Chinese Journal of Physics 67 (2020) 615–630

Contents lists available at ScienceDirect

Chinese Journal of Physics

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

Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption

Qiang Lai*,[a], Zhiqiang Wan[a], Akif Akgul[b], Omer Faruk Boyraz[b], Mustafa Zahid Yildiz[b]

[a] School of Electrical and Automation Engineering, East China Jiaotong University, Nanchang, 330013, China
[b] Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, Serdivan 54050, Sakarya, Turkey

ARTICLE INFO

Keywords:
Memristive chaotic system
Chaos
Coexisting attractors
Circuit implementation
Fingerprint encryption

ABSTRACT

In this paper, a new memristive chaotic system was constructed from three-dimensional Lorenz-type system. The system has infinitely many equilibria and exhibits coexisting attractors. The dynamic evolution corresponds to the parameters and the coupling strength indicate that the system is easy to generate chaos. Also the bifurcation diagrams from different initial conditions determine the coexistence of multiple attractors. An electronic circuit is done for verifying the physically existence of the system. Based on this system, chaos-based random number generator and the corresponding randomness tests are studied. An algorithm for touchless fingerprint encryption is established. Some comparative tests illustrate the effectiveness of the algorithm.

1. Introduction

Memristor which was postulated as the fourth basic circuit element by Chua [1] has been generally accepted as a special nonlinear resistor with memory function. Since the realization of the first solid state memristor by Hewlett-Packard Laboratory [2] in 2008, the research of memristor has developed rapidly with the establishment of many significant achievements. The interesting nonlinear feature and memory function of memristor enable it to have great potential application values ranging from power electronics to artificial intelligence. The recent interesting application of memristor is to create chaos as a nonlinear function (or element) of systems (or circuits). The chaotic systems (or circuits) with memristor is usually called as memristive chaotic systems (or circuits). In 2008, Itoh and Chua found the first memristive chaotic circuit by replacing the Chua's diode with memristor [3]. Henceforth, more memristive chaotic systems and their complex properties were investigated [4–6]. Muthuswamy and Chua designed the simplest memristive chaotic circuit with a linear passive inductor, a linear passive capacitor and a nonlinear active memristor [7], and physically realized a flux-controlled memristor via off-the-shelf components and practically implemented the corresponding memristive chaotic circuit on a breadboard [8]. Bao et al. constructed an interesting chaotic circuit with two memristors from the typical Chua circuit [9], and studied the hidden extreme multistability and hyperchaos of a memristive system [10]. By introducing a memristor to Lu system, Li et al. proposed a new memristive system and verified its hyperchaos by topological horseshoe analysis [11]. Corinto and Forti studied the bifurcation without parameters in memristor circuits via the flux-charge analysis method [12]. Jin et al. presented two-memristor-based chaotic Shinriki oscillator with extreme multistability and studied its FPGA digital implementation [13]. Wen et al. investigated the bursting oscillations of a novel parametrically driven memristive chaotic system and showed its existence of local bifurcation [14]. Lai et al. studied the complex dynamics, circuit realization and synchronization of a memristive chaotic system with infinitely many coexisting attractors [15]. The complex dynamics of memristor-based Hopfield neural network were also

* Corresponding author.
E-mail address: laiqiang87@126.com (Q. Lai).

https://doi.org/10.1016/j.cjph.2020.08.018
Received 5 April 2020; Received in revised form 25 August 2020; Accepted 26 August 2020
Available online 01 September 2020

analyzed [16,17]. Currently the study of memristive chaotic system has been of recent interest in academic and engineering fields.

Chaos has been generally recognized to be applicable to image encryption and secure communication. For obtaining complex chaotic series and improving its application effects, scholars have constructed many different types of chaotic systems [18–24]. In addition to the complexity of chaotic system itself, a good encryption algorithm can also improve the encryption performance. Chaos-based encryption is an efficient means to solve the intractable problem of fast and highly secure encryption. Based on hyperchaotic systems, Norouzi and Mirzakuchaki established a new image encryption method composed of key stream generation process and one-round diffusion process, and verified its effectiveness by using the number of pixel change rate (NPCR) and unified average changing intensity (UACI) tests [25]. Lai et al. gave an extended Lu system and presented its image encryption application [26]. Hua et al. proposed an interesting image encryption algorithm via two dimensional Logistic-adjusted-Sine map, and illustrated that it has better performance than some existing algorithms [27]. Alawida et al. put forward a novel image cipher via the perturbation of hybrid chaotic system [28]. Peng et al. design the image encryption algorithm according to a new memristive chaotic circuit [29]. Vlols et al. gave a fingerprint image encryption scheme based on a chaotic true random bit generator from a double-scroll chaotic circuit [30]. Hung and Hu presented a new perspective on communication using chaos and verified the proposed communication scheme with temporal transfer entropy are robust against external noise and some traditional attacks [31]. Luo et al. studied the image encryption based on the synchronization of memristive chaotic system [32]. Vidhya et al. used the parametric switching chaotic system to design the image encryption algorithm and showed the high key sensitivity and plain text sensitivity of the algorithm [33]. Jamal et al. proposed a robust steganographic method according to the improved chaotic-range systems [34]. Han et al. studied the fingerprint encryption using multi-scroll chaos by setting initial values as the private key [35]. Recently the touchless fingerprint encryption has gradually become one of the most important encryption ways with the widespread use of fingerprints in daily life. Touchless fingerprint recognition perform contactless identification and verification operations without touching any device during the acquisition of images processes, yielding a more sterile environment for identification. The accuracy and reliability of touchless fingerprint recognition have made it widely concerned in safety system construction of hospitals, courthouses, industry, banks and other public institutions.

Both the generation and application of memristive chaotic systems are important research issues producing tremendous practical engineering values. The existing work mainly focused on the generation of memristive system without considering its encryption application. Also some encryption applications are touchbased encryption but a few are touchless encryption. Thus this paper will create a novel memristive chaotic system and realize it via electronic circuit, and then study its touchless fingerprint encryption. Theoretical and numerical analysis will illustrate all the obtained results. The framework of this paper is as follows. Section 2 introduces the proposition of the new memristive chaotic system. Section 3 gives the details of its dynamic analysis. Section 4 implements the new system by circuit. Section 5 studies its touchless fingerprint encryption. Section 6 presents the conclusion summary.

2. The memristive chaotic system

In 2004, Liu et al. established the following Lorenz-type system [36]

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - xz \\ \dot{z} = -cz + x^2 \end{cases} \tag{1}$$

which generates a butterfly strange attractor with the parameters $a = 10$, $b = 40$, $c = 3$. The system (1) can be transformed into the following equivalent circuit model

$$\begin{cases} C_x\dot{x} = y/R_2 - x/R_1 \\ C_y\dot{y} = x/R_4 - xz/R_3 \\ C_z\dot{z} = -z/R_5 + x^2/R_6 \end{cases} \tag{2}$$

and implemented by an electronic circuit with three voltage states x, y, z, as illustrated in Fig. 1. Denote the reference resistor and capacitor as R and C, then we have $C_x = C_y = C_z = C$, $R_3 = R_6 = R$ and $R/R_1 = R/R_2 = a$, $R/R_4 = b$, $R/R_5 = c$ showed a good accordance with the parameters of system (1).

Based on system (2), we introduce a flux-controlled memristor M (in Fig. 1) to system (2) as an additional feedback input for

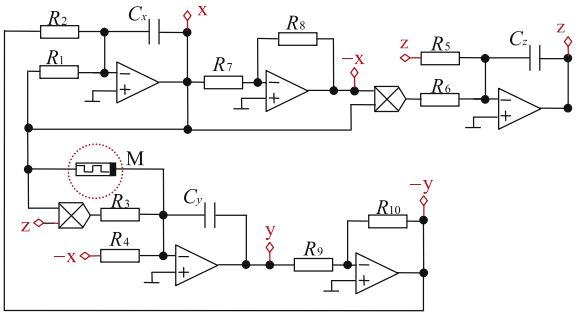

Fig. 1. Circuit implementation of system (1) with flux-controlled memristor.

constructing a memristive system. Here the memristor M is defined as the nonlinear constitutive relation between the terminal voltage v and terminal current i given by [8]

$$i = M(u), \quad \dot{u} = v \tag{3}$$

where $M(u) = dq(u)/du$ is the incremental memductance implying the slope of the scalar function $q(u)$. For a flux-controlled memristor, the $q(u)$ is usually characterized by a cubic monotone-increasing nonlinear function $q(u) = mu + pu^3$. Thereby we have $M(u) = m + 3pu^2$ with positive parameters $m > 0, p > 0$.

