IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AUDIO ENCRYPTION USING MODIFIED CHAOTIC MAPS AND DNA ENCODING FOR SECURING AUDIO TRANSMISSION

Authors:

Ms. Lina Nandanwar
Department of Mathematics,
Fergusson College(Autonomous),
Pune, India

Ms. Pooja Rathi
Department of Mathematics,
Fergusson College (Autonomous),
Pune, India

Mrs. Vrushali Limaye
Department of Mathematics,
Fergusson College(Autonomous),
Pune, India

ABSTRACT

The proposed research is based on a smart strategy for encrypting audio files using Chaotic map and DNA Encoding. It targets the important parts of sound to protect from unethical use. Chaotic map puzzles hackers and DNA adds a layer of mystery, making it very secure indeed.

Algorithm is tested for various statistical test like correlation analysis, information entropy analysis, scatter plots diagrams, histogram, mean squared error, PSNR and NIST tests, these show it's strong and dependable. A great thing is, once you decode the audio, it sounds just as good as before. So, if you're into sharing secret tunes, this approach suits you well.

Keywords : Sound scrambling, DNA encoding, Multimedia data, Henon map, Hybrid chaotic map

I. INTRODUCTION

Advancements in computer and communication technologies have resulted in fast-growth of digital data transmission, leading to the need of robust protection mechanisms to secure sensitive multimedia contents (e.g., audio data). As cyberattacks and unauthorized access are becoming more common, encryption methods are critical for maintaining the confidentiality and integrity of this data [1], [2], [3]. Although modern cryptographic algorithms like DES, AES, and LFSR remain relevant across numerous domains, they are typically intensive in computation and costly for use in a cryptographic system with large audio files [3], [4]. This redundancy highlights the need for optimized and secure encryption methods suitable for multimedia data such as audio.

Several recent studies discuss utilizing chaotic map to propose new cryptosystems based on chaotic behavior and the initial value dependent sensitivity of chaotic systems. These distinctive features render chaotic maps very appropriate for cryptographic applications after [5], [6], [7] since they ensure an adequate amount of randomness and unpredictable behavior. Although high-dimensional (HD) chaotic maps can enhance security by complex data distribution and improved resistance to attacks, but their computational cost restricts their use [8], [9]. In contrast, onedimensional (1D) chaotic maps require low complexity during implementation but have downsides such as predictability and malicious attacks with [10], [11].

In order to address these issues, researchers have proposed improving the performance of 1D chaotic maps using methods such as cascading systemsand switching between chaotic maps methods [13], [14], [15]. Additionally, integrating DNA encoding with chaotic map systems has proven effective in enhancing the complexity and randomness of encryption schemes that are less vulnerable to attacks [3], [16]. In [5], [17], the joint application of chaotic maps and DNA encoding has been demonstrated to be particularly efficient in audio data encryption.

A novel audio encryption framework is proposed based on modified chaotic maps and DNA encoding. By utilizing the high entropy generation of chaotic maps along with the intrinsic complexity of DNA encoding, the proposed framework presents a very low-complexity and high-security system for audio data. Moreover, selective encryption is employed to minimize the use of resources by concentrating on critical sections of the audio data like peaks, thus ensuring the audio integrity. This method decreases workloads while preserving the strongest security by encrypting the most sensitive data portions.

The vital commitments of this work are as per the following:

1. Development of a hybrid encryption framework combining modified chaotic maps and DNA encoding for securing audio data.
2. Implementation of selective encryption to target critical audio segments, reducing processing overhead while maintaining high security.

3. Comprehensive validation of the proposed scheme through metrics such as Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), and the NIST Statistical Test Suite [18], [19].

II. METHODOLOGY

A. Basic Method: Affine Cipher

The Affine Cipher is a substitution cipher that applies a mathematical transformation to every audio sample. The transformation is described by the subsequent equation:

$$T(s) = ((p.s) + q) mod L$$

Where,

- T(s) is the converted (encrypted) audio sample.
- s is the original audio sample, represented as a numerical value.
- p and q are the keys used for encryption.
- L is the modulus, commonly the range of values for audio samples (e.g., 256 for 8-bit audio facts).

Process:

- Convert the audio sample values into numerical layout (if not already in numeric shape).
- Apply the Affine Cipher transformation to every audio sample with the use of the equation above.
- The audio samples are transformed into new encrypted values that obscure the original audio facts.

