








# Secured Communication of Speech Signal Using the Discrete Cosine Transform Based on Hyperchaos-System

Noureddine Aissaoui<sup>1</sup><sup>a</sup>, Fethi Demim<sup>2</sup><sup>b</sup>, Abdenebi Rouigueb<sup>3</sup><sup>c</sup>, Hadjira Belaidi<sup>6</sup><sup>d</sup>,  
Ali Zakaria Messaoui<sup>4</sup><sup>e</sup>, Kahina Louadj<sup>5</sup><sup>f</sup>, Abdelkrim Nemra<sup>2</sup><sup>g</sup>, Ahmed Allam<sup>7</sup>, Yasmine Saidi<sup>7</sup>,  
Said Sadoudi<sup>1</sup> and Mohamed Salah Azzaz<sup>1</sup>

<sup>1</sup>Laboratoire Systèmes Electronique et Numériques, Ecole Militaire Polytechnique, Bordj El Bahri, Algiers, Algeria

<sup>2</sup>Laboratory of Guidance and Navigation, Ecole Militaire Polytechnique, Bordj El Bahri, Algiers, Algeria

<sup>3</sup>Laboratory of Artificial Intelligence and Virtual Reality, Ecole Militaire Polytechnique, Bordj El Bahri, Algiers, Algeria

<sup>4</sup>Complex Systems Control and Simulators Laboratory, Ecole Militaire Polytechnique, Bordj El Bahri, Algiers, Algeria

<sup>5</sup>Laboratoire d'Informatique, Mathématiques, et Physique pour l'Agriculture et les Forêts, Université de Bouira, Algérie

<sup>6</sup>Signals and Systems Laboratory, Institute of Electrical and Electronic Engineering,

University M'Hamed Bougara of Boumerdes, Algeria

<sup>7</sup>Ecole Nationale Polytechnique, Algiers, Algeria

**Keywords:** Chaos-Based Cryptography, Secure Chaotic Communication, Speech Signal, Discrete Cosine Transform, Encryption-Based Diffusion.


**Abstract:** This paper proposes a novel approach that combines chaos-based encryption and Discrete Cosine Transform (DCT) to ensure high-level speech security and robustness against attacks. In this approach, the encryption process is based on Lorenz's hyperchaotic system, which utilizes the One Time Pad approach to encrypt the speech DCT coefficients. The effectiveness of this approach has been validated through experiments on two PCs interconnected via real-time serial communication links (USB-RS232), which showed that the original speech is effectively hidden, and the proposed solution is highly resistant to possible attacks. Moreover, the proposed solution can be implemented in real-time applications using technologies such as FPGA.


## 1 INTRODUCTION


Speech-based communication has taken an important place in many fields, such as civil applications like trade, military defence, telephone banking and teleconferences, etc. This type of communication is in continuous evolution with the continuous investigation for better speeds, improved mobility and especially high confidentiality. The exchange of important confidential information via unsecured communication provides easy access to secret information


and facilitates the hacking process. Today's security devices are mainly based on encrypted systems that guarantee specific requirements. On one hand, the current encryption methods such as Rivest Shamir Adleman (RSA), Data Encryption Standard (DES) systems, and Rivest Cipher 4 (RC4) have already been defeated and are therefore no more secured. In this context, it is necessary to provide using other methods that are secure and have not yet been broken with the generation of microprocessors, such as Cipher 5 or the Advanced Encryption Standard (AES). Thus, chaotic cryptography is one of the alternatives created in the last ten years, particularly quantum cryptography, even though it cannot be opened due to its characteristics and obscures the data from its original form into difficult-to-understand data.


In 1990, L.M. Pecora et al. established the practical feasibility of synchronization between two identi-


<sup>a</sup> <https://orcid.org/0000-0002-5328-2414>


<sup>b</sup> <https://orcid.org/0000-0003-0687-0800>

<sup>c</sup> <https://orcid.org/0000-0001-5699-2721>

<sup>d</sup> <https://orcid.org/0000-0003-2424-626X>

<sup>e</sup> <https://orcid.org/0000-0001-5753-5776>

<sup>f</sup> <https://orcid.org/0000-0002-4203-6357>

<sup>g</sup> <https://orcid.org/0000-0001-9237-9449>

cal chaotic systems, thus proving the exploitation and efficient application of chaotic systems in communications (Pecora and Carroll, 1990). In 1993, K.M. Cuomo et al. proved that for some chaotic systems, Lorenz for example, the synchronization property, according to the technique of L.M. Pecora et al. is robust despite small perturbations in the coupling signal. This property allowed these researchers to propose the first scheme of a chaotic communication system based on the principle of Chaotic Addition Masking (Cuomo and Oppenheim, 1993).

