Article

Real-Time Synchronisation of Multiple Fractional-Order Chaotic Systems: An Application Study in Secure Communication

Bachir Nail [1], Mahedi Abdelghani Atoussi [1,†], Slami Saadi [2,†], Imad Eddine Tibermacine [3,†] and Christian Napoli [3,4,5,*]

1   Faculty of Science and Technology, University of Djelfa, BP 3117, Djelfa 17000, Algeria;
    nail_bachir@yahoo.fr (B.N.); m.atoussi@univ-djelfa.dz (M.A.A.)
2   Faculty of Exact Sciences & Informatics, University of Djelfa, BP 3117, Djelfa 17000, Algeria;
    s.saadi@univ-djelfa.dz
3   Department of Computer, Automation and Management Engineering, Sapienza University of Rome,
    Via Ariosto, 25, 00185 Roma, Italy; tibermacine@diag.uniroma1.it
4   Institute for Systems Analysis and Computer Science, Italian National Research Council, Via dei Taurini, 19,
    00185 Roma, Italy
5   Department of Computational Intelligence, Czestochowa University of Technology, ul. J.H. Dabrowskiego 69,
    42-201 Czestochowa, Poland
*   Correspondence: cnapoli@diag.uniroma1.it
†   These authors contributed equally to this work.

Abstract: In this paper, we use two Fractional-Order Chaotic Systems (FOCS)—one for the sender and one for the receiver—to determine the optimal synchronisation for a secure communication technique. With the help of the Step-By-Step Sliding-Mode Observer (SBS-SMO), this synchronisation is accomplished. An innovative optimisation method, known as the artificial Harris hawks optimisation (HHO), was employed to enhance the observer's performance. This method eliminates the random parameter selection process and instead selects the optimal values for the observer. In a short amount of time, the secret message that could have been in the receiver portion (signal, voice, etc.) was successfully recovered using the proposed scheme. The experimental validation of the numerical results was carried out with the assistance of an Arduino microcontroller and several electronic components. In addition, the findings of the experiments were compared with the theoretical calculations, revealing a satisfactory level of agreement.

Keywords: fractional-order systems; secure communication; Chua's systems; synchronisation; chaotic systems; harris hawks optimisation; Arduino; microcontroller

1. Introduction

The field of fractional calculus is a subfield of mathematical analysis that has garnered the interest of a number of academics due to its intriguing potential as a one-of-a-kind modelling tool across a wide range of scientific and engineering fields. Fractional differential equations are utilised because it was discovered that simulating experimental dynamics using these equations delivers better performance and superior results, enabling the construction of powerful controllers. Out of the many advantages that this discipline offers, model generalisation and long-term memory stand out as particularly advantageous. Furthermore, fractional-order modelling is superior when it comes to attempting to build a connection between any two places. It is possible to collect data for the instance of interest at any time from a model that is of fractional order. When we use an integer-order model, however, we are only able to obtain information that is relevant to this particular circumstance. Based on the problem at hand and the information gathered, one would select the most appropriate operator for the model. The definition proposed by Caputo is one of the most widely accepted in current usage.

In addition to investigating the numerous possibilities beyond the peculiar behaviour of dynamical systems across a variety of domains such as electrochemistry [1], viscoelasticity [2], and biology [3], it is possible to observe a great number of practical applications of fractional calculus in contemporary theory [4–7]. As a challenging area of mathematics, chaos theory is characterised by unexpected and complex behaviour. It focuses on deterministic laws and underlying patterns that are hyper-sensitive to the initial conditions. Chaos theory is a subject that is tough to study. In the past three decades, chaotic systems have emerged as a subject of research. Some examples of chaotic systems include the Lorenz system, the unified chaotic system, the Rossler system, the Lu system, and the Chen system [8–11]. There are numerous applications of these highly effective systems that have benefited from their chaotic and unpredictable behaviour, including commerce, electricity, healthcare, mathematics, chemical and biological reactors, and security [8–11]. Additionally, these systems have been successfully applied in a wide variety of control fields, including secure communication. According to the findings of researchers, the combination of chaos theory and fractional calculus could produce superior outcomes in terms of secure communication. This is due to the fact that FOCS exhibit significantly more intricate behaviour [12–16].

It is guaranteed that a sliding-mode observer produces a set of state estimates directly proportional to the transmitter's real output, which is one of the unique characteristics of the observer we employed in this study. Another powerful tool is the optimal SBS-SMO. Many studies, such as [17,18], have resulted from the development of methods for synchronising chaotic systems with fractional order employing a sliding mode observer; thus, it is clear that there has been a lot of work in this area. An innovative approach to communication security is suggested in this paper. It involves synchronising two fractional-order Chua oscillators with an ideal SBS-SMO. The third-state derivative of fractional order of the chaotic system contains the message in the emitter portion. It is believed that the receiving procedure is flawed; hence, an SBS-SMO is employed to verify that the master and slave are communicating and obtaining the secret data.

The importance of fractional-order chaotic systems lies in their applications in various areas and fields, such as fractional evolution hemivariational inequalities generated by non-instantaneous impulses, which was examined in [19]. In [20], an innovative approach to the encryption of colour images was proposed, where the algorithm was based on extended DNA coding, the Zig-Zag transform, and a fractional-order laser system [21]. Other notable works in this area include "Achieving Superior Multi-Image Encryption Through the Use of Recently Conceived Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map" [22] and "Fragmentary Fractional Order Systems: Modeling and Initialization Using the Infinite State Representation" [23].

To achieve a secure real-time communication scheme, this work makes the following contributions:

- The computation of the fractional order in the microcontroller needs memory allocation to compute the cumulative integration; this limitation in the memory of the atmega328p microcontroller was solved by using the numerical approximation method, Rung Kutta 4.
- The noise produced by the electronics components, which negatively affects the quality of the transmitted and received data, was solved in two ways: two capacitors were added to the circuit to enhance the NRF24LO1 module's performance, and a stochastic filter was implemented to filter the estimated input (message) in the slave part.
- The optimal SBS-SMO parameters were chosen using HHO.

