Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-15867-z

Circuit realization and FPGA-based implementation of a fractional-order chaotic system for cancellable face recognition

Iman S. Badr[1] · Ahmed G. Radwan[2,3] · El-Sayed M. EL-Rabaie[1] · Lobna A. Said[3] · Walid El-Shafai[1,4] · Ghada M. El-Banby[5] · Fathi E. Abd El-Samie[1,6]

Received: 26 November 2022 / Revised: 24 March 2023 / Accepted: 16 May 2023

Abstract
Biometric security has been developed in recent years with the emergence of cancellable biometric concepts. The idea of the cancellable biometric traits is concerned with creating encrypted or distorted traits of the original ones to protect them from hacking techniques. So, encrypted or distorted biometric traits are stored in databases instead of the original ones. This can be accomplished through non-invertible transforms or encryption schemes. In this paper, a cancellable face recognition algorithm is introduced based on face image encryption through a fractional-order multi-scroll chaotic system. The fundamental concept is to create random keys that will be XORed with the three components of color face images (red, green, and blue) to obtain encrypted face images. These random keys are generated from the Least Significant Bits of all state variables of a proposed fractional-order multi-scroll chaotic system. Lastly, the encrypted color components of face images are combined to produce a single cancellable trait for each color face image. The results of encryption with the proposed system are full-encrypted face images that are suitable for cancellable biometric applications. The strength of the proposed system is that it is extremely sensitive to the user's selected initial conditions. The numerical simulation of the proposed chaotic system is done with MATLAB. Phase and bifurcation diagrams are used to analyze the dynamic performance of the proposed fractional-order multi-scroll chaotic system. Furthermore, we realized the hardware circuit of the proposed chaotic system on the PSpice simulator. The proposed chaotic system can be implemented on Field Programmable Gate Arrays (FPGAs). To model our generator, we can use Verilog Hardware Description Language HDL, Xilinx ISE 14.7 and Xilinx FPGA Artix-7 XC7A100T based on Grunwald-Letnikov algorithms for mathematical analysis. The numerical simulation, the circuit simulation and the hardware experimental results confirm each other. Cancellable face recognition based on the proposed fractional-order chaotic system has been implemented on FERET, LFW, and ORL datasets, and the results are compared with those of other schemes. Some evaluation metrics containing Equal Error Rate (EER), and Area under the Receiver Operating Characteristic (AROC) curve

✉ Walid El-Shafai
welshafai@psu.edu.sa; eng.waled.elshafai@gmail.com; walid.elshafai@el-eng.menofia.edu.eg

Extended author information available on the last page of the article

Published online: 07 March 2024

are used to assess the cancellable biometric system. The numerical results of these metrics show EER levels close to zero and AROC values of 100%. In addition, the encryption scheme is highly efficient.

Keywords Fractional-order chaos · Cancellable face recognition · PSpise · FPGA

1 Introduction

Nowadays, non-integer or fractional-order chaotic systems are becoming very interesting topics for engineers, physicists, and mathematicians, because most real physical systems are inherently nonlinear. Their application fields have become more and more important because of the utilization of fractional-order mathematics in several real-world fields, such as electronic systems, machine systems, mathematics, signal generators [16, 19], biology, robotics, synchronization, random number generators, communication security and image processing.

It is important to note that many papers have been published presenting implementations of integer-order chaotic systems, and systems using analog integrated circuit technology and digital hardware like micro-controllers, and FPGAs. This is not the case for fractional-order chaotic systems that are mathematical models comprising fractional derivatives in nonlinear equations that are difficult to solve, analytically.

However, analog implementations using passive circuit components, multipliers, and amplifiers suffer from the high sensitivity to any variation process, which requires more complex analog circuitry to solve the fractional derivatives. In addition, digital implementations suffer from the problem of degradations due to the reduced number of bits to perform computer arithmetic operations. So, we require more complex digital hardware to implement memory blocks.

The main objective of the recent works is oriented to introducing alternatives for the analog/digital implementations of fractional-order chaotic oscillators, trying to provide details on the synthesis and physical realization using either analog or digital electronics. Moreover, fractional-order chaotic systems are used for cancellable biometric applications to enhance the security of biometric systems. In the past few years, the theoretical design and circuit implementation of many different chaotic systems have attracted more and more attention of engineers. They used them in many real-world applications, such as secure communication [27], random number generators, image processing, encryption [10], and cancellable biometric recognition. After the first family of n-double scroll (multi-scroll) chaotic attractors was introduced by Suykens and Vandewalle, the authors utilized quasi-linear function techniques [22]. These techniques can be used to generate multi-scroll chaotic systems with high complexity in many applications because of their high sensitivity to initial conditions and change of parameters. Badr et al. [4] presented partial encryption for cancellable biometrics, but the proposed system in this paper depends on full encryption.

Recent works have concentrated on fractional-order mathematical models of chaotic systems to evaluate their equilibrium points, and stability, in addition to performing numerical simulations with appropriate methods in the frequency and time domains, such as Caputo, Grünwald-Letnikov, and Adams-Bashforth-Moulton methods. Under certain conditions, analog and digital hardware of integer-order chaotic systems are relatively simple to implement.

The Grünwald-Letnikov method is utilized to calculate the fractional derivative of a function $g(t)$.

$$ {}_aD_t^q g(t) = \lim_{h \to 0} \frac{1}{h^q} \sum_{i=0}^{\lfloor (t-a)/h \rfloor} w_i^{(q)} g(t - ih), \tag{1} $$

where $g(t)$ is a continuous function, q is any positive real number, in the range of $0 < q < 1$ for the fractional-order chaotic system and h is the step size. $w_i^{(q)}$ denotes the binomial coefficients calculated with the following formula:

$$ w_0^{(q)} = 1, \quad w_i^{(q)} = \left(1 - \frac{q+1}{i}\right) w_{i-1}^{(q)}, \quad i = 1, 2, 3, \ldots \tag{2} $$

Figure 3 shows that the magnitude of binomial coefficient $w_i^{(q)}$ approaches zero, when the index increases. In other words, when fractional order q tends to an integer value, the dependence of the values of the binomial coefficients decreases. A fractional-order system of three differential equations has the following general form:

$$ \begin{aligned} D^{q_1} x &= S(x, y, z, t) \\ D^{q_2} y &= P(x, y, z, t) \\ D^{q_3} z &= Q(x, y, z, t) \end{aligned} \tag{3} $$

This system can be simulated based on GL definition with the following set of equations:

$$ \begin{aligned} x_{t_k} &= S\left(x\left(t_{k-1}\right), y\left(t_{k-1}\right), z\left(t_{k-1}\right)\right) h^{q_1} - \sum_{i=1}^{n} w_i^{(q_1)} x\left(t_{k-i}\right) \\ y_{t_k} &= P\left(x\left(t_{k-1}\right), y\left(t_{k-1}\right), z\left(t_{k-1}\right)\right) h^{q_2} - \sum_{i=1}^{n} w_i^{(q_2)} y\left(t_{k-i}\right) \\ z_{t_k} &= Q\left(x\left(t_{k-1}\right), y\left(t_{k-1}\right), z\left(t_{k-1}\right)\right) h^{q_3} - \sum_{i=1}^{n} w_i^{(q_3)} z\left(t_{k-i}\right) \end{aligned} \tag{4} $$

where $n = L$ denotes the approximated window variation of the GL operator, and if $n = k$, this means that all state memory is used in the calculations. The proposed system is able to overcome the drawbacks of the previous methods. It allows complete hiding of biometric patterns instead of partial hiding in [4]. It helps to enhance user privacy, while maintaining a high degree of security. Moreover, a fractional-order multi-scroll chaotic system is exploited in the generation of cancellable templates. The utilization of multiple keys enhances the degree of security.

In this paper, we introduce a proposed chaotic system that generates multi-scroll chaotic attractors. The paper is organized as follows. Section 2 presents the literature survey. Section 3 present a construction of the proposed multi-scroll chaotic system and its properties. Section 4 presents the description of the fractional-order multi-scroll chaotic system. In Section 5, circuit realization is presented for the proposed chaotic system. In Sections 6, FPGA realizations are studied to implement the multi-scroll chaotic system and present some experimental results. Section 7 presents the simulation results. Section 8 presents the cancellable face recognition scheme based on the proposed fractional-order multi-scroll chaotic system. Finally, the conclusions are introduced in the last section.

2 Literature survey

Multiple chaotic attractors can be generated by chaotic systems. Several valuable results have been introduced in [9, 25]. For example, Cui et al [9] presented a multi-scroll chaotic system, which generates multi-scroll chaotic attractors based on sinusoidal nonlinear terms. A new color image encryption scheme was produced based on the fractional-order multi-scroll Chen chaotic system and the DNA mutation principle [11].

Liang et al. [12] presented a multi-scroll chaotic system, which generates multi-scroll chaotic attractors based on a nonlinear exponential function and Chua system. San-Um et al. [18] designed the multi-scroll chaotic system by using a delay differential equation, which employs a piecewise-linear nonlinear function with a tiny delay time. An X- and Heart-shape multi-scroll chaotic system was produced based on the Lorenz circuit and adding a staircase nonlinear function to the system. Soliman et al. [20] designed a multi-scroll chaotic system. Chang et al. [5] presented a multi-scroll chaotic system based on piecewise nonlinear functions to generate a multi-scroll chaotic attractor that is used in secure audio communication.

In addition, Ozoguz et al. [15] presented a multi-scroll chaotic attractor using smooth hyperbolic tangent functions. With different system parameters, Xiong et al. [25] proposed single, double, three, and four chaotic attractors and designed a circuit schematic diagram for realization.

The methods of implementation of chaotic systems represent a vital topic to be studied in real engineering applications. The methods that generate multi-scroll chaotic attractors comprise analog circuits of simple passive components (resistors and capacitors) and an operational amplifier [7, 26], and digital FPGA circuits (embedded system) [5, 24]. For example, in [7], Chen et al. designed an electronic circuit to generate multi-scroll chaotic attractors based on piecewise-linear functions. In addition, based on a sgn function, Cui et al. presented n-scroll chaotic attractors and their circuit realizations to implement the multi-scroll chaotic system [8]. Additionally, in [26], Yan et al. introduced a circuit realization to implement the new 5D fractional-order mutli-scroll chaotic system, whose equations contain cross products and power functions.

