JTE HCM-UTE
ISSN: 2615-9740

JOURNAL OF TECHNICAL EDUCATION SCIENCE
Ho Chi Minh City University of Technology and Engineering
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

Reproducible Audio Chaotic Masking With a Chua-Type Oscillator and Key-Sensitivity Analysis

Thi Tuoi Phan[1], Vu Thang Nguyen[2], Anh Tuan Phan[3], Duc Hung Pham[1*]
[1]*Hung Yen University of Technology and Education, Vietnam*
[2]*Dai Nam University, Vietnam*
[3]*Control Automation in Production and Improvement of Technology Institute (CAPITI), Vietnam*

[*]Corresponding author. *Email: duchung.pham@mail.utehy.edu.vn*

ARTICLE INFO

Received: 25/02/2026
Revised: 08/04/2026
Accepted: 21/04/2026
Online First: 12/05/2026
Published:

KEYWORDS

Chaotic masking;
Audio encryption;
Chua-type oscillator;
Key sensitivity;
Numerical integration (ode45).

ABSTRACT

This paper presents a reproducible software-based demonstration of audio chaotic masking using a Chua-type chaotic oscillator. A discrete chaotic keystream is generated by numerically integrating a nonlinear ordinary differential equation with the ode45 solver, using sample-aligned short-interval integration. The recorded audio signal is encrypted through linear additive masking with a scaled chaotic state sequence and recovered by subtracting an identically regenerated sequence using the same system parameters and initial conditions. The study emphasizes the sensitivity of decryption accuracy to key mismatch, where even slight perturbations of the initial condition lead to significant reconstruction degradation. Quantitative evaluation metrics including normalized RMSE, reconstruction SNR, and correlation coefficient are employed to assess masking effectiveness and recovery fidelity. The proposed implementation serves as a transparent and replicable educational baseline for chaos-based communication research, while also highlighting the inherent security limitations of simple additive chaotic masking schemes.

Doi: https://doi.org/10.54644/jte.2026.2108

1. Introduction

Chaos refers to long-term, non-repeating, and hard-to-predict behavior that can arise in deterministic systems. A key feature is extreme sensitivity to initial conditions, so even tiny differences at the start can lead to dramatically different outcomes over time [1]. In recent years, chaos-based secure communication has emerged as a new area of research in communications. It originated from studies of chaotic dynamical systems and began to find practical applications in electrical engineering, particularly in the early 1990s [2]. Cyber physical systems (CPSs) integrate control, communication, and computation to tightly connect physical processes with digital intelligence. As a result, they show strong promise in applications such as smart cities, smart grids, smart manufacturing, and intelligent transportation. [3]. Although such systems are intricate by design, their dependence on interconnected networks for data exchange expands the attack surface, making them more vulnerable to exploitation and high-impact security compromises [4]. In recent years, the study of chaos has emerged as a key component in various scientific investigations [5], [6]. Chaos-based communication systems have been adopted in various engineering domains, including chemical process dynamics, power transmission networks, and biological applications [5], [7], [8]. In the scientific literature, the development, regulation, and synchronization of chaos have been widely investigated [9]. Recently, autonomous chaotic oscillators have become a popular research topic because they can be used in many science and engineering applications, such as secure communication systems based on chaos [10], cryptography [11] or wide-band communication systems [12]. Chaotic circuits that use one or more operational amplifiers have become especially interesting due to their ease of implementation [13]. Chaotic wave forms are aperiodic during oscillation and inherently nonlinear. These characteristics make them attractive for communication applications, where they can enhance security by reducing the risk of interception and limiting unauthorized access to transmitted data [14]. Chaos-based masking schemes require accurate