This paper is structured as follows. Fractional calculus is described in Section 2. The transmitter model is explained along with the injection of secret information in Section 3. In Section 4, the SBS-SMO and the recovered message are carefully revealed. In Section 5, the receiver model is discussed in detail. The optimisation algorithm used with the sliding-mode observer is explained in Section 6. In Section 7, it is shown that the proposed secure communication method works successfully through real-time validation.

2. Fundamental on Fractional Calculus

The Grünwald–Letnikov definition, the Riemann–Liouville definition, and the Caputo definition are the three most common ways to describe the general fractional differintegral [24].

Definition 1 ([25]). *Caputo presented a novel definition of the derivative of fractional order, which is described as follows:*

$$D^a f(x) = \frac{1}{\Gamma(1-\alpha)} \int_0^t (t-\pi)^{-\alpha} \frac{df(\tau)}{d\tau} d\tau \tag{1}$$

It is important to highlight Euler's gamma function, which is the most powerful component in fractional calculus. It is defined as follows:

$$\Gamma(n) = \int_0^\infty t^{n-1} e^{-t} dt$$

As a generalisation of a factorial, this function takes the following form:

$$\Gamma(n) = (n-1)!$$

Definition 2 ([25]). *In the case of $0 < \alpha < 1$ and $f(t)$ being a causal function of t, that is, $f(t) = 0$ for $t < 0$, the Riemann–Liouville integral is defined as:*

$$_0D_t^{-\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_0^t \frac{f(\tau)}{(t-\tau)^{1-\alpha}} d\tau, \text{ for } 0 < \alpha < 1, t > 0 \tag{2}$$

Definition 3 ([25]). *The Grünwald–Letnikov fractional-order derivative is defined as:*

$$D^a f(x) \approx \frac{1}{\Delta^\alpha} \sum_{j=0}^{j=[t/\Delta]} (-1)^j \binom{\alpha}{j} f(t-j\Delta) \tag{3}$$

$\Delta = 0.001$ *is the time step used in the simulation.*

3. The Transmitter System's Configuration

Many electric and magnetic phenomena can be modelled using fractional calculus. Many chaotic systems have been extended using non-integer-order derivatives, drawing inspiration from Chua's oscillator and other well-known chaotic systems. In this section, we outline the transmitter system [26]:

$$\begin{cases} D^{q_1} x(t) = \delta_1 \left[-y(t) + \alpha x^2(t) + \beta x^3(t) \right] \\ D^{q_2} y(t) = \delta_2 [x(t) - Ry(t) - z(t)] \\ D^{q_3} z(t) = \delta_3 [i_0 - \gamma y(t)] \end{cases} \tag{4}$$

where $\delta_1 = \frac{1}{C_1}, \delta_2 = \frac{1}{L}$, and $\delta_3 = \frac{1}{C_3}$. $D^{[q]} = [D^{q_1} D^{q_2} \ldots D^{q_n}]^T$ represents the fractional-order differentiation vector operator $q_i \in \Re_+, i = 1, 2, \ldots, n$. If all the orders of the derivative q_i are equal, which is $q_i = q, i = 1, 2, \ldots, n$, the system is said to be of equivalent fractional order (commensurate) if and only if the fractional orders are equal. Take the example of a commensurate fractional-order system, which is defined as

$$D^q x(t) = f(x(t)) + g(x(t))u(t)$$
$$y(t) = h(x(t)) \tag{5}$$

Table 1 presents the parameters used in the transmitter system, with the state variables' initial conditions (x, y, z) set at zero. Figures 1–3 illustrate the time responses of the system's

states(x, y, z), and Figure 4 illustrates the three-dimensional space of the chaotic attractor in (x, y, z).

Table 1. Parameter values of the model given in Equation (4).

Parameter	$q_1 = q_2 = q_3$	α	β	γ	δ_1	δ_2	δ_3	R	i_0
Value	0.9	1.5	-1	0.0035	100	1	1	0.1	0.0005
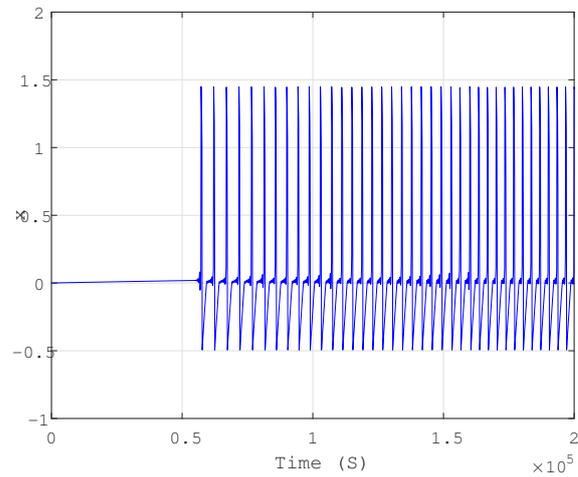
Figure 1. Time response of state variable x for initial condition of zero.
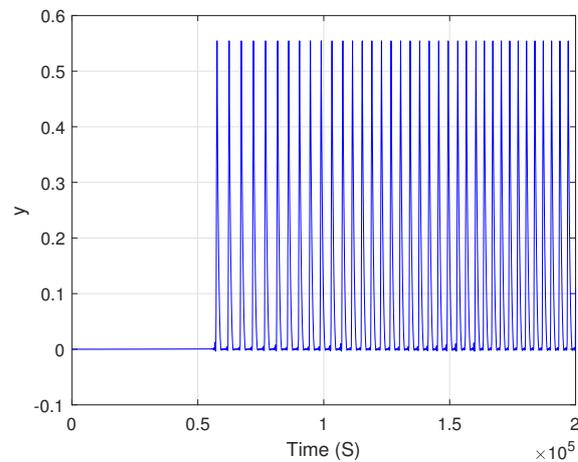
Figure 2. Time response of state variable y for initial condition of zero.
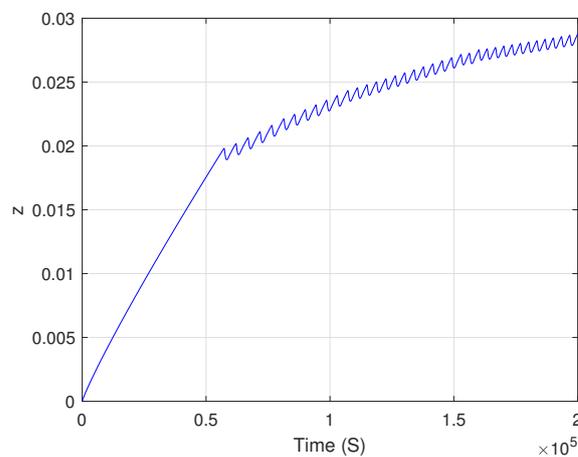
Figure 3. Time response of state variable z for initial condition of zero.
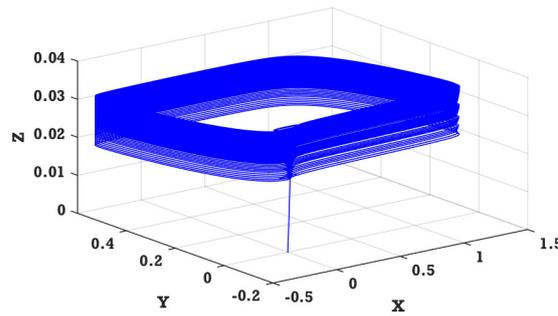
Figure 4. Time responses of state variables x, y, z for initial conditions of zero.

