applied system innovation

MDPI

Article

Optimizing Security and Cost Efficiency in N-Level Cascaded Chaotic-Based Secure Communication System

Talal Bonny * and Wafaa Al Nassan

Department of Computer Engineering; University of Sharjah, Sharjah P.O. Box 27272, United Arab Emirates; walnassan@sharjah.ac.ae

* Correspondence: tbonny@sharjah.ac.ae; Tel.: +971-6-5053940

Abstract: In recent years, chaos-based secure communication systems have garnered significant attention for their unique attributes, including sensitivity to initial conditions and periodic orbit density. However, existing systems face challenges in balancing encryption strength with practical implementation, especially for multiple levels. This paper addresses this gap by introducing a novel N-level cascaded chaotic-based secure communication system for voice encryption, leveraging the four-dimensional unified hyperchaotic system. Performance evaluation is conducted using various security metrics, including Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), Percent Residual Deviation (PRD), and correlation coefficient, as well as Field-Programmable Gate Array (FPGA) resource metrics. A new Value-Based Performance Metrics (VBPM) framework is also introduced, focusing on both security and efficiency. Simulation results reveal that the system achieves optimal performance at N = 4 levels, demonstrating significant improvements in both security and FPGA resource utilization compared to existing approaches. This research offers a scalable and cost-efficient solution for secure communication systems, with broader implications for real-time encryption in practical applications.

Keywords: hyperchaotic; cascaded chaotic system; security analysis; secure communication system; field-programmable gate array; voice encryption

Citation: Bonny, T.; Al Nassan, W. Optimizing Security and Cost Efficiency in N-Level Cascaded Chaotic-Based Secure Communication System. *Appl. Syst. Innov.* **2024**, *7*, 107. https://doi.org/10.3390/asi7060107

Academic Editor: Andrzej Białas

Received: 26 July 2024
Revised: 12 October 2024
Accepted: 18 October 2024
Published: 31 October 2024

1. Introduction

In recent decades, there has been increasing interest in the study of dynamical systems, particularly chaotic systems. Chaotic systems are traditional nonlinear dynamical systems that are sensitive to initial conditions, a phenomenon often referred to as the butterfly effect. This effect implies that when two identical chaotic systems start with nearly the same initial conditions, their trajectories diverge exponentially over time, leading to significantly different outcomes.

The development of chaotic systems started in 1963 when Lorenz discovered a three-dimensional (3D) chaotic system for weather modeling [1]. In 1979, Rossler introduced a four-dimensional (4D) system describing the dynamics of chemical reactions, known as a hyperchaotic system, which is chaos with more than one positive Lyapunov exponent [2]. Hyperchaos has been studied intensively in different fields due to its interesting properties such as high capacity, enhanced security, and increased efficiency [3].

Many types of chaotic/hyperchaotic systems have been introduced in both continuous-time and discrete-time domains. Examples of continuous-time systems include Chua's circuit [4,5], Duffin, and Lu and Chen systems. In contrast, the Logistic map, Henon map [6], Henon 3D map, and Lorenz discrete map [7] are examples of discrete-time systems.

Previous research in this area has explored various techniques for implementing secure communication systems, including electronic circuits [8,9], FPGA implementation [10], and memristor-based circuits [11,12]. In addition, secure communication systems can also be realized through post-quantum encryption algorithms [13], quantum-secure

communications [14], and physical layer security [15]. While these approaches focus on providing robustness against quantum attacks or ensuring security at the communication layer, the proposed chaotic-based encryption offers an alternative based on the intrinsic unpredictability of chaotic systems, making it an effective method for data masking and encryption.

The study of chaos is very important because of its applications in robotics [16,17], cryptography [18], neural network [19], secure communication [20], etc.

The protection of multimedia files against copying or attacking across public channels has become a research subject in recent years [21,22]. The first chaos-based secure communication system introduced in 1993 is additive chaos masking. This method involves using identical chaotic oscillators at both the transmitter and the receiver [23–26]. One state variable of the oscillator on the transmitter side, known as the chaotic mask signal, is added to the message signal giving the transmitted signal. Since the chaotic signal is very complex, the information message cannot be extracted without knowing the exact value of the mask signal. This scheme has drawbacks such as sensitivity to noise in the channel and parameter mismatches between the identical chaotic oscillators in the transmitter and the receiver [27]. Moreover, as demonstrated in [28], it has a relatively low degree of security, as researchers were able to predict the carrier behavior and break the system by subtracting the predicted values from the carrier, thereby reconstructing the message signal through some processing operations.

To date, many attack methods have been developed to break the chaotic communication system and schemes. Therefore, there remains a requirement and necessity to develop a scheme that can be potentially employed against attacks.

In the literature, many papers have used the chaos cascade concept to construct new chaotic systems, which increases the value of Lyapunov exponents and expands the parameter space [29,30]. Kharel [31] proposed a chaos-based cryptosystem called the cascaded chaotic masking technique, which improves security by using two chaotic signals to increase the complexity of the encrypted signal. In [26], the authors used multiple double levels of chaotic masking to encrypt a speech signal. This approach was implemented by using Lorenz and Rossler systems. Furthermore, the author in [32] proposed a new chaotic map, named tent delay-sine cascade with logistic map (TDSCL), for image encryption. In [33], the authors developed a long-distance encryption system using the chaos masking technique, employing three cascaded lasers, called vertical-cavity surface-emitting lasers (VCSELs), to develop the proposed system. More references related to cascaded chaotic systems are listed in Table 1.

Table 1. Related work for cascaded chaotic masking.

Ref.	Used Chaotic Systems	Levels of Masking
[34] 2012	Lorenz System	1, 2
[35] 2014	Seed map	2
[33] 2017	Optical chaos with TD signature suppression	3
[25] 2017	Lur'e system	1, 2
[36] 2018	Quantum cascade lasers	2
[32] 2020	Tent Delay-Sine cascade with Logistic Map	2
[26] 2020	Rossler chaotic flow system	1, 2
[29] 2021	discrete memristive maps	2, 3

The ideal number of cascaded levels has not been thoroughly discussed in the aforementioned references in Table 1. They mainly focused on using a specific number of cascaded systems without taking into consideration the general performance and the cost of a secure communication system. Although the use of multiple cascaded chaotic systems increases the key-space and the complexity of encrypted signals, it also increases the execution time and the cost of the system. Recognizing the ideal quantity of cascaded tiers is essential as it directly impacts the system's security and resource efficiency. Achieving a bal-

ance between optimizing security and reducing resource overhead is crucial, with practical consequences for sectors that depend on secure, fast data transfer.