In 2003, A.S. Dmitriev developed a new application base-chaos in communications called Direct Chaotic Communication (DCC) (Dmitriev et al., 2003). This new chaotic-based technology has opened a new field of application of chaos, namely ultra-wideband communications. In 1997, T. Yang et al. published the first work presenting the concept of chaotic encryption systems (Yang and Chua, 1997). In this context, they proposed to integrate cryptography into chaotic communication systems to improve the security degree of the latter. Chaotic pseudo-random sequences have desirable cryptographic properties, such as good randomness, deterministic dynamics, structure complexity, and sensitivity to initial conditions. Therefore, cryptanalysts have adopted several cryptographic standards based on chaos theory.

Subsequently, P.G. Vaidya et al. proposed chaotic cryptography with chaotic timing in 1998 (Vaidya and Ronge, 1998). The chaos-based digital cryptography system, based on pseudo-random number generators, does not depend on the chaos timing; it uses the initial conditions and control parameters as the secret key (Li et al., 2001). The one-dimensional logistic map is often used as a Pseudo-Random Number Generator (PRNG) in encryption, for example M.H.A. Samah et al. introduced a method where the logistic map is used to scatter the samples and the one-dimensional circular map is used to confuse the samples (Samah and Eihab, 2013). E. Mosa et al. (Mosa et al., 2009) presented cryptography in the transformation domain, based on the two-dimensional Baker map. The three-dimensional Lorenz map as a pseudo-random number generator is discussed by B.S. Sattar (Sadoudi and Azzaz, 2009).

In 2009, S. Sadoudi and M.S. Azzaz, developed a hardware implementation of the Rossler chaotic system to secure communication (Sadoudi and Azzaz, 2009) (Sattar and Rana, 2015), followed by a new auto-switched chaotic system and its Field Programmable Gate Array (FPGA) implementation is presented in (Azzaz et al., 2013b), as well as some work based on synchronized hybrid chaotic genera-

tors is proposed in (Azzaz et al., 2013a). In the same year, S. Sadoudi et al. developed a wireless hyperchaotic communication system for secure real-time image transmission (Sadoudi et al., 2013). Subsequently, in the same year, they proposed an FPGA real-time implementation of Chen's chaotic system to secure chaotic communications (Sadoudi et al., 2009). Several works are proposed founded on real-time FPGA implementation of Lorenz's chaotic generator, Duffing's chaotic attractor and experimental synchronization technique for chaotic communications (Azzaz et al., 2009), (Sadoudi et al., 2014) and (Sadoudi et al., 2015).

Currently, from 2020 to 2022, several researchers have been working on implementing FPGA-based real-time chaos secure encryption systems, as well as chaos-based video encryption algorithms (Azzaz et al., 2019)-(Hadjadj et al., 2022). Secure communication is crucial in the digital age, with data privacy and confidentiality being paramount concerns. One promising method for encrypting speech signals is the use of the Discrete Cosine Transform (DCT) based on hyperchaos-system. Hyperchaos-system employs hyper-chaotic systems, which are even more unpredictable than traditional chaotic systems, adding an extra layer of security to the encryption process (Zghair et al., 2021). Combining the DCT with hyperchaos-system allows efficient encryption of speech signals while ensuring accurate reconstruction at the receiver's end. This novel approach presents an effective solution for secure speech signal communication (Sathiyamurthi and Ramakrishnan, 2022).

In this paper (Abdallah and Meshoul, 2022), authors propose multilayer cryptosystems for audio communication encryption by continuously fusing audio signals with speech signals without silent periods. Three levels of encryption (fusion, substitution, and permutation) are considered, and the proposed approach shows increased security compared to one-dimensional logistic map-based encryption techniques.