The Inclusion of Private Information

Equation (4) is modified by adding a new term $m(t)$ (secret information), which is injected into the third derivative $z(t)$ rather than $x(t)$ in order to enhance the safety of the communication system. The model of the transmitter system can be expressed as follows:

$$\begin{cases} D^{q_1}x(t) = \delta_1\left[-y(t) + \alpha x^2(t) + \beta x^3(t)\right] \\ D^{q_2}y(t) = \delta_2[x(t) - Ry(t) - z(t)] \\ D^{q_3}z(t) = \delta_3[i_0 + m(t) - \gamma y(t)] \end{cases} \tag{6}$$

Remark 1. *The secret message $m(t)$ is considered as an unknown to be estimated and can represent a signal, voice, or image. In the simulation section, interactive examples are investigated.*

4. SBS-SMO Theory

According to [27], designing the SBS-SMO for integer-order nonlinear systems usually involves a sequential method. This method involves injecting virtual inputs produced from the iterative first-order SBS-SMO. Accurately estimating $m(t)$ and x_i, $i = \overline{1, n}$ is our objective.

The triangular representation of the commensurate fractional-order nonlinear system is given as follows:

$$\begin{aligned} \frac{d^q(x_{j-1}, y_{j-1}, z_{j-1})(t)}{dt} &= \rho_{j-1}(x_j, y_j, z_j)(t) + \psi_{j-1}(x_j, y_j, z_j)(t)) \\ \frac{d^q(x_j, y_j, z_j)(t)}{dt} &= a(x, y, z) + b(x, y, z)m(t) \\ y(t) &= x(t) \end{aligned} \tag{7}$$

where $y(t) \in \mathbb{R}$ is the measured output, $m(t) \in \mathbb{R}$ is the secret message, and the nonlinear functions are denoted by $a(x)$, $b(x)$, and Ψ_i, $i = \overline{1, n-1}$. The parameters $\rho_i \in \mathbb{R}^+$ are all non-zero constants.

Consider that the system in Equation (7) is a bounded-input bounded-state system, and $b(x)$, $a(x)$, and $m(t)$ are bounded, i.e.,

Assumption 1. $|x_i(t)| \leq d_i, i = \overline{1, n}, \quad |m(t)| \leq M_s.$

Assumption 2. $|a(x)| \leq A_s, \quad |b(x)| \leq B_s$ *and* $b(x) \neq 0$ *for all* $x \in \mathcal{D} \subset \mathbb{R}^n.$

The purpose is to use the step-by-step first-order siding observers to estimate the state variables and the unknown input $m(t)$. Following the same approach used with integer-order systems, the following equations characterise the suggested sliding-mode observer that injects the available observed output signal $y(t)$

$$\frac{d^q(\hat{x}_{j-1}, \hat{y}_{j-1}, \hat{z}_{j-1})(t)}{dt} = \rho_{j-1}(\hat{x}_j, \hat{y}_j, \hat{z}_j)(t) + \psi_{j-1}\big(Y(t), (\tilde{x}_j, \tilde{y}_j, \tilde{z}_j)(t)\big)$$
$$+ E_{j-2}\mu_{j-1}\operatorname{sign}(\tilde{e}_{j-1}) \tag{8}$$
$$\frac{d^q(\hat{x}_j, \hat{y}_j, \hat{z}_j)(t)}{dt} = E_{j-1}\mu_j\operatorname{sign}(\tilde{e}_j), \quad j = \overline{2, n}$$

The secret message estimation is defined as follows:

$$\widehat{m}(t) = b(\tilde{x}, \tilde{y}, \tilde{z})^{-1}\big(-a(\tilde{x}, \tilde{y}, \tilde{z}) + E_{j-1}\mu_j\operatorname{sign}(\tilde{e}_j) \tag{9}$$

The terms μ_j in Equation (9) are parameters that are only positive and developed to guarantee the observer's convergence.

The following are the definitions of the auxiliary variables $(\tilde{x}_i, \tilde{y}_i, \tilde{z}_i)$:

$$(\tilde{x}, \tilde{y}, \tilde{z})(t) = (\hat{x}, \hat{y}, \hat{z}) + \frac{1}{\rho_i}E_{i-1}\mu_{i-1}\operatorname{sign}(\tilde{e}_{i-1}), i = \overline{2, n} \tag{10}$$

The intermediate estimation errors $\tilde{e}_i(t)$ are expressed as

$$\tilde{e}_i(t) = (\tilde{x}_i, \tilde{y}_i, \tilde{z}_i)(t) - (\hat{x}_i, \hat{y}_i, \hat{z}_i)(t), \quad i = \overline{1, n} \tag{11}$$

where $\tilde{x}(t) = x(t) = Y(t)$ through construction. The estimation errors are expressed as

$$e_i(t) = (x_i, y_i, z_i)(t) - (\hat{x}_i, \hat{y}_i, \hat{z}_i)(t), \quad i = \overline{1, n} \tag{12}$$

Remark 2. *To obtain the convergence condition, the rule of the switching logic E_i must achieve:*

$$E_i, i = \overline{1, n-1}\begin{cases} \|\tilde{x}_i(t) - \hat{x}_i(t)\| \leq \varepsilon, & \varepsilon \ll 0 \\ E_i = 0 & otherwise \end{cases} \tag{13}$$