Example

If we've got an audio pattern price s = 65, with keys p=5 and q=3 and L=256, the encrypted value T(s) can be:

T(65)=(5·65 + 3)mod256=328mod256= 72

Thus, the transformed audio sample is 72.

Limitation

- The Affine Cipher is simple and susceptible to bruteforce assaults due to the fact it could be effortlessly cracked whilst the keys p and q are recognized or guessed.

B.Increasing Complexity: Permutation Cipher The Permutation Cipher is a more advanced cipher where the audio samples are shuffled according to a permutation key. This key rearranges the samples in a non-linear order so you can't directly read the audio data without the key.

Process

1. A key is generated which is usually a random sequence of numbers that tells us how the audio samples will be rearranged.
2. Each audio sample in the sequence is mapped to a new position according to the permutation key. The transformation of the sample sequence a=(a1,a2,…,an) is done by :

$$R(a) = \pi(\mathrm{k})$$

Where,

- $a$is the original audio sequence.
- π(k) is the permutation function, defined by the key k.

The permutation shuffles the samples, so it's hard to recognize.

Example

If the original audio sequence is a=[65,72,80,90] and the permutation key is k=[3,1,4,2], the shuffled sequence R(a) will be:

R(a)=[80,65,90,72]

Notes

- The Permutation Cipher doesn't change the data itself but just shuffles it. If you get the key, you can get the original sequence back.

C. Transition to Chaotic Maps for Enhanced Security To further strengthen the encryption process, chaotic maps were introduced into the framework. These maps, rooted in chaos theory, are capable of generating highly sensitive and unpredictable sequences, making them ideal for robust encryption. The inherent randomness of chaotic maps, coupled with their deterministic properties, makes them resilient to cryptographic attacks. A slight change in the initial parameters can lead to vastly different outputs, providing an added layer of security, as visualized in **Figure 1.**

a. Logistic Map

The Logistic Map is a well-known chaotic system frequently employed in encryption due to its sensitivity to initial conditions. Its behavior is described by the following transformation :

$$z_{n+1} = \mu z_n(1 - z_n)$$

Where,

- z_n: Current value, constrained within the range [0,1].
- μ : Control parameter, varying between 0 and 4.
- z_{n+1}: Next value in the sequence.

The behavior of the Logistic Map changes significantly as μ varies:

- For 0 < μ <1 : The values decrease and converge to zero, exhibiting no chaotic behavior. For 1 ≤ μ < 3 : The sequence stabilizes at a constant value.
- For 3 ≤ μ < 3.57 : Oscillations appear, doubling in frequency as μ increases.
- For 3.57 ≤ μ <4 : The sequence enters a chaotic regime, exhibiting extreme sensitivity to initial conditions.
- At μ = 4 : Maximum chaos is achieved, though some specific initial conditions may result in periodic outputs. **Process**

1. **Start with an Initial Value:** Pick a starting number (z_0), which is often chosen randomly.
2. **Generate the Sequence:** Use the Logistic Map equation iteratively to create a series of values.
3. **Chaotic Behavior:** The sequence depends heavily on the starting value z_0 and the parameter μ, making it unpredictable without knowing these specifics.

Rationale

- **Sensitivity to Initial Conditions:** Even a tiny change in the starting value z_0 can completely change the sequence. This ensures that without the exact z_0 and μ, it's almost impossible to guess or replicate the sequence.
- **Simplicity and Effectiveness:** The Logistic Map is a straightforward mathematical tool, but it's powerful enough to generate highly random and unpredictable sequences. That's why it's a great

choice for encryption—it adds complexity without being computationally heavy.

b. Modified Chaotic Map

The Modified Chaotic Map extends traditional chaotic systems by introducing customized parameters to amplify randomness and complexity. The transformation follows this equation:

$$w_{n+1} = 1 - 2\,(\cos(\gamma.\cos(w_n)e_{|\epsilon|.\gamma.\cos(w_n)})2$$

Where,

- w_n : Current value in the sequence. ▪ γ: Control parameter that influences the system's sensitivity.
- ϵ : An additional term to inject randomness. Key characteristics include:
  - γ = 3: Increases unpredictability and randomness, making the sequence highly secure for encryption.
  - Initial condition $w_1 = 0$: A slight variation in this starting value results in vastly different sequences, enhancing security further.