In light of this conflict, further research is required to determine the effects of changing the number of cascaded levels on system efficiency and security. Our work aims to bridge this gap by conducting a practical study that examines the impact of increasing the number of cascaded levels on the system's overall performance and resource utilization. In this paper, we propose a secure communication system for voice encryption based on the cascaded structure using the 4D unified hyperchaotic system, we illustrate the efficiency of using different number of cascaded levels, (from N = 1 to N = 20), on the quality of encryption. Various security metrics are then applied to test the performance of the systems such as Correlation coefficient analysis, Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), Percent Residual Deviation (PRD), and timing analysis. Moreover, the proposed systems are realized on FPGA in order to determine the implementation cost. Finally, to evaluate the whole performance of the communication systems, we propose a new metric, termed Value-Based Performance Metrics (VBPM), which integrates multiple metrics for a holistic assessment. This metric is used to compare different cascaded chaotic systems that employ different values of N levels.

The main contributions of this paper are summarized as follows:

1. Introduce a novel N-level cascaded chaotic-based secure communication system for voice encryption using the 4D unified hyperchaotic system.
2. Investigate the effect of increasing the number of cascaded levels on encryption quality.
3. Implement the proposed system on FPGA and analyze its performance using various parameters.
4. Analyze the effect of increasing the number of cascaded levels from N = 1 to N = 20 to reach the best performance by measuring various of metrics.
5. Introduce VBPM as a new performance metric for evaluating the system's overall performance.
6. Demonstrate the superiority of the proposed system compared to other related works in terms of security and efficiency.

The remainder of this paper is organized as follows. The architecture of the proposed N-levels cascaded chaotic-based secure communication system is presented in Section 2. Section 3 describes the hardware realization on FPGA of the proposed scheme. The performance analysis of the proposed secure communication systems for voice encryption is presented in Section 4, using multiple metrics when the number of cascaded levels is increased from N = 1 to 20. Section 5 presents the results of a comparative analysis. Finally, the conclusions are discussed in Section 6.

2. Model Description of the N-Levels Cascaded Chaotic-Based Secure Communication System for Voice Encryption

Chaos-based encryption systems are highly effective for secure communication due to their sensitivity to initial conditions and complexity, generating hard-to-decipher, pseudo-random signals. As the demand for stronger security grows, particularly in fields like voice encryption and real-time data transmission, researchers have explored using cascaded chaotic systems. Cascading multiple chaotic systems significantly enhances encryption strength by increasing signal complexity and expanding the key-space, making the encryption more secure.

This section will give a general overview of the structure of secure communication system for voice encryption based on N-level cascaded 4D unified hyperchaotic system. Additionally, it will include a detailed description of the system's structure and its mathematical representation, highlighting the underlying principles and assumptions that

govern its operation. First, we introduce the mathematical representation of the 4D unified hyperchaotic system used in this paper, which is given in (1) as follows:

$$\begin{aligned} \dot{x}_1 &= a_1(x_2 - x_1) + x_4 \\ \dot{x}_2 &= a_2 x_1 - x_1 x_3 + b_4 x_2 \\ \dot{x}_3 &= x_1 x_2 - a_3 x_3 \\ \dot{x}_4 &= 0.2 x_4 + 0.1 x_2 x_3 \end{aligned} \tag{1}$$

where $(x_1, x_2, x_3, x_4) \in R^4$ are state variables. a_1, a_2, a_3 and a_4 are positive parameters. The proposed system has a chaotic behaviors when the parameters are $a_1 = 45$, $a_2 = 3$, $a_3 = 10$ and $10 \leq a_4 \leq 40$.

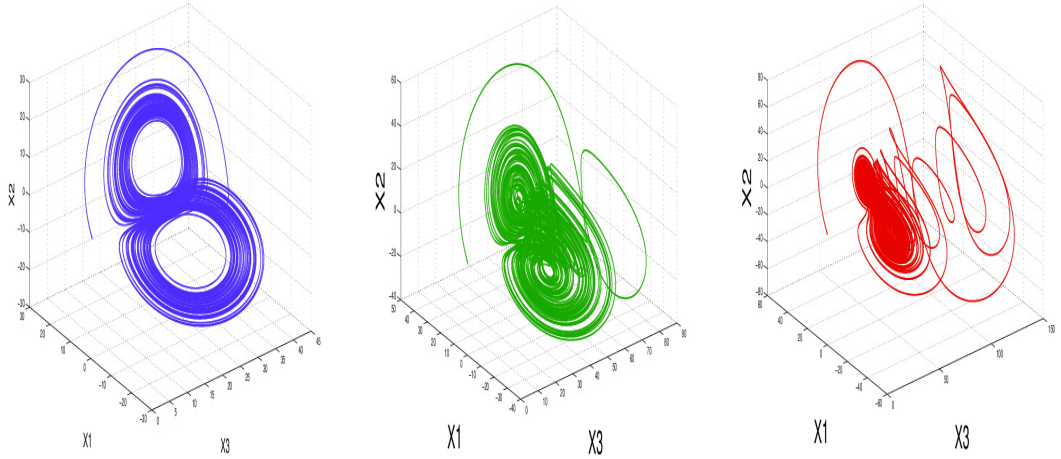
Based on the value of parameter a_4, the proposed oscillator shows a hyperchaotic behaviors in different regions:

1. When $a_4 = 13$, the output hyperchaotic attractor is similar to Lorenz attractor.
2. When $a_4 = 27$, the output hyperchaotic attractor is similar to Lu attractor.
3. When $a_4 = 36$, the attractor is similar to Chen attractor.

Figure 1, reveals the chaotic attractors generated by Equations (1) for different values of parameter a. When $a = 13, 27$, and 37, the resulting attractors will be similar to the Lorenz, Lü, and Chen systems, respectively. The fourth-order Runge–Kutta integrator, which has high algorithmic accuracy in numerical simulation and due to its high accuracy and efficiency in solving ordinary differential Equations (ODEs), which are critical for accurately modeling the behavior of the chaotic systems [37]. The used simulation parameters are fixed step size (0.001), $a_1 = 45$, $a_2 = 3$, $a_3 = 10$, $a_4 = [13, 27, 36]$, and the initial conditions are $x(0) = [1, 1, 1, 1]^T$. Extended detailed analysis of proposed system available in [38].

Figure 2 shows the principle of cascaded structure of N_{th}chaotic systems using the unified 4D hyperchaotic system. The principle of cascaded structure is mainly to construct a new hyperchaotic system with its own performance. In this context, the additive cascaded technique used in this paper, enhances the overall complexity of the chaotic signals generated, significantly increasing the key-space and improving the security of the encryption process.

To illustrate the proposed secure communication scheme using the additive cascaded technique, consider a series connection of the 4D unified hyperchaotic system given in (1), where the output of the first 4D hyperchaotic system is fed into the input of the second one producing another chaotic signal that is connected to the input of the next oscillator recursively till the N_{th} oscillator.