Abdelaty et al. [1] studied an FPGA implementation to realize n-scroll chaotic systems based on Product Integration (PI) rules. Additionally, in [24], FPGA circuits were used to implement the multi-scroll chaotic system based on sgn function series. All of these digital and analog circuits are important to generate multi-scroll chaotic attractors. Generally, FPGA circuits are the most popular ones due to lower cost and higher capacity compared to other methods.

3 Construction of the proposed multi-scroll chaotic system and its properties

Motivated by the structure of the model in [13], a new 3D autonomous chaotic system using sgn function series is expressed as follows:

$$\begin{cases} \dot{x} = -uz + uf(z) \\ \dot{y} = z + x - y \\ \dot{z} = -by \end{cases} \tag{5}$$

Table 1 Eigenvalues of each equilibrium point

Eqilibrium	Eigenvalue 1	Eigenvalue 2	Eigenvalue 3
at $z + 2m = 0$	-2.3211	$1.1605 + 4.2474j$	$1.1605 - 4.2474j$
at $z + 2m < 0$	2.3211	$-1.1605 + 4.2474j$	$-1.1605 + 4.2474j$
at $z + 2m > 0$	2.3211	$-1.1605 + 4.2474j$	$-1.1605 + 4.2474j$

The nonlinear sgn function is defined as:

$$f(z) = \sum_{k=-m}^{m} \text{sgn}(z + 2m) \tag{6}$$

Here, x, y and z are three dynamic variables, while u and b are positive control parameters. Also, m is a natural number, and the sgn function is denoted by the following equation:

$$\text{sgn}(z) = \begin{cases} 1, & z > 0 \\ 0, & z = 0 \\ -1, & z < 0 \end{cases} \tag{7}$$

The equilibrium points of the system of (5) can be obtained by setting the right-hand side of the system, represented by (5), equal to zero. This yields the following equations:

$$\begin{cases} -uz + uf(z) = 0 \\ z + x - y = 0 \\ -by = 0 \end{cases} \tag{8}$$

where $b = 15$, $u = 3$ and $m = 1$. The Jacobian matrix can be obtained by linearizing the system in Equation (5) at all equilibrium points and at different values of b and u, as shown in the following equation:

$$J_{(z_l)} = \begin{pmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} & \frac{\partial f_1}{\partial z} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} & \frac{\partial f_2}{\partial z} \\ \frac{\partial f_3}{\partial x} & \frac{\partial f_3}{\partial y} & \frac{\partial f_3}{\partial z} \end{pmatrix} = \begin{bmatrix} 0 & 0 & -u(1 - 2\delta(z_l + 2m)) \\ 1 & -1 & 1 \\ 0 & -b & 0 \end{bmatrix} \tag{9}$$

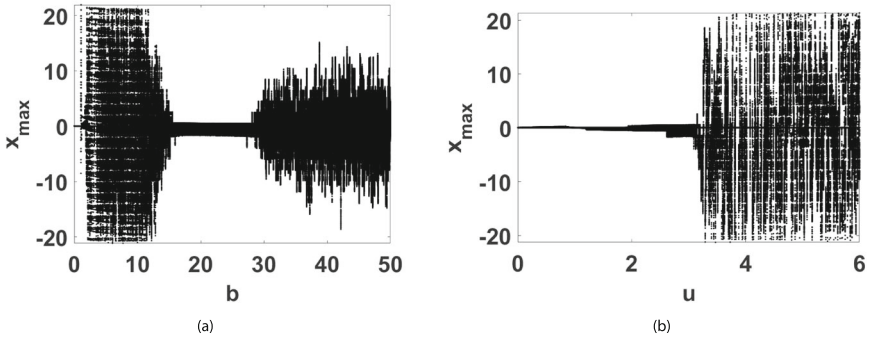


Fig. 1 Bifurcation diagram of the system in Equation (5) on variable x (a) at the parameter b, (b) at the parameter u

From the Jacobian matrix, we can get the characteristic equation of the form $|\lambda I - J_{(z_i)}|$, leading to the system represented by Equation (10). Therefore, the eigenvalues are evaluated for each equilibrium point. The resulting eigenvalues can be obtained as shown in Table 1.

$$\begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} - \begin{bmatrix} 0 & 0 & -u(1-2\delta\,(z_i+2m)) \\ 1 & -1 & 1 \\ 0 & -b & 0 \end{bmatrix} = \begin{bmatrix} \lambda & 0 & +u(1-2\delta\,(z_i+2m)) \\ -1 & \lambda+1 & -1 \\ 0 & b & 0 \end{bmatrix} \tag{10}$$

By fixing the parameters $u = 3$ and $h = 0.009$ and varying the parameter b, the bifurcation diagram is shown in Fig. 1a. In the range of $b \in [0, 50]$, the system is chaotic. Likewise, by fixing the parameters $b = 15$ and $h = 0.009$ and varying the parameter u, the bifurcation diagram is shown in Fig. 1b. In the range of $u \in [0.02, 6]$, the system is chaotic, but in the range of $u \in [0.001, 0.02]$, the system is not chaotic.

Figure 2 shows the chaotic attractor of the proposed chaotic system and the chaotic time series in x, y, and z.

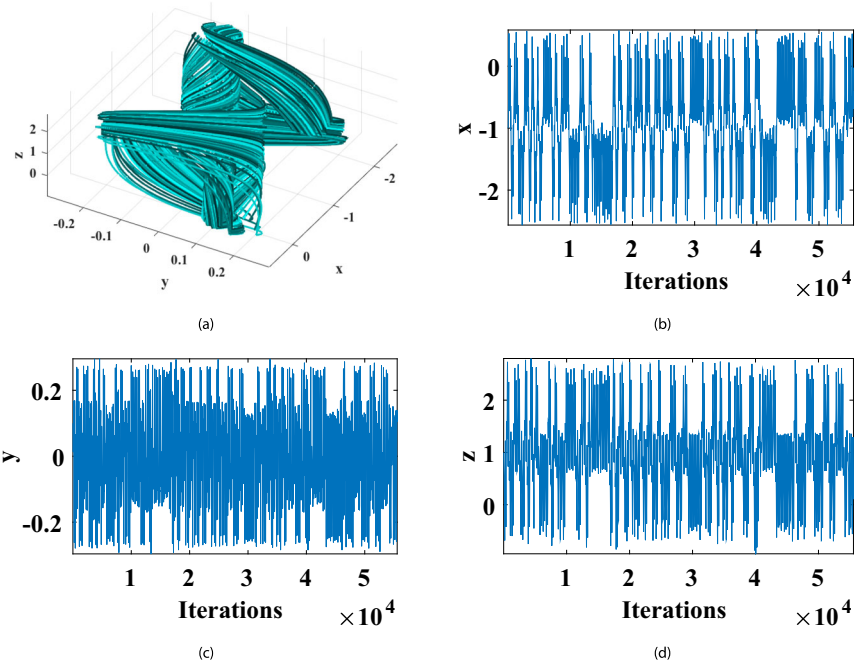


Fig. 2 At $u = 3$, $b = 15$, and $h = 0.009$ (a) x, y, z phase portraits of the system represented by Equation (5), (b), (c) and (d) time series of state variables x, y, and z, respectively, using the initial conditions ($x(0)$, $y(0)$, $z(0)$)=(-1, 0.1, 1)

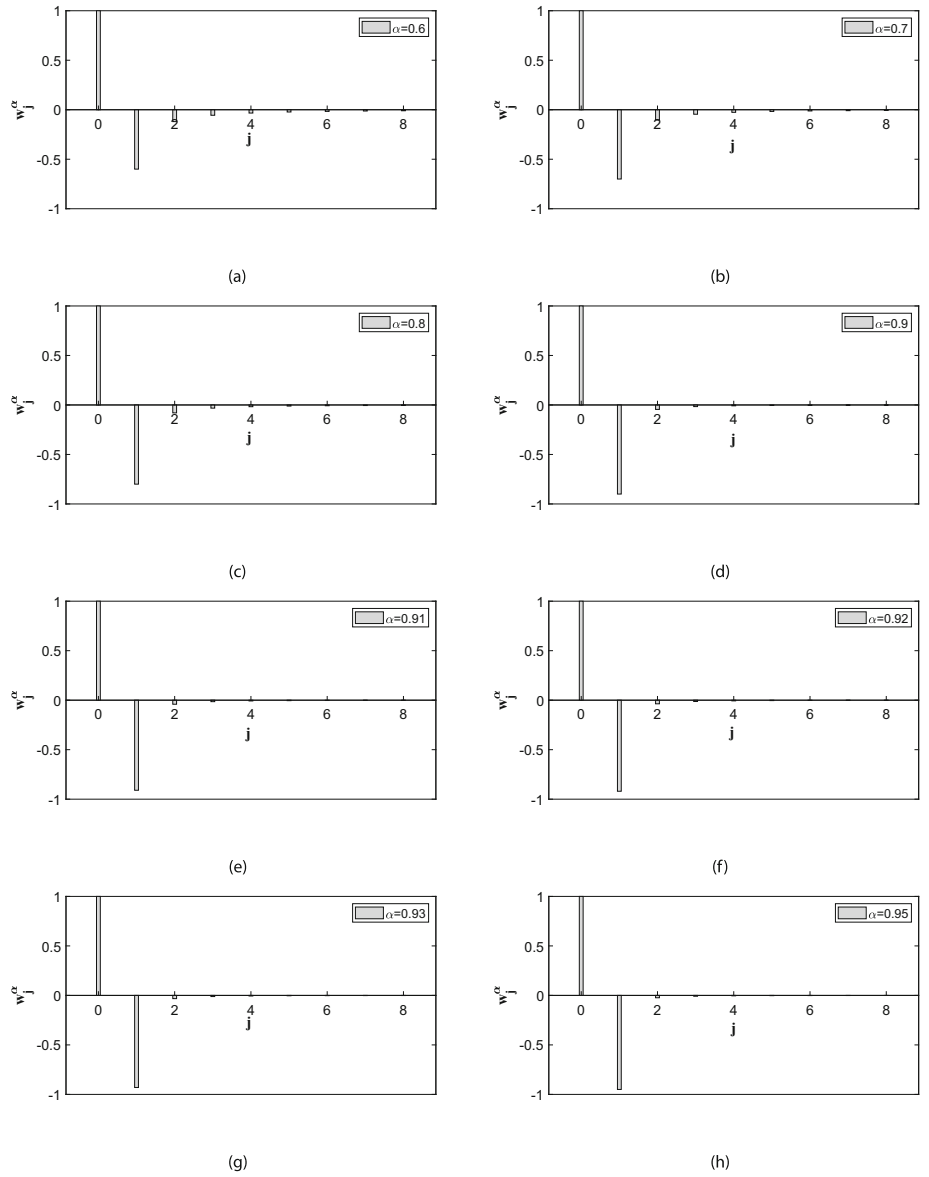


Fig. 3 Graphical representation of the response of binomial coefficient $w_i^{(q)}$ versus index i for (a) $q = 0.6$, (b) $q = 0.7$, (c) $q = 0.8$, (d) $q = 0.9$, (e) $q = 0.91$, (f) $q = 0.92$, (g) $q = 0.93$, (h) $q = 0.95$