Then the memristive circuit is modeled by

$$\begin{cases} C_x\dot{x} = y/R_2 - x/R_1 \\ C_y\dot{y} = x/R_4 - xz/R_3 - M(u)x \\ C_z\dot{z} = -z/R_5 + x^2/R_6 \end{cases} \tag{4}$$

and its corresponding dimensionless equations can be written as

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - xz - kM(u)x \\ \dot{z} = -cz + x^2 \\ \dot{u} = x \end{cases} \tag{5}$$

where k denotes the coupling strength of the memristor M, a, b, c are all positive constants. It is easy to verify that the system (5) is dissipative with its divergence $\nabla V = \partial\dot{x}/\partial x + \partial\dot{y}/\partial y + \partial\dot{z}/\partial z + \partial\dot{u}/\partial u = -a - c < 0$, which suggests that the system is able to generate a bounded attractor. Let $\dot{x} = \dot{y} = \dot{z} = \dot{u} = 0$, we obtain the line equilibria of system (5) which can be described by a set $\Omega = \{(x, y, z, u)|x = y = z = 0, u = \phi\}$, ϕ is an arbitrary real number. Linearizing the system (5) at the equilibrium, we can obtain its corresponding characteristic equation

$$\lambda(\lambda + c)(\lambda^2 + a\lambda + akM(u) - ab) = 0 \tag{6}$$

If $kM(u) < b$, then the equilibrium is unstable as the Eq. (6) has positive root. If $kM(u) > b$, the stability of the equilibrium can be verify by using the center manifold theorem as it is a non-hyperbolic equilibrium with zero eigenvalue $\lambda = 0$.

Let $a = 10$, $b = 36$, $c = 8$, $k = 1$, $m = 4.8$, $p = .02$ and simulate the phase portraits of system (5), we can observe that its trajectory starting from initial value (1,1,1,1) moves in a bounded region and finally yields an attractor, as shown in Fig. 2. The Lyapunov exponents of system (5) are calculated as $L_1 = 0.6522$, $L_2 = 0.0542$, $L_3 = 0.0000$, $L_4 = -18.7064$ and the corresponding Lyapunov dimension is

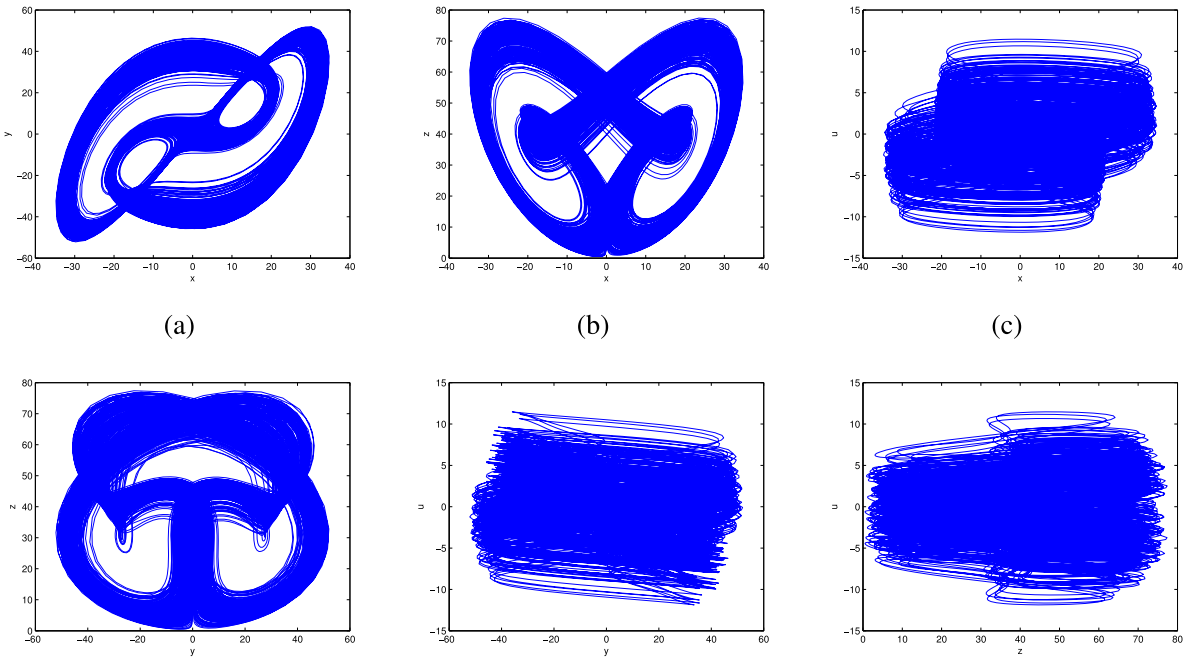

Fig. 2. Chaotic attractor with parameters $a = 10$, $b = 36$, $c = 8$, $k = 1$, $m = 4.8$, $p = .02$ and initial value (1,1,1,1).

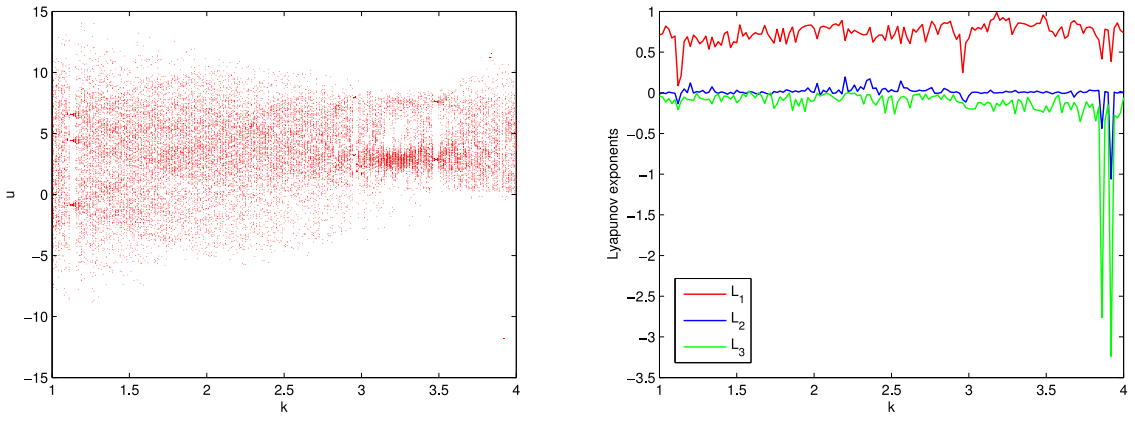

Fig. 3. Bifurcation diagram and Lyapunov exponent spectrum with the variation of $k \in [1, 4]$.

$$D_L = \sigma + \sum_{i=1}^{\sigma} L_i/|L_{\sigma+1}| = 3 + (L_1 + L_2)/|L_4| = 3.0378$$

where σ is defined by $\sum_{i=1}^{\sigma} L_i > 0$ and $\sum_{i=1}^{\sigma+1} L_i < 0$. Thus we can determine that the attractor is hyperchaotic with two positive Lyapunov exponents and fractional Lyapunov dimension.

3. Complex dynamical investigation

Let the parameters $a = 10$, $b = 40$, $c = 8$, $m = 3$, $p = .02$ and initial values $x_0 = (1, 1, 1, 1)$, we can plot the bifurcation diagram and Lyapunov exponent spectrum to illustrate the chaos of system (5) with the variation of coupling strength $k \in [1, 4]$, as shown in Fig. 3. Fig. 3(b) shows the first three Lyapunov exponents $L_1 > L_2 > L_3$. The fourth Lyapunov exponent L_4 is less than -15. The largest Lyapunov exponent $L_1 > 0$ suggests that system (5) keeps its chaotic state when the coupling strength changes from 1 to 4. The bifurcation diagram and Lyapunov exponent spectrum of system (5) under the parameter conditions $a = 10$, $c = 8$, $k = 1$, $m = 3$, $p = .02$ and initial conditions $x_0 = (1, 1, 1, 1)$ show that system (5) is almost always in chaotic state within $b \in [30, 50]$, as illustrated in Fig. 4. Thus we can conclude that system (5) is easy to yield chaos. The Fig. 5 shows the chaotic attractor of system (5) with $b = 30$.

Suppose the parameters $a = 10$, $b = 30$, $k = 1$, $m = 3$, $p = .02$, we can generate the bifurcation diagrams and Lyapunov exponents of system (5) versus $c \in [5, 20]$ respectively from initial values $x_{01} = (1, 1, 1, 1)$ (red branch) and $x_{02} = (-1, -1, -1, -1)$ (green branch), as illustrated in Fig. 6. It is clear that system (5) performs different attractors from initial values x_{01}, x_{02} yielding coexisting attractors. The Fig. 7 shows the coexisting chaotic, quasi-periodic, periodic attractors for $c = 8.8, 14, 20$.

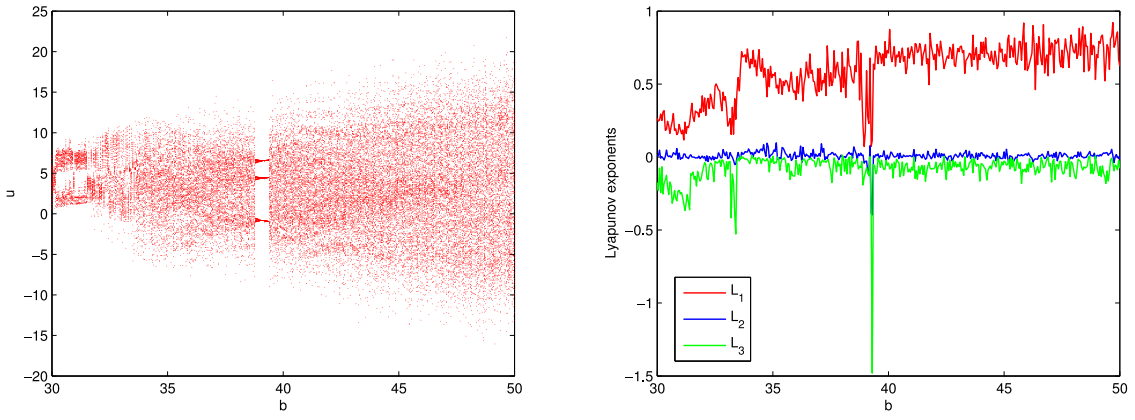

Fig. 4. Bifurcation diagram and Lyapunov exponent spectrum with the variation of $b \in [30, 50]$.