(**a**) $a = 13$(Lorenz Attractor) (**b**) $a_4 = 27$ (LU Attractor) (**c**) $a_4 = 36$ (Chen Attractor)

Figure 1. Phase attractors of the unified hyperchaotic oscillator when $a_4 = [13, 27, 36]$.

Figure 2. Block diagram of N-levels cascaded chaotic oscillators.

Figure 3 illustrates the encryption/decryption scheme using an N-levels cascaded chaotic system. In this scheme, on the transmitter side, the voice signal is initially masked by the output of the first 4D oscillator. To further enhance the security and randomness of the encrypted signal, the output from each subsequent level of the cascaded oscillators is used to successively mask the signal. This process generates the final encrypted signal, which is then transmitted through the communication channel. Based on the encryption scheme, the encrypted signal can be described as follows:

$$X_t(t) = m(t) + c_1X_1 + c_2X_2 + c_3X_3 + \ldots + c_NX_N \tag{2}$$

where m(t) is the original information message, $X_1, X_2, X_3 \ldots X_N$ are the state vectors generated from each level in the cascaded system and $c_1, c_2, c_3 \ldots c_N$ are selectable gains.

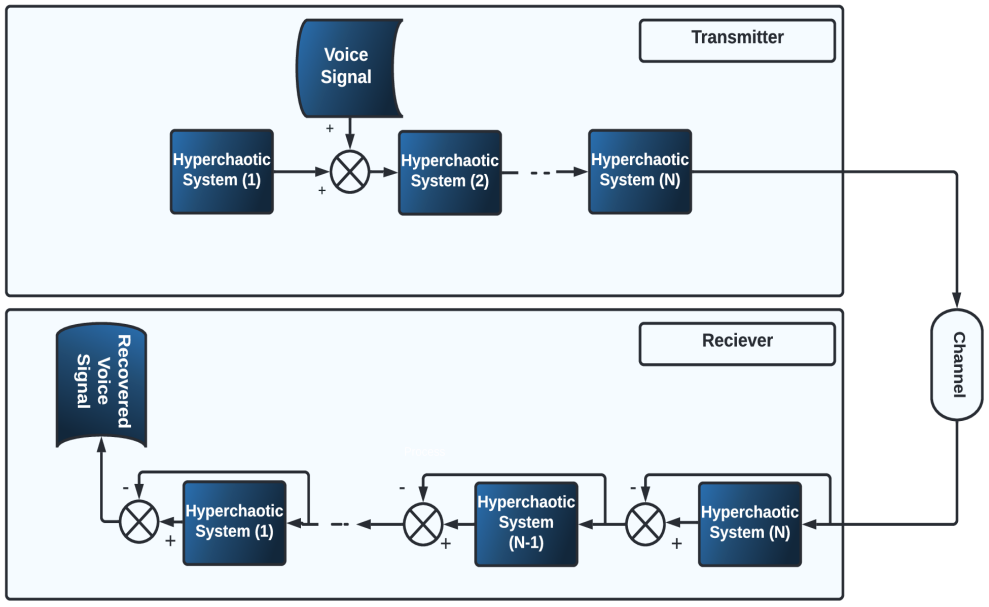


Figure 3. Block diagram of N-level cascaded chaos-based secure communication system.

On the receiver side, to unmask the original voice message, the output of the first chaotic system is subtracted from the cascaded chaotic system recursively till the last system produces the recovered information message that is similar to the original one.

In this study, we use the following assumptions to ensure that our secure communication system will recover the information signal correctly:

Assumption 1. *The cascaded systems on the transmitter side are similar to the systems on the receiver side.*

The cascaded systems at both ends must exhibit similar dynamics for successful signal decryption. If the systems are not similar, the chaotic signals will differ, leading to a mismatch in the decryption process and possible communication failure.

Assumption 2:. *Each hyperchaotic system on the receiver side is synchronized to its opposite one on the transmitter side.*

Since the chaotic oscillators are sensitive to the initial conditions, the synchronization is essential to make the generated chaotic signals on the receiver side synchronized, allowing for successful decryption. Without synchronization, the encrypted signal cannot be accurately interpreted by the receiver, leading to errors in the recovered data.

Based on the previous assumptions and the decryption scheme, the recovered signal can be described as follows:

$$m_r(t) = X_t(t) - c_1Y_1 - c_2Y_2 + c_3Y_3 - \ldots - c_NY_N \tag{3}$$

where $m_r(t)$ is the recovered voice signal, $X_t(t)$ is the received encrypted signal, $Y_1, Y_2, Y_3 \ldots Y_N$ are the state vectors generated from each level in the cascaded system in the receiver side which are similar to $X_1, X_2, X_3 \ldots X_N$ state vectors, respectively, and $c_1, c_2, c_3 \ldots c_N$ are selectable gains.

3. Hardware Implementation

The proposed secure communication systems are implemented on FPGA platform for different values of N (from N = 1 to N = 20). The main block in the studied systems is the 4D unified hyperchaotic system. The forward Euler integration method is used to determine the numerical solution of the 4D hyperchaotic system shown in (4).

$$\begin{aligned} x_1[n+1] &= x_1[n] + h(a_1(x_2[n] - x_1[n]) + x_4[n]) \\ x_2[n+1] &= x_2[n] + h(a_2x_1[n] - x_1[n]x_3[n] + b_4x_2[n]) \\ x_3[n+1] &= x_3[n] + h(x_1[n]x_2[n] - a_3x_3[n]) \\ x_4[n+1] &= x_4[n] + h(0.2x_4[n] + 0.1x_2[n]x_3[n]) \end{aligned} \tag{4}$$

where $[n]$ and $[n+1]$ are the current and the next states, respectively. x_1, x_2, x_3, and x_4 are output state variables of the master system, $a_1 = 45$, $a_2 = 3$, $a_3 = 10$, $a_4 = [13, 27, 36]$ are the coefficient parameters, and the initial conditions are $x(0) = [1, 1, 1, 1]^T$. The initial conditions of the state variables are $x_0 = [1, -1, 1, -1]$, while the discretization step size is h = 0.001.

Figure 4 shows the basic hardware blocks required for the implementation which are adders, subtractors, multipliers, and delays.

Then, the hardware implementation of the N-levels cascaded chaotic-based secure communication system in Figure 3 is done by using the VHDL code. Each system is realized on the FPGA **Cyclon V** platform. We use the 32-bits fixed-point arithmetic representation for all the variables and constants for the FPGA implementation. This representation has 1-bit for the sign, 7-bits for the integer part, and 24-bits for the fractional part.