Cryptography is a mathematical discipline allowing one to perform operations on an intelligible text to ensure some security properties of the information. This work aims to secure speech communication via an encryption system based on the chaotic PRNG technique using a transmission channel-based USB-RS232. Hybrid chaotic PRNG-based cryptography is secure and has powerful confusion and diffusion properties necessary for strong encryption. Each unit in the confusion and scattering area wants to block the derivation of the secret write key or the possible prevention of the original message. While scattering

increases the repetition of the clear text over the encrypted text key to make it obscure, confusion is used to make the invalid encrypted text. Only confusion can make stream encryption work; otherwise, stream encryption and block encryption require to scatter.

This paper is organized as follows: Section II describes hyper-chaotic systems and presents a hyper-chaotic system based-speech encryption using a Discrete Cosine Transformation. While, in Section III, the speech encryption process is proposed. Then, in Section IV, the simulations and experiment results are presented. At last, Section V concludes the paper and gives some future works.

## 2 HYPERCHAOTIC SYSTEM BASED-SPEECH ENCRYPTION

A dynamical system can generate hyperchaos if it has at least four state variables. It is modeled by at least four nonlinear differential equations. The mathematical model of a nonlinear dynamical system represents a four dimensional hyper chaotic system as follows:

$$\begin{cases} \frac{\partial x}{\partial t} = hy - ax + yz \\ \frac{\partial y}{\partial t} = hx - by - xz \\ \frac{\partial z}{\partial t} = -dz + xy + w^2 \\ \frac{\partial w}{\partial t} = xy + cw \end{cases} \quad (1)$$

where  $(x, y, z, w)$  are state variables and  $(a, b, c, d, h)$  represent system parameters. The initial states and the eventual control parameters show that this system is chaotic as:  $x(0) = 0.8, y(0) = 0.3, z(0) = 10.1, w(0) = 4.5, a = 5, b = -0.5, c = 2.2, d = 1, h \geq 4.85$ . The final state of a chaotic system is extremely sensitive to small changes in the initial state. With chaotic attractor, the phase diagram is the set of trajectories that are the solutions of the hyper-chaotic system as shown in Eq. (1), represented in the phase plane initiated from different initial conditions. A chaotic switching-rule allows the specified chaotic system to change its behaviour, while still producing complicated chaotic attractors. The properties of the chaotic system are so interesting for data encryption. Thus, we have developed an encryption system based on a hyper-chaotic function. The hyperchaotic system is used as a PRNG. Scattering of speech samples in this domain is performed only by Discrete Cosine Transformation (DCT) using PRNG, as shown in Figure 1. Before the transmission of the encrypted speech signal using DCT, it is converted into the time domain by the Inverse Discrete Cosine Transformation (IDCT). In the reception phase, we will apply the inverse operation of encryption to recover the original speech signal. It

is useful to note that the generation of the key stream encryption is done by the same initial values, as well as the same control parameters.

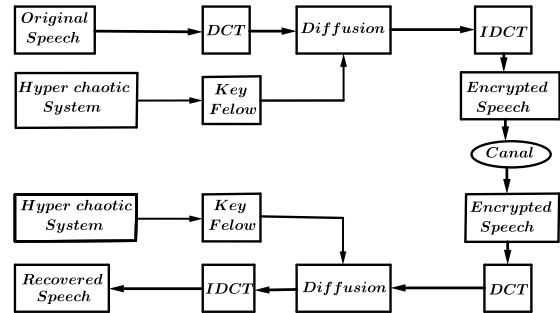


Figure 1: Encryption process flowchart.

Nowadays, telecommunication technologies are involved everywhere. The large-scale use of modern speech communication technologies via the Internet or mobile telephony requires securing information exchanges. The concept of security involves performing transformations on the original speech signal to mask it, making it unintelligible to unauthorized users, while ensuring the possibility of reconstituting it for authorized users. To meet these requirements, several methods of processing the speech signal have been proposed in the literature.

