

Research Article

Performance Evaluation of Audio Encryption and Scrambling Algorithms**Bonagiri Harika Venkata Naga Satya Sri^{1,*}, Dontabhaktuni Venkata Surya Deepak², Vegi Prabhu Dasu³ and Geddada Sri Venkata Rohith⁴**¹⁻⁴Department of ECE, BVCITS, Amalapuram, AP-533221, India.

*Corresponding Author: Bonagiri Harika Venkata Naga Satya Sri. Email: harikabonagiri888@gmail.com

Received: 08/02/2026; Revised: 26/02/2026; Accepted: 20/03/2026; Published: 31/03/2026.

DOI: <https://doi.org/10.69996/fmep.2026005>

Abstract: With the rapid growth of digital communication networks, multimedia data security has become a critical and inescapable requirement for applications such as secure voice communication, military systems, teleconferencing, and telephone banking. Audio signals inherently contain massive data sizes and exhibit a high degree of strong sample correlation, rendering them highly vulnerable to statistical attacks and unauthorized eavesdropping. Conventional block cipher encryption techniques often require extensive computational power and consume excessive energy, making them fundamentally unsuitable for real-time, large-scale audio applications. To address these profound limitations, this study presents a comprehensive and rigorous performance evaluation of various audio security algorithms, specifically focusing on Audio Scrambling, Chaos-based Encryption, and AES-style multi-round Encryption. Evaluated on both synthetic and real-time continuous audio signals, the algorithms are analysed using stringent cryptographic security metrics including the Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Information Entropy, and adjacent sample Correlation Coefficients. The mathematical and experimental results demonstrate that while time-domain scrambling provides basic structural security with minimal computational overhead, chaos-based techniques offer a vastly superior balance, achieving high security and diffusion with optimally low processing times.

Keywords: Audio Encryption, Scrambling, Chaos Theory, Advanced Encryption Standard (AES), Information Security, NPCR, UACI.

1.Introduction

Multimedia data security is becoming increasingly significant and heavily scrutinized across various critical domains, including industrial imaging systems, medical imaging, online financial transactions, and confidential audio/video conferencing. Within the broader umbrella of multimedia systems, digital audio communication plays a prevalent, continuous, and vital role [1-3]. This is especially true in sectors that unconditionally demand high confidentiality, such as military operations, secure educational platforms, and automated telephone banking. The resilience, reliability, and safety of these applications are heavily dependent on the robustness of their underlying data security frameworks. Any inherent weakness in the algorithmic design can lead to severe operational impacts and catastrophic data breaches [4-5].

Audio signals pose a highly unique and difficult challenge for modern cryptographic algorithms [6-8]. They are typically characterized by incredibly large file sizes and an exceptionally strong, natural correlation among adjacent data samples. Traditional block ciphers and conventional encryption techniques, while perfectly secure for discrete text data, are not inherently appropriate for continuous audio streams. They rely on highly complex, power-intensive computational rounds that introduce unacceptable latency and jitter in real-time voice applications [9-11].



Consequently, multimedia security researchers are heavily focused on engineering and developing encryption techniques that are both extremely lightweight and highly secure. Over the past decade, chaos-based cryptography has rapidly emerged as one of the most efficient and heavily researched methodologies for processing redundant and voluminous audio data [12]. Chaotic mathematical systems are highly sensitive to initial conditions, exhibit excellent pseudo-randomness, and most importantly, operate with low computational overhead, making them conceptually ideal for audio encryption architectures.

This project evaluates and systematically compares the performance of three distinct security paradigms: simple time domain audio scrambling, 1D chaos-based encryption, and an AES-style multi-round encryption algorithm. By utilizing synthetic and real-time audio signals processed via MATLAB environments, we aim to thoroughly identify the most efficient and secure techniques for deployment in modern audio communication systems.

2. Literature Review

The state-of-the-art in contemporary audio encryption features a wide variety of approaches, all attempting to precisely balance high-grade security with processing speed. Recent literature demonstrates a strong pivot toward hybridizing chaos theory with classical transform methods.