In this paper, we measure FPGA resource utilization and maximum clock frequency, which are crucial metrics that influence the cost and performance of FPGA-based encryption systems, particularly as the number of encryption levels (N) increases. Finding the right balance between logic utilization and maximum frequency is key to optimizing the FPGA design. A design with low resource usage lowers the cost of hardware implementation, while a high frequency ensures the system's performance remains fast and efficient. By examining how these parameters change with N levels, the paper aims to identify the most cost-effective FPGA implementation that offers robust encryption with minimal resource overhead and maximal processing speed. This balance is vital for practical applications where both cost and performance are important constraints. Table 2 shows FPGA resources utilization of N-level chaotic-based secure communication system for varying numbers of levels (N) from 1 to 20. The maximum frequency for the studied systems was between 31.08 MHz when N = 1 and 29.69 MHz when N = 7. The utilization of FPGA resources increases with an increasing value of N, for number of chaotic systems levels greater than

N = 7, the system exceeds the capacity of the Cyclone V FPGA, which may require a more advanced FPGA model or additional resources to accommodate the implementation.

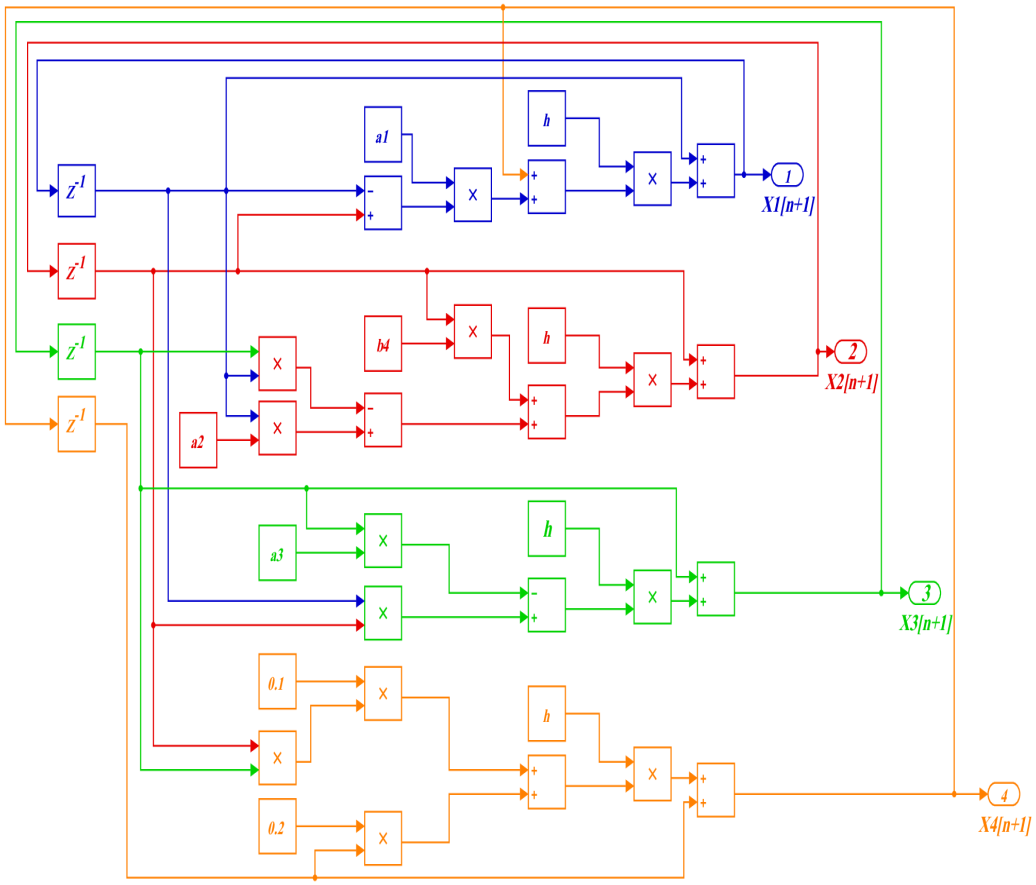


Figure 4. The basic blocks for FPGA-based 4D unified hyperchaotic systems.

Table 2. FPGA resource utilization and maximum operating frequency for the N-level chaotic-based secure communication system using different values of N.

FPGA Resources	Number of Levels											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**15**	**20**
Logic Utilization (in ALMs) %	14	27	41	55	69	79	93	105	120	132	184	263
Maximum Frequency(MHz)	31.08	30.19	30.97	31.29	30.42	30.58	29.69	-	-	-	-	-

4. Numerical Simulation

The proposed system is simulated on MatLAB (2020) for voice encryption in this section. The selected voice signal for this test has a sampling rate of 8 kHz. To study the efficiency of the increasing number of levels on the security of encryption, twelve different values of N are considered for comparison. Then, to demonstrate the efficiency of increasing the number of cascaded levels,from N = 1 to N = 20, on the security of encrypted signal/decrypted. In addition, the security analysis using different performance metrics is introduced for different values of N, i.e., the number of levels such as Signal-To-Noise Ratio (SNR), Peak Signal-To-Noise Ratio (PSNR), Percent Residual Deviation (PRD), Correlation Coefficient (CC) and encryption(te)/decryption time(td). In addition, we consider the utilization of FPGA resources and the clock frequency for each system to manage the cost of the systems.

4.1. Signal-to-Noise Ratio (SNR)

SNR is one of the most widely used objective measurements that evaluates the power of the original voice signal. For the given original signal $x(i)$ and the obtained encrypted speech signal $y(i)$, the SNR is defined as:

$$SNR = 10log_{10}(\frac{\sum x(i)^2}{\sum (x_i - y_i)^2}) \text{ dB} \quad (5)$$

Suppose the value of SNR is positive, this indicates that the power of the encrypted signal covers the original signal and vice versa, for the negative value indicate that the encryption signal covers the original one [39]. In the context of security, higher SNR suggests that the encryption system is resilient to noise attacks, as any added noise has minimal impact on signal integrity.

Table 3 indicates the values of SNR for different values of N, where the absolute values of the SNR increase as the number of levels in the system increases, implying that the noise introduced by the encryption becomes more significant. This increased noise level contributes to making the encryption more robust against attacks, as it becomes increasingly difficult to recover the original signal without the decryption key.

Table 3. Security analysis of N-level cascaded coupled chaotic systems.