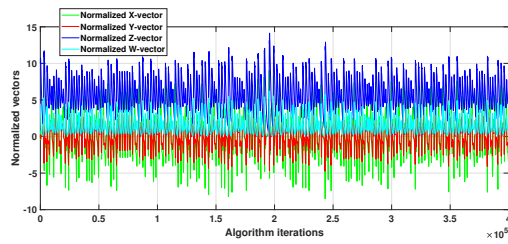
In the case of key management for streaming encryption, it has been generated using a four-dimensional hyper-chaotic system as seen in Figure 2 which represents the simulation results. This figure shows the change of variables over time, all variables of the states whose starting point is the point mentioned in the initial conditions. These initial conditions and parameters of the system are the key functions, which are given as input to the hyper-chaotic system. At the output of the PRNG, the state variables are given random values, and the normalization operation of each key is presented as follows:

$$\bar{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (2)$$

where  $x_{min}$  is the minimum value of the generated key and  $x_{max}$  is the maximum value of the generated key stream encryption. The normalized key is converted to a 16-bit integer as follows:

$$\tilde{x}_i = (\text{round}(\bar{x}_i \times 10^{15})) \bmod 2^{16} \quad (3)$$

where  $i = \{1, 2, 3, \dots, N_s\}$  and  $N_s$  is the number of samples of the speech signal.


 Figure 2: Normalized key to different variables  $x, y, z$  and  $w$ .

### 3 SPEECH ENCRYPTION PROCESS

To perform this process, we have chosen an audio recording of 4.5 seconds with a sampling rate of 8000  $HZ$ . In the example illustrated in Figure 3 (a), the original speech signal is recorded and then converted to the **Wav** format using a time domain representation. By definition, the audiogram graphically represents the evolution of the capacity or intensity of a speech to see its temporal envelope. A Discrete Cosine Transform (DCT) describes a finite sequence of data points in terms of the sum of cosine functions varying in frequency. It is used in signal and image processing and especially in data compression. Indeed, it has an exceptional energy aggregation property, and the low-frequency coefficients carry the information. In this case, Figure 3 (b) shows the original speech signal in transformation mode (Azzaz et al., 2019). The chaotic signals in the process of masking the speech signal are based on the streaming process. At the output of the PRNG, the keys stream encryption has given random values, followed by a normalization operation for each key; after this operation, each normalized key will be converted into a 16-bit coded integer and the encryption operation is performed by the XOR operator between the key stream encryption and the transformed speech scrambles to completely encrypt the speech signal. However, before this operation, the transformed speech scrambles are converted into equivalent decimal values using 16-bit quantization. The samples are processed in a fixed-size block, where the block size depends on the random key size (Sadoudi et al., 2015) (Kaibou et al., 2021). The following process presents the diffusion using the XOR function between each number of samples of the intercepted speech signal and the key converted to a 16-bit integer, as follows:

$$\tilde{e}_i = \tilde{m}_i \oplus \tilde{x}_i \quad (4)$$

where  $\tilde{x}_i$  presents the key converted to a 16-bit integer,  $\tilde{m}_i$  defines the samples of the original speech, and  $\tilde{e}_i$  presents the encrypted samples. If the correlation

Table 1: Correlation coefficient and SNR results.

Key	Correlation $r_{m,e}$	SNR (dB)
x(t)	0.000003713	-263.9514
y(t)	0.0003711	-263.9649
z(t)	-0.002972	-263.9557
w(t)	0.003713	-263.9682

coefficient is zero, the original and encrypted signals are different. The smaller the values of the correlation coefficient, the better the cryptographic process. It can be calculated as follows:

$$r_{m,e} = \frac{cov(m,e)}{\sigma_m \sigma_e} \quad (5)$$

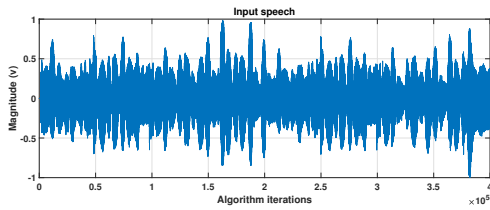
where  $cov(m,e)$  is the covariance between the original signal  $m$  and the encrypted signal and  $\sigma_m, \sigma_e$  are the standard deviations of the signal  $m$  and signal  $e$ .