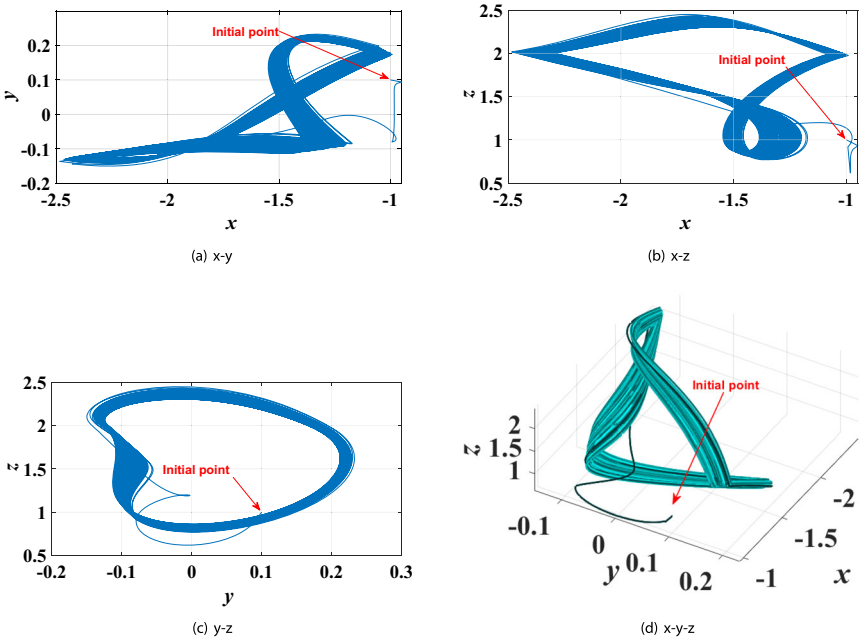


Fig. 4 Simulation results of the proposed fractional-order chaotic system projected onto (a) $x - y$ plane, (b) $x - z$ plane, and (c) $y - z$ plane, where and x, y, and z are state-space portraits of the proposed fractional-order chaotic system based on GL method

4 Description of the fractional-order multi-scroll chaotic system

A proposed 3D autonomous fractional-order multi-scroll chaotic system based on the non-linear sgn function series is represented as follows:

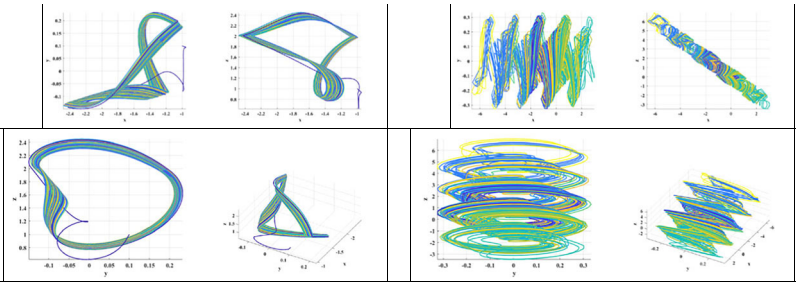
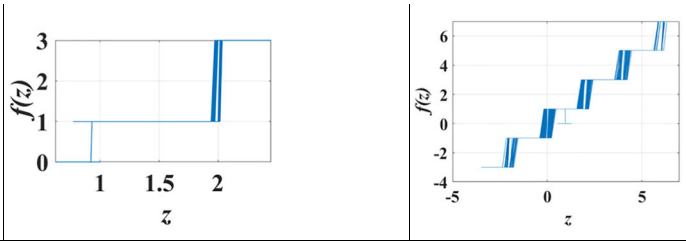
$$\begin{cases} \frac{d^q x}{dt^q} = -uz + u(\sum_{k=-n}^{n} \text{sgn}(z + 2n)) \\ \frac{d^q y}{dt^q} = z + x - y \\ \frac{d^q z}{dt^q} = -by \end{cases} \tag{11}$$

Here, x, y and z are three state variables, while u, and b are non-negative parameters. Also, n is a natural number and sgn function is defined by the following equation:

$$\text{sgn}(z) = \begin{cases} 1, & z > 0 \\ 0, & z = 0 \\ -1, & z < 0 \end{cases} \tag{12}$$

where $u = 3, b = 15, h = 0.009, q = 0.95$ and the initial values of the three state variables are $(x(0), y(0), z(0)) = (-1, 0.1, 1)$. From MATLAB simulation, we obtained phase diagram of the proposed fractional-order chaotic attractor between state variables $x - y$ and $x - z$, $y - z$, and $x - y - z$ as shown in Fig. 4. Table 2 shows the continuous responses of the proposed fractional-order chaotic system versus the parameter h.

Table 2 Chaotic attractors and their nonlinear behavior

	u=3, b=15, h=0.00, q=0.95	u=3, b=15, h=0.05, q=0.95
Chaotic attractors		
Nonlinear function		

5 Circuit design of the proposed fractional-order chaotic system

5.1 Fractional integrator approximation

According to Matsuda approximation [14], the linear approximated transfer function $F(s)$ of a fractional integrator of order 0.95 is

$$F(s) = \frac{1}{s^{0.95}} \approx \frac{s^3 + 1.486 \times 10^5 s^2 + 1.214 \times 10^8 s + 5.022 \times 10^9}{9.763 \times 10^4 s^3 + 9.321 \times 10^7 s^2 + 4.502 \times 10^9 s + 1.196 \times 10^9} \tag{13}$$

The implementation of Equation (13) in Laplace domain is seen in Fig. 5a. Box "F" represents the fractional-order differential unit between a and b. The transfer function $H(s)$ of this box, which equals $\frac{1}{C_0 F(s)}$, is given by:

$$H(s) = \frac{1}{C_0 s^{0.95}} = \frac{1/C_1}{s + 1/R_1 C_1} + \frac{1/C_2}{s + 1/R_2 C_2} + \frac{1/C_3}{s + 1/R_3 C_3} + R_0 \tag{14}$$

where C_0 is a unit parameter. Thus, if we consider the capacitor $C_0 = 10\,nF$, by comparing the two equations (13) and (14), we obtain the values of circuit elements: resistors and capacitors as $R_0 = 1024\,\Omega$, $R_1 = 20\,k\Omega$, $R_2 = 360\,k\Omega$, $R_3 = 419410\,k\Omega$, $C_1 = 47.36\,nF$, $C_2 = 55.41\,nF$, and $C_3 = 8.92\,nF$. According to Charef approximation [6], at $q = 0.95$, the approximated transfer function $F(s)$ is:

$$\frac{1}{s^{0.95}} \approx \frac{1.2834 s^2 + 18.6004 s + 2.0833}{s^3 + 18.4738 s^2 + 2.6574 s + 0.003} \tag{15}$$

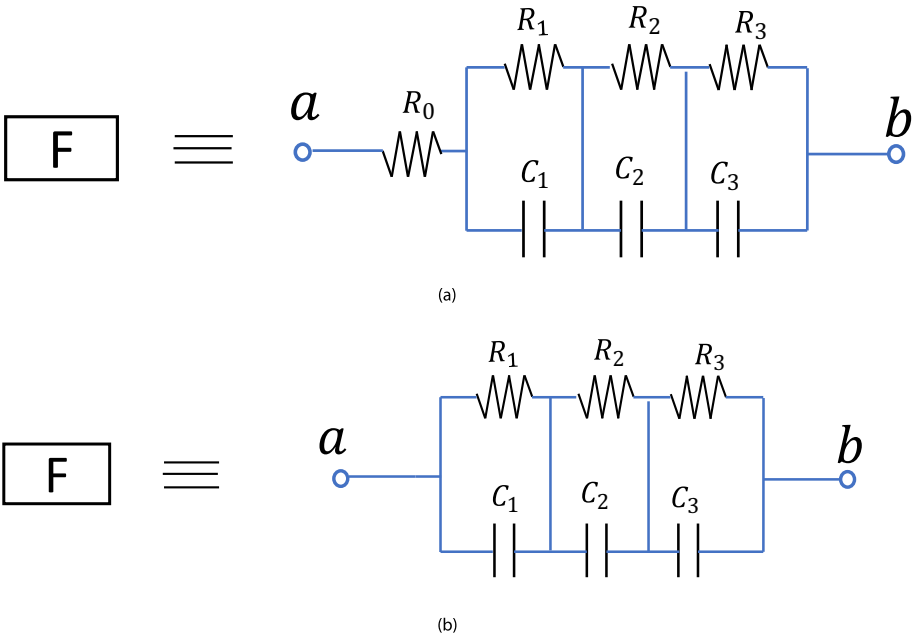


Fig. 5 The fractional-order circuit unit with order $q = 0.95$ (a) according to Matsuda approximation, (b) according to Charef approximation

The transfer function $H(s) = \frac{1}{C_0 s^{0.95}}$ is given by:

$$H(s) = \frac{R_1}{sR_1C_1 + 1} + \frac{R_2}{sR_2C_2 + 1} + \frac{R_3}{sR_3C_3 + 1} \tag{16}$$

The realization of Equation (16) is given in Fig. 5b. If C_0 is equal to $10\,nF$, we obtain the values of resistances and capacitances as $R_1 = 15.266\,k\Omega$, $R_2 = 151100\,k\Omega$, $R_3 = 69.291\,G\Omega$, $C_1 = 35.739\,nF$, $C_2 = 46.06\,nF$, and $C_3 = 12.67\,nF$.