Number of Levels (N)	SNR	PSNR	PRD	Correlation Coefficient CC	Encryption Time (te) µs	Decryption Time (td) µs
1	−60.10	11.15	$1.0124 \times 10^{+5}$	0.0027	0.32	0.23
2	−65.41	12.39	$1.8650 \times 10^{+5}$	0.0011	0.47	0.30
3	−69.02	12.56	$2.8242 \times 10^{+5}$	0.0006	0.74	0.46
4	−71.68	12.47	$3.8411 \times 10^{+5}$	0.0004	0.81	0.47
5	−73.99	11.95	$5.0087 \times 10^{+5}$	0.0005	1.1	0.6
6	−75.98	11.37	$6.3008 \times 10^{+5}$	0.0006	1.2	0.7
7	−77.76	10.73	$7.7353 \times 10^{+5}$	0.0008	1.3	0.7
8	−79.34	10.18	$9.2707 \times 10^{+5}$	0.0011	1.8	0.8
9	−79.34	10.18	$1.1057 \times 10^{+6}$	0.0014	1.8	0.9
10	−80.87	9.56	$1.3088 \times 10^{+6}$	0.0017	1.9	1
15	−82.33	8.95	$2.5864 \times 10^{+6}$	0.0020	3	1.6
20	−92.02	7.44	$3.9904 \times 10^{+6}$	0.0018	4	2

4.2. Peak Signal-to-Noise Ratio (PSNR)

PSNR refers to the ratio between the maximum possible power of original speech signal and the power of encrypted signal. A higher PSNR indicates that the encryption or reconstruction is of higher quality [40]. The higher the PSNR value, the better the quality of the encrypted signal. The PSNR is obtained based on the following equation:

$$PSNR = 10log_{10}(\frac{MAX(x_i^2)}{\sum (x_i - y_i)^2})) \text{ dB} \quad (6)$$

In Table 3, the maximum value of PSNR is opposite to the N = 3, and any increase in the levels leads to a decrease in the value of PSNR.

4.3. Percent Residual Deviation (PRD)

This parameter measures the deviation of the encrypted speech signal from the original signal [41]. For the original voice signal $x(i)$ and the encrypted voice signal $y(i)$, the PRD is calculated as:

$$PRD = 100(\sqrt{\frac{\sum (x_i - y_i)^2}{\sum (x(i))^2}}) \quad (7)$$

The calculation of the (PRD) for different voice signals is given in Table 3. PRD quantifies the relative difference between the original and encrypted signals. This metric can be used as a security metric since an encryption system with high PRD ensures that the original data is sufficiently concealed, making it more difficult for attackers to distinguish or reverse-engineer the encrypted content. The large obtained value of PRD shows that the encrypted signal has highly deviated from the original voice signal, in which case represents better security. In other words, increasing the number of levels results in a greater deviation between the original voice signal and the encrypted signal.

4.4. Correlation Coefficient (CC) Analysis

The correlation coefficient (cc) is a numerical measure of correlation whose values are $[-1, 1]$. It is a statistical evaluation to measure the quality of the encryption system. Calculating the correlation coefficient between the two signals expresses the linear relationship between the corresponding signals. Values near $|1|$ indicate a strong relationship between the two samples, and values near zero indicate the weakest relationship between the two samples. A lower correlation suggests a more secure encryption process, as the encrypted signal is less predictable based on the original data; hence, it cannot possibly be predicted by attackers [41].

Table 3 indicates the values of correlation coefficient for different number of levels. Based on the results, the minimum value of the correlation coefficient is opposite to the N = 4, and any increase in the levels leads to an increase in the value of the correlation coefficient.

4.5. Timing Analysis

Measuring the required time to encrypt/decrypt a voice signal depends on the operating system, programming language, and CPU frequency. Although measuring the encryption/decryption time does not directly impact the security of the system, it reflects the execution efficiency of the encryption algorithm. Timing analysis is crucial for identifying the optimal encryption system, as it helps achieve a higher level of security in less time. Table 3 shows the results of encryption/decryption time for each voice sample of the original voice signal using different values for N-Levels. The PC specs are Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz hp LAPTOP-UFTCGPRC, 8 GB RAM, Windows10. The results show that increasing the number of levels N creates more time delay in the process of encryption/decryption as expected.

Table 3 shows the performance metrics of N-level cascaded coupled chaotic systems using 12 different values of N. The results are obtained using the fourth-order Runge–Kutta integrator with a fixed step size (0.001). The parameter values for all the cascaded hyperchaotic systems in the transmitter and receiver are $a_1 = 45$, $a_2 = 3$, $a_3 = 10$ and $a_4 = 13$ and the initial conditions are $x(0) = [1, 1, 1, 1]^T$, $y(0) = [1, 1, 1, 1]^T$. Based on the security metrics presented in Table 3, we observe that as the number of levels (N) increases, SNR, PSNR, and PRD values also increase, indicating improved security. Conversely, the decreasing values of the correlation coefficient (CC) suggest enhanced security as well. However, increasing the number of cascaded levels also leads to longer encryption and decryption times, as the algorithm becomes more complex.

5. Experimental Results

This section aims to derive a single value that encapsulates the overall performance by integrating the data points calculated from various metrics. As seen in Tables 2 and 3, increasing the number of cascaded levels improves certain metrics, but not all. For example, metrics such as SNR, PSNR, PRD, and FPGA maximum frequency (F_{max}) show a direct correlation with the number of cascaded levels. Conversely, the correlation coefficient, encryption time, decryption time, and FPGA logic utilization (LUT) exhibit an inverse relationship. To facilitate a more efficient comparison across the studied systems, a performance index or cost function is necessary since it combines all metrics into a single value

representing the system's overall quality. This unified performance measure allows for a more comprehensive analysis of how increasing the number of cascaded levels affects the general performance of chaotic systems.

In this section, we introduce a new measure called Value-Based Performance Metrics (VBPM) to evaluate the studied systems based on both security metrics and resource utilization, as discussed in Section 4. The returned values of VBPM can assist in the comparison since higher values of VBPM reflects higher quality.

The mathematical description of VBPM is shown in Equation (8):

$$VBPM = \frac{\frac{1}{i}(|SNR| + PSNR + PRD + F_{max})}{\frac{1}{j}(CC + t_e + t_d + LUT)} \tag{8}$$

where i indicates the number of direct proportion metrics and j represents inverse proportion ones. In our study, $i = j = 4$.

However, there is an issue when the features are on drastically different scales. For example, considering data in Table 3, the values of $|SNR|$ and PSNR are in the ranges [60.1, 92.02] and [7.44, 12.56], respectively, while the values of PRD are in the range [$1.0124 \times 10^{+5}$, $3.9904 \times 10^{+6}$]. The VBPM should represent the relationship between the values. However, substituting those values in Equation (8) on a large scale, i.e., PRD will completely dominate the others.

The same issue exist for the values of the correlation coefficient, encryption time, and decryption time, where the correlation coefficient values are on the larger scale and dominate the others.

Based on the previous discussion, since the ranges of metrics in Table 3 are diverged, we need to adjust the values of metrics on different scales to a notionally common scale by using normalization. The goal of normalization is to make every data point have the same scale, so each metric is equally important.

Table 4 presents the normalized values for the performance metrics used in the comparison, along with the corresponding VBPM values for all the studied systems. The values in Tables 2 and 3 using min-max normalization, which is one of the most common ways to normalize data.