The determination of the key is based on the best performance in terms of the correlation coefficient. The analysis of the correlation coefficient measures the quality of the encryption system. By analysis, if the correlation coefficient is equal to zero, the original signal and the encrypted signal are considered to be completely different. When the Signal-to-Noise Ratio (SNR) is a negative value in dB, it means that the signal intensity is lower than the noise intensity, making the encrypted data not detectable, and the key represents a good correlation (Hadjadj et al., 2022). In this case, we compute the noise between the original speech signal and the encrypted speech signal as follows:

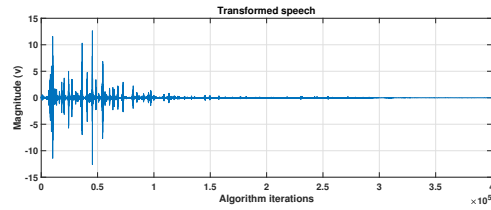
$$SNR = 10 \times \log_{10} \frac{\sum_{i=1}^{N_s} m_i^2}{\sum_{i=1}^{N_s} (m_i - e_i)^2} \quad (6)$$

### 4 SIMULATION RESULTS AND DISCUSSION

Several experimental analyses are performed to test the effectiveness of the speech-based cryptography technique. In this analysis, we will measure the quality of our cryptographic system through the analysis of the coefficient. The latter is given by the correlation between the similar segments in the original speech signal and the encrypted one. Table 1 shows different correlation coefficients for the different keys, and we notice that the key x(t) converges to zero, which indicates a good correlation. These results are close to each other, but we choose the key having the smallest negative value, which is x(t). Self-correlation is a mathematical method to analyze a periodic signal using the cross-correlation of a signal with itself (see



(a) Audiogram of the original speech.



(b) Original speech using a discrete cosine transformation.

Figure 3: Original speech and its DCT over time.

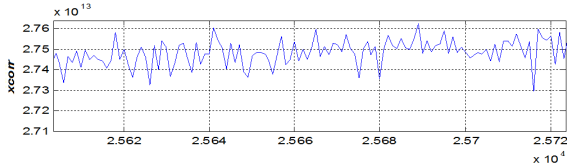


Figure 4: Self-correlation analysis of the key  $x(t)$ .

Figure 4). The proposed key flow gave better correlation values. After selecting the encryption key, the next step is to use this key in masking the speech signal using the diffusion process. An example of a temporal representation of an encrypted signal is shown in Figure 5, which is almost impossible to identify the transmitted speech signal. The obtained results from the simulation demonstrate the disappearance of the speech signal completely, which proves the success of the function of the encryption process. The advantages of chaotic masking based on diffusion are the simplicity of its realization and the possibility of using it to mask analogue or digital signals with high SNR channels. As far as the security analysis of the speech signal is considered, we will test the efficiency and robustness of our cryptographic system for the encryption of a speech signal by analyzing the two signals presented in Figure 6. It is a measure of the similarity of the signal to itself over time. Typically, the correlation is maximal for a zero-time delay. The principle of correlation is to extract future predictive information from the predicted signal values. In this part, we tested the efficiency and robustness of our adopted encryption system. From Figure 7, we can notice that the autocorrelation of the encrypted signal is like white noise converging to zero. Therefore, predicting the signal from its predicted state is not possible. Figure 8 illustrates the diffusion of information in the crypto-system. The histogram is a statistical study tool that is used to illustrate the efficiency of the diffusion of information in the encrypted data brought by the used cryptosystem. As for the original signal history, it is presented in the form of a stripe, as well as with a uniformly presented encrypted signal. In the case of the spectrogram analysis signal, the analysis of the time-frequency distribution of the original speech signals is shown in Figure 9, along with an en-

Table 2: Perceptual evaluation of speech quality based technique.

Original speech	Encrypted speech	Decrypted speech
4.176	1.260	3.952

rypted signal that has a uniform frequency behavior over time. In the encryption process, the encrypted signal in the transformation domain is converted into the time domain by the IDCT and in the decryption process step, the speech signal is recovered at the receiver. The latter must generate the same key stream encryption with the same initial values and control parameters to restore the original speech signal. The received signal is transformed into a frequency representation using DCT. As for the diffusion operation, it is performed between the samples of the encrypted signal and its counterpart of the encryption key. These encrypted samples are converted to equivalent 16-bit decimal values. Note that the key is a 16-bit encoded integer, and the XOR operation between the encrypted samples and the encryption key yields the original signal in its frequency representation, as shown in Figure 10 (a). To recover the original signal, a transformation from the frequency to the time domains is necessary using the inverse DCT, as shown in Figure 10 (b).

In the decryption process step, the signal recovery at the receiving end is still with a scattering operation, but this time it is performed between the encrypted signal samples and its counterpart of the encryption key. These encrypted samples are converted into equivalent 16-bit decimal values.