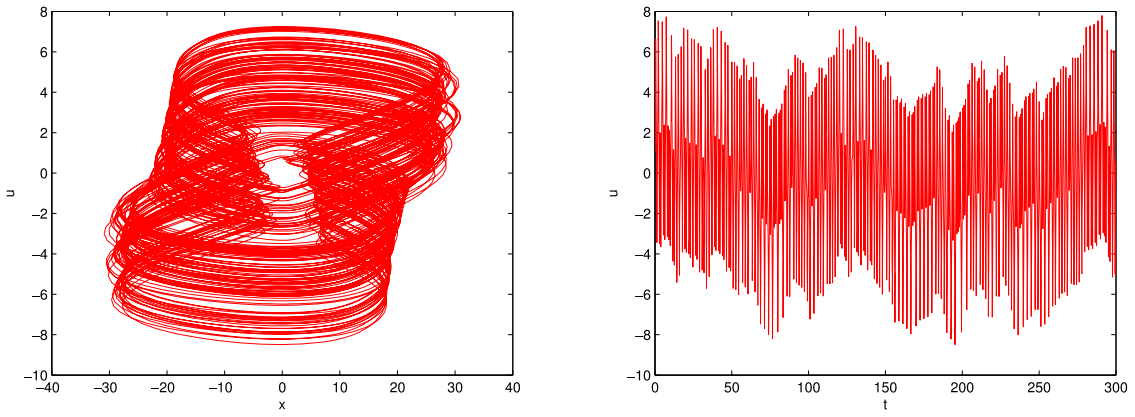

Fig. 5. Chaotic attractor of system (5) with $b = 30$: (a) $x - u$; (b) time series.

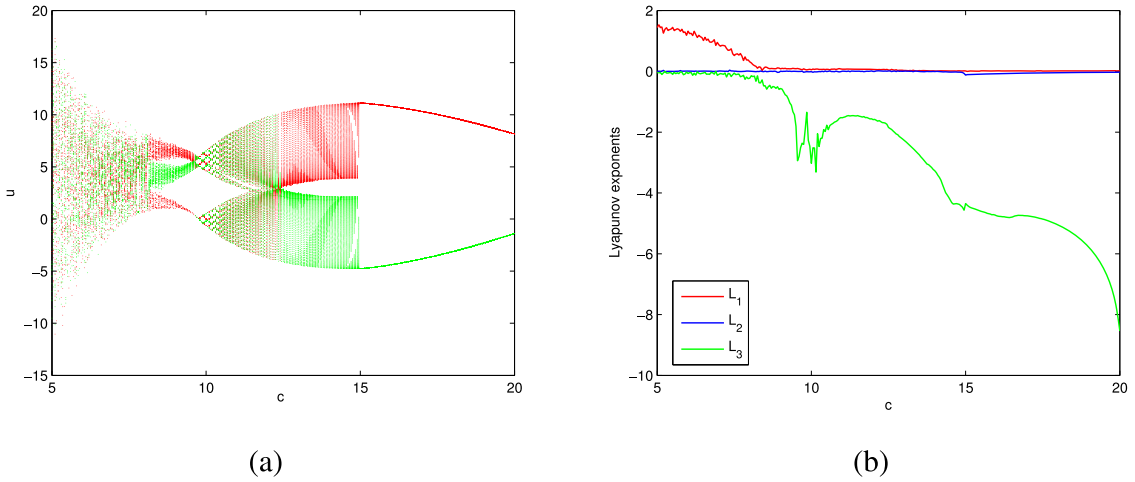

Fig. 6. Bifurcation diagrams and Lyapunov exponents with the variation of $c \in [5, 20]$ from initial values x_{01}, x_{02}.

4. Electronic circuit implementation

Here we will present the electronic circuit implementation of system (5). From the Fig. 2, we know that the amplitude values variables *x, y, z, u* are bounded in the region $(-60, 80)$ which is higher than the standard region $(-15, 15)$ of electronic materials. Thereby we should scaled the system (5) for easily implementing it via electronic circuit. Let $X = x/5$, $Y = y/5$, $X = z/10$, $U = u$, then we obtain the scaled system (5) written as

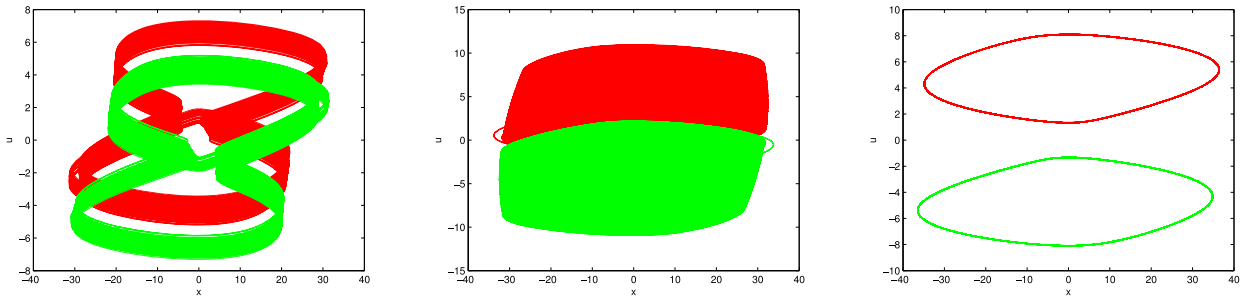

Fig. 7. Coexisting chaotic, quasi-periodic and periodic attractors with: (a) $c = 8.8$; (b) $c = 14$; (c) $c = 20$.

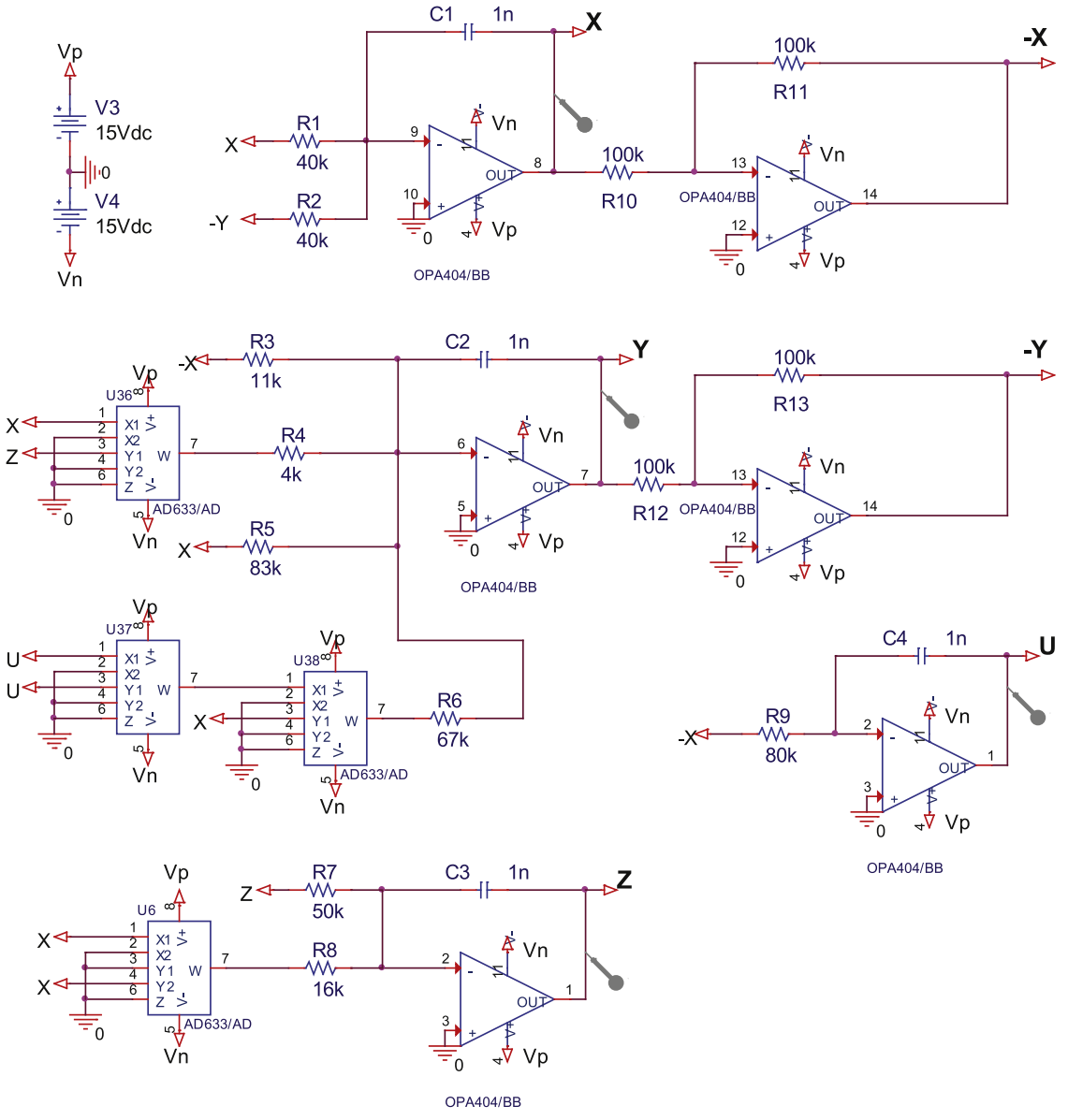

Fig. 8. The circuit schematic of the scaled system.