For each column in Tables 2 and 3, the min-max normalization equation is as follows:

$$NormalizedValue = \frac{value - min}{max - min} \tag{9}$$

where min and max indicate the minimum and maximum values for each studied metric. As a result, the maximum value in each column is normalized to '1', the minimum value to '0', and all other values fall between '0' and '1'. This ensures that all metrics are on a common scale, eliminating distortions caused by differences in their original ranges. After normalization, the values are used in the VBPM Equation (8), to calculate the overall performance efficiency for each configuration. The last column in Table 4 represents the obtained values of VBPM for all the normalized performance metrics. Overall, the system achieves its highest performance when N = 4, where the VBPM value is 6.0775, after which performance begins to degrade. This trend highlights that while increasing the number of cascaded levels improves security and system complexity up to a certain point, adding too many levels may introduce inefficiencies or diminish overall performance, as reflected by the declining VBPM beyond N = 4. Thus, the optimal number of cascaded levels for this system is N = 4, where performance efficiency peaks.

Table 4. Normalized security analysis of N-level cascaded coupled chaotic systems with VBPM.

Number of Levels (N)	SNR	PSNR	PRD	Correlation Coefficient (CC)	Encryption Time (te)	Decryption Time (td)	Logic Utilization	Maximum Frequency	VBPM
1	0	0.7246	0	1	0	0	0	0.8687	1.5748
2	0.1664	0.9668	0.0219	0.3043	0.0408	0.0395	0.0522	0.3125	3.6938
3	0.2794	1	0.0466	0.0870	0.1141	0.1299	0.1084	0.8	5.2676
4	0.3628	0.9824	0.0727	0	0.1332	0.1356	0.1647	1	6.0775
5	0.4352	0.8809	0.1028	0.0435	0.2120	0.2090	0.2209	0.4563	2.8723
6	0.4975	0.7676	0.1360	0.0870	0.2391	0.2566	0.2610	0.5562	2.3800
7	0.5533	0.6426	0.1729	0.1739	0.2663	0.2655	0.3173	0	1.3786
8	0.6028	0.5352	0.2123	0.3043	0.4022	0.3220	0.3655	-	0.9884
9	0.6028	0.5352	0.2583	0.4348	0.4022	0.3785	0.4257	-	0.8642
10	0.6507	0.4141	0.3150	0.5652	0.4293	0.4350	0.4739	-	0.7314
15	0.6964	0.2949	0.6390	0.6957	0.7283	0.7740	0.6827	-	0.5678
20	1	0	1	0.6087	1	1	1	-	0.5542

Figure 5 provides a graphical representation of VBPM for different values of N, illustrating the relationship between the number of cascaded levels and system performance. It is evident that as the number of levels (N) increases, the VBPM rises, reaching a peak at N = 4. However, further increasing the number of levels beyond 4 results in a gradual decline in VBPM.

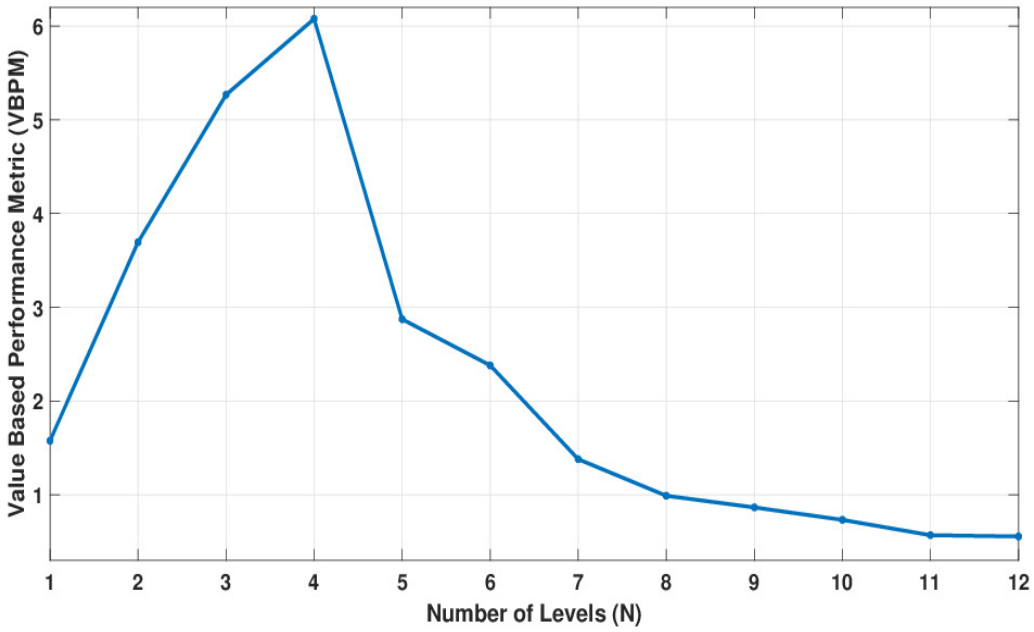


Figure 5. Value-Based Performance Metric (VBPM) for different values of N.

Comparison with Existing Work

While our proposed system shows significant improvements in terms of correlation coefficient and SNR, as seen in Table 4, it is essential to thoroughly examine how these results compare with existing work that used different chaotic systems to encrypt voice signals. For instance, the 4-level cascaded chaotic-based secure communication system using the unified hyperchaotic system achieves a correlation coefficient of 0.0004, which is lower than that of some other methods, listed in Table 5, indicating better correlation between the original and encrypted signals. Similarly, the SNR of −71.68 dB indicates stronger encryption, as it is much lower than the other systems, such as the Zaslavsky map (−56.87 dB) and the chaotic circle map (−16.05 dB). This lower SNR highlights the increased noise added to the signal using our proposed encryption system, making it more difficult for an unauthorized party to reconstruct the original signal.

Table 5. Comparison results with related work for voice encryption.

Author	Ref.	Chaotic Oscillators	Correlation Coefficient	SNR in dB
Alwahbani and Bashier 2013	[42]	circle map and logistic map	0.0017	−14.0065
Sheela et al., 2017	[43]	Henon map (2D-MHM) and standard map	−0.0037	-
Sathiyamurthi and Ramakrishnan 2017	[44]	logistic map, tent map, quadratic map, and Bernoulli's map	0.0119	-
Yousif 2019	[45]	Zaslavsky map	−0.00092	−56.8661
Kordov 2019	[46]	chaotic circle map and modified rotation equations	−0.0011166	−16.0483
Gebereselassie et al., 2022	[47]	Chen's hyperchaotic system	−0.0007	-
Proposed System		Unified hyperchaotic system	0.0004	−71.68

It could be concluded that the presented N-Levels cascaded system for voice encryption when (N = 4) overrides the other existing schemes since our proposed scheme offers the best encryption results, so it is difficult to hack the voice signal in the channel during

transmission. In terms of practical implications, our system's high performance in security metrics makes it suitable for real-time secure voice communication systems where the privacy is required. The high SNR, PSNR, and PRD values and low correlation values ensure that encrypted signals are highly resistant to attacks aimed at recovering the original signal. However, the added complexity, particularly with increasing levels (N), might require more computational resources, making the system potentially slower or more resource-intensive compared to simpler chaotic encryption methods.