Process:

1. **Start with an Initial Value:** Pick a starting number (w_0) to begin creating the sequence.
2. **Create the Chaotic Sequence:** Use asimple formularepeatedlyto generate a series of numbers that behaveunpredictably.
3. **Boost the Randomness:** Adjust theextra parameters(γ and ϵ) to makethe sequence evenmore randomand complex. **Rationale:**

- **Better-Randomness-:** Adding parameters like γ and ϵ creates sequences with more variation than simpler maps like Logistic or Henon. This extra randomness makes it great for cryptography, where unpredictability is key.
- **Super Sensitive to Starting Values :** Tiny changes in the starting number or parameters can lead to completely different results. This makes it nearly impossible for someone to figure out the sequence without knowing the exact starting value and settings.
- **Extra-Security-:** The additional parameters make the whole process more complex and harder to crack. This added layer of security ensures that the data stays protected and unpredictable.

c. Henon Map

The Henon Map is a two-dimensional chaotic system often employed in cryptography for its complex, non-linear behavior. It generates points in a sequence using these equations:

$$v_{n+1} = 1 - \alpha v_n^{\,2} + w_n$$

$$w_{n+1} = \beta v_n$$

Where,

- (v_n, w_n) : Current point in the sequence.
- α : A parameter controlling the chaotic dynamics (typically set to 1.4).
- β : A parameter ensuring stability (commonly set to 0.3).

Behavior based on parameters:

- For α<1.4 : The system exhibits repetitive and predictable patterns.
- Around α=1.4 : The sequence becomes chaotic, producing non-repeating values that react sensitively to small changes in initial conditions.
- For β≈0.3 : Ensures the sequence remains within a bounded range while maintaining randomness.

Process :

1. **Initialization:** The Henon Map requires two initial values, v_0 and w_0, which are set as starting points for the sequence generation.
2. **Iterative-Computation:** Using the Henon Map equations:

$$v_{n+1} = 1 - \alpha v_{n\ 2} + w_n$$

$$w_{n+1} = \beta v_n$$

the sequence is iteratively calculated. Here, a and b are parameters that influence the behavior of the map.

3. **Two-Dimensional-Dynamics:** The Henon Map operates in two dimensions, with the interdependence of v and www creating a sequence of points that exhibit complex and non-linear behavior. **Rationale :**

1. **Higher Complexity through Two-Dimensional Interactions:** The Henon Map generates sequences that are more intricate and unpredictable due to its two-dimensional nature. This complexityenhances encryption strength by reducing the likelihood of pattern recognition or correlation to the original data.
2. **Sensitivity to Initial Conditions and Parameters:** The chaotic nature of the Henon Map ensures that even slight changes in initial values (v_0 and w_0) or parameters (a and b) result in vastly different sequences. This sensitivity is crucial for encryption, as it prevents unauthorized reconstruction of the sequence.
3. **Advantage Over One-Dimensional Maps:** Compared to simpler chaotic maps, such as the Logistic Map, the Henon Map offers greater variability and randomness. Its two-dimensional structure provides enhanced unpredictability, making it a more suitable choice for applications requiring robust cryptographic security.

D. Biologically-Inspired DNA Encryption System for Enhanced Security

For advanced encryption complexity, we propose a novel **DNA Encryption System**. In this system, digital data, specifically audio data, is encoded using the four nucleotide bases (A, T, C, G) of DNA. Initially, binary data is translated into DNA sequences using a custom encoding method, followed by the application of advanced DNA operations to enhance security, as visualized in **Figure 2.**

Binary-to-DNA Encoding Process:

In this step, binary data is mapped to DNA sequences. Each binary digit is mapped to a specific nucleotide as follows:

- 0 → A
- 1 → T ▪ 2 → C
- 3 → G

To expand this concept to larger binary groups, we can also map two binary digits to a nucleotide base, as shown below:

- 00 → A
- 01 → T ▪ 10 → C ▪ 11 → G

This encoding scheme can be generalized for larger binary groups for more complex data encryption.