5.2 Description of the circuit

In this section, the circuit is designed in order to realize the proposed system of Equation (11). An electronic circuit diagram of a proposed chaotic system is shown in Fig. 6. The circuit shown in Fig. 6b is for the summation of the nonlinear sgn function signal. The implementation of the proposed fractional-order chaotic system depends on electronic components like resistors, capacitors, and TL082 operational amplifiers. The voltage power supply is equal to ± 15. By analyzing the the circuit implementation of the proposed system shown in Fig. 6, the circuit equations are given by:

$$\begin{cases} D^q x = \frac{R_4}{C_0 R_7}\left[\left(\frac{1}{R_5}\right) z - \left(\frac{1}{R_6}\right) f(z)\right] \\ D^q y = \frac{R_8}{C_0 R_{12}}\left[\left(\frac{1}{R_9}\right) x + \left(\frac{1}{R_{10}}\right) y - \left(\frac{1}{R_{11}}\right) z\right] \\ D^q z = \frac{R_{15}}{C_0 R_{17}}\left[\left(\frac{1}{R_{16}}\right) y\right] \end{cases} \tag{17}$$

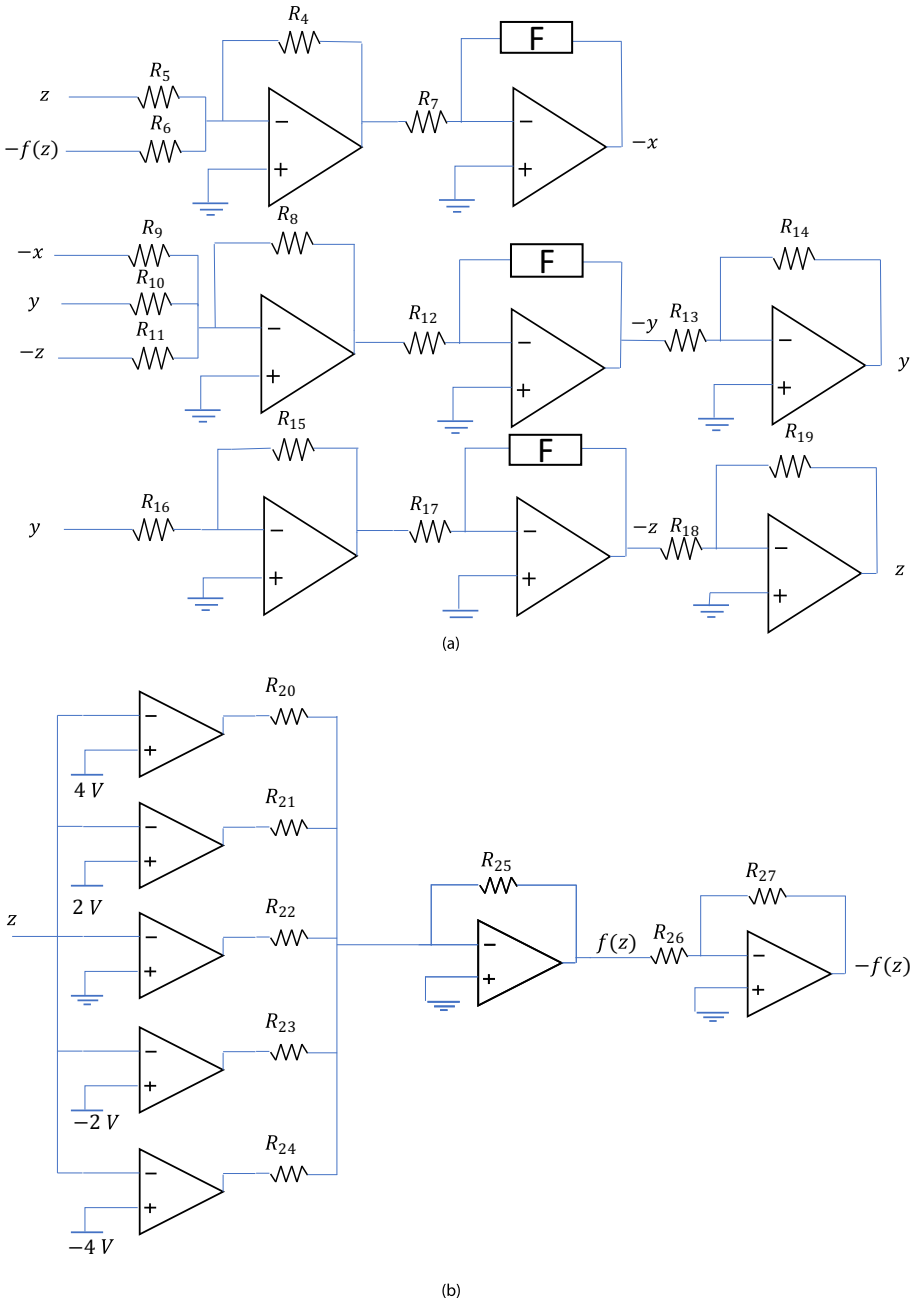
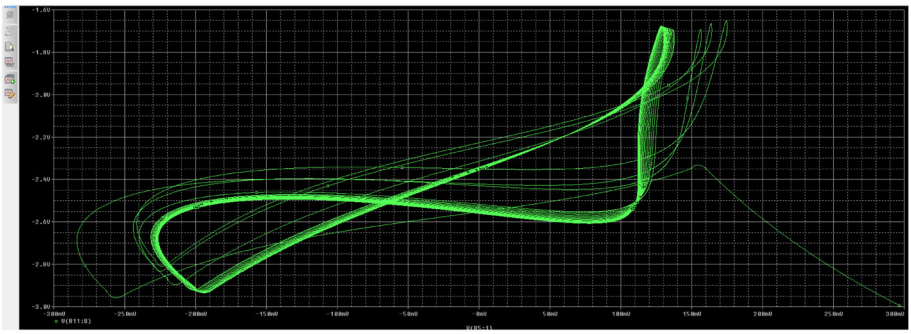
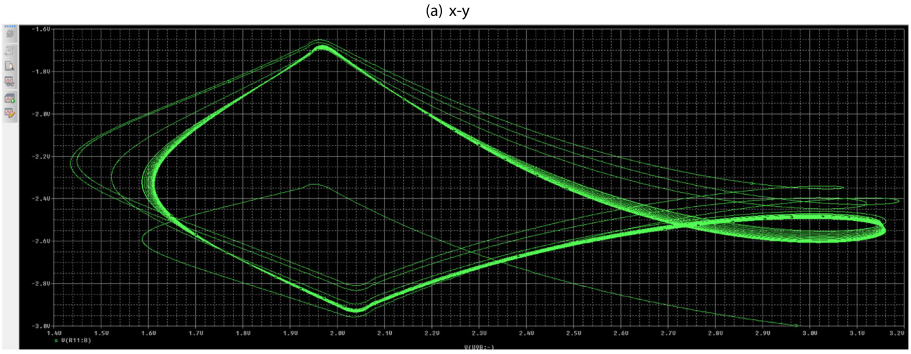


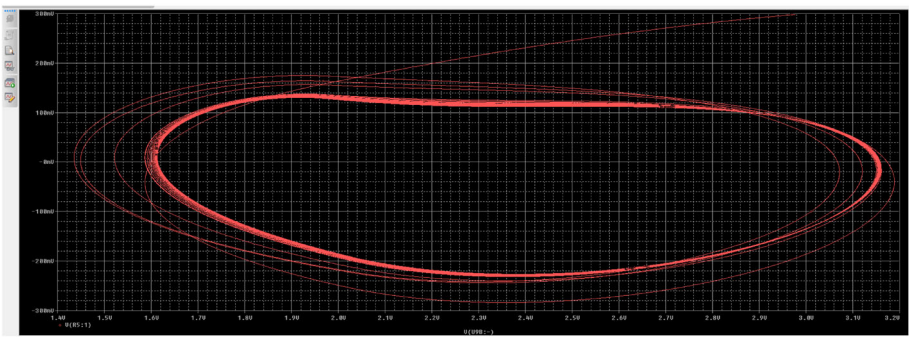
Fig. 6 Electronic circuit schematic diagram to implement the proposed chaotic system of Equation (11) showing the state variables x, y, z at (a), (b) circuit realization of the sgn function $\sum_{k=-2}^{2} \text{sgn}(z + 2m)$



(a) x-y



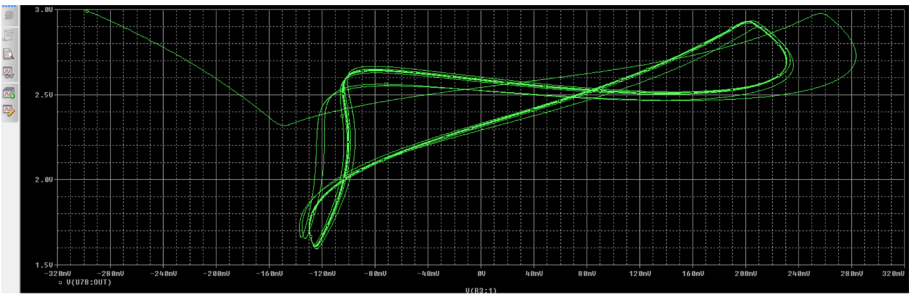
(b) x-z



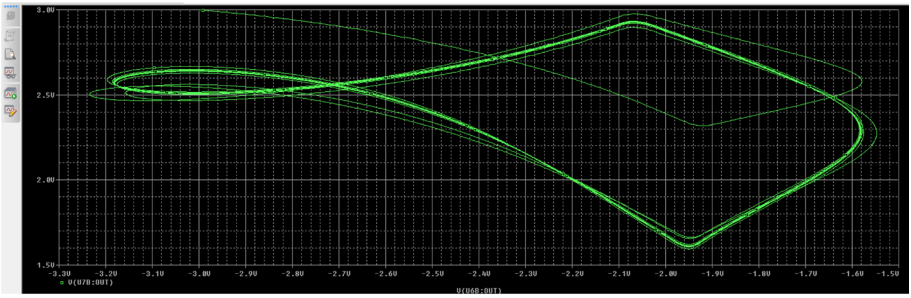
(c) y-z

Fig. 7 Pspice simulation results of the fractional-order chaotic system at fractional order $q = 0.95$