synchronization at the receiver. In practice, however, two nominally identical chaotic oscillators can deviate due to nonidealities, noise, and parameter variations. As a result, extensive research has been carried out to develop synchronization techniques that compensate for these mismatches [15]. Recently, major advances have been made in secure communication based on chaotic synchronization. Self-synchronization between two or more chaotic nonlinear oscillators can be used to build encoding and decoding blocks. To implement this concept in practice, several encoder–decoder circuit designs have been suggested [8]. The chaotic masking of audio signals was simulated in a numerical simulation environment using the Lorenz, Rössler, Sprott, Chen and Arneodo chaotic oscillator models [16]. Recent studies on chaos-based secure communication have mainly focused on new hyperchaotic designs, synchronization mechanisms, and hardware-oriented audio or voice encryption implementations [10], [12], [17]. By comparison, relatively few works provide a transparent end-to-end software workflow with sufficient implementation detail for straightforward educational or laboratory replication. Therefore, the present study revisits a Chua-type oscillator not to claim novelty in the chaotic model itself, but to establish a reproducible and code-faithful baseline for audio chaotic masking and quantitative key-sensitivity analysis. Chaos-based communication and encryption techniques exploit the broadband, aperiodic, and parameter-sensitive nature of chaotic signals. In chaotic masking, a low-amplitude message is added to a chaotic carrier to form a transmitted signal; the message is recovered at the receiver by subtracting a synchronized or identically reproduced chaotic carrier. This paper documents a computational implementation of chaotic masking for audio acquired from a microphone. The main objective is not to propose a new cryptosystem, but to present a clean, code-faithful description, so that the demonstration can be reproduced and used as a baseline for more rigorous research. In this work, a software demonstration chaotic masking framework is developed to illustrate the practical implementation of chaos-based audio encryption. Unlike theoretical studies focusing on synchronization design or cryptographic enhancement, this study emphasizes reproducibility and code-faithful documentation. A Chua-type chaotic oscillator is implemented as an ordinary differential equation and numerically integrated using an ode45 (Dormand–Prince) solver with the conceptual circuit schematic in Figure 1. The generated chaotic state sequence is used as a broadband masking carrier for short-duration recorded audio. The complete encryption–decryption pipeline, including parameter configuration, numerical integration strategy, and key sensitivity verification, is explicitly structured to allow straightforward replication and educational use. This approach provides a clear baseline platform for further investigation of synchronization mechanisms, improved masking strategies, or enhanced security evaluation. Although the overall scheme is intentionally simple (additive chaotic masking), the implemented method offers several practical advantages as a reproducible baseline and an educational demonstration: Code-faithful reproducibility: every algorithmic step (parameter set, initial conditions, integration loop, and masking rule) is derived directly from the reference script, enabling straightforward replication and verification. Low implementation barrier: the pipeline relies on widely available functions (ode45, audio recorder, sound) and does not require specialized hardware or external libraries, making it accessible for classrooms and quick prototyping. End-to-end demonstrator: the manuscript documents the full chain from audio acquisition to encryption, decryption, waveform visualization, and listening tests, which reduces ambiguity for readers attempting to reproduce results. Explicit and interpretable secret key: the key is naturally defined by the Chua-type parameters and initial conditions; the paper shows that even a tiny perturbation of the initial state causes decryption failure, clearly illustrating chaos sensitivity. Deterministic keystream regeneration: by regenerating the same chaotic trajectory under identical settings, the receiver can cancel the chaotic carrier by simple subtraction, avoiding extra synchronization circuitry in this software-only baseline. Unlike modern cryptographic standards, naive chaotic masking can be vulnerable to a variety of attacks and should not be treated as secure for real-world deployment. To better position the contribution of this study, it should be emphasized that the manuscript does not propose a new cryptographic primitive or a new Chua-type chaotic model. Instead, its contribution lies in providing a transparent, reproducible, and code-faithful end-to-end software baseline for audio chaotic masking, in which the complete pipeline from chaotic keystream generation to decryption and key-mismatch evaluation can be directly replicated. This positioning is important because recent studies in chaos-based secure communication often focus on

hyperchaotic architectures, synchronization enhancement, or hardware-oriented realization, whereas fewer works offer a simple and fully reproducible implementation that can serve as an educational benchmark and a baseline reference for subsequent comparative studies.

2. Chaotic Signal Generator

2.1. Chua-type oscillator model

The provided code generates a chaotic sequence by integrating an ODE system implemented in the function chua. The parameter names and the piecewise-linear nonlinearity are consistent with the well-known reduced Chua oscillator form. A typical normalized Chua-type model is: The corresponding conceptual circuit schematic is shown in Figure 1.

$$\begin{aligned} \dot{x} &= \alpha(y - x - f(x)) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{1}$$

where $f(x)$ is a piecewise-linear function determined by slopes m_0 and m_1. In many Chua formulations, $f(x)$ is defined as a three-segment line:

$$f(x) = m_1 x + 0.5(m_0 - m_1)(|x+1| - |x-1|) \tag{2}$$

The numerical integration state vector is arranged as, and the chaotic carrier used for masking is the stored sequence. Because the internal details of chua are not shown, Eqs. (1) -(2) are given as a standard reference model.