Theorem 1. *Let us assume that Assumptions 1 and 2 are accurate. In this situation, given the existence of positive parameters $\mu_i, i = \overline{1, n}$, the observer states $(\hat{x}, \hat{y}, \hat{z})$ and the estimated input $\widehat{m}(t)$ converge to (x, y, z) and the secret message $m(t)$, respectively, within a finite period of time [26].*

5. The Receiver System's Configuration

In order to simplify the receiver design that relies on an SBS-SMO and ensure successful synchronisation, we present a reformulation of Equation (6):

$$\begin{cases} D^{q_1}x(t) = \rho_1\hat{y}(t) + \psi_1(x(t)) \\ D^{q_2}y(t) = \rho_2\hat{z}(t) + \psi_2(x(t), y(t)) \\ D^{q_3}z(t) = a(x) + b(x)m(t) \\ Y(t) = x(t) \end{cases} \tag{14}$$

where

$$\psi_1(x(t)) = \alpha x^2(t) + \beta x^3(t)$$
$$\psi_2(x(t), y(t)) = \delta_2(x(t) - Ry(t))$$
$$\rho_1 = -\delta_1$$
$$\rho_2 = -\delta_2$$
$$a(x) = \delta_3[i_0 - \gamma y(t)]$$
$$b(x) = \delta_3$$

The following sliding-mode observer describes the receiver:

$$
\begin{cases}
D^{q_1}x(t) = \rho_1\hat{y}(t) + \psi_1(Y(t)) + \mu_1\operatorname{sign}(x(t) - \hat{x}(t)) \\
D^{q_2}y(t) = \rho_2\hat{z}(t) + \psi_2(x(t), \tilde{y}(t)) + E_1\mu_2\operatorname{sign}(\tilde{y}(t) - \hat{y}(t)) \\
\qquad\qquad D^{q_3}z(t) = E_2\mu_3\operatorname{sign}(\tilde{z}(t) - \hat{z}(t))
\end{cases}
\tag{15}
$$

The auxiliary variables $\tilde{y}(t), \tilde{z}(t)$ are defined as

$$
\tilde{y}(t) = \hat{y}(t) + \frac{1}{\rho_1}E_1\mu_1\operatorname{sign}(x(t) - \hat{x}(t))
$$

$$
\tilde{z}(t) = \hat{z}(t) + \frac{1}{\rho_2}E_2\mu_2\operatorname{sign}(\tilde{y}(t) - \hat{y}(t))
$$

The recovered message $m(t)$ is given by

$$
\widehat{m}(t) = \gamma\tilde{y} - i_0 + \frac{1}{\delta_3}E_2\mu_3\operatorname{sign}(\tilde{z}(t) - \hat{z}(t))
$$

6. Selection of the Observer's Optimal Parameters via HHO

In this section, the objective is to determine the optimal settings for the receiver system through the utilisation of the novel HHO in order to accomplish synchronisation. HHO was selected from a range of optimisation strategies documented in the literature due to its superior performance across more than 50 benchmark optimisation issues in comparison to other meta-heuristic algorithms. The concept of HHO was first suggested by Heidari et al. in their study on artificial intelligence [28]. Our secure communication strategy is depicted in Figure 5, whereas the overall HHO framework is depicted in Figure 6. The HHO method is utilised to address the convex optimisation problem, formulated as an objective function (16), aimed at minimising the mean square error (MSE) between the states of the emitter and receiver.

$$
J = \min\sum\left(\begin{array}{c} x(t) - \hat{x}(t) \\ y(t) - \hat{y}(t) \\ \underbrace{z(t) - \hat{z}(t)}_{e} \end{array}\right)^2
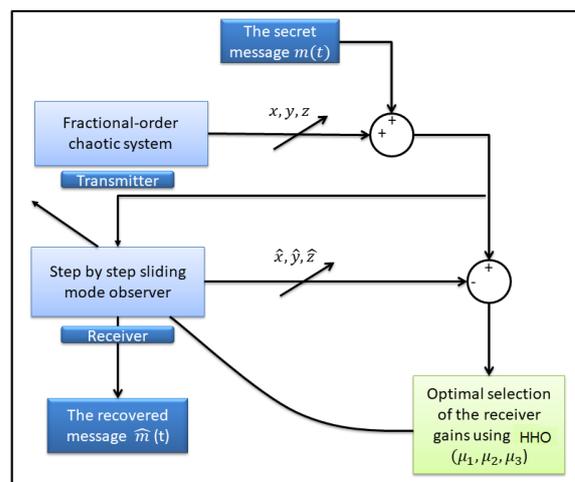\tag{16}
$$

Figure 5. The proposed secure data transmission scheme.

In this section, the effectiveness of the proposed strategy is demonstrated. When it comes to retrieving information in a short amount of time while maintaining high quality, it is essential to make use of specific settings for the sliding-mode observer. Some works in

the literature, on the other hand, use parameters that are chosen at random. As shown in Figures 7 and 8, the proper parameters for the SBS-SMO can be achieved by employing the described process. The simulation's settings and values are presented in Table 2.
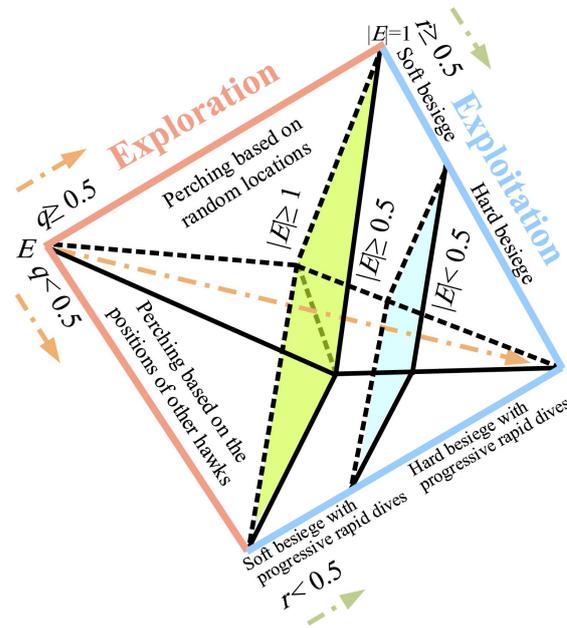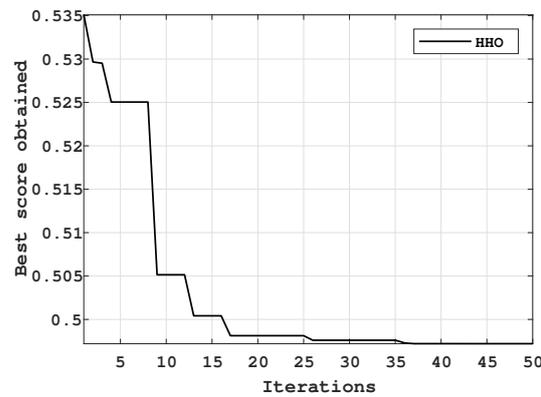

