting infinitely many attractors in active band-pass filter-based mem-
rristive circuit,” Nonlinear Dynamics, vol. 86, no. 3, pp. 1711–1723,
2016.

Ü. Çavuşoğlu, S. Kacar, I. Pehlivan, and A. Zengin, “Secure
image encryption algorithm design using a novel chaos based

O. M. Al-Hazimeh, N. Alhindawi, S. M. A. Hayajneh, and A.
Almomani, “HANON chaotic map - based new digital image
266, 2014.

H. M. Al-Najjar, “Digital image encryption algorithm based on
a linear independence scheme and the logistic map,” in Pro-
cedings of the International Arab Conference on Information

H. Al-Najjar and N. Al-Rousan, “Data hiding in encrypted
image based on multi-chaotic approach,” International Journal of

image encryption using a hybrid genetic algorithm and a DNA
83–93, 2014.

Isnin, “A novel chaotic based image encryption using a hybrid
model of deoxyribonucleic acid and cellular automata,” Optics

S. Lian, J. Sun, and Z. Wang, “A block cipher based on a suitable
use of the chaotic standard map,” Chaos, Solitons & Fractals,

K. Wong, B. S. Kwok, and W. Law, “A fast image encryption
scheme based on chaotic standard map,” Physics Letters, Section

Y. Wu, G. Yang, H. Jin, and J. P. Noonan, “Image encryption
using the two-dimensional logistic chaotic map,” Journal of
Electronic Imaging, vol. 21, no. 1, Article ID 013014, 2012.

algorithm based on self-adaptive wave transmission,” Signal