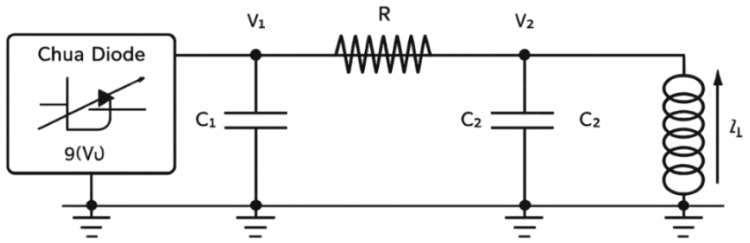

Figure 1. *Conceptual schematic of the normalized Chua circuit used as the chaotic signal generator.*

2.2. Parameter setting and initialization

The parameter setting and initialization of the Chua circuit in this work is shown in Table 1 as below.

Table 1. *Parameter setting and initialization.*

Symbol	Value	Role
α	15.6	Parameter passed into chao
β	28	Parameter passed into chao
m_0	-1.143	Nonlinearity slope parameter in chao
m_1	-0.714	Nonlinearity slope parameter in chao
L	24000	Sequence length; equals f_s × duration
Δt_{int}	$1/f_s \approx 4.167\times10^{-5}$ s	Integration interval aligned to audio sampling
k	10	Mask scaling factor in $y_{enc}(i)=y(i)+k\,x_2(i)$

Secret key (initial condition used to regenerate x_2):

The script integrates the ODE repeatedly for $i = 1 \ldots L$. This produces a discrete chaotic sequence of length L.

3. Numerical Integration Procedure

The code uses an ode45 solver to integrate the chaotic ODE. Since ode45 uses adaptive internal step sizes. This approach is simple and reproducible, but it is computationally heavier than integrating once and sampling, because ode45 is called L times. The end-to-end procedure is summarized in Figure 2.

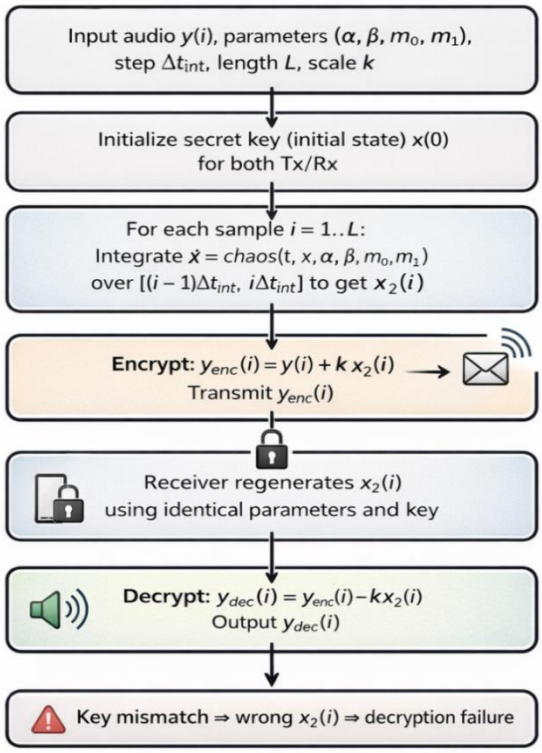

Figure 2. *End-to-end algorithmic flow of chaotic keystream generation and audio masking-based encryption/decryption.*

4. Audio Acquisition and Chaotic Masking

4.1. Audio recording settings

A single-channel audio signal is recorded from the microphone using 's audiorecorder with sampling rate f_s = 24 (kHz) and duration=1 (s). Therefore, the number of samples is N = f_s×duration=24000, which matches the keystream length L. The recorded samples are retrieved as a double-precision array $y(i)$.