Complementary Base Rules:

Once the binary data has been encoded into DNA sequences, complementary rules are applied to introduce further obfuscation:

- A ↔ T
- C ↔ G

These complementary transformations replace each nucleotide base with its corresponding pair, enhancing the encryption. For instance, an encoded sequence ATCGbecomes TAGC after applying these complementary rules.

Mapping Audio Data to DNA:

Binary audio data is first converted into DNA sequences using the above mapping rules. Then, the complementary base pair rules are applied to further enhance security and obscure the original data.

XOR-based Encryption with Chaotic Sequences

To further strengthen the security of the encryption process, **XOR operations** are performed between the DNA-encoded data and a chaotic sequence. This chaotic sequence is generated from a chaotic map, such as the **Logistic Map** or **Henon Map**. The XOR operation between the DNA-encoded value and the chaotic sequence introduces a randomization effect that is difficult to reverse without the correct decoding method and chaotic sequence parameters. Let us represent this operation mathematically as follows:

$$Yi = Di \oplus Pi$$

Where,

- Yi is the transformed value after the XOR operation, corresponding to the modified DNA sequence.
- Di is the DNA-encoded value at position i in the sequence.
- Pi is the corresponding chaotic sequence value at position i.

E.Dual-Layer Encryption: DNA Encoding and Chaotic Maps

In this encryption method, binary data is first transformed into DNA sequences. Each pair of binary digits is matched with one of the four DNA bases: A, T, C, or G. To make the encryption stronger, a complementary rule is applied. For instance, each base is swapped with its counterpart—A becomes T, and C becomes G. This step adds an additional layer of complexity and makes the data harder to decipher.

Next, a chaotic map, such as the Logistic or Henon Map, is used. These maps generate complex and unpredictable sequences, which are then applied to modify the DNAencoded data. This introduces another level of randomness, ensuring that the encrypted data remains secure unless the exact DNA encoding scheme and chaotic map parameters are known.

By combining DNA encoding and chaotic mapping, we achieve a dual-layer encryption system. This means that even if one layer is compromised, the other layer still provides strong protection, making it incredibly difficult for anyone to decrypt the data without having access to both the DNA encoding rules and the chaotic map details.

Finally, the DNA-encrypted audio data undergoes one more step: an XOR operation with the sequence generated by the chaotic map. The final encryption is calculated as follows:

$$Enc_{Final} = Enc_{DNA} \oplus Seq_{chaos}$$

Where,

- $Enc_{Final}$is the final encrypted output.
- $Enc_{DNA}$is the DNA-encrypted audio data. ▪ $Seq_{chaos}$is the sequence created using the chaotic map.

This XOR operation further enhances security by adding another unpredictable layer. Even if someone knows the DNA encoding method, decrypting the data without the correct chaotic map parameters becomes nearly impossible. **Figure 3** provides an illustration of this final encryption step.

KEY BENEFITS OF USING CHAOTIC MAPS AND DNA ENCODING IN AUDIO ENCRYPTION

The use of chaotic maps and DNA encoding in the encryption process significantly strengthens the security and resilience of audio data encryption.

Chaotic Maps:

1. **Unpredictability**: Chaotic maps create keys that are extremely sensitive to initial conditions, which means that even the slightest change can lead to a completely different encryption key. This unpredictability makes it much harder for attackers to anticipate or replicate the encryption keys, thus enhancing the overall security.
2. **Large Key Space**: The wide variety of possible initial conditions in chaotic maps results in an enormous key space. This plays a crucial role in thwarting brute-force attacks, as it drastically increases the number of possible keys that would need to be tested.

Example: Maps like the logistic or henonmap generate sequences with highly complex, non-linear behavior. This ensures that the encryption process is resistant to attacks based on statistical patterns, making it much more secure than simpler encryption methods.

DNA Encoding:

1. **Increased Complexity**: DNA encoding converts numerical data into a symbolic form using characters like A, T, C, and G. This adds an additional layer of complexity to the encryption process, making it harder to decode without the specific rules of encoding.
2. **Parallelism**: DNA encoding allows for parallel processing of the data, which boosts the efficiency of the encryption process. This means that encryption can happen more quickly, even for large data sets, without compromising security. **Example:** When audio data is encoded into DNA and encrypted using chaotic keys, the result is a much more intricate and layered data structure compared to traditional numeric encryption methods. This added complexity makes it significantly more challenging for unauthorized parties to break the encryption.