$$\begin{aligned}
\dot{X} &= a(Y - X)\\
\dot{Y} &= bX - 10XZ - kM(U)X\\
\dot{Z} &= -cZ + 2.5X^2\\
\dot{U} &= 5X
\end{aligned} \tag{7}$$

An electronic circuit composed of multipliers, integrators and amplifier is designed for the scaled system, as illustrated in Fig. 8. By selecting the values of circuit elements in Fig. 8, we can get the output graphics in oscilloscope which correspond to the simulation graphics of system (5) under the corresponding parameter conditions. Set C1 = C2 = C3 = C4 = 1nF, R1 = R2 = 40kΩ, R3 = 11kΩ, R4 = 4kΩ, R5 = 83kΩ, R6 = 67kΩ, R7 = 50kΩ, R8 = 16kΩ, R9 = 80kΩ, R10 = R11 = R12 = R13 = 100kΩ and run the circuit in Pspice, we get the output graphics from the virtual oscilloscope shown in Fig. 9 which are consistent with the simulation graphics of system (5) with the parameters $a = 10$, $b = 36$, $c = 8$, $k = 1$, $m = 4.8$, $p = .02$ shown in Fig. 1. By using the electronic card shown in Fig. 10, we can get the same graphics shown in Fig. 11 which are consistent with Fig. 1 and Fig. 9. It implies that the chaotic attractor of system (5) is well implemented and its physical existence is determined.

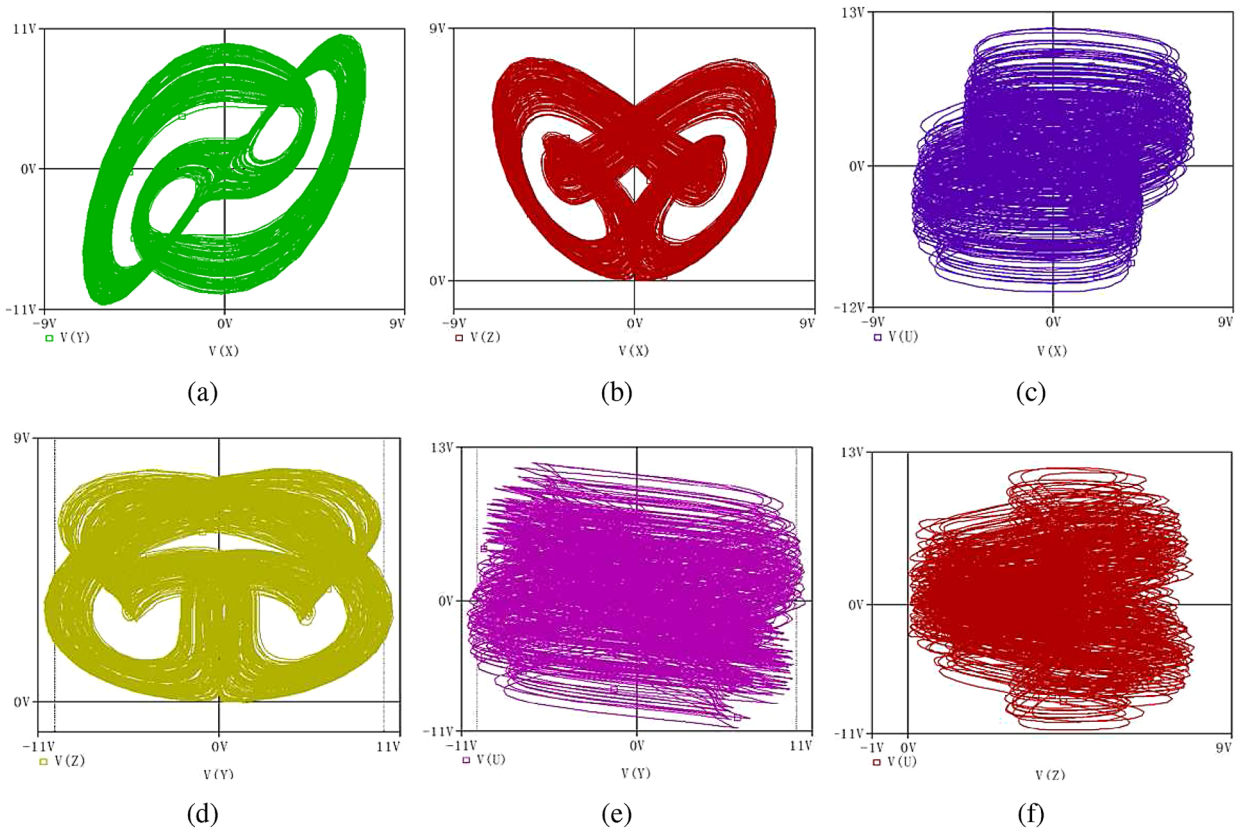

Fig. 9. Phase portraits of the scaled system generate from the Pspice circuit in virtual oscilloscope.

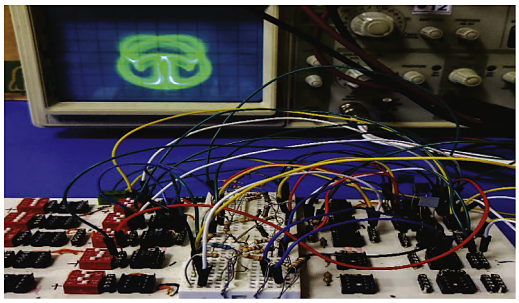

Fig. 10. The experimental circuit of the scaled chaotic system.

5. Touchless fingerprint encryption

5.1. Chaos-based random number generator

In this subsection, we will design a new chaotic random number generator (RNG) for encryption according to system (5). The flowchart for generating the random numbers generated is shown in Fig. 12. First of all, we input the parameters and initial conditions to be used into the system. The required time interval Δh is consistent with that of solving the system (5) by the fourth-order-Runge-Kutta method (RK4). Then the number of least significant bit (LSB) 'a' to be selected by sampling at the determined value Δh is entered from the outside. To generate one million bits, the iterative computation is made for the RK4 solution and the state variables obtained in each iteration are converted into a 32-bit binary system. LSB bits in the determined 'a' amount of the number series converted into a 32-bit binary system are obtained and one million random numbers are generated. The produced Random numbers were subjected to NIST-800-22 and ENT tests to make randomness analysis. If the random numbers generated as a result of the NIST-800-22 and ENT test, the algorithm is terminated. If randomness is not provided as a result of the tests, the value of 'a' is changed. After entering the value 'a', one million random numbers are generated again and these numbers are passed through NIST-800-22 and ENT tests. These steps are repeated until the generated numbers are random.

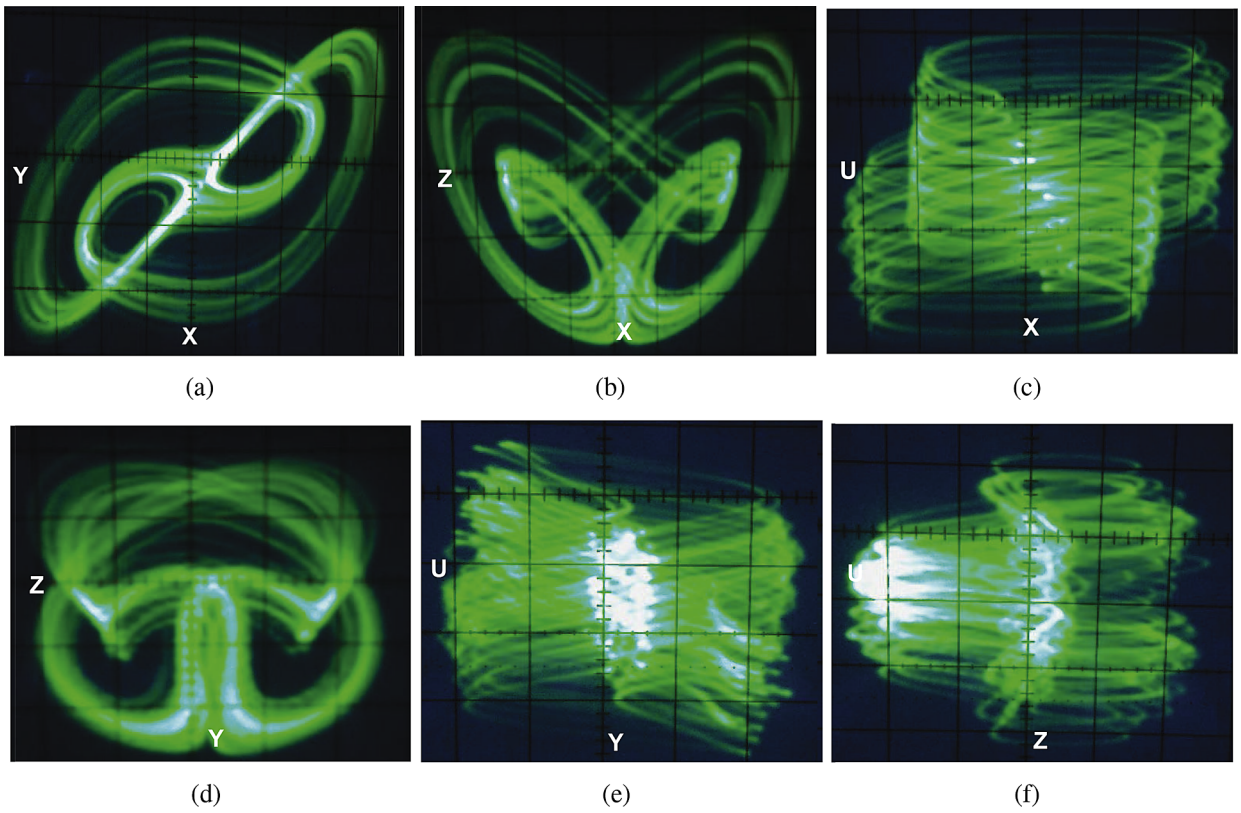

Fig. 11. Phase portraits of the scaled system generate from the experimental circuit in oscilloscope.