Figure 11 is the recovered speech signal in the time domain. According to this example, the reconstructed speech signal corresponds well to the original transmitted original signal. We can see that the original speech signal has been recovered successfully in terms of audio quality with its appropriate characteristics, as seen in Figure 3. Table 2 presents the Perceptual Evaluation of Speech Quality (PESQ) based evaluation technique. The results for the PESQ are almost similar to the original speech, which shows the perfor-

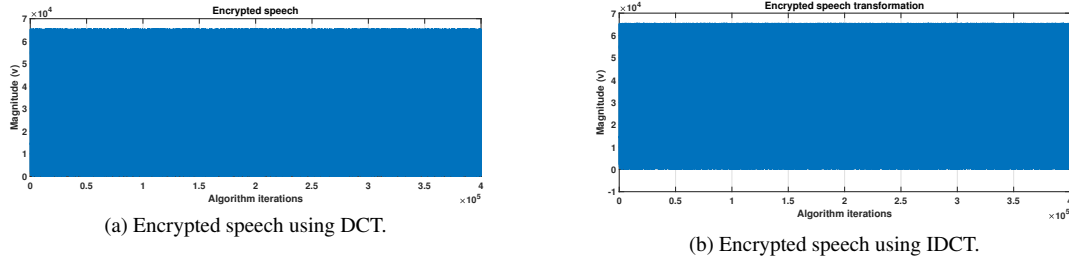


Figure 5: Encrypted speech presentation using transformation process.

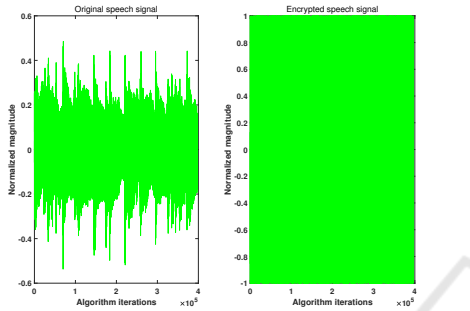


Figure 6: Speech encryption normalization.

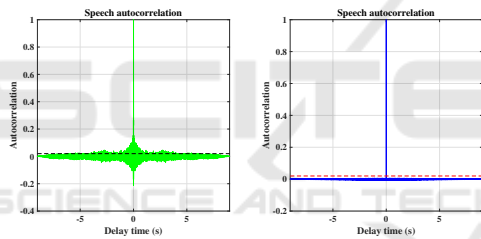


Figure 7: Presentation of speech signal autocorrelation.

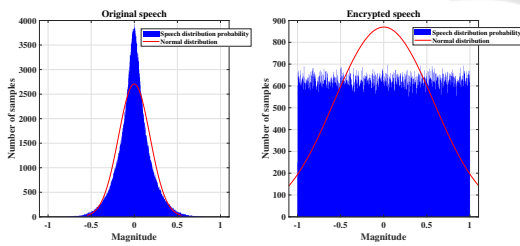


Figure 8: Histogram analysis.

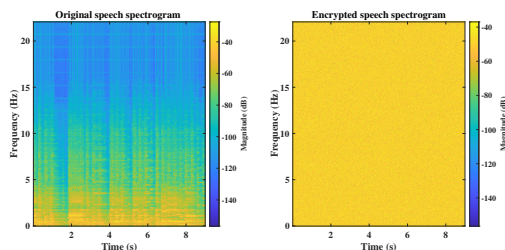


Figure 9: Spectrogram analysis presentation.

mance of our proposition. We used the PESQ method for evaluation in our simulation. Based on PESQ analysis, the results shown in Table 2 depict the rate of loss of the frames. The PESQ scale ( $PESQ > 3$ ), which offers good speech quality and high accuracy, preserves the intelligibility of the signal. The PESQ score obtained between the original and the encrypted speech is lower than the value of 2, which is considered satisfactory.

As for the realization of secure speech communication, speech encryption is done directly in real-time using a USB-RS232 serial communication converter. Figure 12 illustrates this implementation via this transmission channel. In this part, an encryption device is used to transmit speech via two PCs via a graphical interface which is considered as a transmission device for recording and processing the speech signal which will be intercepted by a decryption device with a reverse operation, as shown in Figure 13. In the emission process, we used an HP-PC with Pentium (R) Dual-core CPU T4500 @ 2.30 GHz, 2.00 GB RAM and 64-bit operating system with windows10, while in the reception process, we used a DELL-PC with Pentium (R) Dual-core CPU T4500 @ 2.30 GHz, 2.00 GB RAM and 32-bit operating system with windows7.