III. EFFICIENT SELECTIVE AUDIO ENCRYPTION LEVERAGING CHAOTIC MAP SEGMENTATION

Encryption of audio data is crucial for securing sensitive audio information against unauthorized usage. However, conventional audio encryption methods manipulate the whole audio file and incur more computational costs due to the need to process the entire data, which can be resource-intensive and time-consuming, especially for large or high-quality audio files.With this work, we develop a new selective encrypting method that specifically targets the most essential part of the audio signal. As illustrated in **Figure 5**, the proposed approach balances computational efficiency with data protection, by selectively targeting the segment before the peak.

Process Overview

The particular sound encryption procedure is organized as follows: **1. Peak Recognition**

The primary to do is to search for the sound sign pinnacle, the most elevated top. This pinnacle is a limit where the basic (non-encoded) fragment closes and the scrambled portion starts.

2. Segment Extraction

Subsequent to recognizing the top, next, the sound section from the very start of the sign to the pinnacle is extricated. This piece of the sound is considered delicate and is focused on encryption to guarantee the security of the main piece of the sign.

3. Encryption Interaction

- Standardization: Prior to handling, the extricated portion is standardized so the adequacy levels are uniform across the whole sign.
- Chaotic Map Key Generation: A tumultuous guide is utilized for creating pseudo-irregular grouping which is then utilized as encryption key.
- XOR Activity: The standardized fragment is XORed with the new turbulent grouping to create the encoded portion.

4. Reintegration

After encryption, the adjusted (encoded) section is reintegrated with the leftover piece of the first sound sign (from the pinnacle ahead). This interaction guarantees that the encryption is applied exclusively to the delicate part of the sound, leaving the remainder of the sign in one piece.

5. Visualization

At long last, waveform plots of both the first and encoded sound signs are created. These perceptions help to evaluate the encryption's adequacy, representing the way that the designated fragment has been randomized while guaranteeing the decoded segments stay unaltered.

IV. ANALYSIS TECHNIQUES IN ENCRYPTION

A. Mean Square Error (MSE)

The Mean Square Error (MSE) is a measurement used to evaluate the distinction between the first and encoded information by computing the normal of the squared deviations. It evaluates how much the scrambled information contrasts from the first.

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

Where,

- O_i is the value from the original data.
- E_i is the comparing esteem from the scrambled information.
- $N$is the complete number of pieces of information.

Interpretation

A higher MSE indicates that the encryption effectively obscures the original data, making it more difficult for unauthorized parties to decipher.

Threshold

While there is no strict threshold, a higher value relative to the original data range demonstrates effective encryption.

B. Entropy

Entropy measures the degree of randomness or uncertainty in data. Higher entropy values imply better randomness in the encrypted data, which is desirable for cryptographic security. The entropy formula is:

$$H = -\sum_{i=1}^{M} P_i.\log_2 P_i$$

Where,

- $H$is the entropy (measured in bits).
- $P_i$is the probability of occurrence of the i^{th}symbol in the data.
- $M$is the total number of unique symbols in the data.

Interpretation

For an ideal 8-bit system, the entropy value should be 8, indicating maximum randomness, where all symbols are equally likely. **Threshold**

- H≥7. 8: Sufficient randomness for encryption.
- H<7 : Indicates patterns in the encrypted data, reducing security.

C. Histograms

A **Histogram** visually represents the frequency distribution of data points. In the context of encryption:

- **For Original Data**: Patterns or periodic structures might be visible.
- **For Encrypted Data**: A flat, uniform histogram indicates high randomness, which is ideal for encryption.

Interpretation

A well-encrypted dataset should have a histogram with values evenly spread across all possible ranges, showing no recognizable patterns.

Threshold

A **flat and uniform histogram** is desirable, as it shows all possible values occur with roughly equal probability.

D. Scatter Plots

Scatter plots show the relationship between the original and encrypted data. It is plotted as a series of points:

- Horizontal axis (X): Original data values.
- Vertical axis (Y): Encrypted data values.

Interpretation

- If encryption is strong, the points in the scatter plot appear randomly scattered without any noticeable pattern.
- If encryption is weak, the points align in a line or curve, revealing a relationship between the original and encrypted data.

Threshold

Complete randomness in the scatter plot suggests the absence of correlations, which is ideal.