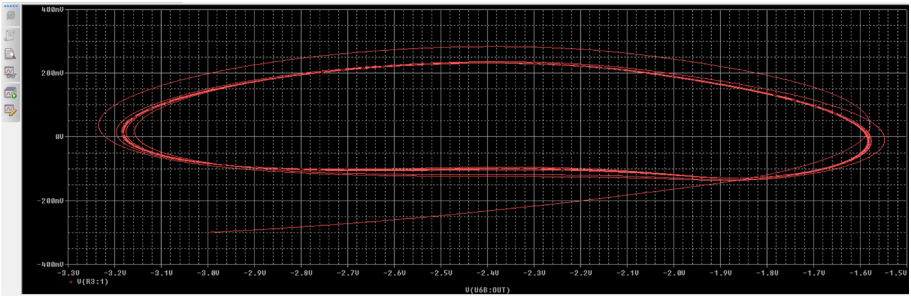
where the parameter values of the circuit schematic diagram are given by $R_4 = 72\ k\Omega$, $R_5 = 24\ k\Omega$, $R_6 = 24\ k\Omega$, $R_7 = 200\ k\Omega$, $R_8 = 72\ k\Omega$, $R_9 = 72\ k\Omega$, $R_{10} = 72\ k\Omega$, $R_{11} = 72\ k\Omega$, $R_{12} = 200\ k\Omega$, $R_{13} = 10\ k\Omega$, $R_{14} = 10\ k\Omega$, $R_{15} = 72\ k\Omega$, $R_{16} = 4.8\ k\Omega$, $R_{17} = 200\ k\Omega$, $R_{18} = 10\ k\Omega$, $R_{19} = 10\ k\Omega$, $R_{20} = 13.5\ k\Omega$, $R_{21} = 13.5\ k\Omega$, $R_{22} = 13.5\ k\Omega$, $R_{23} = 13.5\ k\Omega$, $R_{24} = 13.5\ k\Omega$, $R_{25} = 1\ k\Omega$, $R_{26} = 10\ k\Omega$, and $R_{27} = 10\ k\Omega$. Simulation results using OrCAD PSpice software are shown in Figs. 7 and 8. They are compatible with the MATLAB numerical simulation results as shown in Fig. 4.



(a) x-y



(b) x-z



(c) y-z

Fig. 8 Pspice simulation results of the fractional-order chaotic system at a fractional order $q = 0.95$

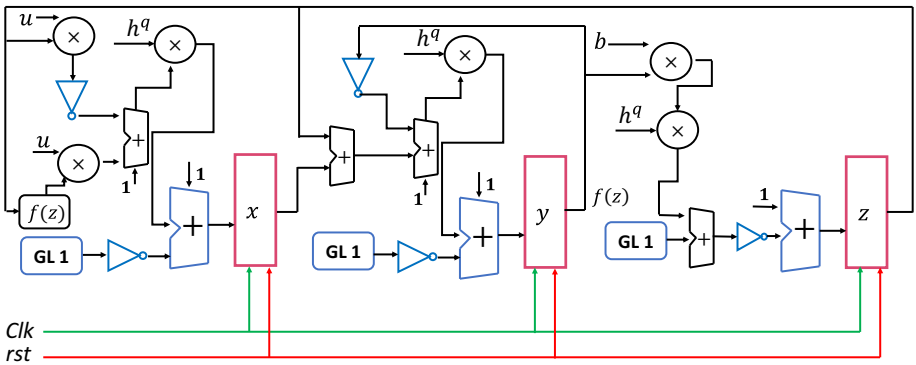


Fig. 9 Hardware architecture of the proposed fractional-order chaotic system

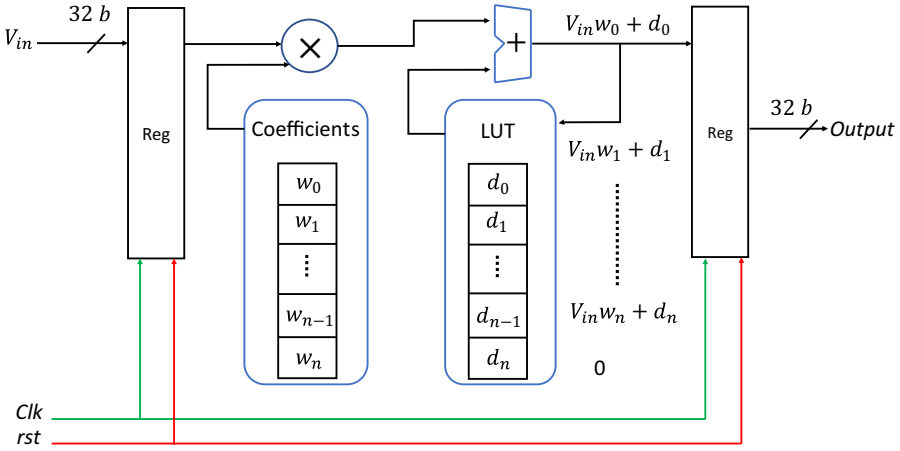


Fig. 10 Hardware design of GL derivatives

6 FPGA implementation

A large capacitor can be used to store the system state, when we use analog integrators, which can be used to create chaotic generators. Chaos generated from analog integration is sensitive to temperature and process variations. Digital implementation does not require capacitors, but it is based on registers to store the system state with a compact size and improved performance. The hardware implementation of the proposed system is shown in Fig. 9, according to the numerical solution given in Equation (4). Three registers are used to store the numerical solution of state variables x, y, and z. To present these state variables in FPGA implementation, we can use 32-bit fixed point numbers that are divided into 8 bits for the integer part and 24 bits for the fractional part.

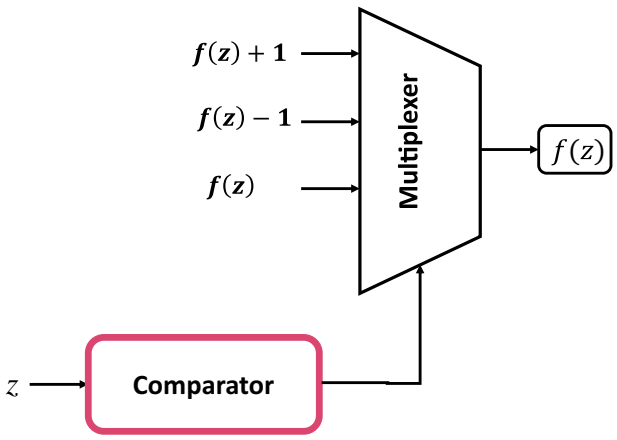


Fig. 11 The piecewise function $f(z)$

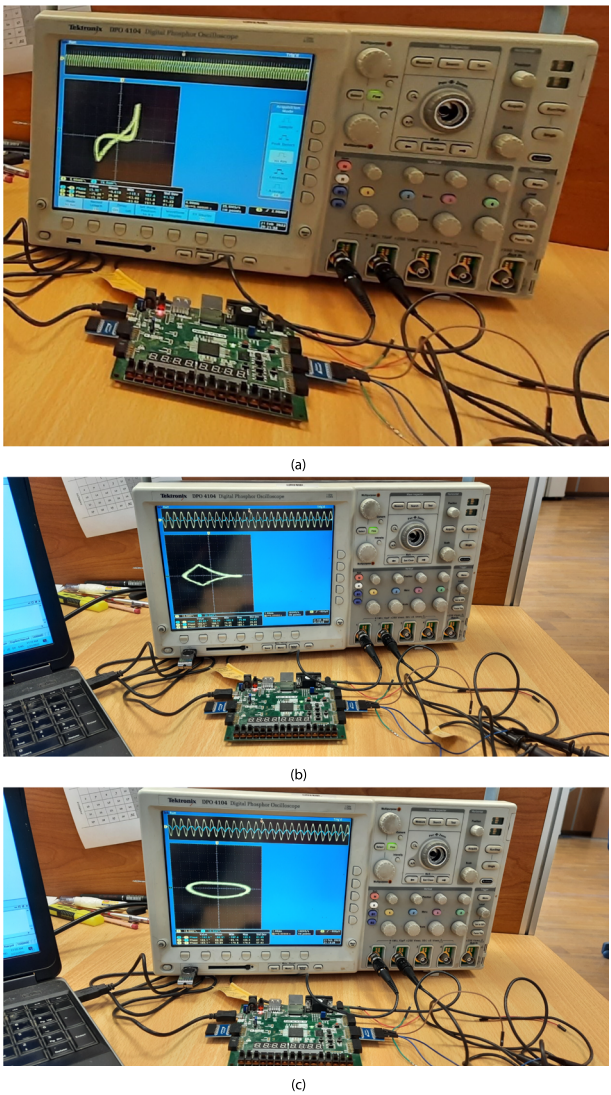


Fig. 12 Experimental results of the proposed chaotic system for parameters $q = 0.95$, $b = 14$, $u = 3$ and $h = 0.009$ (a) $x - y$ plane, (b) $x - z$ plane, (c) $y - z$ plane

The first LUT in Fig. 10 stores the values of coefficients with 22 fixed-point numbers, a 2-bit integer part and a 20-bit fractional part. The proposed design shown in Fig. 9 needs 6 multipliers, a piecewise function $f(z)$, 7 adders, and 3 GL blocks to calculate the numerical solution for state variables x, y, and z. The GL block is implemented in Fig. 10 based on [23] to compute the summation in Equation (4). The piecewise function $f(z)$ is utilized to calculate the non-linear function $\sum_{k=-n}^{n} \text{sgn}(z + 2n)$ as shown in Fig. 11. In the proposed design, the quantity h^q is constant. It is computed with a step size h, and fractional order q. The carry of each adder is one. To perform the subtraction operations, the two's complement is used.