Figure 6. Structure of HHO.

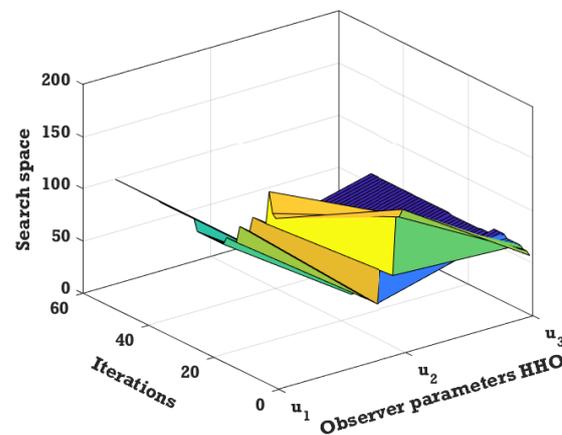**Figure 7.** The greatest possible HHO score attained during iterations.

Figure 8. The optimisation vector of the HHO algorithm and its dynamic changes.

Table 2. Parameters and values used in simulations and in real time.

Parameters	Values
Search agents	15
Max iteration	50
Parameters [μ_1 μ_2 μ_3]	$[185.3, 80.1, 145.08]$

7. Results and Discussion

Figures 9–11 show the responses of the states (x, y, z) and their estimations $(\hat{x}, \hat{y}, \hat{z})$. Figure 12 shows the collective estimation errors for the three state variables. This proves that the two FOCS can be synchronised optimally within a finite amount of time. The initial conditions are assumed to be $(x(0) = y(0) = z(0) = 0)$, whereas the responding system's initial conditions are all set to zero $(\hat{x}(0) = \hat{y}(0) = \hat{z}(0) = 0)$.
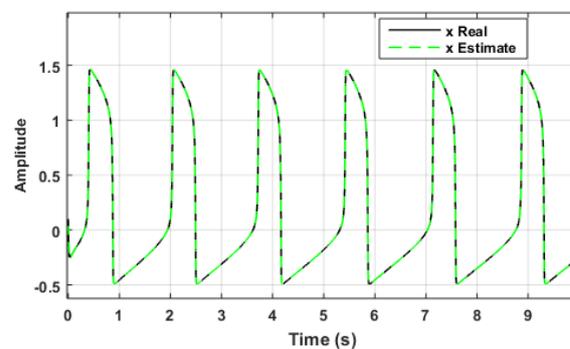
Figure 9. Data set synchronisation of x and $\hat{x}$.
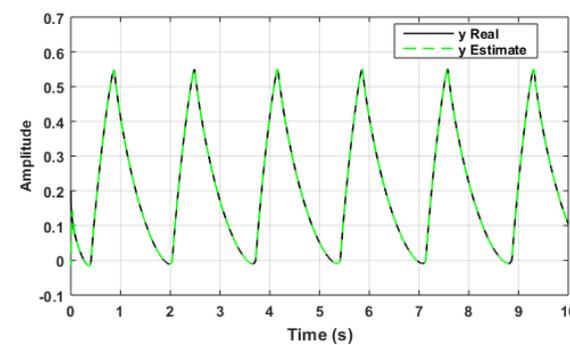
Figure 10. Data set synchronisation of y and $\hat{y}$.
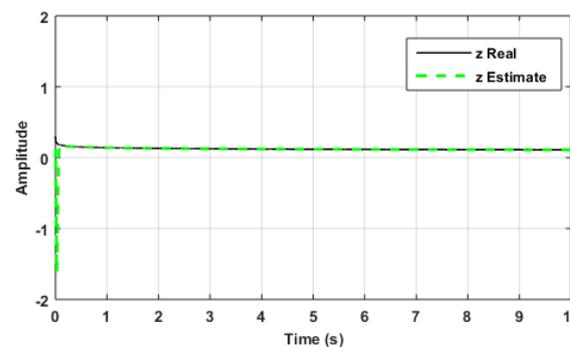
Figure 11. Data set synchronisation of z and $\hat{z}$.
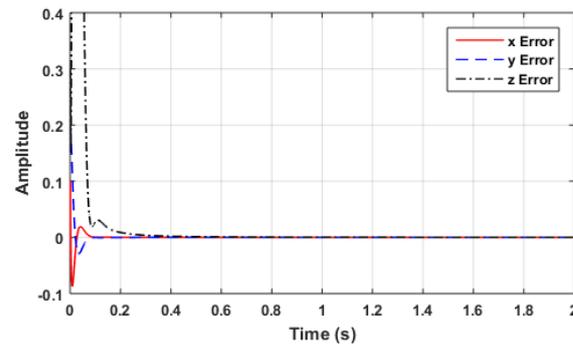
Figure 12. The estimation errors: *x* error, *y* error, and *z* error.