E. Correlation Coefficient

The **Correlation Coefficient** measures the linear relationship between two datasets. It is calculated using:

$$R = \frac{\sum(X_i - X)(Y_i - Y)}{\sqrt{\sum(X_i - X)^2 . \sum(Y_i - Y)^2}}$$

Where,

- X_i , Y_i is the data values from the original and encrypted datasets, respectively.
- X, Y is the mean values of X and Y.

Interpretation

- R ≈ 0: Weak or no correlation (ideal for encryption).
- R ≈ ±1: Strong correlation (undesirable for encryption).

Threshold

- |R|≤0.1: Acceptable randomness and encryption quality.
- |R| ≥ 0.9 (decrypted vs. original): Ensures data fidelity post-decryption.

E. NIST Successful Test

The NIST suite includes several tests to evaluate the randomness of encrypted data. Here are the key ones:

a. **Frequency Test**: Ensures that the number of 0s and 1s in the binary sequence is roughly equal, indicating uniformity in the sequence.
b. **Runs Test**: Evaluates whether sequences of identical bits (runs) occur as expected in a random sequence.
c. **Approximate-Entropy-Test-**: Measures the complexity and randomness of a sequence by comparing the frequency of overlapping patterns of all lengths.
d. **Cumulative Sums Test (Cusum)**: Checks for deviations from randomness by summing values in the sequence cumulatively.

Threshold

Passing all NIST tests confirms the encrypted data's randomness and suitability for secure cryptography.

F. Signal-to-Noise Ratio (SNR)

The Signal-to-Noise Ratio (SNR) is an action used to measure the degree of sign strength comparative with foundation clamor. In encryption, it is utilized to assess how much clamor has been presented during the encryption cycle.

The equation for SNR is:

$$SNR = \frac{\text{Noise Power}}{\text{Signal Power}}$$

Where,

- Signal Power alludes to the force of the first information.
- Noise Power refers to the power of the difference between the original and encrypted data.

Interpretation

- A higher SNR esteem demonstrates less clamor and a more grounded encryption process, it is very much protected to suggest that the first information.
- A lower SNR proposes that the encryption interaction has presented critical commotion, which might make decoding troublesome.

Threshold

Higher SNR values are better, with values more like 1 being great, showing a negligible commotion influence. An exceptionally low SNR might flag a wasteful encryption process.

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

The Peak Signal-to-Noise Ratio(PSNR) is a variation of SNR, explicitly intended for looking at the nature of information (like pictures or sound) after encryption. It is determined by estimating the pinnacle blunder between the first and encoded information, standardized by the greatest conceivable pixel (or test) esteem.

The formula for PSNR is:

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

Where,

- MAX is the most extreme conceivable pixel esteem (e.g., 255 for 8-cycle pictures).
- MSE is the Mean Square Mistake between the first and scrambled information.

Interpretation

- A higher PSNR esteem shows that the scrambled information is nearer to the first, meaning the encryption insignificantly affects the information's quality.
- A lower PSNR recommends that the encryption has fundamentally modified the first information, which might show shortcomings in the encryption cycle.

Threshold

PSNR values more prominent than 30 dB are by and large thought to be great, with values over 40 dB showing astounding encryption execution, where the encoded information intently looks like the first information.

ENSURING QUALITY OF DECRYPTED AUDIO

A few of the important metrics to ensure quality decrypted audio are:

Objective Measurements:

- Signal-to-Noise Ratio (SNR) and Peak Signal-toNoise Ratio (PSNR): The higher the value, the less the distortion and the decrypted audio would match the original audio.
- MSE: The lower the value, the less quality lost in encryption and decryption.
- Correlation, The original signal and the decrypted signal will have a high correlation with each other, indicating effective decryption without changing many things.
- Information Entropy: The information entropy value of the original audio and the decrypted audio is close, which shows that the randomness and structure of the audio after decryption still exists.

Before and After Encryption Comparison:

The comparison using metrics such as SNR, PSNR, MSE, and correlation gives us a clear picture of the minimal quality loss experienced by decrypted audio.

Simulation Results:

Simulations evaluate decryption reliability in the presence of noise, and minor loss of data bits, reaffirming robustness of the method, and consistency across different audio types, such as speech and music.