However, one of the limitations of our approach is the increased encryption and decryption time as the number of levels grows, which can be a drawback in real-time applications. Additionally, for N > 7, the FPGA resources were exceeded, which limits the scalability on certain hardware platforms.

6. Conclusions

In this study, we explored N-level cascaded chaotic-based secure communication systems for voice encryption employing a 4D unified hyperchaotic system. This adaptable structure accommodates chaotic oscillators of varying dimensions, offering flexibility in implementation. Through numerical simulations in Matlab/Simulink, we applied this unified hyperchaotic oscillator to voice encryption and evaluated system performance across key metrics, including Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), Percent Residual Deviation (PRD), correlation coefficient, FPGA resource utilization, and clock frequency. A novel performance metric, Value-Based Performance Metrics (VBPM), was introduced to consolidate these parameters into a single value for easier comparison. Our findings show that while security improves with an increase in cascaded levels, the optimal performance was achieved at N = 4, with diminishing returns beyond this point. Compared to existing methods, our system performed favorably, particularly in terms of correlation coefficient and SNR, underscoring its potential for enhancing secure communications. The broader implications of this research are significant for secure communication systems, particularly in fields such as military, governmental, and financial voice encryption. By cascading chaotic oscillators, our system enhances security, making unauthorized decryption more difficult. However, the system's scalability is limited by increasing encryption/decryption time and FPGA resource consumption, especially beyond N = 7. This highlights the need for more advanced hardware or optimized designs for real-time applications. In the future, the integration of quantum encryption with chaos-based methods offers a promising avenue for further enhancing communication security [48]. Quantum encryption mechanisms, driven by breakthroughs in quantum teleportation and quantum computing, could be combined with chaos-based encryption to build advanced systems for securing multimedia files. This could represent the next evolution in secure communication systems, offering unprecedented levels of security. Further work could focus on optimizing the system for faster encryption and more efficient resource use, exploring alternative chaotic oscillators, and extending the approach to other types of data, such as image and video encryption.

Author Contributions: T.B. contributed to the conceptualization of the study, developed the methodology, supervised the research, managed the project, and participated in writing, reviewing, and editing the manuscript. W.A.N. was involved in the development of the methodology and played a significant role in writing the original draft of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This article does not contain any studies involving human or animal participants performed by any of the authors. Thus, ethical approval was not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author as they are part of ongoing research.

Conflicts of Interest: I declare that the authors have no competing interests or other interests that might be perceived to influence the results and/or discussion reported in this paper.

References

1. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
2. Rössler, O.E. Continuous chaos—Four prototype equations. *Ann. N. Y. Acad. Sci.* **1979**, *316*, 376–392. [CrossRef]
3. Rajagopal, K.; Jahanshahi, H.; Varan, M.; Bayır, I.; Pham, V.T.; Jafari, S.; Karthikeyan, A. A hyperchaotic memristor oscillator with fuzzy based chaos control and LQR based chaos synchronization. *AEU-Int. J. Electron. Commun.* **2018**, *94*, 55–68. [CrossRef]
4. Matsumoto, T.; Chua, L.; Komuro, M. The double scroll. *IEEE Trans. Circuits Syst.* **1985**, *32*, 797–818. [CrossRef]
5. Holmes, P. A nonlinear oscillator with a strange attractor. *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Sci.* **1979**, *292*, 419–448.
6. Hénon, M. A two-dimensional mapping with a strange attractor. In *The Theory of Chaotic Attractors*; Springer: Berlin/Heidelberg, Germany, 1976; pp. 94–102.
7. Sprott, J.C.; Sprott, J.C. *Chaos and Time-Series Analysis*; Oxford University Press: Oxford, UK, 2003; Volume 69. Available online: https://test-sprott.physics.wisc.edu/chaostsa/answers/SOLUTIONS.pdf (accessed on 25 July 2024).
8. Beyene, G.A.; Rahma, F.; Rajagopal, K.; Al-Hussein, A.B.A.; Boulaaras, S. Dynamical Analysis of a 3D Fractional-Order Chaotic System for High-Security Communication and its Electronic Circuit Implementation. *J. Nonlinear Math. Phys.* **2023**, *30*, 1375–1391. [CrossRef]
9. Fa-Qiang, W.; Chong-Xin, L. Hyperchaos evolved from the Liu chaotic system. *Chin. Phys.* **2006**, *15*, 963. [CrossRef]
10. Bonny, T.; Al Debsi, R.; Majzoub, S.; Elwakil, A.S. Hardware optimized fpga implementations of high-speed true random bit generators based on switching-type chaotic oscillators. *Circuits Syst. Signal Process.* **2019**, *38*, 1342–1359. [CrossRef]
11. Muthuswamy, B. Implementing memristor based chaotic circuits. *Int. J. Bifurc. Chaos* **2010**, *20*, 1335–1350. [CrossRef]
12. Sambas, A.; Miroslav, M.; Vaidyanathan, S.; Ovilla-Martínez, B.; Tlelo-Cuautle, E.; Abd El-Latif, A.A.; Abd-El-Atty, B.; Benkouider, K.; Bonny, T. A New Hyperjerk System with a Half Line Equilibrium: Multistability, Period Doubling Reversals, Antimonotonocity, Electronic Circuit, FPGA Design and an Application to Image Encryption. *IEEE Access* **2024**, *12*, 9177–9194. [CrossRef]
13. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef] [PubMed]
14. Pan, D.; Lin, Z.; Wu, J.; Zhang, H.; Sun, Z.; Ruan, D.; Yin, L.; Long, G.L. Experimental free-space quantum secure direct communication and its security analysis. *Photonics Res.* **2020**, *8*, 1522–1531. [CrossRef]
15. Zhang, J.; Rajendran, S.; Sun, Z.; Woods, R.; Hanzo, L. Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wirel. Commun.* **2019**, *26*, 92–98. [CrossRef]
16. Nakamura, Y.; Sekiguchi, A. The chaotic mobile robot. *IEEE Trans. Robot. Autom.* **2001**, *17*, 898–904. [CrossRef]
17. Li, C.H.; Song, Y.; Wang, F.Y.; Wang, Z.Q.; Li, Y.B. A chaotic coverage path planner for the mobile robot based on the Chebyshev map for special missions. *Front. Inf. Technol. Electron. Eng.* **2017**, *18*, 1305–1319. [CrossRef]
18. AlMutairi, F.; Bonny, T. New Image Encryption Algorithm Based on Switching-type Chaotic Oscillator. In Proceedings of the 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 19–21 November 2019; pp. 1–5.
19. Chen, G.; Zhou, J.; Liu, Z. Global synchronization of coupled delayed neural networks and applications to chaotic CNN models. *Int. J. Bifurc. Chaos* **2004**, *14*, 2229–2240. [CrossRef]
20. Bonny, T.; Nasir, Q. Clock glitch fault injection attack on an FPGA-based non-autonomous chaotic oscillator. *Nonlinear Dyn.* **2019**, *96*, 2087–2101. [CrossRef]
21. Manhil, M.M.; Jamal, R.K. A novel secure communication system using Duffing's chaotic model. *Multimed. Tools Appl.* **2024**, 1–14. [CrossRef]
22. Karawanich, K.; Chimnoy, J.; Khateb, F.; Marwan, M.; Prommee, P. Image cryptography communication using FPAA-based multi-scroll chaotic system. *Nonlinear Dyn.* **2024**, *112*, 4951–4976. [CrossRef]
23. Cuomo, K.M.; Oppenheim, A.V.; Strogatz, S.H. Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process.* **1993**, *40*, 626–633. [CrossRef]
24. Cuomo, K.M.; Oppenheim, A.V. Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.* **1993**, *71*, 65. [CrossRef] [PubMed]
25. Abd, M.H.; Tahir, F.R.; Al-Suhail, G.A.; Pham, V.T. An adaptive observer synchronization using chaotic time-delay system for secure communication. *Nonlinear Dyn.* **2017**, *90*, 2583–2598. [CrossRef]
26. Hussein, E.A.; Khashan, M.K.; Jawad, A.K. A high security and noise immunity of speech based on double chaotic masking. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 4270. [CrossRef]
27. Busawon, K.; Canyelles-Pericas, P.; Binns, R.; Elliot, I.; Ghassemlooy, Z. A brief survey and some discussions on chaos-based communication schemes. In Proceedings of the 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), Budapest, Hungary, 18–20 July 2018; pp. 1–5.
28. Short, K.M. Steps toward unmasking secure communications. *Int. J. Bifurc. Chaos* **1994**, *4*, 959–977. [CrossRef]
29. Yuan, F.; Bai, C.J.; Li, Y.X. Cascade discrete memristive maps for enhancing chaos. *Chin. Phys. B* **2021**, *30*, 120514. [CrossRef]
30. Yuan, F.; Li, Y.; Wang, G. A universal method of chaos cascade and its applications. *Chaos Interdiscip. J. Nonlinear Sci.* **2021**, *31*, 021102. [CrossRef]