7.1. Retrieving the Secret Message

The purpose of this section is to use the properties and characteristics of the SBS-SMO, specifically synchronisation and estimating the unknown inputs, for the information encryption process. First, we include the secret information, which we consider to be the sin, square, sawtooth, and voice signals. These signals are represented by the following formulations: $m(t) = 0.1sin(2t), m(t) = 0.1square(2t), m(t) = 0.1sawtooth(2t)$, and $m(t) = voice$, respectively. As shown in Figures 13–16, the recovered messages in the receiver system are similar to the original ones, with $(x(0) = y(0) = z(0) = 0)$ and $(\hat{x}(0) = \hat{y}(0) = \hat{z}(0) = 0)$. Additionally, Table 3 presents a comparison between the proposed work and the work in [26] across four distinct error messages: sin, square, sawtooth, and voice. Although [26] did not succeed in retrieving the voice message, we made an attempt to recover it for comparison with our own voice signal, revealing an MSE close to zero during the recovery process.
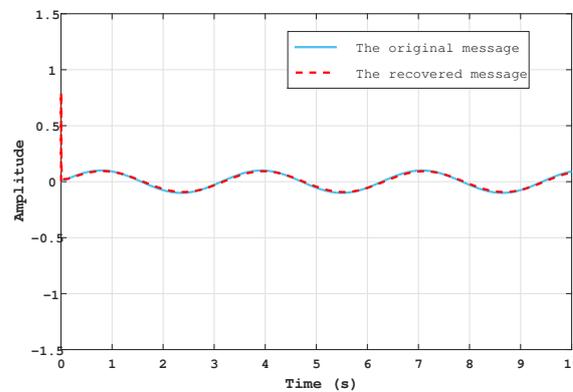

Figure 13. The original message (sinusoidal wave $m(t) = \sin(t)$) and the recovered $\hat{m}(t)$.
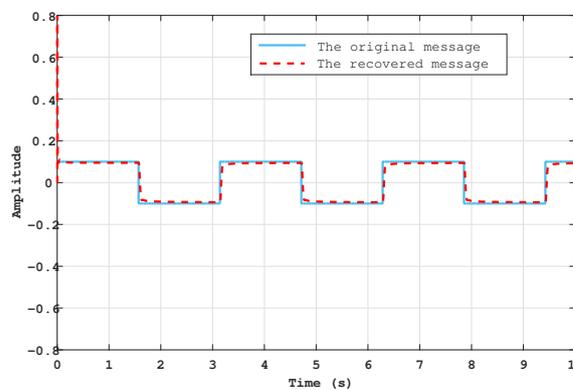

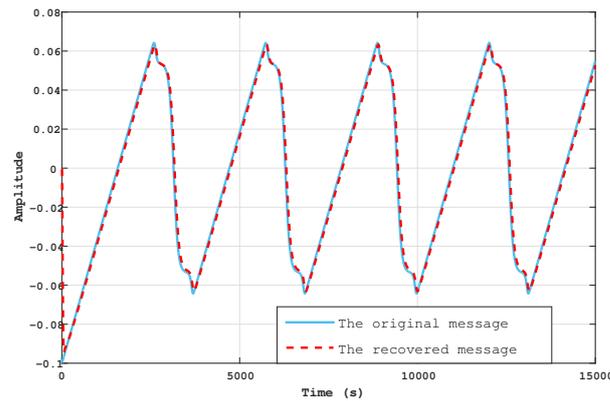**Figure 14.** The original message ($m(t) = $ square(t)) and the recovered $\hat{m}(t)$.

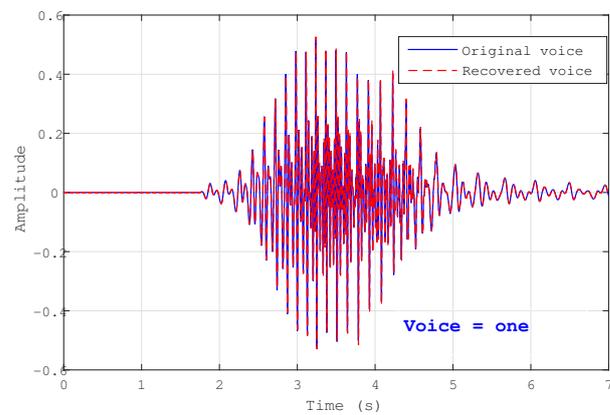**Figure 15.** The original message ($m(t)$ = sawtooth(t)) and the recovered $\hat{m}(t)$.

Figure 16. The original message ($m(t)$ = voice) and the recovered $\hat{m}(t)$.

Table 3. Comparison of different kinds of messages.

Methods	Sin Message	Square Message	Sawtooth Message	Voice Message
Proposed	7.5211×10^{-5}	2.1165×10^{-4}	2.0181×10^{-5}	6.2521×10^{-4}
[26]	8.2397×10^{-4}	0.0024	0.0022	0.0069

7.2. Security Analysis and Check

Two primary modifications were made in order to evaluate the level of security provided by the proposed secure transmission technique. These included alterations in the initial conditions and the sequence of transmissions between the transmitter and receiver. Due to the significance of the original voice message, it was selected from among the other messages that were received (Figure 17). We only made a tiny modification in the initial conditions of the transmitter system's first state, which were ($x(0) = 10^{-6}$, $y(0) = z(0) = 0$). As a result of our investigation, the message that was contained was completely lost by the receiver as well. The second check involved a small modification in the first state order of the transmitter system. As depicted in Figure 18, the value of q_1 was 0.905, the value of q_2 was 0.9, and the value of q_3 was 0.9. In addition, we discovered that the message that was inserted had been completely missed.

The fractional order of the chaotic system q was chosen randomly; the sensitivity of the chaotic system to this fractional order is advantageous. A small change in q was accompanied by a significant change in the behaviour of the system, which complicated the decoding of the proposed communication scheme's encryption. Therefore, it was considered key to the decryption process. The same fractional order can be used on both sides, sender and receiver, with the same initial state conditions. Different values can be

used as well, but for synchronisation to occur, the observer's parameters must be chosen corresponding to this case.
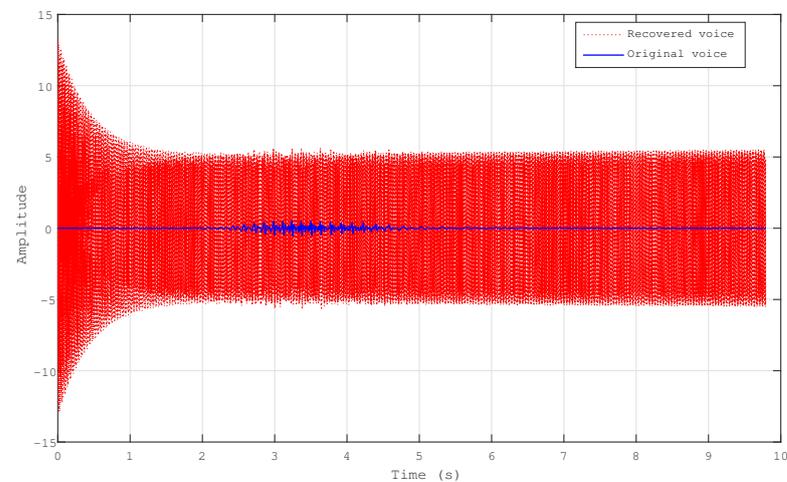