## 5 CONCLUSIONS

This study advances secure communication through hyper-chaotic systems, leveraging chaotic behavior for effective speech signal encryption using logistic and sinusoidal maps. Validation via stringent transmission tests on encrypted speech using RS232 protocol between two PCs demonstrates strong encryption efficiency, signal-to-noise ratio, and bit error rate performance, confirming the method's robustness in securing speech communication.

Our work's utilization of hyper-chaotic systems and its successful implementation of real-time encryption signify a compelling step towards enhancing speech communication security. The integration

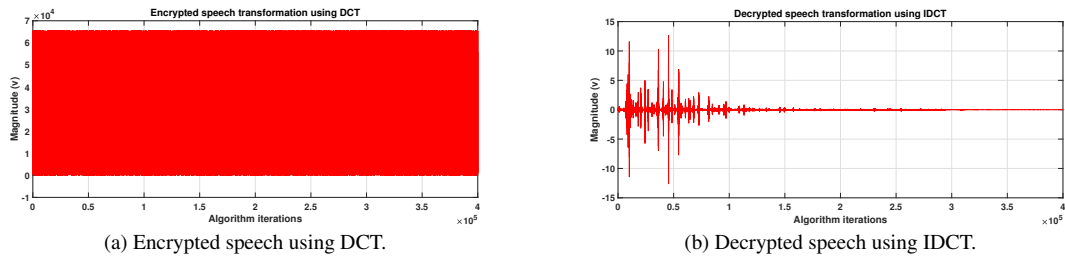


Figure 10: Encrypted and Decrypted speech presentation using transformation process.

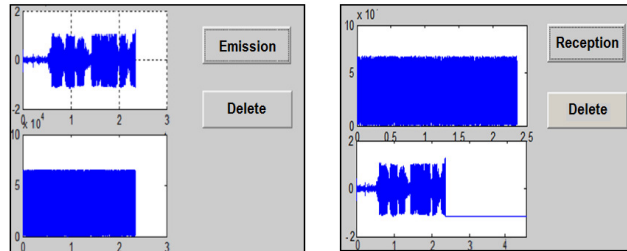


Figure 13: Graphical interface for transmission and reception of encrypted speech.

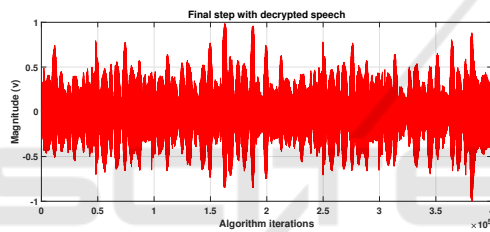


Figure 11: Final step with the decrypted speech signal.

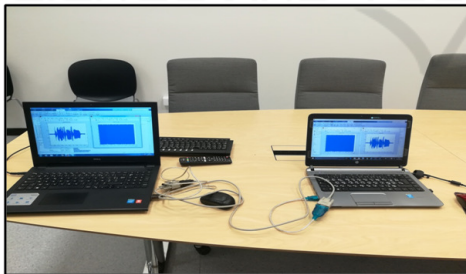


Figure 12: Experimental validation of the proposed approach of secured speech.

of chaotic systems in this context paves the way for further advancements and applications in secure communication methods. This research opens up exciting possibilities for developing novel and practical solutions to safeguard communication in various domains.

In addition, future work could extend the proposed approach beyond speech signals to other types of signals, such as images and videos. Adapting the algorithm for different signal types would allow for addressing security concerns in various domains and applications.

Moreover, implementing the algorithm on different hardware platforms, such as FPGAs and microcontrollers, will be a key focus to achieve real-time performance and ensure portability for practical deployments. This will allow the method to be integrated into various systems and devices, enhancing its usability in real-world scenarios.

Additionally, exploring the design space of hyperchaotic systems is planned to further optimize the proposed algorithm. Evaluating its performance in terms of security and computational complexity under various conditions will help in understanding its strengths and limitations. This evaluation will be crucial in assessing the potential advantages of the method compared to existing solutions.