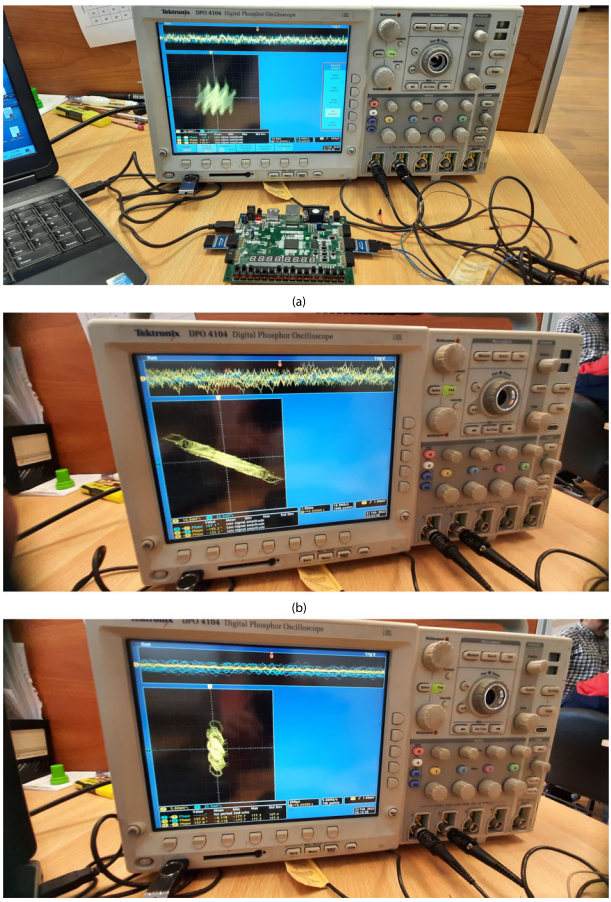
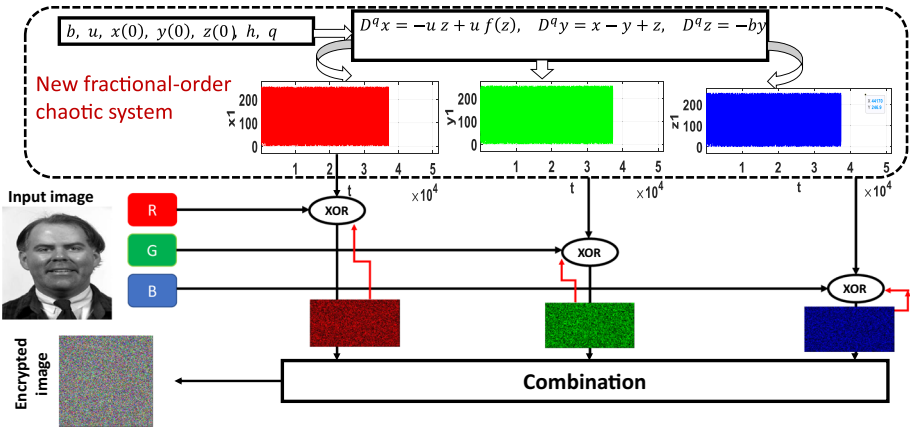


Fig. 13 Experimental results of the proposed multi-scroll fractional-order chaotic system for parameters $q = 0.95$, $b = 14$, $u = 3$ and $h = 0.05$ (a) $x - y$ plane, (b) $x - z$ plane, (c) $y - z$ plane

7 Measurements

The digital chaotic generator of the proposed system is realized based on Verilog HDL, Xilinx ISE 14.7 and Xilinx FPGA Artix-7 XC7A100T. To validate the results, we can take the data from the RTL simulation and use MATLAB. Experimental results are shown in Figs. 12 and 13 using the same parameters described before on the oscilloscope. To display the chaotic attractor on the oscilloscope, the FPGA generates two serial outputs with 12 bits in digital format. In order to display the output waveform on the digital oscilloscope DPO 4104, the output must be converted from digital to analog using the Pmod DAC 2.



(a)

Fig. 14 Block diagram of image encryption based on the proposed fractional-order chaotic system

8 Application of fractional-order chaotic system

By using the same datasets shown in Fig. 14, MATLAB is used to separate the three color components of the input color biometric template. This figure illustrates the experimental ciphering outcomes in terms of RGB 227 × 227 × 3 images. In the proposed system, the XOR process is accomplished between the RGB color components and the LSBs of x, y, and z, which are the state variables of the fractional-order multi-scroll chaotic system. So, the R component of face biometric images is XORed with the LSB of x state variable. Likewise, the LSBs of z and y state variables are XORed with the B and G components, respectively, as clarified in Fig. 15.

The evaluation of the suggested system discussed previously is presented in this section. In addition, the performance and efficiency of the suggested cancellable biometric system are compared with those of other different related schemes. Furthermore, we compare it with other different schemes from several perspectives. These comparisons are based on calculating correlation scores, AROC, encryption efficiency, and histograms of face biometrics. All obtained outcomes tested on the ORL, LFW, and FERET datasets confirm the high performance of the suggested cancellable biometric system compared to other related schemes.

The security performance of the suggested cancellable biometric system is verified by comparing its efficacy with those of the cancellable biometric approaches based on Haar wavelet fusion, Gaussian Random Projection (RP) after Intuitionistic Fuzzy Logic (IFL), Gaussian RP after homomorphic transform, and fractional-order Lorenz chaotic system. The encryption outcomes are shown in Figs. 16 (a)-(d), while the histogram outcomes of the ciphered biometrics are demonstrated in Figs. 16 (e)-(h) for the suggested system and other related schemes. It is evident from the attained distributions of the collected histograms that they are very different from those of the original biometric samples.

The probability curves of the correlation coefficients of unlicensed and licensed users are presented in Figs. 16 (i)-(l). The ROC distributions are shown in Figs. 16 (m)-(p). The achieved outcomes for the suggested and related cancellable face recognition systems demon-

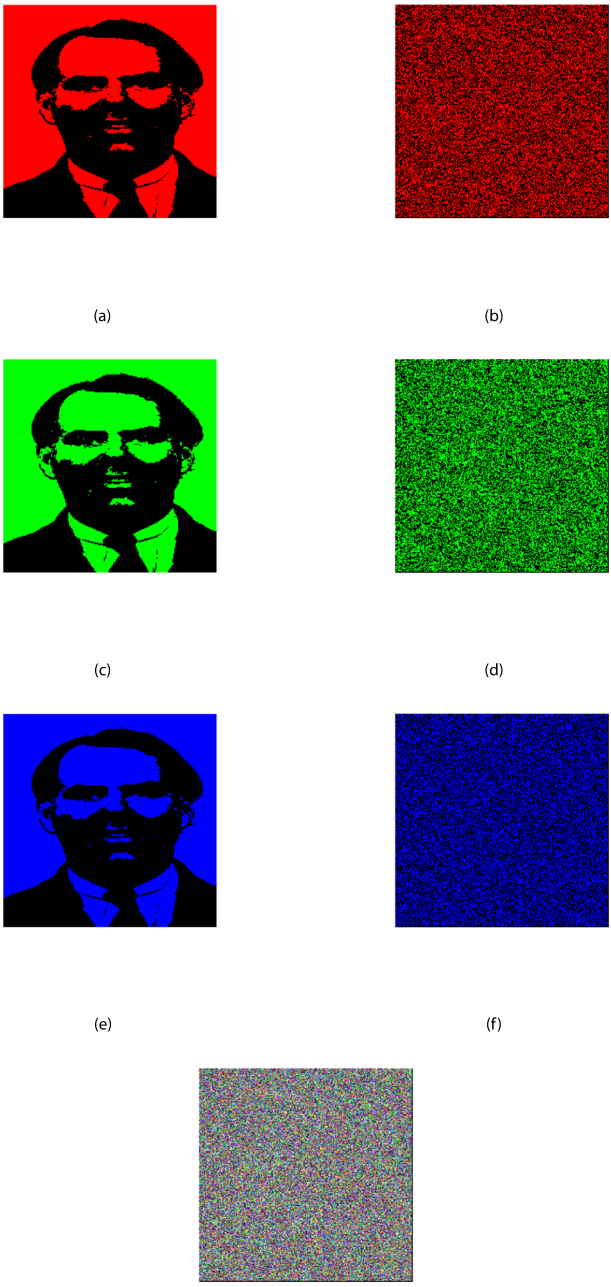


Fig. 15 Encryption stages of a color face with the fractional-order chaotic system (a) R component, (b) encrypted R component, (c) G component, (d) encrypted G component, (e) B component, (f) encrypted B component, (g) generated cancellable template