The randomness tests of the produced numbers are done with NIST-800-22 and ENT tests. It is made up of 16 different tests within the NIST-800-22 test, which is internationally accepted and needs a series of 1,000,000 numbers. For the NIST-800-22 test bit sequence to be considered successful, it must pass all of these tests successfully. In the NIST-800-22 test, the results are evaluated according to the P-value that can be changed. If the P-value is accepted as 0.001 as a condition, the P-value must be greater than 0.001 for the bit test to be successful. There are 16 different statistical tests in the NIST-800-22 test that define the randomness of the bit sequences [37]. NIST-800-22 test results of random numbers generated from the variables *x, y, z, u* are shown in Table 1. It can be concluded that the random numbers generated from the last 8 bits values of *x, y, z, u* provided randomness since all the numbers pass the tests.

The ENT test is a test application developed by Walker, which applies various tests to the byte arrays produced by pseudo-random number generator applications [38]. There are 5 different statistical tests in the ENT test that define the randomness of the bit sequences. The average values of ENT test results of random numbers obtained from *x, y, z, u* are shown in Table 2. It was concluded that the random numbers produced according to Table 2 provided randomness. Table 3 shows the comparison of ENT test results for the random numbers with the corresponding studies in literature [39–41].

5.2. Encryption of touchless fingerprint images

In this subsection, we will consider the encryption of touchless fingerprint images based on system (5). In Algorithm 1, the pseudo code of determining the coordinates to be made XOR is given for encryption the touchless fingerprint images, and the pixel order derived from the values of variable x of system (5) has made the encryption process even more complicated. In Algorithm 2, the encryption pseudo code of the contactless fingerprint images is given. The variable 'a' in Algorithm 2 is a kind of counter. Firstly, the order of the rows and columns where XOR operation will be performed is determined. The variable 'xor_sequence' from the result of Algorithm 2 divides the total number of columns of the image and returns the row coordinate as a result of rounding. As a result of taking the mode according to the total column number value in the image, the column gives the coordinate value.

The fact that the encrypted image resulting from the chaos-based encryption process is completely different from the original image showing a good encryption, but it does not means that a complete security is provided. For this, the performance of the encryption performance should be demonstrated via some statistical security analysis. Here the security analysis of encryption is performed for each phase of the system using entropy, correlation, differential attack (NPCR, UACI) and histogram methods for three different touchless fingerprint images of 256 × 256 pixels. When the results are examined, the histogram analysis results of the original images in Fig. 13 and the results of the encrypted images in Fig. 14 are completely different from each other. While the

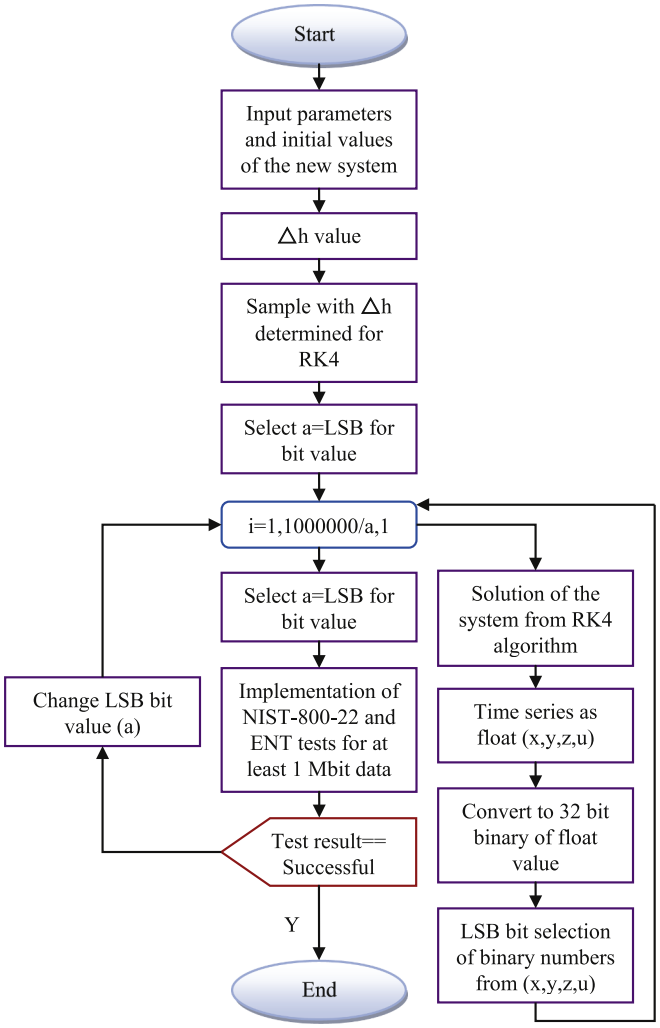

Fig. 12. Flowchart of the RNG algorithm.

Table 1
NIST-800-22 test results of random numbers obtained from *x, y, z, u*.

Statistical Tests	P-value (*x*-8bit)	P-value (*y*-8bit)	P-value (*z*-8bit)	P-value (*u*-8bit)	Results
Frequency test	0.2145	0.4879	0.8872	0.7455	Successful
Frequency test within a block	0.4978	0.3797	0.6798	0.8452	Successful
Cumulative sums test	0.3798	0.2987	0.8749	0.6745	Successful
Runs test	0.2978	0.4879	0.0987	0.1879	Successful
Tests for longest-run-of-ones	0.7945	0.6617	0.3798	0.5579	Successful
Binary matrix rank test	0.8798	0.4975	0.2648	0.3279	Successful
Discrete fourier transform test	0.0456	0.4521	0.1278	0.6159	Successful
Non-overlapping template matching	0.9785	0.0174	0.1245	0.0345	Successful
Overlapping template matching	0.2898	0.6428	0.2895	0.1895	Successful
Maurer's universal statistical test	0.8027	0.3788	0.4625	0.2985	Successful
Approximate entropy test	0.5312	0.3789	0.4025	0.1820	Successful
Random excursions ($x = -4$)	0.3048	0.2789	0.1789	0.7924	Successful
Random excursions variant ($x = -9$)	0.4278	0.3789	0.2879	0.1952	Successful
Serial test-1	0.8796	0.2174	0.3798	0.7954	Successful
Serial test-2	0.9217	0.3789	0.2879	0.8648	Successful
Linear complexity test	0.2780	0.3470	0.6782	0.3722	Successful

Table 2
ENT test results of random numbers obtained from *x, y, z, u*.

Test	Average (Proposed Method)	Result
Arithmetic Mean	127.4994	Successful
Entropy	7.9997	Successful
Correlation	0.0001007	Successful
Chi Square	259,052	Successful
Monte Carlo	3.14290 (error = 0.0004)	Successful

Table 3
Proposed method's ENT test results compare with other models.

Method	Arithmetic Mean	Entropy	Correlation	Chi Square	Chi Square
Proposed method	127.4994	7.99987	0.0001007	259.052 (71.13%)	3.14290 (error = 0.0004)
Stoyanov et al.[39]	127.5013	7.99750	–0.000147	–	3.14057 (error = 0.0300)
Seetharam et al. [40]	122.8850	7.71330	–0.058927	–	3.08813 (error = 1.7000)
Akhshani et al. [41]	127.7714	7.9999	0.000108	255.190	3.14062 (error = 0.0310)
Optimal results	127.5000	8.0000	0.000000	10% – 90%	3.14159 (Pi)

```
Start;
[row column]=size(image);
series=1:row*column;
for i=1:row*column; do
    number=mod(x(i), (0.0000001*(row*column+1-i)))*1000000;
    xor_sequence(i)=series(number);
    series(number)=[];
end for
End.
```

Algorithm 1. Sequence of XOR operation algorithm pseudo code.

density in the histogram graphics of the original images is in a certain region in Fig. 13, the histogram graphics are homogeneously distributed in the encrypted images in Fig. 14. The homogeneity of histogram distributions indicate that encryption is successful.

In Table 4, the correlation coefficients of touchless fingerprint images give a result close to 1, whereas correlation coefficients for encrypted images are very close to zero, such as -0.00019, -0.0011, 0.00018. As a result of these values, encryption has been shown to be very successful. The correlation coefficients obtained in some recent studies are shown in Table 5. It has been found that the correlation coefficients obtained from encrypted touchless fingerprint images are better than most literature studies. Additionally, all the correlation coefficients of the encrypted image in the proposed algorithm were less than 0.01. This indicates a very small association between adjacent pixels.