To facilitate a comprehensive evaluation, performance metrics and execution times will be provided. These measurements will enable researchers and practitioners to assess the efficiency and effectiveness of the proposed method for various applications and scenarios. Making informed decisions about the best implementation approach will be essential for successful deployment. Investigating error correction codes and compression techniques will enhance the system's robustness and signal integrity during transmission and storage.

## REFERENCES

Abdallah, H. and Meshoul, S. (2022). A multilayered audio signal encryption approach for secure voice communication. pages 1–18.

- Azzaz, M., Tanougast, C., and Benssalah, A. (2019). An efficient and lightweight multi-scroll chaos-based hardware solution for protecting fingerprint biometric templates. pages 1–13.
- Azzaz, M., Tanougast, C., Sadoudi, S., and Bouridane, A. (2013a). Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption. pages 2035–2047.
- Azzaz, M., Tanougast, C., Sadoudi, S., and Dandache, A. (2009). Real-time fpga implementation of lorenz's chaotic generator for ciphering telecommunications. In *Proceedings of Joint IEEE North-East Workshop on Circuits and Systems and TAISA Conference*, pages 1–4.
- Azzaz, M., Tanougast, C., Sadoudi, S., Fella, R., and Dandache, A. (2013b). A new auto-switched chaotic system and its fpga implementation. pages 1792–1804.
- Cuomo, K. and Oppenheim, A. (1993). Circuit implementation of synchronized chaos with applications to communications. In *Physical Review Letters*.
- Dmitriev, A., Kyarginsky, B., Panas, A., and Starkov, S. (2003). Experiments on direct chaotic communications in microwave band. pages 1495–1507.
- Hadjadj, M., Sadoudi, S., Azzaz, M., Bendecheche, H., and Kaibou, R. (2022). A new hardware architecture of lightweight and efficient real-time video chaos-based encryption algorithm. pages 1–14.
- Kaibou, R., Azzaz, M., Benssalah, M., Tegui, D., Hamil, H., Merah, A., and Akrou, M. (2021). Real-time fpga implementation of a secure chaos-based digital crypto-watermarking system in the dwt domain using co-design approach.
- Li, S., Mou, X., and Cai, Y. (2001). *Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-Cipher Cryptography*. Lecture Notes in Computer Science book series, London.
- Mosa, E., Messiha, N., and Zahran, O. (2009). Chaotic encryption of speech signals in transform domains. In *Proceedings of IEEE International Conference on Computer Engineering and Systems, Cairo, Egypt*.
- Pecora, L. and Carroll, T. (1990). Synchronization in chaotic systems. In *Physical Review Letters*.
- Sadoudi, S. and Azzaz, M. (2009). Hardware implementation of the rossler chaotic system for securing chaotic communication. In *Proceedings of 5th International Conference of Sciences of Electronic, Technologies of Information and Telecommunications*.
- Sadoudi, S., Azzaz, M., Djeddou, M., and Benssalah, M. (2009). An fpga real-time implementation of the chen's chaotic system for securing chaotic communications. pages 467–474.
- Sadoudi, S., Azzaz, M., and Tanougast, C. (2014). Novel experimental synchronization technique for embedded chaotic communications. In *Proceedings of IEEE International Conference on Control, Decision and Information Technologies*, pages 669–672.
- Sadoudi, S., Tanougast, C., and Azzaz, M. (2015). Journal of engineering science and technology review.
- Sadoudi, S., Tanougast, C., Azzaz, M., and Dandache, A. (2013). Design and fpga implementation of a wireless hyperchaotic communication system for secure real-time image transmission. pages 1–18.
- Samah, M. and Eihab, B. (2013). Speech scrambling based on chaotic maps and one time pad. In *Proceedings of IEEE International Conference on Computing Electrical and Electronics Engineering, Khartoum, Sudan*.
- Sathiyamurthi, P. and Ramakrishnan, S. (2022). Speech encryption using hybrid-hyper chaotic system and binary masking technique. pages 6331–6349.
- Sattar, B. and Rana, S. (2015). A proposed voice encryption based on random lorenz map with dct permutation. page 90.
- Vaidya, P. and Ronge, H. (1998). Implementation of chaotic cryptography with chaotic synchronization. In *Physical Review Letters*.
- Yang, T. and Chua, L. (1997). Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication.
- Zghair, H. K., Mehdi, S., and Sadkhan, S. (2021). Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system. pages 1–14.