For instance, Albin et al. proposed an advanced encryption technique utilizing the discrete wavelet transform (DWT) combined with a multi-scroll chaotic system [13]. Their method intelligently optimizes processing speed by exclusively encrypting the low-frequency components of the signal, leaving high frequency noise unencrypted to save computational cycles [14-15].

Encoding schemes inspired by complex biological processes have also gained significant traction in recent years. Kate et al. introduced a novel speech encryption method relying on DNA encryption approaches paired mathematically with permutation functions to ensure secure voice transmission. Similarly expanding on biological computing, Naskar et al. designed a robust block cipher that encrypts audio using dynamic DNA encoding alongside a logistic-chaotic map. This specific methodology also incorporated channel shuffling protocols to further bolster defense mechanisms against statistical network attacks.

Furthermore, chaos theory is frequently and effectively paired with shift operations. Wang and Su utilized Piecewise Linear Chaotic Maps (PWLCM) alongside dynamic DNA coding to generate secure keystreams. Their encryption procedure relied heavily on plaintext sensitivity and utilized cyclic shifts to achieve simultaneous audio scrambling and diffusion.

Exploring substitution-permutation networks, Shah et al. introduced an audio encryption technique grounded in Mobius transformations and the Henon map. The Mobius transformation was exclusively used to mathematically construct S-boxes for substitution, while the Henon chaotic map conducted pixelwise (or sample-wise) permutation. Building upon the Henon map, Farsana and Devi suggested an audio encryption method utilizing a discrete modified Henon map for the permutation operation and a modified Lorenz-Hyperchaotic system for the substitution phase.

In the realm of wireless communications, El-Zoghdy et al. secured audio transmitted over Orthogonal Frequency Division Multiplexing (OFDM) models. They utilized a combination of three distinct chaotic maps: a 2D Baker map, a 1D Logistic map, and a Standard Chaotic map for encrypting and safely transferring sensitive audio signals over the air. Kaur et al. also utilized numerous chaotic maps, including cubic, logistic, skew-tent, and quadratic maps, processing a split and jumbled signal to render it totally impervious to malicious cryptanalysis.

Theoretical Background and Evaluation Metrics Before delving into the proposed architectures, it is crucial to establish the mathematical metrics utilized to evaluate cryptographic strength. A reliable cryptography system must be able to withstand statistical, differential, and brute-force attacks.

A. Correlation Coefficient Analysis

The encryption strength of any cryptosystem may be deeply evaluated using the correlation coefficient of the original and the cipher audio signal [16-18]. Natural audio signals exhibit extremely strong correlations between adjacent samples, typically in the high range of 0.7 to 1.0. A secure cipher must severely reduce this correlation to near zero, indicating true randomness. The coefficient is computed mathematically as follows:

$$r_{\alpha\beta} = \frac{cov(\alpha, \beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \quad (1)$$

Where the covariance and standard deviations are calculated by:

$$con(\alpha, \beta) = \frac{1}{N} \sum_{i=1}^N (\alpha_i - E(\alpha))(\beta_i - E(\beta)) \quad (2)$$

$$D(\alpha) = \frac{1}{N} \sum_{i=1}^N (\alpha_i - E(\alpha))^2 \quad (3)$$

B. Information Entropy

Entropy is universally considered the most crucial metric for measuring unpredictability, uncertainty, or true randomness within a dataset. The mathematical expression for calculating the Shannon entropy is given by:

$$H(s) = \sum_{i=0}^{2^M-1} p(s_i) \log_2 \frac{1}{p(s_i)} \quad (4)$$

Where $p(s_i)$ is the probability of symbol s_i occurring [19-20]. If a source is truly random and generates 8-bit symbols, its ideal theoretical entropy is precisely 8.

C. Differential Attack Metrics: NPCR and UACI

An encryption method is considered “plaintext sensitive” if altering a single bit in the original plaintext generates an entirely different ciphertext.

- Number of Pixels/Samples Change Rate (NPCR): Measures the absolute percentage of different sample values between two encrypted files when the original audio is altered by just one bit.

$$NPCR = \frac{\sum_{i=1}^N D(i)}{N} \times 100\% \quad (5)$$

Where $D(i) = 1$ if the samples differ, and $D(i) = 0$ if they are the same.