Fig. 15 shows the correlation distributions. It can be observed that the distribution in the original images is diagonal and the distribution in the encrypted images is homogeneous. The fact that the correlation distributions are homogeneous shows that the encryption is good. In Table 6, it can be seen that the entropy values of the encrypted images are very close to 8, which is the highest possible value for a 256 × 256 pixel image. This value indicates that the random distribution in encryption is statistically very strong.

The encryption quality analysis of the proposed algorithm is studied as well. The maximum deviation value which measures the deviation between the pixel values of the original image and encrypted image is an important parameter for checking the statistical security of encryption. The higher the maximum deviation value, the better the encryption algorithm. The maximum deviation value is expressed as follows

$$D = \frac{l_0 + l_{255}}{2} + \sum_{m=1}^{254} l_m$$

where l_m is the difference of histogram of the original image and cipher image at value m. l_0 and l_{255} are the difference values at index 0 and 255. However the maximum deviation alone is not sufficient to prove the statistical randomness of an encrypted image. The encryption algorithm should randomly change the pixel values in the image to be statistically strong and durable. Thereby is necessary to introduce the irregular deviation value which given by

```
Start;
[row column]=size(image);
index=0, a=0;
for i=1:row; do
    for j=1:column; do
        a=a+1 row2=ceil(xor_sequence (a)/column) column2=mod(xor_sequence(a),column);
        bin = decimal to binary (image (row2, column2), 8);
        if (mod(i+j,3)==1); then
            rng=y_rng;
        else if (mod(i+j,3)==2); then
            rng=z_rng;
        else rng=u_rng;
        end if
        for n=1:bit_number(bit_number=1 or 8); do
            index=index+1
            number(n)=(bitxor(rng(index), bin(n));
        end for
        image_encryption(i,j) = binary to decimal(number)
    end for
end for
End.
```

Algorithm 2. Image encryption algorithm pseudo code.

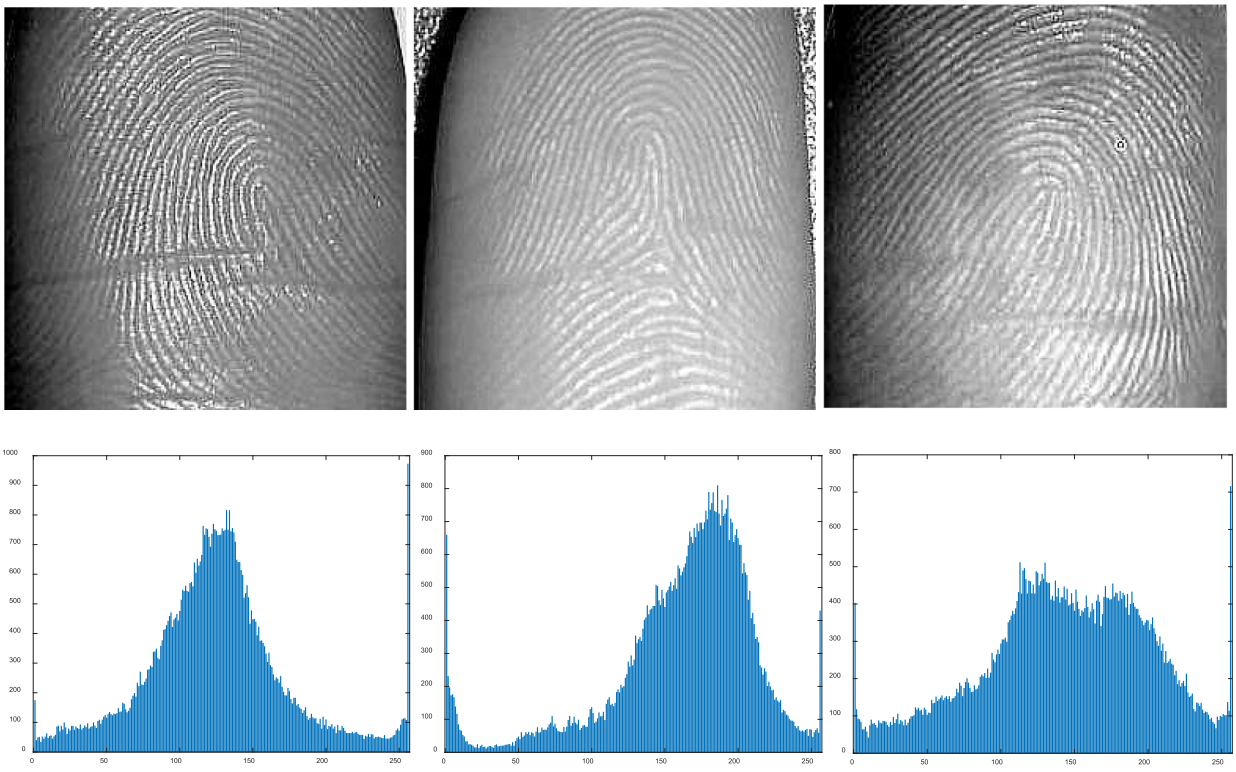

Fig. 13. Touchless fingerprint images and histogram distributions.

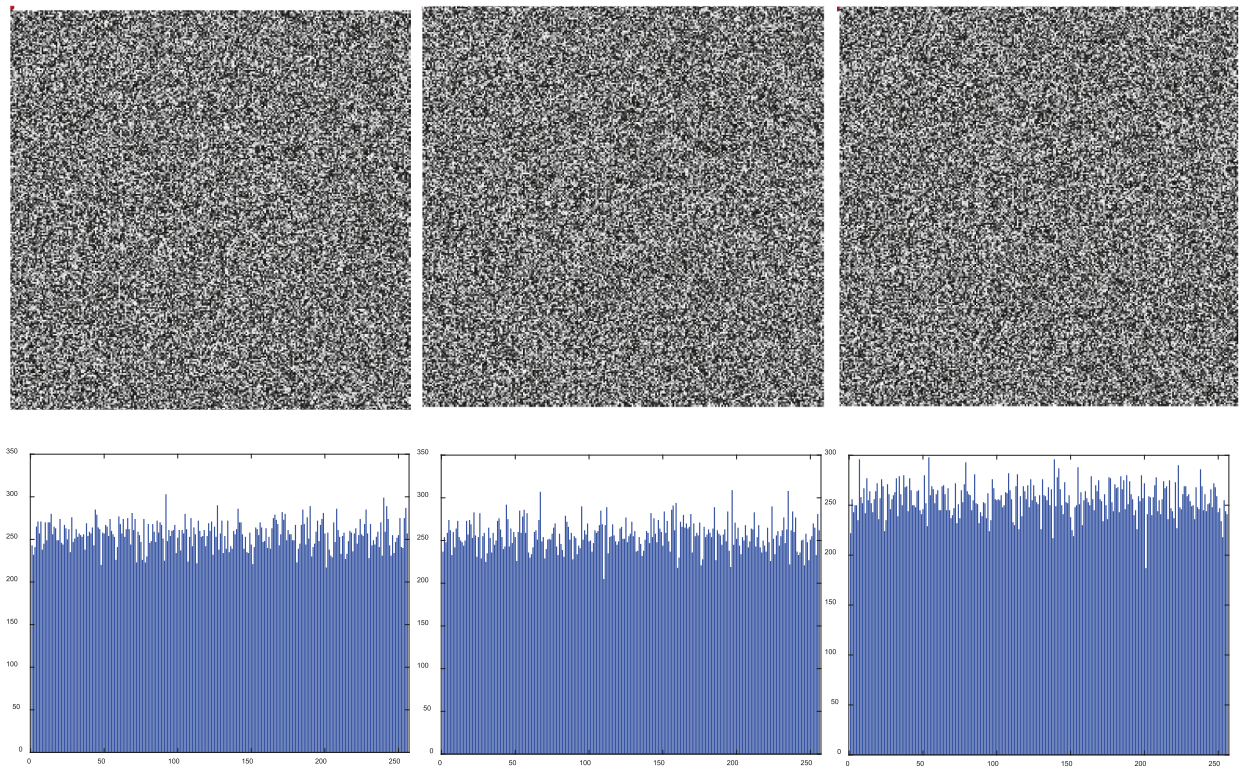

Fig. 14. Encrypted touchless fingerprint images and histogram distributions using random numbers.

Table 4
Correlation coefficients of unencrypted and encrypted image.

Image	Horizontal	Vertical	Diagonal
Unencrypted image (8 bits)	0.94530	0.82450	0.91450
Encrypted image (8 bits)	-0.00017	-0.00011	0.00018

Table 5
Comparison of correlation coefficients on the encrypted images.

Algorithm	**Horizontal**	**Vertical**	**Diagonal**
Proposed method	-0.00017000	-0.00011000	0.00018000
Wu et al. [42]	-0.00021501	0.001491250	0.00402635
Zhang et al. [43]	0.000533462	0.000286785	0.00210009
Hsiao et al. [44]	0.000196000	0.000181000	0.00019500
Li et al. [45]	0.001300000	0.000800000	0.00660000
Sahari et al. [46]	-0.00073600	0.000187000	0.00059200
Kaur et al. [47]	0.012000000	-0.00630000	0.00580000
Cao et al. [48]	-0.00740000	0.001900000	-0.0017000
Zhang et al. [49]	0.007730000	-0.01103000	0.01454000
Chen et al. [50]	-0.00280000	0.017100000	-0.0022000
Xu et al. [51]	0.001900000	0.026300000	0.01960000

$$I_D = \sum_{i=0}^{255} |h_i - M_h|$$

where h is the absolute difference of original image and encrypted image. A smaller I_D indicates that the histogram is near uniformity and increases the statistical characteristics of encryption.