31. Kharel, R. Design and Implementation of Secure Chaotic Communication Systems. Ph.D. Thesis, Northumbria University, Newcastle upon Tyne, UK, 2011.
32. Zhang, G.; Ding, W.; Li, L. Image encryption algorithm based on tent delay-sine cascade with logistic map. *Symmetry* **2020**, *12*, 355. [CrossRef]
33. Liu, Y.; Xie, Y.; Ye, Y.; Zhang, J.; Wang, S.; Liu, Y.; Pan, G.; Zhang, J. Exploiting Optical Chaos With Time-Delay Signature Suppression for Long-Distance Secure Communication. *IEEE Photonics J.* **2017**, *9*, 1–12. [CrossRef]
34. Pan, J.; Ding, Q.; Du, B. A new improved scheme of chaotic masking secure communication based on Lorenz system. *Int. J. Bifurc. Chaos* **2012**, *22*, 1250125. [CrossRef]
35. Zhou, Y.; Hua, Z.; Pun, C.M.; Chen, C.P. Cascade chaotic system with applications. *IEEE Trans. Cybern.* **2014**, *45*, 2001–2012. [CrossRef]
36. Waried, H.H. Synchronization of quantum cascade lasers with mutual optoelectronic coupling. *Chin. J. Phys.* **2018**, *56*, 1113–1120. [CrossRef]
37. Yu, Z.; Du, B.; Kong, D.; Chai, Z. A 4D conservative chaotic system: Dynamics and realization. *Phys. Scr.* **2024**, *99*, 085263. [CrossRef]
38. Wang, X.Y.; Zhao, G.B. Hyperchaos generated from the unified chaotic system and its control. *Int. J. Mod. Phys. B* **2010**, *24*, 4619–4637. [CrossRef]
39. Bonny, T.; Nassan, W.A.; Baba, A. Voice encryption using a unified hyper-chaotic system. *Multimed. Tools Appl.* **2022**, 1–19. [CrossRef]
40. Al Nassan, W.; Bonny, T.; Baba, A. A New Chaos-Based Cryptoystem for Voice Encryption. In Proceedings of the 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 25–26 November 2020; pp. 1–4.
41. Mohamed, M.A.; Bonny, T.; Sambas, A.; Vaidyanathan, S.; Nassan, W.A.; Zhang, S.; Obaideen, K.; Mamat, M.; Nawawi, M.; Kamal, M. A Speech Cryptosystem Using the New Chaotic System with a Capsule-Shaped Equilibrium Curve. *Comput. Mater. Contin.* **2023**, *75*. Available online: https://www.techscience.com/cmc/v75n3/52569 (accessed on 25 July 2024).
42. Bashier, E. Speech scrambling based on chaotic maps and one-time pad, Computing, Electrical and Electronics Engineering (ICCEEE). In Proceedings of the International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), Khartoum, Sudan, 26–28 August 2013; pp. 128–133.
43. Sheela, S.; Suresh, K.; Tandur, D. Chaos based speech encryption using modified Henon map. In Proceedings of the 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 22–24 February 2017; pp. 1–7.
44. Sathiyamurthi, P.; Ramakrishnan, S. Speech encryption using chaotic shift keying for secured speech communication. *EURASIP J. Audio Speech Music Process.* **2017**, *2017*, 1–11. [CrossRef]
45. Yousif, S.F. Speech Encryption Based on Zaslavsky Map. *J. Eng. Appl. Sci.* **2019**, *14*, 6392–6399. [CrossRef]
46. Kordov, K. A novel audio encryption algorithm with permutation-substitution architecture. *Electronics* **2019**, *8*, 530. [CrossRef]
47. Gebereselassie, S.A.; Roy, B.K. A new Secure Speech Communication Scheme Based on Hyperchaotic Masking and Modulation. *IFAC-PapersOnLine* **2022**, *55*, 914–919. [CrossRef]
48. Paul, B.; Trivedi, G. Post quantum cryptography algorithms: A review and applications. In Proceedings of the 7th ASRES International Conference on Intelligent Technologies, Jakarta, Indonesia, 16–18 December 2022; Springer: Singapore, 2022; pp. 3–17.