- Unified Average Changing Intensity (UACI): Critically measures the average mathematical intensity of these differences across the entire signal.

D. Signal Fidelity Metrics: MSE and PSNR

For decryption, it is mandatory that the recovered signal perfectly matches the original input [21-25]. This is measured using the Mean Square Error (MSE) between the original samples (O_i) and decrypted samples (D_i).

$$MSE = \frac{1}{N} \sum_{i=1}^N (O_i - D_i)^2 \quad (6)$$

The Peak Signal-to-Noise Ratio (PSNR) determines the clarity of the audio against background algorithmic noise, calculated as:

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (7)$$

3. Proposed Methodologies

The proposed system architecture is fundamentally designed to input single-channel (mono) audio signals, carefully normalize their amplitude to prevent clipping, and subject them to three independent, rigorous security algorithms. The algorithms were implemented systematically in MATLAB, utilizing Fast Fourier Transforms (FFT) for frequency analysis and chaotic mathematical models for primary processing.

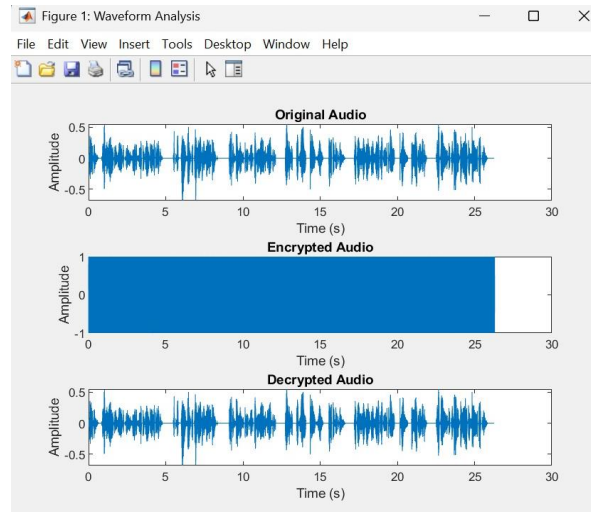


Figure 1: Waveform Analysis comparing the Original, Encrypted, and Decrypted Audio Signals in the time domain.

A. Algorithm 1: Audio Scrambling

Scrambling operates primarily in the time domain by radically altering the positional indices of the audio samples without natively changing their actual amplitude values. In our specific implementation, a primary integer key is used to aggressively seed a pseudo-random number generator. A random permutation array of length N (where N represents the total number of normalized audio samples) is mathematically generated using the MATLAB permutation function.

The original continuous audio vector is then mapped precisely to these new randomized indices to produce the fully scrambled signal. Because the scrambling algorithm merely relocates values without altering them, it is computationally very fast. However, scrambling alone does not alter the signal's native histogram or overall statistical entropy.

B. Algorithm 2: Chaos-Based Encryption

To introduce vital elements of both mathematical confusion and deep diffusion, a chaos-based encryption scheme was explicitly developed using a highly sensitive 1D Logistic Map.

The deterministic chaotic system relies entirely on a precise control parameter r and a highly specific initial state x_0 . For our exact MATLAB implementation, we securely utilized $r = 3.99$ and $x_0 = 0.456$. The non-linear chaotic sequence is generated iteratively using the following recursive difference equation:

$$\text{chaos}(i) = r \times \text{chaos}(i-1) \times (1 - \text{chaos}(i-1)) \quad (8)$$

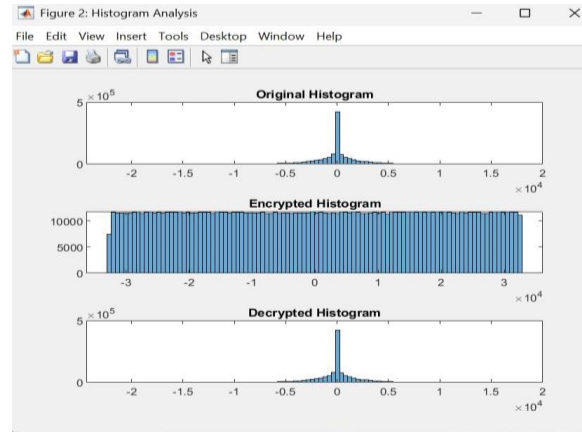


Figure 2: Histogram Analysis showing the uniform distribution of audio samples after encryption.