Figure 17. The original message m = voice and the recovered $\hat{m}(t)$ with initial conditions $x(0) = 10^{-6}$, $y(0) = 0$, $z(0) = 0$, and $(\hat{x}(0) = \hat{y}(0) = \hat{z}(0) = 0)$. The order for both the transmitter and receiver is $q_1 = q_2 = q_3 = 0.9$.
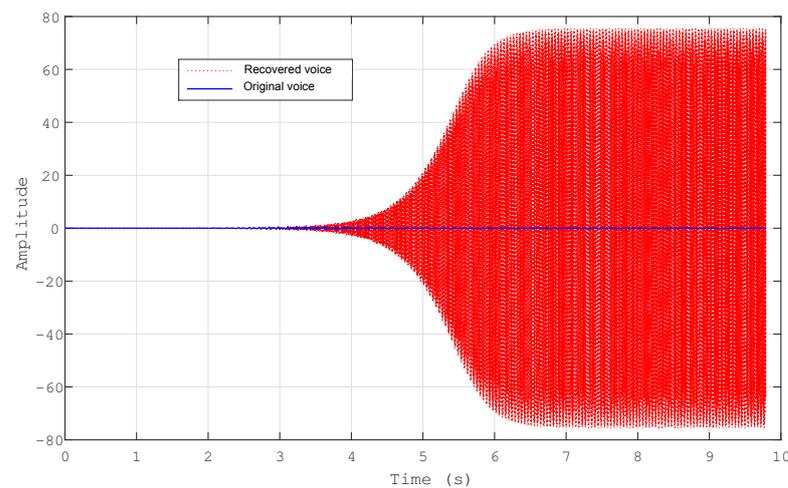

Figure 18. The original message m = *voice* and the recovered $\hat{m}(t)$ with initial conditions $(x(0) = y(0) = z(0) = 0)$ and $(\hat{x}(0) = \hat{y}(0) = \hat{z}(0) = 0)$. The orders for the transmitter are $q_1 = 0.905$, $q_2 = q_3 = 0.9$, whereas those for the receiver are set to 0.9.

7.3. Experimental Validation

Figure 19 shows the experimental validation of the proposed secure communication scheme. We implemented the FOCS and SBS-SMO in the two microcomputers in the transmitter and the receiver, respectively. The discrepancy between the theoretical and the experimental aspects has been minimised through mathematical tools such as Rung Kutta 4, approximation between fractional and integer transfer functions, and the Kalman filter. Wireless transmission was facilitated by the NRF24L01 module. The obtained results confirm the validity of the proposed idea from both mathematical and numerical aspects and its readiness for application in the experimental field.
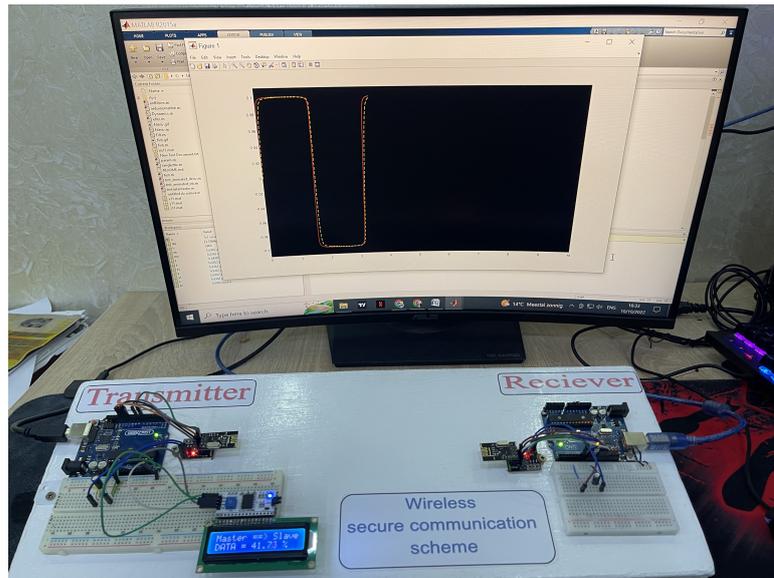
Figure 19. Real-time investigation.

8. Conclusions

A novel approach to enhancing the security of encrypted communications is proposed in this article. The proposed method involves the utilisation of a novel optimisation algorithm in order to achieve the highest level of performance for the observer. To ensure synchronisation between the emitter and receiver, we established an ideal SBS-SMO device on the reception side.

In this work, we succeeded in transferring many pure mathematical concepts from digital simulations and incorporating them into electronic circuits and microcontrollers so that people could exploit them in their daily lives. Rung Kutta 4 was used to solve the limitation in the memory of the atmega328p microcontroller to compute the cumulative integration, as without it, we would need a memory allocation. We added capacitors to the circuit to enhance the NRF24L01 module's performance, and a stochastic filter was implemented to denoise the recovered input (message) in the received part.

According to the obtained results, we have come to the conclusion that confidential information can only be recovered by outside individuals if the following details are provided:

- The type of chaotic system utilised, such as Lorenz, Rossler, Chua's, and Chen, among others.
- The dynamic parameters of the chaotic system.
- The order and initial conditions of the system, as well as the state in which the message was embedded.
- The mechanism of the synchronisation process, such as a controller or observer, and the specific type of controller or observer.
- The characteristics of the encrypted and decrypted data, such as text, images, voice, and video.

On the other hand, assembling all of this equipment is an extraordinarily challenging task.