Another method used to measure encryption quality is the deviation from uniform histogram which given by

$$D_H = \frac{\sum_{C_i}^{255} |H_{C_i} - H_c|}{MxN}$$

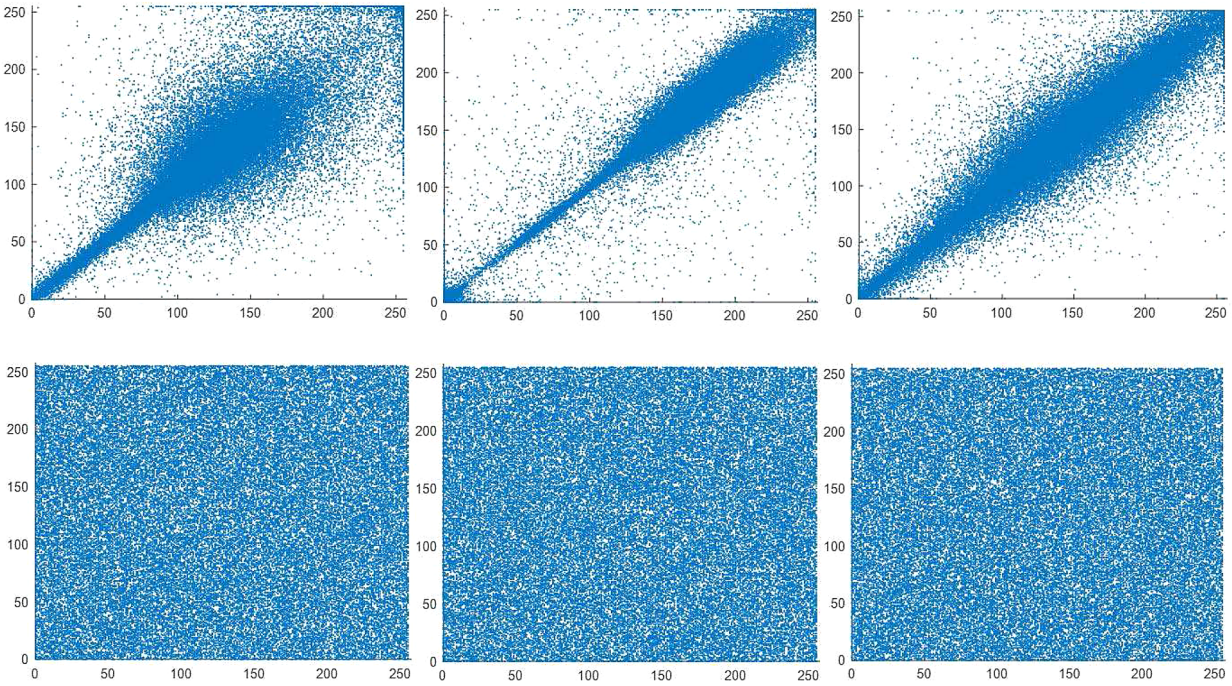

Fig. 15. Correlation maps of three different touchless fingerprint images and encrypted images.

Table 6
Entropy coefficients of three sample images.

No.	Sample Images	Entropy
1	Fingerprint image	7.0745
	Encrypted image	7.9975
2	Fingerprint image	6.9948
	Encrypted image	7.9982
3	Fingerprint image	7.1875
	Encrypted image	7.9977

Table 7
Maximum deviation, irregular deviation and deviation from uniform histogram.

No.	Test Image	Maximum Deviation	Irregular Deviation	Deviation From Uniform Histogram
1	Fingerprint image	24,451	18,648	0.03542
2	Fingerprint image	28,486	20,145	0.03845
3	Fingerprint image	25,348	17,985	0.03154

Table 8
Comparison of information entropy with the existing algorithms.

Algorithms	Entropy
Proposed method	7.9982
Li et al. [45]	7.9992
Sahari et al. [46]	7.9982
Kaur et al. [47]	7.9989
Chen et al. [50]	7.9891
Xu et al. [51]	7.9974

Table 9
NPCR and UACI of encrypted touchless fingerprint.

No.	Sample Images	NPCR	UACI
1	Encrypted fingerprint image	99.741	33.508
2	Encrypted fingerprint image	99.724	33.512
3	Encrypted fingerprint image	99.746	33.502

where MxN is the size of image, C_i is the gray level of pixel (0–255), H_c is the histogram of encrypted image and H_{C_i} is the histogram value at index i. The smaller D_H value shows the more consistent distribution of histograms and the higher standard of encryption. Table 7 shows the maximum deviation, irregular deviation and deviation from uniform histogram values of the encrypted images.

Table 8 shows some entropy values obtained from the existing encryption algorithm. The entropy value of the encrypted image based on the proposed encryption algorithm is very close to 8. It shows that the proposed encryption method can withstand malicious attacks effectively, and the entropy value is consistent with the exiting literature. Comparing the degree of similarities between two distinct images is an important metric. The method of differential analysis is used in image encryption to measure that value. The key used for a good encryption must be sensitive to mismatches according to Kerckhoff's scenario. A small change of key in the encrypted image causes very serious differences. Two differential analyses were performed to measure and assess these sensitivities. The NPCR and UACI are often used, which are expressed as follows

$$NPCR = \frac{1}{RC}\sum_{i=1}^{R}\sum_{j=1}^{C} Dif(i,j) \times 100\% \tag{8}$$

$$Dif(i,j) = \begin{Bmatrix} 1, & when\ V_1(i,j) \neq V_2(i,j) \\ 0, & when\ V_1(i,j) = V_2(i,j) \end{Bmatrix} \tag{9}$$

$$UACI = \frac{1}{RC}\frac{\sum_{i=1}^{R}\sum_{j=1}^{C}|V_1(i,j) - V_2(i,j)|}{255} \times 100\% \tag{10}$$

where R is the total number of rows in the image, C is the total number of columns, V_1 is the unencrypted image pixel value and V_2 is the encrypted image pixel value. The NPCR shows the number of pixels replaced and the UACI indicates the average value of the pixels that have been changed [52].

NPCR and UACI results obtained as a result of differential attack also show that the encryption is successful and resistant against attacks. When all these results are considered together, it can be said that encryption is successful and provides high security. In Table 9, NPCR and UACI analyzes between three different encrypted images and contactless fingerprint images are given. NPCR indicates the number of pixels changed and UACI indicates the average value of the pixels changed [52]. In previous studies, as an indicator of strong encryption, it was agreed that NPCR is greater than 99.6% and UACI is equivalent to 30% or greater [53]. Table 10 lists the NPCR and UACI values obtained from twelve different image encryption algorithms. The NPCR and UACI values of the proposed encryption algorithm are obtained as 99.73% and 33.51%, respectively. The proposed encryption algorithm has been found to be superior to many algorithms improved in recent years in terms of its ability to prevent differential attacks.

6. Conclusions

Based on a Lorenz-type system, this work created a new four-dimensional memristive chaotic system with line equilibria and coexisting attractors. The dynamic behavior analysis of the system corresponds the parameters and coupling strength indicated that the system is easy to yield chaos and coexisting attractors. The circuit implementation of the system was studied as well. Also we considered the application of the system on touchless fingerprint encryption. According to the system, the chaos-based random

Table 10
NPCR and UACI of encrypted touchless fingerprint.

Algorithms	NPCR (mean)	UACI (mean)
Proposed method	99.73	33.51
Wu et al. [42]	99.60	33.42
Zhang et al. [43]	99.79	28.29
Hsiao et al. [44]	99.61	33.46
Li et al. [45]	99.60	33.43
Sahari et al. [46]	99.61	33.45
Kaur et al. [47]	99.67	33.58
Cao et al. [48]	99.60	33.48
Zhang et al. [49]	88.99	30.21
Chen et al. [50]	99.59	33.42
Xu et al. [51]	99.62	33.51

number generator and the corresponding randomness tests were established. An algorithm for touchless fingerprint encryption was proposed, and its effectiveness and security were verified by some experimental tests.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61961019, the Key Research and Development Program of Jiangxi Province of China under Grant 20181BBE50017, and the Youth Key Project of Natural Science Foundation of Jiangxi Province of China under Grant 20202ACBL212003. This work was also supported by the Scientific and the Research Council of Turkey (TUBITAK) under Grant No. 117E284.