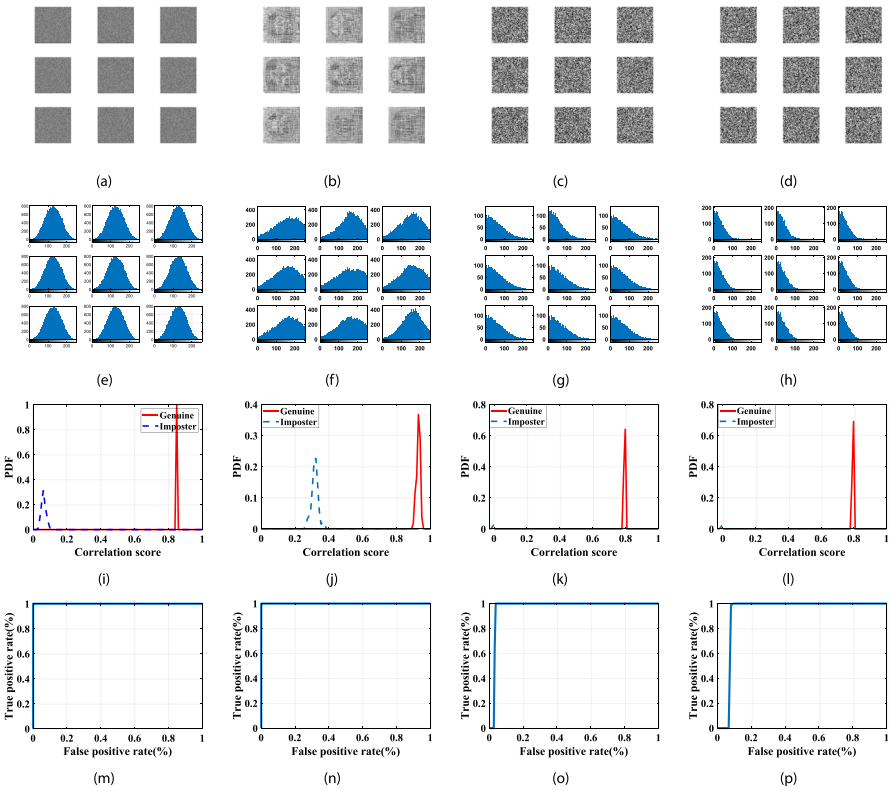


Fig. 16 Results on FERET dataset (a) encrypted faces with the proposed system (b) encrypted faces with the fractional-order Lorenz chaotic system [4], (c) encrypted faces with RP after homomorphic transform scheme [2], (d) encrypted faces with Gaussian RP after IFL scheme [2], (e) histograms of images in (a), (f) histograms of images in (b), (g) histograms of images in (c), (h) histograms of images in (d), (i) PDFs for the proposed system, (j) PDFs for cancellable face recognition based on fractional-order Lorenz chaotic system, (k) PDFs for cancellable face recognition based on RP after homomorphic transform [2], (l) PDFs for cancellable face recognition based on Gaussian RP after IFL scheme [2], (m) ROC curve for the proposed system, (n) ROC curve for cancellable face recognition based on fractional-order Lorenz chaotic system [4], (o) ROC curve for cancellable face recognition based on RP after homomorphic transform [2], (p) ROC curve for cancellable face recognition based on Gaussian RP after IFL scheme [2]

strate that the attained AROC values reach 100% for the suggested cancellable biometric system, which guarantees the high robustness and security of the suggested system (Figs. 17 and 18).

The estimated values of all assessment metrics used in the simulation experiments to evaluate the security performance and robustness strength of all examined cancellable biometric systems are summarized in Table 3. It is noticed from the obtained outcomes that the suggested system has high AROC values that are close to 1 and the lowest EER values. In addition, the obtained average correlation values of licensed users for the proposed system are higher than those of the related schemes.

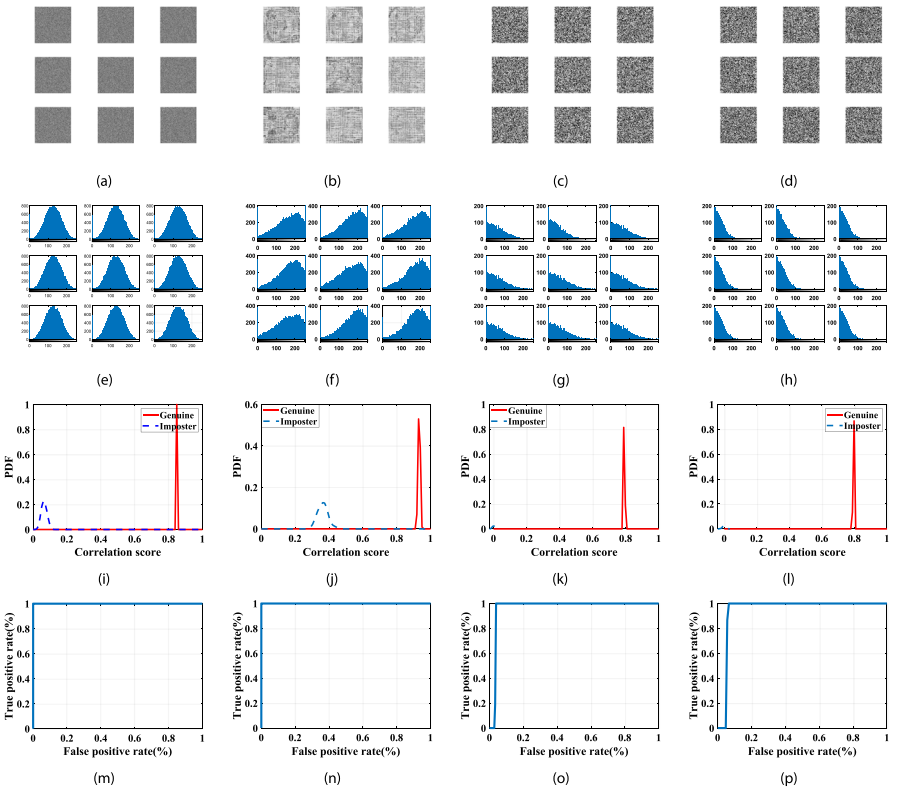


Fig. 17 Results on LFW dataset (a) encrypted faces with the proposed system (b) encrypted faces with the fractional-order Lorenz chaotic system [4], (c) encrypted faces with RP after homomorphic transform scheme [2], (d) encrypted faces with Gaussian RP after IFL scheme [2], (e) histograms of images in (a), (f) histograms of images in (b), (g) histograms of images in (c), (h) histograms of images in (d), (i) PDFs for the proposed system, (j) PDFs for cancellable face recognition based on fractional-order Lorenz chaotic system, (k) PDFs for cancellable face recognition based on RP after homomorphic transform scheme [2], (l) PDFs for cancellable face recognition based on Gaussian RP after IFL scheme [2], (m) ROC curve for the proposed system, (n) ROC curve for cancellable face recognition based on fractional-order Lorenz chaotic system [4], (o) ROC curve for cancellable face recognition based on RP after homomorphic transform scheme [2], (p) ROC curve for cancellable face recognition based on Gaussian RP after IFL scheme [2]

Moreover, Table 4 offers all assessment parameters of the suggested and related cancellable biometric systems for the LFW biometric dataset. The same assessment is performed on the ORL biometric dataset. The primary difference between the three examined LFW, ORL, and FERET biometric datasets is that the ORL biometric dataset includes gray-scale biometric images. Consequently, we carry out the XOR operation on a single image component. Likewise, the findings on the ORL biometric dataset are organized in Table 5. From all presented comparisons between the proposed and related cancellable biometric systems, it is revealed that the proposed system has superior performance in terms of lower EER, lower computational cost, and higher AROC values. Moreover, a comparison of the results with those of other state-of-the-art schemes for cancellable face recognition is shown in Table 6.

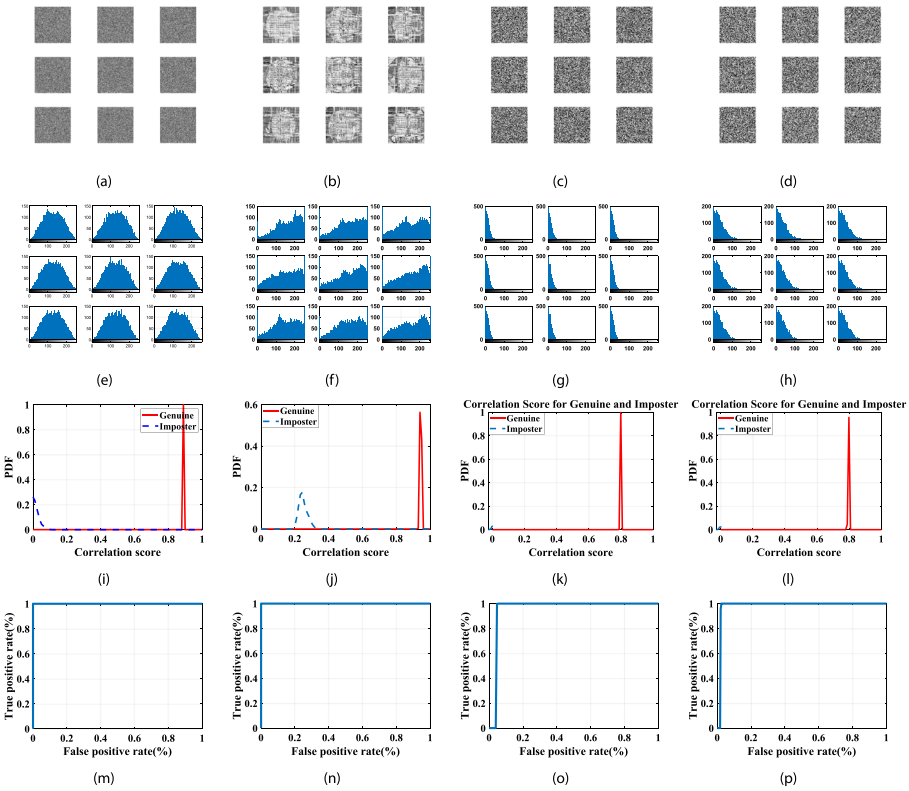


Fig. 18 Results on ORL dataset (a) encrypted faces with the proposed system (b) encrypted faces with the fractional-order Lorenz chaotic system [4], (c) encrypted faces with RP after homomorphic transform scheme [2], (d) encrypted faces with Gaussian RP after IFL scheme [2], (e) histograms of images in (a), (f) histograms of images in (b), (g) histograms of images in (c), (h) histograms of images in (d), (i) PDFs for the proposed system, (j) PDFs for cancellable face recognition based on fractional-order Lorenz chaotic system, (k) PDFs for cancellable face recognition based on RP after homomorphic transform scheme [2], (l) PDFs for cancellable face recognition based on Gaussian RP after IFL scheme [2], (m) ROC curve for the proposed system, (n) ROC curve for cancellable face recognition based on fractional-order Lorenz chaotic system [4], (o) ROC curve for cancellable face recognition based on RP after homomorphic transform scheme [2], (p) ROC curve for cancellable face recognition based on Gaussian RP after IFL scheme [2]

9 Conclusions

This paper presented a fractional-order chaotic system and a multi-scroll chaotic system. In our proposed multi-scroll chaotic system, the number of scrolls is controlled by the parameters instead of changing the discontinuous functions and generating a multi-scroll chaotic system. In addition, the circuit realization of this system is introduced and discussed. Moreover, the proposed system is implemented with FPGA. OrCAD-PSpice simulation results, experimental results of FPGA-based implementation of the proposed system and numerical