4.2. Encryption and decryption rules

The encryption is performed by adding the message sample and a scaled chaotic sample. Let k be the scaling constant (Choose k = 10). This value was selected empirically as a compromise between masking effectiveness and amplitude control of the encrypted waveform. If k is chosen too small, the chaotic carrier is insufficient to adequately conceal the time-domain and time-frequency characteristics of the original audio, so salient structures of the plaintext signal may remain observable in the encrypted waveform or spectrogram. Conversely, excessively large values of k amplify the chaotic component beyond what is necessary for masking, thereby increasing the dynamic range of the encrypted signal and potentially causing clipping or playback distortion in practical audio handling.

Encryption:

$$y_{\text{enc}}(i) = y(i) + k x_2(i) \tag{3}$$

Decryption:

$$y_{\text{dec}}(i) = y_{\text{enc}}(i) - k\,x_2(i) \approx y(i) \tag{4}$$

In this work, the fixed choice k=10 is adopted to ensure a clear and reproducible demonstration of the masking–demasking process without introducing obvious clipping artifacts in the considered audio samples.

5. Key Sensitivity Demonstration

To illustrate sensitivity to initial conditions, the code repeats the keystream generation with two incorrect keys and decrypts using the mismatched sequence. In case applies a tiny perturbation to the secret initial condition, e.g., $\dot{x}_1(1) = \mathbf{0.100001}$ instead of 0.1, while keeping all other states unchanged. The recovered waveform is visibly distorted and audibly degraded because the chaotic carrier cannot be canceled.

6. Experimental Results

The reference script produces six subplots illustrating the full pipeline. For a conference manuscript, the plots can be summarized as follows:

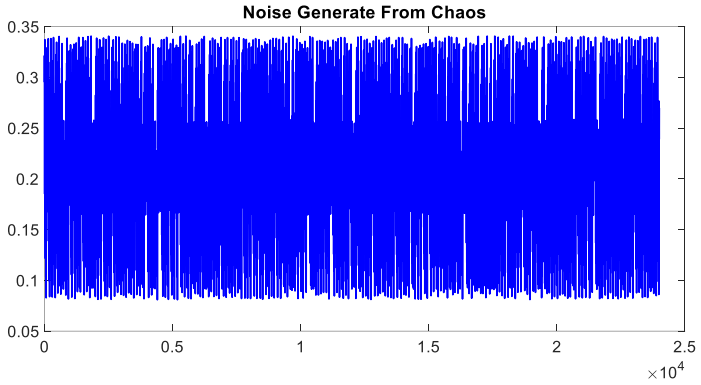

Figure 3. *Chaotic mask sequence used as noise-like carrier.*

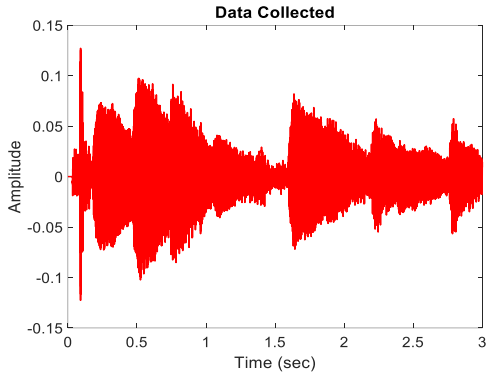

Figure 4. *Recorded audio waveform y(i).*

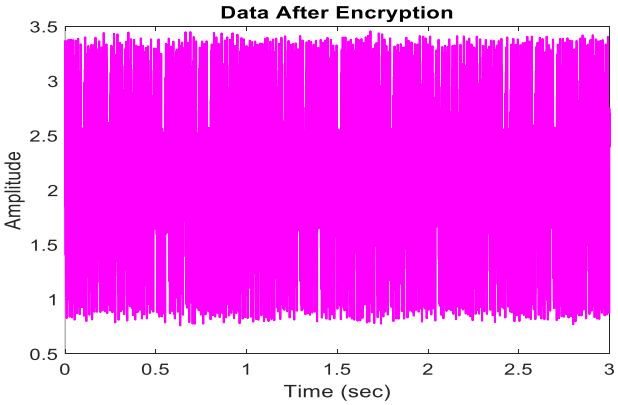

Figure 5. *Encrypted waveform* $y_{\text{enc}}(i) = y(i) + k\,x_2(i)$.

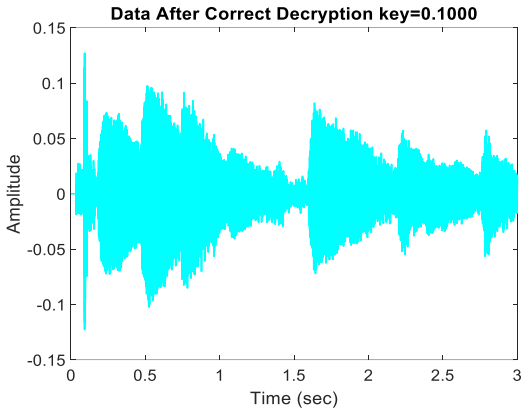

Figure 6. *Decrypted waveform using the correct key,* $y_{\text{dec}}(i) = y_{\text{enc}}(i) - k\,x_2(i) \approx y(i)$.

In addition to waveform plots, the script plays back the encrypted and decrypted audio using sound. Subjectively, the encrypted audio is noise-like, while correct decryption restores intelligibility. Incorrect keys fail to cancel the chaotic carrier and leave residual noise that dominates the recovered signal.

JTE
HCM-UTE
ISSN: 2615-9740

JOURNAL OF TECHNICAL EDUCATION SCIENCE
Ho Chi Minh City University of Technology and Engineering
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

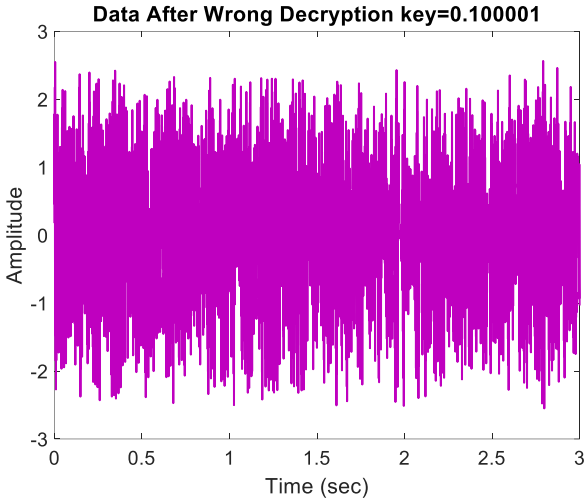

Figure 7. *Decrypted waveforms using incorrect keys (Case A).*

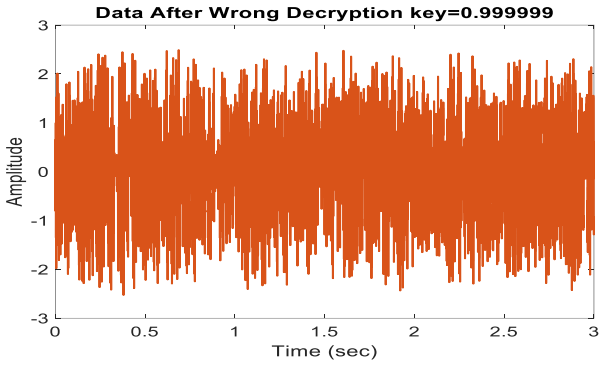

Figure 8. *Decrypted waveforms using incorrect keys (Case B).*

6.1. Waveform-level analysis

Figures 3–8 validate the end-to-end pipeline. The keystream $x_2(i)$ behaves as a noise-like carrier with bounded amplitude (Figure 3). The original recorded audio waveform $y(i)$ is shown in Figure 4. When the mask is added to the audio, the encrypted waveform $y_{enc}(i)$ becomes visibly perturbed and perceptually unintelligible (Figure 5). Using the correct key, the subtraction operation cancels the carrier and restores the waveform shape (Figure 6), Figure 7 presents decrypted waveforms using incorrect keys (Case A in Table 2) and finally Figure 8 presents the decrypted waveforms using incorrect keys (Case B in Table 2). Any residual error is primarily due to numerical mismatch in regenerated $x_2(i)$, which is minimized here by using identical parameters, identical solver settings, and per-sample integration over.

6.2. Spectral and statistical characteristics

Chaotic masking aims to make the transmitted waveform resemble broadband noise. In practice, this can be validated by (1) comparing the power spectral density of $y(i)$ and $y_{enc}(i)$ and (2) plotting short-time Fourier transform (STFT) spectrograms. A successful mask produces a flattened spectrum and obscures the speech formants/harmonics that are clearly visible in the plaintext spectrogram. After correct decryption, the recovered spectrogram should closely match that of $y(i)$, indicating cancellation of the chaotic carrier.

6.3. Quantitative reconstruction and obfuscation metrics

Beyond visual inspection, reproducible evaluation can be reported using objective metrics computed from the recorded audio y(i), the encrypted signal $y_{enc}(i)$, and the recovered signal $y_{dec}(i)$. Recommended measures include:

• Normalized RMSE:

$$\mathrm{NRMSE} = \frac{\|y_{\mathrm{dec}} - y\|_2}{\|y\|_2} \tag{5}$$

• Reconstruction SNR:

$$\mathrm{SNR}_{\mathrm{rec}} = \mathbf{10}\log_{\mathbf{10}}\left(\frac{\|y\|_2^2}{\|y_{\mathrm{dec}} - y\|_2^2}\right) \tag{6}$$

• Pearson correlation:

$$\rho = \mathrm{corr}\left(y_{\mathrm{dec}}, y\right) \tag{7}$$

Table 2. *Quantitative reconstruction metrics for correct and incorrect keys.*

Case	SNR_{rec} (dB)	NMSE	Pearson ρ
Correct key	305.7257	2.675657e-31	1.000000
Wrong key (Case A)	-37.0656	5.088205e+03	-0.001090
Wrong key (Case B)	-45.4773	3.529675e+04	-0.008803

Table 2 reports objective reconstruction metrics for the decrypted audio under the correct secret key and two mismatched-key scenarios (Case A and Case B). With the correct key, the regenerated chaotic carrier is numerically identical to the one used in encryption; therefore, subtraction cancels the mask almost perfectly. This is reflected by SNR_{rec} = 305.7257 dB, NMSE = 2.675657×10^{-31}, and Pearson $\rho = 1$, i.e., the recovered waveform is indistinguishable from the plaintext up to floating-point precision. When the key is incorrect, the chaotic trajectories diverge rapidly and the carrier cannot be canceled. In Case A (tiny perturbation of the initial condition), the reconstruction collapses with SNR_{rec} = -37.0656 dB, NMSE = 5.088205×10^{3}, and $\rho = 1$, indicating an error-dominated output with essentially zero linear similarity to the original audio. In Case B (a different mismatch), the degradation is even stronger: SNR_{rec} = -45.4773 dB, NMSE = 3.529675×10^{4}, and $\rho = 0.008803$. Compared with Case A, Case B increases the normalized error by about 6.9 times and lowers SNR_{rec} by 8.41 dB, consistent with the exponential sensitivity of chaotic dynamics to key mismatch. Overall, Table 2 confirms that correct decryption is strictly key-dependent: only an identical parameter/initial-condition set reproduces the keystream required for cancellation, whereas even slight deviations produce decorrelated, noise-like residuals.

For completeness, the reported NMSE is defined as $||y_{dec} - y||^2_2 / ||y||^2_2$, and NRMSE = sqrt (NMSE). Therefore, the extremely small NMSE in the correct-key case implies near-zero relative error, while the very large NMSE values in Case A and Case B indicate that the residual error energy dominates the recovered signal. Likewise, negative SNR_{rec} means the reconstruction error power exceeds the plaintext power, and rho near zero confirms practical decorrelation between y_{dec} and y.

6.4. Discussion and Limitations

A further limitation concerns synchronization realism. Because the study is implemented entirely in software, the transmitter and receiver do not evolve as two independently running physical Chua circuits; instead, the same chaotic trajectory is regenerated deterministically from the same numerical key. Consequently, the manuscript should not be interpreted as demonstrating robustness to hardware desynchronization. In an actual circuit realization, parameter spread, finite op-amp bandwidth, bias drift, quantization, and measurement noise would introduce mismatch and could prevent straightforward carrier cancellation. Addressing this issue would require an explicit synchronization layer, for example Pecora-Carroll synchronization, observer-based reconstruction, adaptive parameter estimation, or feedback-coupled synchronization, together with tolerance and noise analysis.

This study intentionally isolates a simple additive chaotic masking scheme in a fully software-based environment; therefore, its limitations should be stated explicitly. The framework is useful for demonstrating deterministic keystream regeneration and key sensitivity, but it does not provide the formal security guarantees expected from modern cryptographic systems. Because the message is masked by direct addition of a chaotic carrier, the scheme may remain vulnerable, in principle, to signal separation, parameter-estimation, or model-reconstruction attacks under stronger adversarial assumptions. In addition, the present experiments are conducted on short audio segments under ideal numerical conditions, without channel noise, quantization effects, or hardware mismatch. More specifically, the present implementation assumes ideal deterministic regeneration of the chaotic carrier under identical numerical conditions. In a practical hardware realization, two nominally identical Chua oscillators would inevitably diverge because of component tolerances, thermal drift, circuit noise, and parameter mismatch. Therefore, the software-only regeneration strategy adopted here should not be interpreted as a substitute for physical chaos synchronization. Real circuit implementations would require explicit synchronization or mismatch compensation mechanisms, such as observer-based,

adaptive, or Pecora–Carroll-type synchronization methods, which are outside the scope of this baseline study.

The evaluation scope is also limited. The manuscript verifies reconstruction quality and key-mismatch failure, but it does not benchmark against conventional ciphers, advanced chaos-based audio encryption schemes, or hardware-oriented synchronization designs. Likewise, the masking gain k is chosen empirically for the tested signal range, and the repeated ode45 integration favors reproducibility over computational efficiency. Future work should therefore examine larger audio datasets, spectrogram-level masking performance, robustness under practical impairments, faster numerical realization, and comparative evaluation against both standard cryptographic methods and contemporary chaos-based approaches.

Future work will therefore focus on a hardware-aware extension of the present baseline, including paired analog/digital Chua implementations, synchronization under component tolerances, robustness under channel noise and ADC/DAC quantization, and experimental comparison between deterministic regeneration and dynamic synchronization methods.

Accordingly, the contribution of this work should be understood as a reproducible implementation baseline and an educational benchmark, rather than as a fundamentally new secure cryptographic scheme.

7. Conclusion

This paper presents a reproducible end-to-end implementation of audio chaotic masking based on a Chua-type oscillator, including keystream generation, sample-aligned numerical integration, additive masking, deterministic regeneration, and objective evaluation. The results confirm strict key sensitivity: correct-key decryption yields near-perfect recovery, whereas slight initial-condition mismatch produces rapid divergence, large reconstruction error, and near-zero correlation. Although the additive masking structure is not intended as a secure replacement for modern cryptographic methods, the implementation provides a transparent baseline and a practical educational demonstration for future chaos-based communication studies.

For clarity, the reported decryption performance is limited to software regeneration under matched numerical settings and should not be interpreted as proof of synchronization robustness in physical hardware. The presented framework is intended as a reproducible benchmark from which future studies can incorporate explicit synchronization circuits or observer-based receivers for real-world implementation.

Conflict of Interest

The authors declare no conflict of interest.

REFERENCES

[1] N. Ali-Pacha, N. Hadj-Said, A. M'Hamed, and A. Belghoraf, "Lorenz's attractor applied to the stream cipher (Ali-Pacha generator)," *Chaos, Solitons & Fractals*, vol. 33, no. 5, pp. 1762–1766, 2007.
[2] A. Abel and W. Schwarz, "Chaos communications—principles, schemes and systems," *Proc. IEEE*, vol. 90, no. 5, pp. 691–710, 2002.
[3] D. Zhang, Q. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber-physical systems," *ISA Trans.*, vol. 116, pp. 1–16, 2021.
[4] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.
[5] S. Bendoukha, S. Abdelmalek, and A. Ouannas, "Secure communication systems based on the synchronization of chaotic systems," *in Mathematics Applied to Engineering, Modelling, and Social Issues, Springer*, pp. 281–311, 2019
[6] C. M. Lin, D. H. Pham, and T. T. Huynh, "Synchronization of Chaotic System Using a Brain-Imitated Neural Network Controller and Its Applications for Secure Communications," i*n IEEE Access*, vol. 9, pp. 75923-75944, 2021
[7] C. M. Lin, D. H. Pham, and T. T. Huynh, "Encryption and Decryption of Audio Signal and Image Secure Communications Using Chaotic System Synchronization Control by TSK Fuzzy Brain Emotional Learning Controllers," in *IEEE Transactions on Cybernetics*, vol. 52, no. 12, pp. 13684-13698, Dec. 2022
[8] T. Bonny and W. A. Nassan, "Highly-secured chaos-based communication system using cascaded masking technique and adaptive synchronization," *Multimedia Tools and Applications*, vol. 82, pp. 34229–34258, 2023, doi: 10.1007/s11042-023-14643-3.
[9] Q. D. Nguyen, V. N. Giap, D. H. Pham, and S. C. Huang, "Fast Speed Convergent Stability of T-S Fuzzy Sliding-Mode Control and Disturbance Observer for a Secure Communication of Chaos-Based System," in *IEEE Access*, vol. 10, pp. 95781-95790, 2022.
[10] D. H. Pham, T. T. Huynh, and C. M. Lin, "Secure transmission of medical image using a wavelet interval type-2 TSK fuzzy brain-imitated neural network," *Soft Computing*, vol. 29, pp. 2311–2329, 2025.
[11] K. Cho and T. Miyano, "Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 2, pp. 478–487, 2015, doi: 10.1109/TCSI.2014.2365767.

[12] X. Wu, K. Hu, S. He, H. Wang, and Z. Zhang, "A fractional-order Chua's system: System model, numerical simulations, hidden dynamics, DSP implementation and voice encryption application," *AEU - International Journal of Electronics and Communications*, vol. 192, art. no. 155691, 2025, doi: 10.1016/j.aeue.2025.155691.
[13] P. Ketthong, W. San-Um, B. Srisuchinwong, and M. Tachibana, "A simple current-reversible chaotic jerk circuit using inherent tanh(x) of an op-amp," *IEICE Electron. Express*, vol. 14, no. 17, pp. 1–7, 2017.
[14] S. N. Lagmiri, N. Elalami, and J. Elalami, "New Eight Dimensional Hyperchaotic Cryptosystem," *International Journal of Computer Applications*, vol. 7, no. 5, pp. 19–24, Sep.–Oct. 2017, doi: 10.26808/rs.ca.i7v5.03.
[15] M. Elkholy, H. M. El Hennawy, and A. Elkouny, "Real-time implementation of secure communication system based on synchronization of hyperchaotic systems," in *Proc. 33rd Nat. Radio Sci. Conf. (NRSC)*, Aswan, Egypt, 2016, doi: 10.1109/NRSC.2016.7450849.
[16] A. Almali and D. Ikici, "The simulation of sound signal masking with different chaotic oscillations and its circuit application," *Turk. J. Electr. Eng. Comput. Sci.*, vol. 24, pp. 4284–4293, 2016.
[17] Y. Cao and H. Liu, "An audio encryption algorithm based on a non-degenerate 2D integer domain hyper chaotic map over GF(2n)," *Multimedia Tools and Applications*, vol. 83, pp. 79377–79396, 2024.

Thi Tuoi Phan is the lecturer at the Faculty of Electronics and Electrical Engineering of Hung Yen University of Technology and Education, Vietnam.
Email: phantuoihy88@gmail.com. ORCID: https://orcid.org/0009-0004-0580-2878

Vu Thang Nguyen is the lecture at the Faculty of Electronics and Electrical Engineering of Dai Nam University, Vietnam.
Email: thangnv.utehy@gmail.com. ORCID: https://orcid.org/0009-0003-5338-0748

Anh Tuan Phan is with Control Automation in Production and Improvement of Technology Institute (CAPITI), 89 Ly Nam De, Hoan Kiem, Ha Noi,Vietnam.
Email: phananhtuan51@gmail.com. ORCID: https://orcid.org/0009-0008-1161-6819

Duc Hung Pham is with Faculty Electrical and Electronic, Hung Yen University of Technical and Education, Vietnam.
Email: duchung.pham@utehy.edu.vn. ORCID: https://orcid.org/0000-0003-3344-1593.