References

[1] L.O. Chua, Memristor-the missing circuit element, IEEE Trans Circ. Theory 18 (1971) 507–519.
[2] D.B. Strukov, G.S. Snider, D.R. Stewart, R.S. Williams, The missing memristor found, Nature 453 (2008) 80–83.
[3] M. Itoh, L.O. Chua, Memristor oscillators, Int. J. Bifur. Chaos 18 (2008) 3183–3206.
[4] B.C. Bao, Z. Ma, J. Xu, Z. Liu, Q. Xu, A simple memristor chaotic circuit with complex dynamics, Int. J. Bifur. Chaos 21 (2011) 2629–2645.
[5] V.T. Pham, S. Jafari, S. Vaidyanathan, S. Volos, X. Wang, A novel memristive neural network with hidden attractors and its circuitry implementation, Sci. China-Tech. Sci. 59 (2016) 358–363.
[6] J. Kengne, A.N. Negou, D. Tchiotsop, Antimonotonicity, chaos and multiple attractors in a novel autonomous memristor-based jerk circuit, Nonlinear Dyn. 88 (2017) 2589–2608.
[7] B. Muthuswamy, L.O.C. B, Simplest chaotic circuit, Int. J. Bifur. Chaos 20 (2010) 1567–1580.
[8] B. Muthuswamy, L.O. Chua, Implementing memristor based chaotic circuits, Int. J. Bifur. Chaos 20 (2010) 1335–1350.
[9] B.C. Bao, G. Shi, J. Xu, Z. Liu, S. Pan, Dynamics analysis of chaotic circuit with two memristors, Sci. China–Tech. Sci. 54 (2011) 2180–2187.
[10] B.C. Bao, H. Bao, N. Wang, M. Chen, Q. Xu, Hidden extreme multistability in memristive hyperchaotic system, Chaos Solit. Fract. 94 (2017) 102–111.
[11] Q. Li, H. Zeng, J. Li, Hyperchaos in a 4d memristive circuit with infinitely many stable equilibria, Nonlinear Dyn. 79 (2015) 2295–2308.
[12] F. Corinto, M. Forti, Memristor circuits: bifurcations without parameters, IEEE Trans. Circ. Syst.-I: Regular Papers 64 (2017) 1540–1551.
[13] Q. Jin, F. Min, C.B. Li, Infinitely many coexisting attractors of a dual memristive shinriki oscillator and its FPGA digital implementation, Chin. J. Phys. 62 (2019) 342–357.
[14] Z. Wen, Z. Li, X. Li, Bursting dynamics in parametrically driven memristive jerk system, Chin. J. Phys. 66 (2020) 327–334.
[15] Q. Lai, Z. Wan, P.D.K. Kuate, H. Fotsin, Coexisting attractors, circuit implementation and synchronization control of a new chaotic system evolved from the simplest memristor chaotic circuit, Commun. Nonlinear Sci. Numer. Simul. 89 (2020) 105341.
[16] B.C. Bao, H. Qian, Q. Xu, M. Chen, J. Wang, Y. Yu, Coexisting behaviors of asymmetric attractors in hyperbolic-type memristor based hopfield neural network, Front. Comput. Neurosci. 11 (2017) 81.
[17] F. Parastesh, S. Jafari, H. Azarnoush, B. Hatef, H. Namazi, D. Dudkowski, Chimera in a network of memristor-based hopfield neural network, European Phys. J.-Special Topics 228 (2019) 2023–2033.
[18] S. Dadras, H.R. Momeni, A novel three-dimensional autonomous chaotic system generating two, three and four-scroll attractors, Phys. Lett. A 373 (2009) 3637–3642.
[19] Q. Lai, A. Akgul, C.B. Li, G. Xu, U. Cavusoglu, A new chaotic system with multiple attractors: dynamic analysis, circuit realization and S-box design, Entropy 20 (2018) 12.
[20] J. Kengne, Z.T. Njitacke, H.B. Fotsin, Dynamical analysis of a simple autonomous jerk system with multiple attractors, Nonlinear Dyn. 83 (2016) 751–765.
[21] Q. Lai, P.D.K. Kuate, F. Liu, H.H.C. Iu, An extremely simple chaotic system with infinitely many coexisting attractors, IEEE Trans. Circ. Syst.-II: Express Briefs 67 (2020) 1129–1133.
[22] Q. Lai, A. Akgul, M. Varan, J. Kengnec, A.T. Erguzel, Dynamic analysis and synchronization control of an unusual chaotic system with exponential term and coexisting attractors, Chin. J. Phys. 56 (2018) 2837–2851.
[23] P. Gholamin, A.H.R. Sheikhani, A new three-dimensional chaotic system: dynamical properties and simulation, Chin. J. Phys. 55 (2017) 1300–1309.
[24] Q. Lai, S. Chen, Generating multiple chaotic attractors from sprott b system, Int. J. Bifur. Chaos 26 (2016) 1650177.
[25] B. Norouzi, S. Mirzakuchaki, A fast color image encryption algorithm based on hyper-chaotic systems, Nonlinear Dyn. 78 (2014) 995–1015.
[26] Q. Lai, B. Norouzi, F. Liu, Dynamic analysis, circuit realization, control design and image encryption application of an extended lu system with coexisting attractors, Chaos Solit. Fract. 114 (2018) 230–245.
[27] Z. Hua, Y. Zhou, Image encryption using 2d logistic–adjusted-sine map, Inf. Sci. (Ny) 339 (2016) 237–253.
[28] M. Alawida, A. Samsudin, J.S. Teh, R.S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, Signal Process. 160 (2019) 45–58.
[29] G. Peng, F. Min, Multistability analysis, circuit implementations and application in image encryption of a novel memristive chaotic circuit, Nonlinear Dyn. 90 (2017) 1607–1625.
[30] C.K. Volos, I.M. Kyprianidis, I.N. Stouboulos, Fingerprint images encryption process based on a chaotic true random bits generator, Int. J. Multimedia Intell. Securi. 1 (2010) 320–335.
[31] Y.C. Hung, C.K. Hu, Chaotic communication via temporal transfer entropy, Phys. Rev. Lett. 101 (2008) 244102.
[32] J. Luo, S. Qu, Y. Chen, Z. Xiong, Synchronization of memristor-based chaotic systems by a simplified control and its application to image en-/decryption using DNA encoding, Chin. J. Phys. 62 (2019) 374–387.
[33] R. Vidhya, M. Brindha, N.A. Gounden, A secure image encryption algorithm based on a parametric switching chaotic system, Chin. J. Phys. 62 (2019) 26–42.
[34] S.S. Jamal, S. Farwa, A.H. Alkhaldi, M. Aslam, M.A. Gondal, A robust steganographic technique based on improved chaotic-range systems, Chin. J. Phys. 61 (2019) 301–309.
[35] F. Han, J. Hu, Y. Wang, Fingerprint images encryption via multi-scroll chaotic attractors, Appl. Math. Compu. 185 (2007) 931–939.
[36] C. Liu, T. Liu, L. Liu, K. Liu, A new chaotic attractor, Chaos Solit. Fract. 22 (2004) 1031–1038.
[37] L.E. Bassham, A.L. Rukhin, J. Soto, J.R. Nechvatal, M.E. Smid, E.B. Barker, S.D. Leigh, M. Levenson, M. Vangel, D.L. Banks, N.A. Heckert, J.F. Dray, S. Vo, SP 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST, Gaithersburg, MD, USA, NIST Special Publication 1, 2010, pp. 800–822.
[38] J. Walker, ENT-a pseudorandom number sequence test program, 2008, Available online: www.fourmilab.ch/random/.
[39] B. Stoyanov, K. Kordov, A novel pseudorandom bit generator based on chirikov standard map filtered with shrinking rule, Math. Prob. Eng. (2014) 986174. 2014

[40] D. Seetharam, S. Rhee, A.e. p. r. n.g.f.l.-p.s.n.w. networks, IEEE Int. Conf. Local Comput. Netw. (2004).
[41] A. Akhshani, A. Akhavan, A. Mobaraki, S. Lim, Z. Hassan, Pseudo random number generator based on quantum chaotic map, Commun. Nonlinear Sci. Numer. Simul. 19 (2014) 101–111.
[42] Y. Wu, J.P. Noonan, G. Yang, H. Jin, Image encryption using the two-dimensional logistic chaotic map, J. Electr. Imag. 21 (2012) 013014.
[43] Y.Q. Zhang, X.Y. Wang, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, Inf. Sci. (Ny) 273 (2014) 329–351.
[44] H.I. Hsiao, J. Lee, Fingerprint image cryptography based on multiple chaotic systems, Signal Process. 113 (2015) 169–181.
[45] Z. Li, C. Peng, L. Li, X. Zhu, A novel plaintext-related image encryption scheme using hyper-chaotic system, Nonlinear Dyn. 94 (2018) 1319–1333.
[46] M.L. Sahari, I. Boukemara, A pseudo-random numbers generator based on a novel 3d chaotic map with an application to color image encryption, Nonlinear Dyn. 94 (2018) 723–744.
[47] M. Kaur, V. Kumar, Efficient image encryption method based on improved lorenz chaotic system, Electron. Lett. 54 (2018) 562–564.
[48] W. Cao, Y. Zhou, C.P.P. Chen, L. Xia, Medical image encryption using edge maps, Signal Process. 132 (2017) 96–109.
[49] J. Zhang, D. Hou, H. Ren, Image encryption algorithm based on dynamic DNA coding and chen's hyperchaotic system, Math. Prob. Eng. (2016) 6408741. 2016
[50] X. Chen, C.J. Hu, Adaptive medical image encryption algorithm based on multiple chaotic mapping, Saudi J. Bio. Sci. 24 (2017) 1821–1827.
[51] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Opt. Lasers Eng. 78 (2016) 17–25.
[52] C. Fu, J.J. Chen, H. Zou, W.H. Meng, Y.F. Zhan, Y. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, Opt. Express 20 (2012) 2363–2378.
[53] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, J.B. Rayappan, Pixel scattering matrix formalism for image encryption-a key scheduled substitution and diffusion approach, AEU-Int. J. Electr. Commun. 69 (2015) 562–572.