Table 3 Results on LFW dataset

	Proposed System	Fractional-order Lorenz chaotic system [4]	Gaussian RP + IFL scheme [2]	RP + homomorphic transform scheme [2]
Average correlation of licensed users	0.8518	0.9334	0.7925	0.7938
Average correlation of unlicensed users	0.0649	0.3626	-2.4666×10^{-4}	-0.0014
EER	0	0	0.4723	0.0053
FAR	0	0	0.0350	0.0262
FRR	0	0	0.9393	0.0070
AROC	1	1	0.9680	0.9791
Variance of licensed users	4.9343×10^{-7}	2.9439×10^{-5}	3.7476×10^{-6}	4.1428×10^{-6}
Variance of unlicensed users	1.7382×10^{-4}	7.3485×10^{-4}	3.8352×10^{-5}	3.0621×10^{-5}

Table 4 Results on FERET dataset

	Proposed System	Fractional-order Lorenz chaotic system [4]	Gaussian RP + IFL scheme [2]	RP + homomorphic transform scheme [2]
Average correlation of licensed users	0.8516	0.9283	0.7930	0.7939
Average correlation of unlicensed users	0.0622	0.3173	5.9159×10^{-4}	-0.0016
EER	0	0	0.4016	0.0191
FAR	0	0	0.0335	0.0469
FRR	0	0	0.7989	0.0312
AROC	1	1	0.9695	0.9629
Variance of licensed users	1.2278×10^{-6}	1.0524×10^{-4}	4.7433×10^{-6}	3.2173×10^{-6}
Variance of unlicensed users	1.6158×10^{-4}	4.0476×10^{-4}	6.2590×10^{-5}	6.5960×10^{-5}

Table 5 Results on ORL dataset

	Proposed System	Fractional-order Lorenz chaotic system [4]	Gaussian RP + IFL scheme [2]	RP + homomorphic transform scheme [2]
Average correlation of licensed users	0.8891	0.9429	0.7977	0.7939
Average correlation of unlicensed users	0.0024	0.2479	2.1823×10^{-4}	-6.1422×10^{-4}
EER	0	0	0.0112	0.0230
FAR	0	0	0.0243	0.0420
FRR	0	1	0.0196	0.0397
AROC	1	0.9799	0.9669	
Variance of licensed users	1.0614×10^{-6}	1.8815×10^{-5}	9.433110^{-6}	3.252410^{-6}
Variance of unlicensed users	6.1559×10^{-4}	5.2167×10^{-4}	4.5505×10^{-5}	7.1261×10^{-5}

simulation confirm each other. Cancellable face recognition based on the proposed fractional-order chaotic system has been implemented on FERET, LFW, and ORL datasets, and the results are compared with those of other schemes.

Table 6 Comparison between the state-of-the-art (SOTA) methods based on AROC

Method	AROC
Proposed system on ORL dataset	1
Proposed system on FERET dataset	1
Proposed system on LFWT dataset	1
Fractional-order scheme on ORL dataset [4]	1
Fractional-order scheme on FERET dataset [4]	1
Fractional-order scheme on LFWT dataset [4]	1
Gaussian RP after IFL scheme on ORL dataset [2]	0.9720
RP after homomorphic transform on ORL dataset [2]	0.9774
Gaussian RP after IFL scheme on FERET dataset [2]	0.9744
RP after homomorphic transform scheme on FERET dataset [2]	0.9294
Gaussian RP after IFL scheme LFWT dataset [2]	0.9668
RP after homomorphic transform scheme on LFWT dataset [2]	0.9694
Scheme in [3]	0.998
Scheme in [21]	0.9997
Scheme in [17]	0.9984

Acknowledgements The authors are very grateful to all the institutions given in the affiliation list for performing this research work, successfully. The authors would like to thank Prince Sultan University for their support.

Author Contributions All authors equally contributed.

Funding The authors did not receive support from any organization for the submitted work.

Availability of data and material All data are available upon request from the corresponding author.

Declarations

Ethics approval and consent to participate All authors contributed and accepted to submit the current work.

Consent for publication All authors accepted to submit and publish this work.

Competing interests The authors have neither relevant financial nor non-financial interests to disclose.

References

1. Abdelaty AM, Roshdy M, Said LA, Radwan AG (2020) Numerical simulations and FPGA implementations of fractional-order systems based on product integration rules. IEEE Access 8:102093–102105
2. Algarni AD, El Banby GM, Soliman NF, Abd El-Samie FE, Iliyasu AM (2020) Efficient implementation of homomorphic and fuzzy transforms in randomprojection encryption frameworks for cancellable face recognition. Electronics 9(6):1046
3. Algarni AD, El Banby G, Ismail S, El-Shafai W, Abd El-Samie FE, Soliman NF (2020) Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy 22(12):1361
4. Badr IS, Radwan AG, EL-Rabaie ESM, Said LA, El Banby GM, El-Shafai W, Abd El-Samie FE (2021) Cancellable face recognition based on fractionalorder lorenz chaotic system and haar wavelet fusion. Digital Signal Processing 116:103103
5. Chang D, Li Z, Wang M, Zeng Y (2018) A novel digital programmable multi-scroll chaotic system and its application in FPGA-based audio secure communication. AEU-International Journal of Electronics and Communications 88:20–29
6. Charef A, Sun HH, Tsao YY, Onaral B (1992) Fractal system as represented by singularity function. IEEE Trans Autom Control 37(9):1465–1470
7. Chen L, Pan W, Wu R, Wang K, He Y (2016) Generation and circuit implementation of fractional-order multi-scroll attractors. Chaos, Solitons Fractals 85:22–31
8. Cui L, Lu M, Ou Q, Duan H, Luo W (2020) Analysis and circuit implementation of fractional order multi-wing hidden attractors. Chaos, Solitons Fractals 138:109894
9. Cui L, Luo W-H, Ou Q-L (2021) Analysis and implementation of new fractional-order multi-scroll hidden attractors. Chinese Physics B 30(2):020501
10. Guan Z-H, Huang F, Guan W (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1–3):153–157
11. Hao J, Li H, Yan H, Mou J (2021) A new fractional chaotic system and its application in image encryption with dna mutation. IEEE Access 9:52364–52377
12. Liang J, Zhang N, Qian G (2017) Design of multi-scroll chaotic attractors using nonlinear exponential function. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp 797–801. IEEE
13. Ma Y, Li Y, Jiang X (2015) Simulation and circuit implementation of 12-scroll chaotic system. Chaos, Solitons Fractals 75:127–133
14. Matsuda K, Fujii H (1993) H (infinity) optimized wave-absorbing control-analytical and experimental results. J Guid Control Dyn 16(6):1146–1153
15. Ozoguz S, Elwakil AS, Salama KN (2002) N-scroll chaos generator using nonlinear transconductor. Electron Lett 38(14):685–686

16. Rajasekar V, Predić B, Saracevic M, Elhoseny M, Karabasevic D, Stanujkic D, Jayapaul P (2022) Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. Scientific Reports 12(1):1–11
17. Sameh LA, Egila MG, Shawky H, Elsaid MKH, El-Shafai W, Abd El-Samie FE et al (2020) Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. Multimedia Tools and Applications, pp 1–26
18. San-Um W, Srisuchinwong B (2011) A simple multi-scroll chaotic delay differential equation. In The 8th Electrical Engineering/Electronics, Computer, Telecommunications and 1Information Technology (ECTI) Association of Thailand-Conference 2011, pp 137–140. IEEE
19. Selimović F, Stanimirović P, Saračević M, Selimi A, Krtolica P (2020) Authentication based on the image encryption using delaunay triangulation and catalan objects. Acta Polytechnica Hungarica 17(6)
20. Soliman NS, Tolba MF, Said LA, Madian AH, Radwan AG (2018) FPGA implementation of x-and heart-shapes controllable multi-scroll attractors. In 2018 IEEE International Symposium on Circuits and Systems (ISCAS), pp 1–5. IEEE
21. Soliman RF, El Banby GM, Algarni AD, Elsheikh M, Soliman NF, Amin M, Abd El-Samie FE (2018) Double random phase encoding for cancelable face and iris recognition. Appl Opt 57(35):10305–10316
22. Suykens JAK, Vandewalle J (1993) Generation of n-double scrolls (n= 1, 2, 3,4,...). IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 40(11):861–867
23. Tolba MF, AbdelAty AM, Soliman NS, Said LA, Madian AH, Azar AT, Radwan AG (2017) FPGA implementation of two fractional order chaotic systems. AEU-International Journal of Electronics and Communications 78:162–172
24. Wang F, Wang R, Iu HHC, Liu C, Fernando T (2019) A novel multi-shape chaotic attractor and its FPGA implementation. IEEE Transactions on Circuits and Systems II: Express Briefs 66(12):2062–2066
25. Xiong L, Zhang S, Zeng Y, Liu B (2018) Dynamics of a new composite four-scroll chaotic system. Chin J Phys 56(5):2381–2394
26. Yan S, Wang Q, Wang E, Sun X, Song Z (2022) Multi-scroll fractional order chaotic system and finite-time synchronization. Phys Scr
27. Zaher AA, Abu-Rezq A (2011) On the design of chaos-based secure communication systems. Commun Nonlinear Sci Numer Simul 16(9):3721–3737

Authors and Affiliations

Iman S. Badr[1] · Ahmed G. Radwan[2,3] · El-Sayed M. EL-Rabaie[1] · Lobna A. Said[3] · Walid El-Shafai[1,4] · Ghada M. El-Banby[5] · Fathi E. Abd El-Samie[1,6]

Iman S. Badr
seman2055@gmail.com

Ahmed G. Radwan
agradwan@ieee.org

El-Sayed M. EL-Rabaie
srabie1@yahoo.com

Lobna A. Said
L.a.said@ieee.org

Ghada M. El-Banby
ghadaelbanby75@gmail.com

Fathi E. Abd El-Samie
feabdelhamid@pnu.edu.sa ; fathi_sayed@yahoo.com

1 Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

2 Engineering Mathematics and Physics Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt

3 Nanoelectronics Integrated Systems Center (NISC), Nile University, Giza 12588, Egypt

4 Security Engineering Lab, Computer Science Department, Prince Sultan University, 11586 Riyadh, Saudi Arabia

5 Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

6 Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia