



A COMPREHENSIVE SURVEY OF AUDIO ENCRYPTION TECHNIQUES: CLASSICAL, CHAOS-BASED, DNA-INSPIRED, NEURAL, AND QUANTUM-ASSISTED APPROACHES

Halah Waad Khaled*¹, Waleed Abdullah Araheem² and Hakeem Imad Mhaibes³

^{1, 2, 3}Information Technology Department, Technical College of Management-Baghdad, Middle Technical University, Baghdad, Iraq.

²Information Technology Department, Technical College of Management-Baghdad, Middle Technical University, Baghdad, Iraq.

³Middle Technical University / Kut Technical Institute Cybersecurity Techniques Department, Baghdad, Iraq.

¹<https://orcid.org/0009-0003-3630-5017>^{ID}, ²<https://orcid.org/0000-0003-1598-8798>^{ID}, ³<https://orcid.org/0000-0002-4248-0220>^{ID}

Email: *DAC5005@mtu.edu.iq

ARTICLE INFO

Article History

Received: March 13, 2026

Reviewed: April 15, 2026

Accepted: July 15, 2026

Published: August 31, 2026

Keywords:

Audio Encryption Techniques: Classical, Chaos-Based, DNA-Inspired, Neural, and Quantum-Assisted Approaches

ABSTRACT

In this paper, a comparative review of various encryption techniques for audio data, which were introduced between 2015 and 2025, will be discussed to meet the requirements for secure audio data communication. Conventional encryption techniques, such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Substitution Permutation Networks (SPN), are considered to have high resistance to brute-force attacks, yet they may fail when dealing with a data type such as audio because they are deterministic networks. The survey also encompasses chaos-based encryption algorithms, such as multi-dimensional and hyper-chaotic maps, which utilize nonlinearity for improving confusion diffusion and extending the key space. Bio-inspired algorithms integrating the concept of Deoxyribonucleic Acid (DNA) coding techniques and chaotic maps are also described. Furthermore, the survey encompasses the use of Artificial Neural Networks (ANN) and the Neuro-Chaotic Cryptosystem (NeuroChaosCrypt) for encryption purposes because of its adaptive encryption mechanism. Finally, physical-layer techniques and quantum-assisted techniques, like Polarized Light Beam (PLB) Encryption and Quantum-Assisted Secure Audio Communication (QSAC), that provide security guarantees using the principles of physics and quantum computing, also deserve mention.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

I.1 BACKGROUND AND MOTIVATION

The growing use of digital communication technology has led to the increasing transmission of sensitive audio information over various platforms such as mobile communication systems, telemedicine setups, smart infrastructure, and military systems. This has greatly increased the demand for secure audio communication systems that can protect audio information from unauthorized access, modification, and cryptanalytic attacks. The initial work on secure audio communication systems was based on classical cryptographic algorithms. The Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Substitution-Permutation Networks (SPN) formed the basis for secure audio communication systems [1-4]. These deterministic mathematical algorithms provided acceptable performance and robustness against brute-force attacks. However, in the context of audio signals, which have strong temporal correlation properties, their rigid mathematical structure showed some limitations. The analysis of Rijndael in [4] shows its robustness against brute-force attacks but also suggests that statistical and differential cryptanalysis could still be a problem in audio-related scenarios.

I.2 EVOLUTION TOWARDS CHAOS-BASED SOLUTIONS

In order to meet the robustness requirements, some research works have examined the encryption speed in noisy channels and signal distortion. The model proposed in [5] presented a noise-resistant audio encryption model, and the bit-level chaos-based approach in [6] showed strong randomness and lossless audio encryption speed. With the increasing understanding of the deterministic structure limitations, research gradually evolved towards chaotic encryption models. Chaotic dynamic systems are known for their nonlinearity and high sensitivity to initial conditions, which are very useful in producing unpredictable key sequences and improving confusion diffusion. Multidimensional and hyper-chaotic systems, as presented in [7-9], showed increased key space, improved randomness quality, and increased resistance to correlation attacks and differential cryptanalysis.

I.3 DNA, NEURAL, AND HYBRID INTELLIGENT MODELS

In parallel with the design of chaos-based encryption schemes, DNA-based and bio-inspired cryptographic models have been proposed as viable alternatives for improving the security of audio encryption schemes. DNA coding-based models of audio signals utilize bio-inspired encoding schemes, where biological operations such as complementation and substitution are applied for improving the security of audio encryption schemes. The application of DNA coding-based models of chaotic maps, as proposed in [10-12] has been found to improve the security of audio encryption schemes. Recent research has proposed hyperchaotic maps for improving the security of audio encryption schemes. Hyperchaotic maps possess higher dimensionality and sensitivity than traditional chaotic maps, which can be exploited for improving the key space of audio encryption schemes. For example, [13] proposed a new hyperchaotic system with circuit implementation for improving the security of audio encryption schemes. More recently, research has focused on physical-layer and quantum-assisted cryptographic solutions. Optical cryptographic solutions, such as polarized light beam encryption [14], and quantum-assisted secure communication systems, such as QSAC [15] provide security assurances based on physical and quantum theories. These models provide intrusion detection and resistance capabilities beyond those of traditional algorithmic cryptography.

I.4 RESEARCH GAP AND CONTRIBUTION

The growing complexity of attack methods has also been mentioned in machine learning-based cryptanalysis research. As mentioned in [16], the current sophistication of attack methods calls for the development of encryption models that are robust against intelligent adaptive attack methods. Although there are various existing encryption models, current research is typically centered on a single method. Thus, there is a need for a comprehensive survey that compares classical, chaos-based, DNA-inspired, neural, and quantum-assisted audio encryption models in a single framework. Hence, this paper presents a comparative analysis of audio encryption models developed between 2015 and 2025, with a focus on their structural aspects, trade-offs, and research gaps.

I.5 ORGANIZATION OF THE PAPER

The rest of this paper is organized as follows. Section 2 provides a review of the current state of the art in survey research and the relevance of this paper to the current literature. Sections 3 to 7 introduce classical, chaos-based, DNA-inspired, neural, and optical/quantum-assisted audio encryption models. Section 8 introduces the comparative analysis framework. Finally, Sections 9 and 10 conclude the paper and provide future research directions.

II. RELATED WORK

II.1 EXISTING SURVEY PAPERS ON AUDIO ENCRYPTION

Recent studies on secure audio communication have increasingly addressed the limitations of early encryption approaches when applied to highly correlated audio signals. Initial research primarily employed classical cryptographic techniques, including the Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Substitution–Permutation Networks (SPN). Although these methods provided reliable security against brute-force attacks, several studies reported reduced effectiveness under audio-specific statistical and differential analyses. For example, the evaluation presented in [4] confirmed the robustness of AES against brute-force attacks while highlighting structural constraints when applied to audio data. To overcome these limitations, subsequent research shifted toward chaos-based encryption models characterized by strong nonlinearity and sensitivity to initial conditions. Such properties enable the generation of highly unpredictable key streams and improved confusion–diffusion performance. Multidimensional and hyper-chaotic systems, such as those explored in [7], significantly expanded key space and enhanced resistance to correlation and differential attacks. Noise-resilient chaotic schemes, as reported in [5], further demonstrated reliable decryption performance under noisy channel conditions, while comparative studies in [8] showed that three-dimensional chaotic systems outperform two-dimensional counterparts in terms of randomness and security. In parallel, hardware-oriented implementations, including [9], confirmed the feasibility of real-time chaotic audio encryption on embedded platforms. In addition, bio-inspired and DNA-based encryption techniques emerged as effective alternatives by encoding audio samples using nucleotide-based representations and applying biologically motivated operations to achieve deeper nonlinear transformations. Hybrid DNA–chaos models in [10] and multi-chaotic DNA frameworks in [11] reported higher entropy values and significantly reduced correlation. More advanced bio-inspired designs, such as the encryption–compression scheme in [12], further demonstrated the potential of biological encoding to simultaneously enhance security and data efficiency. Recent studies have also explored hyperchaotic frameworks for secure audio encryption. By [13] proposed a new hyperchaotic system with circuit design and demonstrated its applicability in audio encryption. More recently, physical-layer and quantum-assisted encryption techniques have expanded the scope of audio security.

Optical encryption using polarized light beams [14] exploits physical properties of light to achieve transformations that are extremely difficult to intercept, while Quantum-Assisted Secure Audio Communication (QSAC) systems [15] leverage quantum principles to enable intrusion detection through measurable disturbances. Finally, research on machine-learning-driven cryptanalysis, as discussed in [16], has highlighted the ability of modern learning-based techniques to expose vulnerabilities in both classical and chaotic encryption schemes. This emphasizes the necessity for designing audio encryption models that remain robust against intelligent, adaptive attack strategies. Despite the breadth of existing approaches, most prior studies focus on individual encryption paradigms in isolation. This limitation is addressed in the present work by providing a unified comparative framework, supported by the survey of existing studies summarized in Table 1 [17-24], covering advances in audio encryption from 2015 to 2025.

Table 1: Previous Surveys.

Ref ID	Study Title	Year	Datasets Used / Database	Domain Coverage	Algorithm Types	Experimental Validation	Metrics Used	Identified Research Gaps	Contribution in This Survey
[17]	Literature Survey on Recent Audio Encryption Techniques	2016	Not specified	Audio-only	No concrete algorithms (conceptual survey)	No	Time, Complexity	Outdated; no AI, DNA, hyper-chaos, hardware, or quantum	Extends review with chaos, DNA, neural, hybrid & quantum (2018–2025)
[18]	Review on Audio Encryption Algorithms Using Chaos Maps	2021	Not specified	Audio-only	Chaotic maps (Lorenz, Logistic, Tent, Chen)	Partially conceptual	NPCR, UACI, Entropy	No DNA, neural, hardware-chaos, or quantum approaches	Adds 3D/4D hyper-chaos, ANN-chaos, DNA-chaos, hardware chaotic systems
[19]	A Survey on Different Encryption Techniques for Image, Video, Audio & Documents	2021	Mixed multimedia	Multimedia	Classical + chaotic	Basic	PSNR, MSE, Entropy	Audio part weak; no AI, no neural or quantum audio	Provides deep audio-only extension including chaos, AI & hybrid models
[20]	Multimedia Security Using Encryption – A Survey	2023	Multimedia datasets	Multimedia	Classical & chaotic	Yes	PSNR, MSE, Entropy	Audio discussion shallow; no neural or quantum	Adds neural, DNA, hyper-chaos & quantum evaluation for audio
[21]	A Study on Current Scenario of Audio Encryption	2015	Not specified	Audio-only	Classical + basic chaos	Limited	MSE, SNR, Time	No hyper-chaos, no modern noise-tolerant methods	Adds hyper-chaos, DNA, neural, hardware implementations
[22]	Study of Chaotic-Based Audio Encryption Algorithms	2024	Not specified	Audio-only	Multiple chaotic models	Yes	Entropy, Correlation, NPCR	No ANN-chaos, DNA-chaos, optical, or quantum	Adds ANN-chaos, DNA-chaos, hyper-chaos and quantum comparisons
[23]	A Survey of Various Symmetric Encryption Methods	2025	Not specified	Classical cryptography	AES, DES, RC5, Twofish, Blowfish	Yes	Throughput, Time	No chaos, DNA, ML/DL or audio-specific security	Compares classical models vs chaos/DNA/neural in audio encryption
[24]	Hassan – IOP Conference Series (General Encryption Review)	2020	Not specified	General multimedia (includes audio conceptually)	Mixed encryption (conceptual only)	No	None	Very general; not audio-focused; lacks AI, chaos, DNA analysis	Provides historical/theoretical background and positions audio encryption evolution

Source: Authors, (2026).

II.2 LIMITATIONS OF EXISTING SURVEYS

The majority of existing surveys are centered on individual encryption paradigms and do not offer a comprehensive comparison of classical, chaotic, DNA-based, neural, and quantum-assisted encryption paradigms. Moreover, some existing surveys are more inclined toward descriptive discussion rather than analytical evaluation.

II.3 RESEARCH GAP AND POSITIONING OF THIS SURVEY

In order to fill the gaps, the current survey combines various encryption paradigms in a single framework of comparison and offers a comprehensive analysis of the research developments of the past decade, from 2015 to 2025.

III. FUNDAMENTALS OF AUDIO SIGNALS AND ENCRYPTION

III.1 DIGITAL AUDIO SIGNAL REPRESENTATION

In real-world audio encryption systems, audio signals are processed in the form of discrete digital samples, as opposed to continuous signals. Most encryption models are based on Pulse Code Modulation (PCM) audio files, like WAV files, where the audio signal is represented as a series of quantized amplitude levels, as in [3], [7]. A digital audio signal can thus be represented as:

$$A = \{a_1, a_2, \dots, a_n\}$$

Where each a_i represents a discrete sample value. The high temporal correlation between samples justifies the application of permutation and diffusion processes in audio encryption algorithms [7].

III.2 TIME-DOMAIN VS TRANSFORM-DOMAIN PROCESSING

Audio encryption can be performed either in the time domain or in the transform Domain. In Time-domain audio encryption, the algorithm operates directly on discrete audio samples through permutation and diffusion processes, as shown in [6], [7]. In contrast, transform-domain audio encryption involves mathematical transformations before encryption, as shown in [3] and multi-layer transform-based schemes in [25]. Time-domain encryption is more straightforward, while the latter focuses on decorrelation before encryption.

III.3 BASIC CRYPTOGRAPHIC PRINCIPLES

Audio encryption algorithms use basic cryptographic techniques, mainly the concepts of confusion and diffusion. Confusion aims at making the relationship between the key used for encryption and the resulting ciphertext as complex as possible. Diffusion aims at spreading the influence of each input sample over the whole encrypted signal. These techniques have generally been used in classical symmetric encryption schemes such as AES or other block cipher structures [1]. The size of the key space represents the number of possible keys that can be used for the encryption of data. A large key space makes it impossible for attackers to use brute-force techniques, thereby increasing the security of the encryption algorithm, as discussed in [4].

III.4 COMMON SECURITY EVALUATION METRICS

Audio encryption algorithms have been evaluated using various statistical and performance metrics for assessing their randomness, security strength, and reconstruction quality. The commonly reported metrics in the literature for audio encryption algorithms have been information entropy, correlation coefficient, SNR/PSNR, key sensitivity, and differential metrics like NPCR and UACI [6], [7], [10], [11].

III.4.1 Information Entropy

Information Entropy is used to determine the randomness of the encrypted signal. In an ideal encrypted audio signal, the information entropy should be close to the maximum value, indicating a uniform distribution of sample values. Information entropy is commonly used in chaos and DNA-based encryption algorithm assessments, as reported in [7], [10], [11]. The standard Shannon entropy is computed as:

$$H = - \sum_{i=0}^{L-1} p(s_i) \log_2 p(s_i)$$

Where:

- L : the number of possible signal values
- $p(s_i)$: the probability of occurrence of the value s_i

For an ideally encrypted audio signal, H should be close to its maximum value.

For an 8-bit audio signal, the maximum entropy is:

$$H_{\max} = \log_2(256) = 8$$

For a 16-bit audio signal, the theoretical maximum entropy is:

$$H_{\max} = \log_2(65536) = 16$$

III.4.2 Correlation Coefficient

The Correlation Coefficient is used to determine the statistical correlation between adjacent samples in the original and encrypted signals. An effective encryption algorithm will result in a correlation coefficient close to zero, as reported in [7], [11].

The Pearson correlation coefficient is computed as:

$$r_{xy} = \frac{\sum_{i=1}^N (x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^N (x_i - \mu_x)^2} \sqrt{\sum_{i=1}^N (y_i - \mu_y)^2}}$$

Where:

- N : the number of samples
- μ_x : the mean of sequence x
- μ_y : the mean of sequence y

III.4.3 Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR)

Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR) are utilized to assess the quality of reconstruction of the decrypted audio signal. The higher the SNR and PSNR, the higher the reconstruction quality of the decrypted audio signal and lower the distortion between the original and decrypted audio signal, as mentioned in [25], [26]. The peak signal-to-noise ratio (PSNR) is computed as:

$$\text{PSNR} = 20 \log_{10} \left(\frac{\text{MAX}}{\sqrt{\text{MSE}}} \right) \text{ dB}$$

Where:

- MAX: the maximum possible sample value

For example:

- for 8-bit audio, MAX = 255
- for 16-bit PCM audio, MAX = 32767

III.4.4 Key Sensitivity

Key sensitivity is a measure of how an encryption system responds to changes in the encryption key. A good audio encryption algorithm should respond differently when a small change is made in the encryption key, as noted in [7], [10]. A practical key sensitivity rate (KSR) can be computed as:

$$\text{KSR}(\%) = \frac{1}{N} \sum_{i=1}^N D_i \times 100$$

Where:

$$D_i = \begin{cases} 1, & C_1(i) \neq C_2(i) \\ 0, & C_1(i) = C_2(i) \end{cases}$$

and:

- C_1 : the encrypted signal generated using key K
- C_2 : the encrypted signal generated using a slightly modified key $K + \Delta K$
- N : the number of samples

A value close to 100% indicates high key sensitivity.

III.4.5 Differential Attack Metrics (NPCR, UACI)

Differential attack metrics such as the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) can be utilized to test the robustness of encryption schemes to differential attacks. Higher NPCR and UACI values mean that the encryption algorithm has strong resistance to differential attacks because small differences in the plaintext signal lead to large differences in the ciphertext output [10], [11]. The number of sample change rate (commonly written as NPCR in many papers) is computed as:

$$\text{NPCR}(\%) = \frac{\sum_{i=1}^N D_i}{N} \times 100$$

Where:

$$D_i = \begin{cases} 0, & C_1(i) = C_2(i) \\ 1, & C_1(i) \neq C_2(i) \end{cases}$$

and:

- C_1 : the ciphertext obtained from the original plaintext
- C_2 : the ciphertext obtained after introducing a slight change in the plaintext
- N : the number of samples

The unified average changing intensity (UACI) is computed as:

$$UACI(\%) = \frac{1}{N} \sum_{i=1}^N \frac{|C_1(i) - C_2(i)|}{L - 1} \times 100$$

Where:

- L : the number of possible intensity levels
- for 8-bit data, $L = 256$
- for 16-bit data, $L = 65536$

For audio signals, the term NSCR (Number of Sample Change Rate) may be more precise than NPCR, since the comparison is performed on samples rather than pixels.

IV. CLASSICAL AUDIO ENCRYPTION METHODS

Classical audio encryption methods are based on the concept of a deterministic framework such as a block cipher or substitution/permutation networks, which involve the transformation of the data using algorithmic processes [1], [4]. Classical methods focus on the importance of maintaining a structured key management system within a stable mathematical framework. The concept of hybrid and multi-layer systems has also been developed to accommodate classical cryptography in digital audio signal processing [2], [25]. The key characteristics of these classical methods are summarized in Table 2.

Table 2: Classical Audio Encryption Methods.

Ref ID	Study Title	Year	Datasets Used / Database	Domain Coverage	Algorithm Types	Experimental Validation	Metrics Used	Numerical Results (from source)	Identified Research Gaps	Contribution
[1]	Comparative Study Of AES, Blowfish, CAST-128 And DES	2016	Not specified	Audio / General	Classical (AES, Blowfish, CAST-128, DES)	Yes	Avalanche Effect, Integrity	Avalanche Effect (ECB): AES 52.34%, Blowfish 46.09%, CAST-128 49.21%, DES 53.12% Avalanche Effect (CBC): AES 45.31%, Blowfish 49.21%, CAST-128 37.50%, DES 56.25%	No audio-specific statistical analysis; no modern attacks	Provides baseline quantitative comparison of classical ciphers
[2]	The SPN Network for Digital Audio Data Based on ECC	2022	Digital audio signals	Audio	ECC + SPN	Yes	Security level, Time	Results inferred from figures; no explicit numerical tables reported	Not tested on noisy channels; no chaos/DNA comparison	Introduces lightweight ECC-SPN hybrid for audio data
[3]	Encryption of Audio Signals Using the Elzaki Transform	2023	WAV audio files	Audio	Elzaki Transform + Lorenz Chaos	Yes	MSE, SNR, Entropy	Entropy $\approx 7.9-8.0$; SNR and MSE inferred from graphical results (figures) reported in the source paper	Limited randomness analysis; no comparison with chaos-only/DNA	Uses transform-domain preprocessing to reduce audio correlation
[4]	Evaluation of Rijndael Algorithm for Audio Encryption by Brute Force Attack	2024	WAV audio samples	Audio	Classical (AES/Rijndael)	Yes	Key space, Time, Resistance	Key sizes: 128/192/256 bits, Brute-force complexity = 2^{256} (theoretical), successful resistance demonstrated	Only AES tested; no hybrid or adaptive schemes	Demonstrates AES robustness against brute-force in audio context
[25]	A Multilayered Audio Signal Encryption Approach for Secure Voice Communication	2023	Speech recordings	Voice / Audio	Multi-layer classical encryption	Yes	PSNR, Entropy, Time	PSNR > 30 dB, Entropy ≈ 7.9 , increased execution time due to multilayer design	High computational cost; no chaos/DNA integration	Provides multi-stage classical protection for voice communication
[26]	A Novel Digital Audio Encryption	2024	Digital audio samples	Audio / Forensics	Classical + Watermarking	Yes	PSNR, Robustness	PSNR $\approx 28-35$ dB (reported graphically); no	No chaos/quantum	Combines encryption with watermarking

	and Forensics Watermarking Scheme							explicit numerical tables provided	evaluation; added complexity	for security & authentication
[27]	A Digital Audio Data Protection Method Using Parametric Action of Generalised Triangle Group on $GF(2^8)$	2025	Audio datasets	Audio	Algebraic ($GF(2^8)$ group action)	Yes	Entropy, Time	Entropy > 7.9, fast execution reported for small datasets (no exact timing table)	Not compared to chaos/DNA; real-time optimization needed	Introduces strong algebraic structure with high key sensitivity
[28]	A New Encryption Algorithm for Voice Messages on Social Networks (Magic Cube Technology)	2025	Voice messages	Voice / Social Media	Magic Cube + $GF(2^8)$	Yes	Complexity, Security	Large key-space via 3D cube permutations, qualitative security improvement (no numeric tables)	Limited datasets; not tested vs AI-based attacks	Proposes creative 3D classical encryption for voice messaging

Source: Authors, (2026).

Interpretation

The principal classical paradigms use deterministic mathematical structures such as block-cipher frameworks, multilayer architectures, algebraic transformations, and SPN-based models for the encryption of audio. Clearly, the comparative evaluation presented in [1] considers AES, Blowfish, CAST-128, and DES into the foundational layer in traditional cryptography. These techniques have rather poor adaptability to the statistic nature of an audio signal. In contrast, subsequent works describe improvements in classical diffusion and performance enhancement, such as the elliptic-curve-based SPN framework in [2] and the lightweight Elzaki transform method in [3]. Indeed, another assessment of the Rijndael/AES in [4] reconfirms the resistance of the scheme to brute-force attacks but underlines some structural limitations. More recent classical developments, including multilayer encryption in [25], watermark-integrated protection in [26], algebraic encryption via $GF(2^8)$ group action in [27], and geometric permutation using Magic Cube transformations in [28], have shown diverse strategies for enhancing confusion, diffusion, and authenticity within classical models. All these works together have indicated that while classical encryption remains computationally efficient and easy to implement, the fixed structural nature of the process makes it harder to introduce true randomness and key-space expansion compared with chaotic or neural or quantum-assisted paradigms. The need for hybridization of classical cryptography with more dynamic models to meet emergent cryptanalytic and AI-driven security challenges is thus increasingly felt.

V. CHAOS-BASED AUDIO ENCRYPTION METHODS

Chaos-based audio encryption employs chaotic nonlinear dynamics and high sensitivity to initial conditions to produce random key streams. The chaotic behavior is used to improve confusion and diffusion of audio encryption. Due to their dynamic and non-periodic behavior, chaotic models are more appropriate for handling high correlation and dynamic variation of audio data than deterministic approaches [8], [22]. The key characteristics of these Chaos-based methods are summarized in Table 3.

Table 3: Chaotic Encryption Methods.

Ref ID	Study Title	Year	Datasets Used / Database	Domain Coverage	Algorithm Types	Experimental Validation	Metrics Used	Numerical Results	Identified Research Gap	Contribution
[5]	A Noise-Tolerant Audio Encryption Framework Designed by the Application of S8 and Chaotic System	2021	Noisy audio signals (real-time audio communication)	Audio	S8 symmetric group, Chebyshev map, TD-ERCS map, Circle chaotic map	Yes (software simulation)	Entropy, Correlation, SNR, Noise tolerance	Entropy ≈ 7.99 , Correlation ≈ 0 , successful decryption under channel noise, audible decrypted signal	Evaluation limited mainly to noisy channel conditions, with no validation on clean audio scenarios or hardware-based implementation.	Introduces a noise-tolerant chaos-based audio encryption framework that preserves correct decryption under channel distortions.
[6]	A Bit-Level Audio Encryption Algorithm Using a New Hybrid Chaotic Map	2024	Digital audio files	Audio	Hybrid chaotic map, bit-level permutation and substitution	Yes	Entropy, NPCR, UACI	Entropy ≈ 7.99 , NPCR > 99%, UACI $\approx 33\%$	High computational complexity and lack of real-time or hardware validation limit practical deployment.	Proposes a bit-level hybrid chaotic encryption scheme achieving strong confusion and diffusion properties.
[7]	A New Audio Encryption	2024	WAV audio files (various sizes)	Audio	Logistic map, Rössler	Yes (MATLAB implementation)	Entropy, Correlation	Entropy = 7.9918–7.9983, Correlation =	Encryption performance is sensitive to	Develops a hyper-chaotic audio encryption

	Algorithm Based on Hyper-Chaotic System				hyper-chaotic system	on)	NSCR, Encryption time	-0.0081 to 0.0167, NSCR = 99.60%–99.79%, Encryption time = 0.06–1.03 s	synchronization accuracy, and validation is restricted to software simulations.	algorithm with an expanded key space and strong resistance to statistical attacks.
[8]	Chaos-Based Audio Encryption: Efficacy of 2D and 3D Hyper-Chaotic Systems	2024	Digital audio signals	Audio	2D memristive hyper-chaotic map, 3D hyper-chaotic quadratic map	Yes	Entropy, Correlation, Differential analysis	Entropy $\approx$ 8, Correlation $\approx$ 0, 3D system shows higher randomness than 2D	Increased computational overhead and absence of real-time or hardware feasibility analysis.	Provides a comparative study demonstrating the superior randomness and security of 3D hyper-chaotic systems over 2D models.
[9]	Hardware Implementation of a 2D Chaotic Map-Based Audio Encryption System	2024	TIMIT-TTS dataset	Audio / Embedded Systems	2D Logistic-Fraction chaotic map, dynamic S-box, FPGA (Artix-7)	Yes (hardware implementation)	MSE, SNR, Correlation, Throughput, Power	MSE = 1.2156×10^3 , SNR = -26.23 dB, Correlation = 0.002948, Throughput = 2880 Mbps, Power = 0.13 W	Dependence on FPGA hardware limits scalability and portability to software-only platforms.	Demonstrates a real-time chaotic audio encryption system through efficient FPGA implementation.
[13]	Dynamics, Circuit Design, Feedback (Scientific Reports)	2023	Not specified	Audio / Hardware	Circuit-based chaotic system	Yes (circuit validation)	Entropy, Synchronization metrics	Entropy > 7.99, stable chaotic synchronization	The study mainly investigates chaotic circuit dynamics and synchronization stability, with limited direct evaluation on audio signal encryption metrics	Validates stable circuit-based chaotic systems suitable for secure communication applications.
[22]	Study of Chaotic-Based Audio Encryption Algorithms	2024	Multiple audio samples	Audio	Multiple chaotic encryption models	Yes	Entropy, Correlation, NPCR, UACI	Entropy $\approx$ 7.9–8.0, Correlation $\approx$ 0, NPCR > 99%, UACI $\approx$ 33%	Does not include comparisons with neural-chaos, DNA-based, or AI-assisted encryption approaches.	Offers a comprehensive comparative evaluation of multiple chaos-based audio encryption algorithms.
[29]	A Lossless Audio Encryption Method Based on Chebyshev Map	2023	Audio signals	Audio	1D Chebyshev chaotic map	Yes	Entropy, MSE, Key sensitivity	MSE = 0, Entropy $\approx$ 7.99, perfect reconstruction after decryption	Limited comparison with multi-dimensional chaotic systems.	Introduces a lossless chaotic audio encryption method ensuring perfect reconstruction of audio signals.

Source: Authors, (2026).

Interpretation

Chaos-based encryption techniques are some of the most sophisticated methods for the protection of audio signals, due to their nonlinear behavior and extreme sensitivity to initial conditions; these properties allow for the generation of key streams that are highly unpredictable. Noise-tolerant chaotic models, such as that proposed in [5], proved to be highly reliable since correct decryption performance was preserved even under distorted channel conditions. Multidimensional chaotic systems, such as those presented in [7] and [8], achieved remarkable enhancements with regard to the expansion of key space and confusion–diffusion properties, increasing robustness against correlation and differential attacks. A comparison between 2D and 3D chaotic algorithms in [8] highlighted a clear relationship between dimensionality, randomness, and reduced correlation with the original audio signal. Hardware-oriented implementations, as in the design of [9], gave practical proof that chaotic encryption can enable real-time processing in embedded environments. Finally, the lossless encryption model based on a Chebyshev map proposed in [29] introduced an efficient chaotic mechanism that allowed the securing of audio data without any degradation. The discussed studies cumulatively prove that chaos-based encryption offers a robust, flexible, and scalable framework that can meet the ever-increasing security requirements of modern audio communication systems.

VI. DNA AND BIO-INSPIRED AUDIO ENCRYPTION METHODS

The idea of DNA-based audio encryption is based on nucleotide encoding, in which the audio samples are encoded using symbolic biological mappings to increase the complexity of the structure. These methods also include the use of nonlinear mechanisms to increase the diffusion of the keys during the encryption process. Some of these methods also include the use of joint encryption/compression techniques to increase the efficiency of the encryption of the audio samples during secure transmission [10–12]. The key characteristics of these DNA methods are summarized in Table 4.

Table 4: DNA & Bio-Inspired Audio Encryption Methods.

Ref ID	Study Title	Year	Dataset Used	Domain Coverage	Algorithm Types	Experimental Validation	Metrics Used	Key Numerical Results (from paper)	Observed Limitations (based on reported experiments)	Contribution
[10]	An Audio Encryption Algorithm Based on DNA Coding and Chaotic System	2020	Mono & stereo audio signals (piano, human voice, animal, car, drum)	Audio encryption	PWLCM chaotic map + SHA-256 key generation + dynamic DNA coding + XOR diffusion	Yes (simulation)	Correlation, NSCR, UACI, entropy, time	Correlation < 0.1 ; NSCR $\approx 99\%$; UACI $\approx 33\%$; encryption time $\approx 0.034 - 0.037$ s / 1 KB	Experimental evaluation is limited to simulation-based tests on selected audio samples, with no hardware or real-time transmission validation reported.	Demonstrates strong diffusion and key sensitivity through chaos-driven dynamic DNA encoding.
[11]	Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi-Chaotic-Based Dynamic DNA Computations	2020	WAV audio files of different sizes	Secure audio transmission	Self-adaptive bit scrambling + multi-chaotic maps (LCS, HLG) + dynamic DNA + cipher feedback	Yes (extensive experiments)	SNR, PSNR, NSCR, UACI, entropy, correlation, key space	NSCR $\approx 99.99-100\%$; UACI $\approx 35.5-36.2\%$; correlation $\approx 10^{-4}-10^{-5}$; key space $\approx 2^{928}$	Validation focuses on security and statistical metrics, while computational complexity and real-time deployment aspects are not explicitly evaluated.	Introduces a highly secure multi-phase DNA-chaos framework with extremely large key space and strong resistance to differential attacks.
[12]	An Intelligent Audio Encryption and Compression Algorithm Inspired by the Encoding of Various Biological Sequences	2025	Digital audio signals	Audio encryption + compression	Biological-sequence-inspired encoding + joint encryption-compression	Yes (experimental validation)	Entropy, MSE, compression ratio, reconstruction quality	Entropy close to ideal; low MSE after decryption; effective compression without loss of intelligibility	Experiments are reported on digital audio signals without comparison to chaos-DNA or neural-based encryption schemes under identical conditions.	Proposes a unified bio-inspired framework that jointly achieves secure encryption and efficient audio compression.

Source: Authors, (2026).

Interpretation

Both DNA-based and bio-inspired audio encryption techniques are based on the idea of encoding in a nucleotide style and on biologically motivated operations to enhance either confusion or diffusion. Among early works, DNA-chaos hybrid in [10] achieved great enhancements in entropy, decreasing the correlation factor substantially. Multi-chaotic DNA computation in more advanced design [11] expressed higher key sensitivity with increased resistance against differential attacks. Recent bio-inspired models like the one based on sequence encryption-compression in [12] enlarged functionality by combining efficient protection of data with efficient compression. In general, these methods offer powerful nonlinear transformations outperforming many traditional cryptographic methods.

VII. NEURAL AND NEURO-CHAOTIC AUDIO ENCRYPTION METHODS

Neural and neuro-chaotic audio encryption methods have the ability to add flexibility to the security of audio signals by using the capabilities of artificial neural networks and chaotic nonlinear dynamics. Neural networks have the ability to learn complex patterns of signals using learning algorithms. Chaotic dynamics add to the unpredictability of the structure of the system and the generated keys [30], [31]. The key characteristics of these Neural & Neuro methods are summarized in Table 5.

Table 5: Neural & Neuro-Chaotic Audio Encryption Methods.

Ref ID	Study Title	Year	Dataset Used	Domain	Neural Algorithm Type	Experimental Validation	Metrics Used	Numerical Results (from PDF)	Observed Limitations (based on reported experiments)	Contribution
[30]	NeuroChaosCrypt: Revolutionizing Chaotic-Based Cryptosystem With Artificial Neural Networks	2024	Audio signals (8 kHz, 8-bit) and images	Audio and multimedia encryption	ANN-based chaotic system (jerk model)	Yes	CC, SNR, PRD, NPCR, UACI, Time	CC ≈ 0.003 , SNR ≈ -76 dB, PRD $\approx 6.38 \times 10^5$, NPCR $\approx 99.49\%$, Decryption time ≈ 0.008 s (Tables 2–5)	Evaluation is reported for specific signal resolutions and experimental settings, with performance metrics limited to the tested configurations.	Eliminates synchronization requirements and improves decryption speed with an FPGA-ready neuro-chaotic design.

[31]	Memristive Coupled Neural Network Based Cryptosystem	2024	Digital multimedia data (including audio)	Encryption (general)	Memristive Neural Network + Chaos	Yes	Entropy, Key space, Sensitivity	Entropy ≈ 7.99 , key space $> 2^{150}$, high key sensitivity (Section IV)	Experimental evaluation focuses on security metrics and system properties, without reporting real-time audio stream experiments.	Introduces a hardware-oriented neural cryptosystem using memristive coupling.
[32]	A Classification and Retrieval Method for Encrypted Speech Based on Deep Neural Network and Deep Hashing	2020	Encrypted speech samples	Encrypted speech retrieval	DNN + Deep Hashing	Yes	Accuracy, Precision, Recall	Accuracy $\approx 96.2\%$, Precision $\approx 95.4\%$, Recall $\approx 94.8\%$ (Table IV)	Experiments are reported on specific encrypted speech samples and a fixed evaluation setup, with no additional datasets or channel conditions discussed.	Enables intelligent retrieval and classification directly from encrypted speech without decryption.
[33]	Neural Network-Based Cryptography: A Primary Study on the Performances and Techniques	2022	Not specified (conceptual and simulation-based)	General cryptography	ANN-based encryption models	Partial	Throughput, Time	Encryption time reduced by approximately 18–25% compared to classical ciphers (simulation results)	Results are based on simulations and conceptual analysis, with no application-specific (audio) experimental validation reported.	Provides a foundational performance analysis of ANN-based cryptographic systems.

Source: Authors, (2026).

Interpretation

Neural and neuro-chaotic encryption methods have come up with adaptive security that is integrated into neural learning with the nonlinear behavior of chaotic systems. Early neural models, such as encrypted speech retrieval using deep networks [32], showed how intelligent processing can effectively improve protected audio communication. More advanced architectures, including the memristive neural-chaotic architectures [31], expanded the sensitivity of keys and improved the resilience of emerging attacks. Work on neural cryptography [33] provided a deeper basis for detailing how learning based structures support secure key generation, whereas hybrid ANN-chaotic mechanisms [30] had showcased the benefit of blending neural adaptability with chaotic unpredictability. These collectively point out the heightened role of intelligent, dynamically evolving models in shaping next-generation audio encryption.

VIII. OPTICAL AND QUANTUM-BASED AUDIO ENCRYPTION METHODS

In optical and quantum-based methods, there is a shift away from algorithmic models and towards physical-layer models for encrypting audio information. Optical methods are based on light polarization, and quantum methods take advantage of quantum effects to improve communication security [14], [15]. The key characteristics of these Optical / Quantum methods are summarized in Table 6.

Table 6: Optical / Quantum Encryption.

Ref ID	Study Title	Year	Datasets Used / Database	Domain Coverage	Algorithm Types	Experimental Validation	Metrics Used	Numerical Results	Identified Research Gap	Contribution
[14]	Audio Encryption Using Polarized Light Beam	2025	Digitized audio signals mapped to optical domain	Audio	Polarized Light Beam (PLB)-based optical encryption	Yes (simulation + experimental validation)	Correlation coefficient, PSNR, noise robustness	Correlation (original-encrypted) = 0.13, Correlation (original-decrypted) = 0.96; CC = 0.9459 and PSNR = 17 dB under Gaussian noise (variance 0.1); CC = 0.94, PSNR = 14 dB at variance 0.2	Requires specialized optical hardware; experimental setup complexity limits portability and real-time deployment	Introduces an optical-domain audio encryption scheme using polarization states with high reconstruction fidelity and strong resistance to cryptanalytic attacks
[15]	QSAC: Quantum-Assisted Secure Audio Communication Using Quantum Entanglement and Steganography	2025	Audio communication signals encoded in quantum domain	Secure Audio Communication	Quantum entanglement + quantum steganography	Yes (theoretical analysis + experimental validation)	BER, SNR, quantum disturbance indicators	Any eavesdropping attempt causes detectable quantum disturbances; BER increases significantly under interception, enabling reliable intrusion detection	High implementation cost; experimental complexity; limited scalability due to early-stage quantum hardware	Proposes a quantum-assisted secure audio communication framework with intrinsic eavesdropping detection guaranteed by quantum physics

Source: Authors, (2026).

Interpretation

Optical and quantum encryption methods achieve superior protection of audio signals through physical and quantum phenomena instead of a purely mathematical basis. Polarized-light encryption [14], and communication with quantum assistance [15], although very resistant to tapping, have not found wide practical applications so far, mostly due to hardware and implementation issues.

IX. COMPARATIVE FRAMEWORK OF AUDIO ENCRYPTION APPROACHES

This section discusses the structural comparison of the chosen audio encryption models based on their design and implementation structures. The models used in the comparison are different in their mathematical underpinnings, system models, and application domains. Some of the models are based solely on algorithmic models, while others are based on signal processing models, biological models, intelligent models, and physical models. The comparison of the models shows the different methodologies used in the implementation of the models, ranging from fixed models to intelligent models. The key characteristics of the selected audio encryption methods are summarized in Table 7.

Table 7: The comparative analysis of chosen audio-encryption methods.

Ref ID	Study Title	Year	Technique Type	Algorithm / Model	Dataset Used	Metrics Reported	Numerical Results	Main Limitations / Notes	Application Focus
[4]	Evaluation of Rijndael Algorithm for Audio Encryption by Brute Force Attack	2024	Classical (AES-based)	AES (Rijndael) block cipher	Audio files	Key space, brute-force complexity	256-bit key $\rightarrow \approx 4.13 \times 10^{99}$ total permutations	PSNR/SNR metrics not reported; focuses mainly on brute-force evaluation	Secure audio storage systems
[25]	Multilayered Audio Signal Encryption for Secure Voice Communication	2023	Classical + Transform	Multi-layer DCT/DST encryption pipeline	Speech recordings (Audio1–Audio3)	SNR, correlation, execution time	Example Audio1 $\rightarrow$ SNR ≈ -2.70 dB; correlation ≈ 0.00236	Higher computational complexity; negative SNR indicates strong signal distortion	Secure voice communication
[6]	Bit-Level Audio Encryption Using a New Hybrid Chaotic Map	2024	Chaotic	Hybrid chaotic map with bit-level scrambling	Digital audio signals	Histogram analysis, correlation, entropy, key space	Post-encryption correlation ≈ 0 ; entropy reported as high (exact numerical values not explicitly reported)	NPCR/UACI values not explicitly reported in the extracted results	High-security multimedia transmission
[7]	A New Audio Encryption Based on Hyper-Chaotic System	2024	Hyper-Chaotic	Logistic permutation with 4D hyperchaotic diffusion	Speech recordings	Entropy, correlation, differential metrics, execution speed	Described as high-security and real-time capable (exact numerical values not explicitly tabulated)	Computationally intensive; explicit numerical values not reported in extracted results	Defense-level secure communication
[29]	A Lossless Audio Encryption Using Chebyshev Map	2023	Chaotic (Lossless)	Chebyshev chaotic map with lossless reconstruction	Multiple WAV audio files	Correlation, key space, lossless reconstruction	Correlation of encrypted signal $\approx 10^{-4} - 10^{-6}$	SNR/PSNR metrics not reported	Medical and archival audio protection
[10]	Audio Encryption Using DNA Coding and Chaotic System	2020	DNA–Chaos	PWLCM chaotic map with SHA-256 key generation and DNA encoding rules	Mono and stereo audio signals (piano, human voice, car, etc.)	NSCR, UACI, correlation, runtime	Original correlation > 0.9 ; encrypted < 0.1 ; NSCR $\approx 100\%$; UACI $\approx 33.3\%$	DNA operations increase computational complexity	Critical audio security systems
[11]	Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations	2020	DNA–Multi-Chaos	Multi-chaotic maps with dynamic DNA computation and cipher feedback	WAV audio signals	Entropy, UACI, NSCR, correlation	UACI $\approx 35.55\%$; NSCR $\approx 99.995\%$; correlation $\approx 5.3 \times 10^{-3}$	High computational cost	High-security audio transmission
[30]	NeuroChaosCrypt: Revolutionizing Chaotic-Based Cryptosystem With Artificial Neural Networks—A Comparison With Traditional Cryptosystems	2024	Neural–Chaotic	ANN-driven chaotic cryptosystem	Audio and image datasets	Entropy, NPCR, UACI, SNR, PRD, execution time	Entropy ≈ 7.4326 ; NPCR $\approx 99.49\%$; UACI $\approx 0.39\%$	NPCR/UACI numerical results mainly evaluated on image datasets	AI-enhanced secure communication systems
[31]	Memristive Coupled Neural Network Cryptosystem	2024	Neural / Hardware-Chaotic	Memristive coupled neural network model	Digital multimedia datasets	Entropy, key sensitivity	Entropy close to ideal; strong key sensitivity (exact numerical values not explicitly reported)	Limited numerical audio-specific metrics	Real-time embedded security systems
[14]	Audio Encryption Using Polarized Light Beam (PLB)	2025	Optical / Physical-Layer	Polarized Light Beam transformation	Audio signals mapped to optical domain	Correlation, BER, physical analysis	Example: original–encrypted correlation ≈ 0.131 ; original–decrypted ≈ 0.9608	Requires specialized optical hardware	Military and quantum-safe audio communication

Source: Authors, (2026).

Interpretation

The comparative analysis of chosen audio-encryption methods shows how much the security models have diversified to meet the ever-increasing complexity of modern communication environments. While classical methods retain strong resistance against brute-force attacks due to their large key spaces, significant limitations arise when these methods are confronted with correlation or structure-based analyses. Chaotic and hyper-chaotic systems can offer significantly better confusion-diffusion properties, reflected by their near-ideal entropy levels and minimal values of correlation, which makes them particularly effective in protecting highly dynamic audio signals. DNA-based frameworks further reinforce security with biologically inspired transformations that increase nonlinearity and improve differential resistance. Neural and neuro-chaotic models bring adaptability and hardware-accelerated processing, positioning them as strong candidates for real-time intelligent encryption scenarios. Optical and physical-layer methods extend protection beyond computational paradigms by exploiting intrinsic properties of light, offering exceptional resistance against interception despite requiring hardware implementation. Overall, the comparative findings suggest that while each category presents distinct advantages, hybrid schemes integrating chaotic, biological, neural, or physical-layer mechanisms tend to offer a balanced trade-off between security strength, adaptability, and implementation feasibility in next-generation secure audio communication systems.

X. CONCLUSION

The above research work has provided a detailed comparative analysis for audio encryption methods that have been developed between the years 2015 and 2025. These methods include classic encryption techniques, chaos and DNA-based models, neural and neuro-chaotic systems, as well as optical and quantum-based methods. It was noted that classic encryption methods have high strength in terms of immunity from brute-force attacks and efficiency. However, their fixed structure can lead to limits in modeling the statistical properties of audio. On the other hand, chaotic, DNA, and neural-driven encryption models showed better confusion-diffusion capability, larger key space, and better resistance to complex sound patterns. Optical and quantum-computing-assisted techniques offer top-notch security assurance with robust physical guarantees, but they are limited due to complexity issues associated with their implementation. Thus, encryption models that combine chaotic systems, biologic encryption, neural models, and physical layer mechanisms can be considered promising candidates to support secure next-gen sound communication systems with better efficacy.

XI. FUTURE WORK

Future studies could emphasize working on lightweight hybrid encryption frameworks for audio that bring a good balance between security and the ability to handle real-time encryption. Adding the concept of neural learning into chaos and DNA algorithms has not been significantly explored, especially for a channel environment that is noisy and attacked using machine-learning-based attacks. Moreover, a common benchmarking dataset needs to be developed for comparison purposes across various encryption paradigms. Lastly, studies on the practical framework for quantum assistance in encryption systems also need to be explored.

XII. AUTHOR'S CONTRIBUTION

Conceptualization: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Methodology: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Investigation: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Discussion of results: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Writing – Original Draft: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Writing – Review and Editing: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Resources: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Supervision: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

Approval of the final text: Halah Waad Khaled, Waleed Abdullah Araheem and Hakeem Imad Mhaibes.

XIII. REFERENCES

- [1] Y. Mahamat, S. H. Othman, and S. H. Nkiama, "Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm," 2016. [Online]. Available: www.iosrjen.org
- [2] I. Khalid, T. Shah, K. A. Almarhabi, D. Shah, M. Asif, and M. Usman Ashraf, "The SPN Network for Digital Audio Data Based on Elliptic Curve Over a Finite Field," *IEEE Access*, vol. 10, pp. 127939–127955, 2022, doi: 10.1109/ACCESS.2022.3226322.
- [3] S. R. Kareem, "Encryption of Audio Signals Using the Elzaki Transformation and the Lorenz Chaotic System," Sep. 2024. doi: 10.48550/arXiv.2409.14092.
- [4] S. G. Mohammed and N. S. Al-Mothafar, "Evaluation of Rijndael Algorithm for Audio Encryption by Brute Force Attack," *J. Eng.*, vol. 30, no. 11, pp. 128–141, Nov. 2024, doi: 10.31026/j.eng.2024.11.08.
- [5] H. Aziz, S. M. M. Gilani, I. Hussain, A. K. Janjua, and S. Khurram, "A Noise-Tolerant Audio Encryption Framework Designed by the Application of S8Symmetric Group and Chaotic Systems," *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/5554707.
- [6] M. Demirtas, "A BIT-LEVEL AUDIO ENCRYPTION ALGORITHM USING A NEW HYBRID CHAOTIC MAP," *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilim. Derg.*, vol. 27, no. 2, pp. 601–614, Jun. 2024, doi: 10.17780/ksujes.1412850.
- [7] H.A. Qasim, "A new Audio Encryption Algorithm Based on Hyper-Chaotic System," *Mustansiriyah J. Pure Appl. Sci.*, vol. 1, no. 3, pp. 85–94, Oct. 2023, doi: 10.47831/mjpas.v1i3.51.

- [8] T. Haridas, S. D. Upasana, G. Vyshnavi, M. S. Krishnan, and S. S. Muni, "Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems," *Franklin Open*, vol. 8, Sep. 2024, doi: 10.1016/j.fraope.2024.100158.
- [9] H. M. Elrefai, W. S. Sayed, and L. A. Said, "Hardware Implementation of a 2D Chaotic Map-Based Audio Encryption System Using S-Box," *Electron.*, vol. 13, no. 21, Nov. 2024, doi: 10.3390/electronics13214254.
- [10] X. Wang and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," *IEEE Access*, vol. 8, pp. 9260–9270, 2020, doi: 10.1109/ACCESS.2019.2963329.
- [11] R. I. Abdelfatah, "Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations," *IEEE Access*, vol. 8, pp. 69894–69907, 2020, doi: 10.1109/ACCESS.2020.2987197.
- [12] M. Nassef, "An Intelligent Audio Encryption and Compression Algorithm Inspired by the Encoding of Various Biological Sequences," *IEEE Access*, vol. 13, pp. 126334–126354, 2025, doi: 10.1109/ACCESS.2025.3588764.
- [13] S. M. Fu, X. F. Cheng, and J. Liu, "Dynamics, circuit design, feedback control of a new hyperchaotic system and its application in audio encryption," *Sci. Rep.*, vol. 13, no. 1, Dec. 2023, doi: 10.1038/s41598-023-46161-5.
- [14] A. Shikder, S. K. Rajput, N. K. Nishchal, O. Matoba, and Y. Awatsuji, "Audio encryption using polarized light beam," *APL Photonics*, vol. 10, no. 3, Mar. 2025, doi: 10.1063/5.0234393.
- [15] M. R. I. Rifat, M. M. Rahman, M. A. K. Nayon, M. S. Azad, and M. R. C. Mahdy, "QSAC: Quantum-assisted Secure Audio Communication using quantum entanglement, audio steganography, and classical encryption," *Eng. Sci. Technol. an Int. J.*, vol. 70, Oct. 2025, doi: 10.1016/j.jestch.2025.102167.
- [16] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 257–272, Feb. 2024, doi: 10.62411/jcta.9851.
- [17] P. Sudha, "LITERATURE SURVEY ON RECENT AUDIO ENCRYPTION TECHNIQUES," *Int. J. Electron. Commun. Eng. Technol.*, vol. 7, no. 6, pp. 91–95, [Online]. Available: <http://www.iaeme.com/IJECET/index.asp91http://www.iaeme.com/IJECET/issues.asp?JType=IJECET&VType=7&IType=6http://www.iaeme.com/IJECET/issues.asp?JType=IJECET&VType=7&IType=6>
- [18] E. A. Albahrani, T. K. Alshekly, and S. H. Lafta, "A Review on Audio Encryption Algorithms Using Chaos Maps-Based Techniques," 2021, *River Publishers*. doi: 10.13052/jcsm2245-1439.1113.
- [19] A. Poduval, N. Rai, P. Khan, T. Chaudhari, P. Guide, and A. Professor, "A SURVEY ON DIFFERENT ENCRYPTION TECHNIQUES FOR IMAGE, VIDEO, AUDIO AND DOCS," 2021. [Online]. Available: <http://www.ijeast.com>
- [20] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia Security Using Encryption: A Survey," *IEEE Access*, vol. 11, pp. 63027–63056, 2023, doi: 10.1109/ACCESS.2023.3287858.
- [21] R. A. Gandhi and A. M. Gosai, "A Study on Current Scenario of Audio Encryption," Apr. 2015.
- [22] A. Shumran and A. B. A. Al-Hussein, "Study of Chaotic-based Audio Encryption Algorithms: A Review," *Iraqi J. Electr. Electron. Eng.*, vol. 20, no. 2, pp. 85–103, Dec. 2024, doi: 10.37917/ijeee.20.2.8.
- [23] D. D. Mali and S. N. Shinde, "A Survey of Various Symmetric Encryption Methods," 2025, pp. 294–303. doi: 10.2991/978-94-6463-876-9_22.
- [24] N. A. Hassan, F. S. Al-Mukhtar, and E. H. Ali, "Encrypt Audio File using Speech Audio File As a key," in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing Ltd, Nov. 2020. doi: 10.1088/1757-899X/928/3/032066.
- [25] H. A. Abdallah and S. Meshoul, "A Multilayered Audio Signal Encryption Approach for Secure Voice Communication," *Electron.*, vol. 12, no. 1, Jan. 2023, doi: 10.3390/electronics12010002.
- [26] J. He, P. Zhu, Z. Liu, and Y. Cao, "A Novel Digital Audio Encryption and Forensics Watermarking Scheme," *IEEE Access*, vol. 12, pp. 103565–103582, 2024, doi: 10.1109/ACCESS.2024.3434576.
- [27] A. Z. Abbasi, A. Rafiq, and B. M. Alshammari, "A digital audio data protection method using parametric action of generalised triangle group on GF(28)," *Ain Shams Eng. J.*, vol. 16, no. 1, Jan. 2025, doi: 10.1016/j.asej.2024.103193.
- [28] M. M. Al-Ezzi, W. Weiping, A. Monem, S. Rahma, H. A. Al, and M. R. Hassan, "A New Encryption Algorithm for Voice Messages on Social Media Using Magic Cube GF (2^8) Technology 253 Original Scientific Paper," 2025. doi: 10.32985/ijeces.16.3.6.
- [29] M. Demirtaş, "A Lossless Audio Encryption Method based on Chebyshev Map," *Orclever Proc. Res. Dev.*, vol. 2, no. 1, pp. 28–38, Mar. 2023, doi: 10.56038/oprd.v2i1.234.
- [30] T. Bonny and W. Al Nassan, "NeuroChaosCrypt: Revolutionizing Chaotic-Based Cryptosystem With Artificial Neural Networks - A Comparison With Traditional Cryptosystems," *IEEE Access*, vol. 12, pp. 62030–62046, 2024, doi: 10.1109/ACCESS.2024.3395527.
- [31] F. Hamed *et al.*, "Memristive Coupled Neural Network Based Audio Signal Encryption," in *Signal Processing - Algorithms, Architectures, Arrangements, and Applications Conference Proceedings, SPA*, IEEE Computer Society, 2024, pp. 149–154. doi: 10.23919/SPA61993.2024.10715600.
- [32] Q. Zhang, X. Zhao, and Y. Hu, "A classification retrieval method for encrypted speech based on deep neural network and deep hashing," *IEEE Access*, vol. 8, pp. 202469–202482, 2020, doi: 10.1109/ACCESS.2020.3036048.
- [33] J.-L. Foo, K.-W. Ng, and P. Naveen, "Neural Network-Based Cryptography: A Primary Study on the Performances and Techniques," in *Proceedings of the International Conference on Computer, Information Technology and Intelligent Computing (CITIC 2022)*, Atlantis Press International BV, 2022, pp. 68–78. doi: 10.2991/978-94-6463-094-7_6.