Future studies will include:

- Transmitting secure images instead of voice or signal data.
- Improving fractional Chua's systems through real-time implementation of new 4D or 6D fractional chaotic systems.
- Replacing the synchronisation observer with advanced and more recent algorithms such as deep learning and machine learning approaches.

References

1. Oldham, K.B. Fractional differential equations in electrochemistry. *Adv. Eng. Softw.* **2010**, *41*, 9–12. [CrossRef]
2. Giona, M.; Cerbelli, S.; Roman, H.E. Fractional diffusion equation and relaxation in complex viscoelastic materials. *Phys. A Stat. Mech. Its Appl.* **1992**, *91*, 449–453. [CrossRef]
3. Ionescu, C.; Lopes, A.; Copot, D.; Machado, J.A.T.; Bates, J.H.T. The role of fractional calculus in modeling biological phenomena: A review. *Commun. Nonlinear Sci. Numer. Simul.* **2017**, *51*, 141–159. [CrossRef]
4. Morales-Delgado, V.F.; Gómez-Aguilar, J.F.; Saad, K.M.; Khan, M.A.; Agarwal, P. Analytic solution for oxygen diffusion from capillary to tissues involving external force effects: A fractional calculus approach. *Phys. A Stat. Mech. Its Appl.* **2019**, *523*, 48–65. [CrossRef]
5. El-Sayed, A.A.; Agarwal, P. Numerical solution of multiterm variable-order fractional differential equations via shifted Legendre polynomials. *Math. Methods Appl. Sci.* **2019**, *42*, 3978–3991. [CrossRef]
6. Rekhviashvili, S.; Pskhu, A.; Agarwal, P.; Jain, S. Application of the fractional oscillator model to describe damped vibrations. *Turk. J. Phys.* **2019**, *43*, 236–242. [CrossRef]
7. Atoussi, M.A.; Saadi, S.; Nail, B. Design of an optimal step-by-step sliding mode observer for multiple fractional-order chaotic synchronisation with an application to secure communication. *Int. J. Appl. Nonlinear Sci.* **2023**, *4*, 58–71. [CrossRef]
8. L.ü; J.; Chen, G.; Cheng, D.; Celikovsky, S. Bridge the gap between the Lorenz system and the Chen system. *Int. J. Bifurc. Chaos* **2002**, *12*, 2917–2926. [CrossRef]
9. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
10. Rössler, O.E. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
11. Lü, J.; Chen, G. A new chaotic attractor coined. *Int. J. Bifurc. Chaos* **2002**, *12*, 659–661. [CrossRef]
12. Pellicer-Lostao, C.; López-Ruiz, R. A chaotic gas-like model for trading markets. *J. Comput. Sci.* **2010**, *1*, 24–32. [CrossRef]
13. Ditto, W.L. Applications of chaos in biology and medicine. *AIP Conf. Proc.* **1996**, *376*, 175–201.
14. Bodnar, M.; Foryś, U. Three types of simple DDE's describing tumor growth. *J. Biol. Syst.* **2007**, *15*, 453–471. [CrossRef]
15. Lamba, P.; Hudson, J.L. Experiments on bifurcations to chaos in a forced chemical reactor. *Chem. Eng. Sci.* **1987**, *42*, 1–8. [CrossRef]
16. Yang, T.; Chua, L.O. Secure communication via chaotic parameter modulation. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **1996**, *43*, 817–819. [CrossRef]
17. Delavari, H.; Mohadeszadeh, M. Robust finite-time synchronization of non-identical fractional-order hyperchaotic systems and its application in secure communication. *IEEE/CAA J. Autom. Sin.* **2016**, *6*, 228–235. [CrossRef]
18. Tian, X.; Fei, S.; Chai, L. On modified second-order sliding mode synchronization of two different fractional order hyperchaotic systems. *Int. J. Multimed. Ubiquitous Eng.* **2015**, *10*, 387–398. [CrossRef]
19. Durga, N.; Muthukumar, P.; Niezabitowski, M. Approximation and convergence analysis of optimal control for non-instantaneous impulsive fractional evolution hemivariational inequalities. *Results Control Optim.* **2022**, *9*, 1–20. [CrossRef]
20. Meng, F.; Gu, Z. A Color Image-Encryption Algorithm Using Extended DNA Coding and Zig-Zag Transform Based on a Fractional-Order Laser System. *Fractal Fract.* **2023**, *7*, 795. [CrossRef]
21. Roohi, M.; Zhang, C.; Taheri, M.; Basse-O'Connor, A. Synchronization of Fractional-Order Delayed Neural Networks Using Dynamic-Free Adaptive Sliding Mode Control. *Fractal Fract.* **2023**, *7*, 682. [CrossRef]

22. Feng, W.; Wang, Q.; Liu, H.; Ren, Y.; Zhang, J.; Zhang, S.; Qian, K.; Wen, H. Exploiting Newly Designed Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map for High-Performance Multi-Image Encryption. *Fractal Fract.* **2023**, *7*, 887. [CrossRef]

23. Trigeassou, J.-C.; Maamri, N. Modeling and Initialization of Nonlinear and Chaotic Fractional Order Systems Based on the Infinite State Representation. *Fractal Fract.* **2023**, *7*, 713. [CrossRef]

24. Oldham, K.; Spanier, J. *The Fractional Calculus Theory and Applications of Differentiation and Integration to Arbitrary Order*; Elsevier: Amsterdam, The Netherlands, 1974.

25. Kilbas, A.A.; Srivastava, H.M.; Trujillo, J.J. *Theory and Applications of Fractional Differential Equations*; Elsevier: Amsterdam, The Netherlands, 2006; Volume 204.

26. Bettayeb, M.; Al–Saggaf, U.M.; Djennoune, S. Single channel secure communication scheme based on synchronization of fractional-order chaotic Chua's systems. *Trans. Inst. Meas. Control* **2018**, *40*, 3651–3664. [CrossRef]

27. Barbot, J.P.; Djemai, M.; Boukhobza, T. Sliding mode observers. *Sliding Mode Control Eng.* **2002**, *11*, 33.

28. Heidari, A.A.; Mirjalili, S.; Faris, H.; Aljarah, I.; Mafarja, M.; Chen, H. Harris hawks optimization: Algorithm and applications. *Future Gener. Comput. Syst.* **2019**, *97*, 849–872. [CrossRef]