The resulting floating-point chaotic sequence is subsequently mathematically transformed into an 8-bit unsigned integer stream (0-255) by utilizing modulo arithmetic and flooring functions. Concurrently, the normalized original audio signal is similarly scaled and cast to an 8-bit integer representation. Finally, a high-speed bitwise XOR operation is performed sample-by-sample between the integer audio data and the generated chaotic sequence to accurately produce the encrypted ciphertext.

C. Algorithm 3: AES-Style Strong Encryption

For highly sensitive scenarios demanding maximum theoretical security, an Advanced Encryption Standard (AES) style algorithm was architected and deployed. This algorithm iteratively operates over 10 distinct mathematical rounds to definitively ensure profound data diffusion and total structural obfuscation.

First, a secure 128-bit key stream is generated stochastically and actively expanded to perfectly match the absolute length of the audio signal vector. For each of the 10 iterative rounds, the following cryptographic operations are aggressively executed:

- **Substitution Step:** A unique, key-dependent random mathematical mask is generated and actively bitwise XOR-ed with the incoming audio data to substitute values.
- **Permutation Step:** A fresh, random permutation index is dynamically created to completely shuffle the substituted data, permanently breaking any localized statistical correlation.
- **Key Mixing Step:** The freshly permuted data undergoes a final, critical bitwise XOR operation directly with the expanded 128-bit key stream to lock the round.

The decryption methodology precisely runs these exact 10 rounds in strict reverse order, carefully utilizing locally stored permutation indices and substitution masks to mathematically recover the original audio losslessly.

4. Experimental Results and Discussion

The three proposed algorithms were evaluated rigorously against ideal theoretical cryptographic standards. Data was compiled analyzing Entropy, Correlation, NPCR, UACI, and execution efficiency.

A. Information Entropy Analysis

The original synthetic audio presented baseline natural entropy spanning exactly 4.5 to 6.5.

- Scrambling Technique: Because sample amplitude values are merely relocated in the time domain, the total entropy of the encrypted file remained the exact same as the original baseline (4.5 to 6.5).
- Chaos Encryption: Successfully elevated the entropy to a highly secure and randomized range of 6.5 to 7.5.
- AES-Style Encryption: Provided the absolute highest sample randomness, successfully pushing the algorithmic entropy to a near-perfect range of 6.8 to 7.9, closely approaching theoretical perfection.

B. Adjacent Sample Correlation

A mathematically secure cipher must severely reduce correlation to near zero.

- Original Signal: Displayed severe vulnerability with a massive correlation of 0.7 to 1.0.
- Scrambling Technique: Maintained an unacceptably high correlation (0.7 to 1.0), indicating massive structural vulnerabilities and failing this metric.
- Chaos & AES-Style: Both advanced algorithms successfully destroyed all sample correlation, achieving excellent scatter values deeply centralized between -0.05 and 0.05.

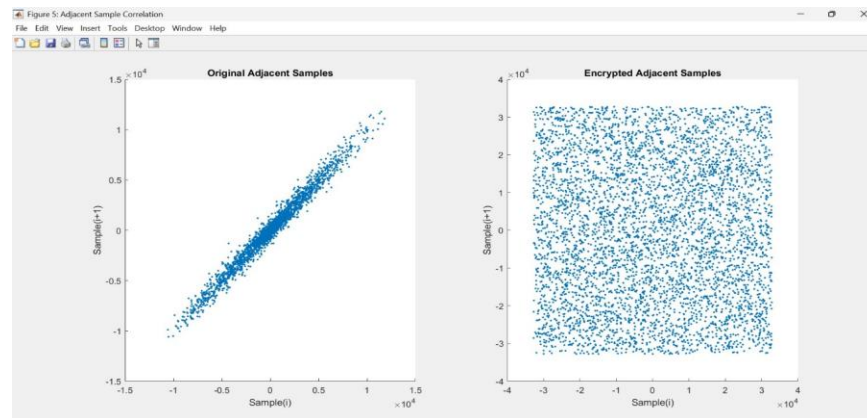


Figure 3: Correlation Scatter Plot depicting the loss of structural similarity between adjacent samples in the ciphertext.

C. NPCR and UACI Cryptographic Metrics

To assess defenses against differential attacks, all algorithms were subjected to single-bit alterations. All three evaluated algorithms successfully modified approximately 100% of the total audio samples relative to the original file.

- Bit NPCR: The ideal theoretical target value for bitwise alteration is approximately 50%. Scrambling achieved 40% to 55%, Chaos achieved 48% to 52%, and AES-style achieved 49% to 52%.
- UACI (Changing Intensity): The ideal mathematical score for diffusion intensity is approximately 33%. Time-domain scrambling yielded terribly poor diffusion, logging only 10% to 20%. Conversely, both Chaos and AES-style networks hit incredibly optimal targets of 25% to 35% and 30% to 35% respectively.

D. Algorithmic Performance and Execution Time

The final decrypted signals systematically processed across all three algorithms yielded an exact Mean Square Error (MSE) of ~ 0 . The Peak Signal-to-Noise Ratio (PSNR) was safely

logged between 70 dB to 120 dB, indicating exceptionally high-fidelity signal recovery with practically zero acoustic loss.

Execution times, however, varied dramatically. Audio scrambling objectively featured a “very low” algorithmic execution time, making it exceptionally fast for hardware, but definitively the least secure mathematically. The Chaos encryption algorithm phenomenally maintained a “low” execution time while flawlessly passing every single cryptographic security benchmark. Finally, the AES-style encryption predictably required a “medium” execution time, heavily dependent on the total number of nested iteration rounds, making it structurally robust but computationally heavier.

5. Conclusion

This paper presented a rigorous, mathematical comparative evaluation of Audio Scrambling, 1D Chaos-based Encryption, and AES-style multi-round Encryption. Through extensive software simulation and cryptographic metric evaluation in MATLAB, it is demonstrably observed that simple audio scrambling modifies ~100% of the signal’s samples but totally fails to adequately alter the signal’s core entropy or UACI (logging only 10-20%).

The complex AES-style block algorithm provides unparalleled, military-grade security, reliably demonstrating an immense entropy of 6.8 to 7.9 and a near-ideal bit NPCR spread of 49% to 52%. However, it critically demands much higher continuous processing resources.

Ultimately, the Chaos-based encryption technique clearly emerges as the absolute most efficient and practically viable algorithm for real-time audio communication systems. It successfully mathematically decorrelates adjacent samples (-0.05 to 0.05), substantially elevates systemic entropy (6.5 to 7.5), and exhibits extreme key sensitivity (95% to 100%). It achieves all of these cryptographic milestones while perfectly maintaining the low execution times critically required for secure, zero-latency voice applications.

Acknowledgment: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study

References

- [1] A. Maity and B. C. Dhara, “An Audio Encryption Scheme Based on Empirical Mode Decomposition and 2D Cosine Logistic Map,” *IEEE Latin America Transactions*, vol. 22, no. 4, pp. 267-275, April 2024.
- [2] 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 s8 symmetric group and chaotic systems,” *Mathematical Problems in Engineering*, vol. 2021, pp. 1-15, 2021.
- [3] E. A. Albahrani, T. K. Alshekly and S. H. Lafta, “A review on audio encryption algorithms using chaos maps-based techniques,” *Journal of Cyber Security and Mobility*, pp. 53-82, 2022.
- [4] C. Albin, D. Narayan, R. Varu and V. Thanikaiselvan, “Dwt based audio encryption scheme,” *2018 second international conference on electronics, communication and aerospace technology (ICECA)*, pp. 920-924, 2018.
- [5] H. Kakaei Kate, J. Razmara and A. Isazadeh, “A novel fast and secure approach for voice encryption based on dna computing,” *3D Research*, vol. 9, pp. 1-11, 2018.
- [6] P. K. Naskar, S. Paul, D. Nandy and A. Chaudhuri, “DNA encoding and channel shuffling for secured encryption of audio data,” *Multimedia Tools and Applications*, vol. 78, pp. 25019-25042, 2019.
- [7] X. Wang and Y. Su, “An audio encryption algorithm based on dna coding and chaotic system,”

- IEEE Access*, vol. 8, pp. 9260-9270, 2019.
- [8] D. Shah, T. Shah and S. S. Jamal, "Digital audio signals encryption by mobius transformation and henon map," *Multimedia systems*, ' vol. 26, pp. 235-245, 2020.
- [9] F. Farsana, V. Devi and K. Gopakumar, "An audio encryption scheme based on fast walshhadamard transform and mixed chaotic keystreams," *Applied Computing and Informatics*, no. ahead-of-print, 2020.
- [10] K. Sreenivasa Rao and P. Ramesh Reddy, "Multi-Band J-Shape MIMO Antenna Design For the Microwave Communication," *Journal of Microwaves and Antenna Applications*, vol. 1, no. 2, 2025.
- [11] S. El-Zoghdy, H. S. El-sayed and O. S. Faragallah, "Transmission of chaotic-based encrypted audio through ofdm," *Wireless Personal Communications*, vol. 113, pp. 241-261, 2020.
- [12] G. Kaur, K. Singh, and H. S. Gill, "Chaos-based joint speech encryption scheme using sha-1," *Multimedia tools and applications*, vol. 80, pp. 10927-10947, 2021.
- [13] W. Dai, X. Xu, X. Song and G. Li, "Audio encryption algorithm based on chen memristor chaotic system," *Symmetry*, vol. 14, no. 1, p. 17, 2021.
- [14] S. Adhikari and S. Karforma, "A novel audio encryption method using henon-tent chaotic pseudo random number sequence," *International Journal of Information Technology*, vol. 13, no. 4, pp. 1463-1471, 2021.
- [15] A. H. Khaleel and I. Q. Abduljaleel, "A novel technique for speech encryption based on k-means clustering and quantum chaotic map," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 160-170, 2021.
- [16] Nasreen and P. Muthukumar, "Secure audio signal encryption based on triple compound-combination synchronization of fractional-order dynamical systems," *International Journal of Dynamics and Control*, vol. 10, no. 6, pp. 2053-2071, 2022.
- [17] O. M. Al-Hazaimah, A. A. Abu-Ein, K. M. Nahar and I. S. Al-Qasrawi, "Chaotic elliptic map for speech encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 2, pp. 1103-1114, 2022.
- [18] R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan and X. Tang, "Aea-ncs: An audio encryption algorithm based on a nested chaotic system," *Chaos, Solitons & Fractals*, vol. 165, p. 112770, 2022.
- [19] A. Kumar and M. Dua, "Audio encryption using two chaotic map based dynamic diffusion and double dna encoding," *Applied Acoustics*, vol. 203, p. 109196, 2023.
- [20] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using hybrid-hyper chaotic system and binary masking technique," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 6331-6349, 2022.
- [21] D. Shah, T. Shah, M. M. Hazzazi, M. I. Haider, A. Aljaedi and L. Hussain, "An efficient audio encryption scheme based on finite fields," *IEEE Access*, vol. 9, pp. 144385-144394, 2021.
- [22] G. Li, X. Xu, and H. Zhong, "A image encryption algorithm based on coexisting multi-attractors in a spherical chaotic system," *Multimedia Tools and Applications*, vol. 81, no. 22, pp. 32005-32031, 2022.
- [23] Aenugu Mahesh Reddy and N. Ramana Reddy, "Design and Evaluation of a Natural Language-Based Chatbot for Smart Farming Advisory Services," *FMEP*, vol. 1, no. 3, pp. 53-65, 2025
- [24] H. Ge, G. Chen, H. Yu, H. Chen and F. An, "Theoretical analysis of empirical mode decomposition," *Symmetry*, vol. 10, no. 11, p. 623, 2018.
- [25] 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.