V.NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Interestingly, the NIST Statistical Test Suite (STS) includes a group of evaluations created by the National Institute of Standards and Technology (NIST). These evaluations assess how unpredictable a sequence of binary digits (a string made of 0s and 1s) appears. Randomness plays a key role in cryptography: it guarantees that keys or numbers produced for coding are not easy to guess. **Why is the NIST test suite important?**

In simple terms, cryptography uses sets of 0s and 1s to hide information. If these sets lack randomness, there's a risk that people with bad intentions might spot patterns and uncover the hidden message. The NIST test suite helps experts check if their sets look like random patterns.

What does it test?

Interestingly, the suite has 15 unique tests to evaluate randomness:

- Frequency test: This checks if the amount of 0s and 1s is roughly equal.
- Block frequency test: Divides the set into parts – checks if each has a fair share of 0s and 1s.
- Runs test: Counts how often 0s or 1s repeat in groups (for instance, 000 or 111).
- Longest run test: Finds the longest repeat of 1s in a section.
- Rank test: Checks if a grid made from the set is complex (just enough).
- Spectral test: Searches for repeating designs in the set.
- Template matching test: Searches for certain designs within the set.
- Entropy Test: Checks if patterns repeat too often.
- Cumulative Sum Test: Tracks the balance between 0s and 1s as the sequence progresses.
- Random Walk Tests : Simulates a random walk based on the sequence and checks its behavior.

How It Works

You input a sequence of 0s and 1s into the test suite, and it performs all these tests. Each test gives a p-value, a number that tells you how random the sequence is. If the p-value is greater than 0.01, the sequence passes that test. If not, it means the sequence might have patterns and isn't random enough.

Where It's Used

To test random number generators in cryptography. To ensure encryption systems are secure. To verify that sequences used in scientific experiments are truly random.

Limitation

The NIST Test Suite doesn't guarantee absolute randomness. It only checks statistical randomness based on specific tests. Also, the tests require a very large number of bits (often millions) to give accurate results.

VI. ANALYSIS OF RANDOMNESS IN ORIGINAL AND ENCRYPTED AUDIO DATA

This segment assesses the viability of the proposed sound encryption strategy by dissecting the haphazardness in the first and scrambled sound signs. The investigation incorporates (1) looking at the string design portrayal of the information (**Table 1**), (2) ascertaining the connection between the first, scrambled, and unscrambled signals (**Table 2**), (3) approving arbitrariness utilizing the **NIST Statistical Test Suite** (**Table 3**).(4) To assess wholesome metrics of the encoded information (**Table 4**), (5) Performing entropy and correlation analyses (**Table 5**), and (6) Analyzing the texture characteristics of the scrambled signal (**Table 6**), (7) envisioning waveforms and disperse plots, and (8) histogram analysis of audio data before and after hybrid encryption.

1.String-Format-Representation:

Table 1 analyzes the first and encoded sound information in string design. The critical change in the scrambled information shows fruitful encryption, disturbing the first sign design.

2. Correlation-Examination :

Table 2 shows the connection between the first, encoded, and unscrambled signals. A low connection between the first and encoded signals affirms successful interruption, while a high relationship between the scrambled and decoded signals shows information respectability during unscrambling.

3. NIST Measurable Experimental outcomes :

To quantitatively survey the arbitrariness of the scrambled information, we utilize the NIST Factual Test Suite. The outcomes, summed up in **Table 3**, show the presentation of the scrambled sound in breezing through different haphazardness assessments, for example, Frequency (Monobit) Test, Runs Test, Approximate entropy Test, Linear Complexity Test. The fruitful finishing of these assessments shows that the scrambled sound areas of strength for displays, making it strong to measurable investigation and likely cryptographic assaults. The NIST test results approve the vigor and security of the encryption technique.

The results of the NIST Statistical Test Suite, as outlined by the National Institute of Standards and Technology (NIST, 2018), confirmed that the encrypted data exhibited high randomness, making it resistant to statistical and cryptographic attack.

4. Error Metrics Analysis :

Evaluations of measure for errors such as MSE, SNR and PSNR are as presented in **Table 4** for encrypted audio data. These measures describes how much the distortion introduced during encrypting the sensitivity. As we can see from the low MSE and high PSNR values, there is little loss of data integrity, guaranteeing reliable encryption methods.

5. Entropy and Correlation Analyzation: The entropy and correlation tests of original and hybrid encrypted audio data are summarized in Table 5. This higher entropy within the ciphered data indicates greater randomness, and the correlation metrics lend credence to the notion that the encryption was enough to destroy the underlying structure.

6. Texture Analysis Based Hybrid Encryption:

Table 6 summarized the Texture Analysis for Hybrid Encryption (Contrast and Homogeneity), used to indicate the noise, and uniformity, of the ciphered wave.

7. Waveform and Scatter Plot Perception : In Figures 1, 2, and 3, it showcased audio data of different encryption methods. Distortion of the amplitude and frequency structure of the original signal due to chaotic maps encryption is presented in Figure 1. DNA-based encryption, as shown in Figure 2, adds complexity to the modified audio, thus improving the level of data security. The scatter plot of original audio (x-axis) vs encrypted audio (y-axis) after using hybrid encryption is shown in figure.3 which indicates the randomness of encrypted audio and the increase in security.

These perceptions further show how the encryption interaction changes the sound sign into a more randomized structure, guaranteeing the security of the information.

8. Histogram Analysis of Audio Data Before and After Hybrid Encryption

Finally, as illustrated in **Figure 4**, histogram analysis of audio data samples is presented to demonstrate changes in distribution post-encryption in comparison to raw audio data samples, affirmingthe efficiency of the hybrid encryption process in providing an adequate level of obfuscation for the audio data set. These visualizations together prove how well the encryption applied randomizes the audio dataand generates Secure Encryption.

Table 1:String Format Representation of Original and Encrypted Audio Data

Sr.No.	Methods	String format for Original Audio Data	String format for Encrypted Audio Data
1.	Affine Cipher	0, 0, 0, 0, 0, ….	0.17969, 0.17969, 0.17969, ….
2.	Permutation Cipher	327667, 327667, 327667, ….	327667, 327667, 327667, ….
3.	Chaotic Map(Logistic Map)	422, 422, 422, 422, 422, 422, 422, 422, 422, 422, ...	32329, -32283, -32607, -31307,28255, -16969,13937, ….
4.	Chaotic Map(Modified Chaotic Map)	422, 422, 422, 422, 422, 422, 422, 422, 422, 422, ...	7338, -29605, -20793, 6366, 23335, 21277, 3515, ….
5.	Chaotic Map(Henon Map)	0.012885,0.012885,0.012885,0.012885,….	-0.001680, -0.541444,0.043658, 0.917322,0.286073, ….
6.	DNA Encoding	0.0039216, 0.0039216, 0.0039216, 0.0039216, ...	0.67059, 0.67059, 0.67059, 0.67059, 0.67059, ….

Table 2 :Correlation Metrics Between Original, Encrypted, and Decrypted Audio Signals

Sr.No.	Methods	Correlation Between Original Audio and Encrypted Audio	Correlation Between Original Audio and Decrypted Audio
1.	Affine Cipher	0.6747	0.9822
2.	Permutation Cipher	0.092851	0.99998
3.	Chaotic Map(Logistic Map)	-0.01922	1
4.	Chaotic Map(Modified Chaotic Map)	-0.0377	1
5.	Chaotic Map(Henon Map)	0.0091992	1
6.	DNA Encoding	0.55362	1

Table 3 : Analysis of Randomness in Original and Encrypted Audio Data Using Statistical Testing

Sr No.	NIST test	Result value (P-value)	Status
1.	Frequency (Monobit) Test	0.0413	Successful
2.	Frequency Test within a block	0.9365	Successful
3.	Runs Test	0.3181	Successful
4.	Test for the longest run of Ones in a block	0.0871	Successful
5.	Non-Overlapping template	0.0248	Successful
6.	Binary Matrix Test	0.6598	Successful
7.	Maurer's Universal Statistical Test	0.2821	Successful
8.	Linear Complexity Test	0.7326	Successful
9.	Serial Test	P-value 1:0.0763 P-value 2:0.3211	Successful
10.	Approximate entropy Test	0.0835	Successful
11.	Cumulative sums(cusum)Test	P-value Forward:0.0477 P-value Reverse:0.07234	Successful

Table 4 : Error Metrics for Audio Data Using Hybrid Encryption

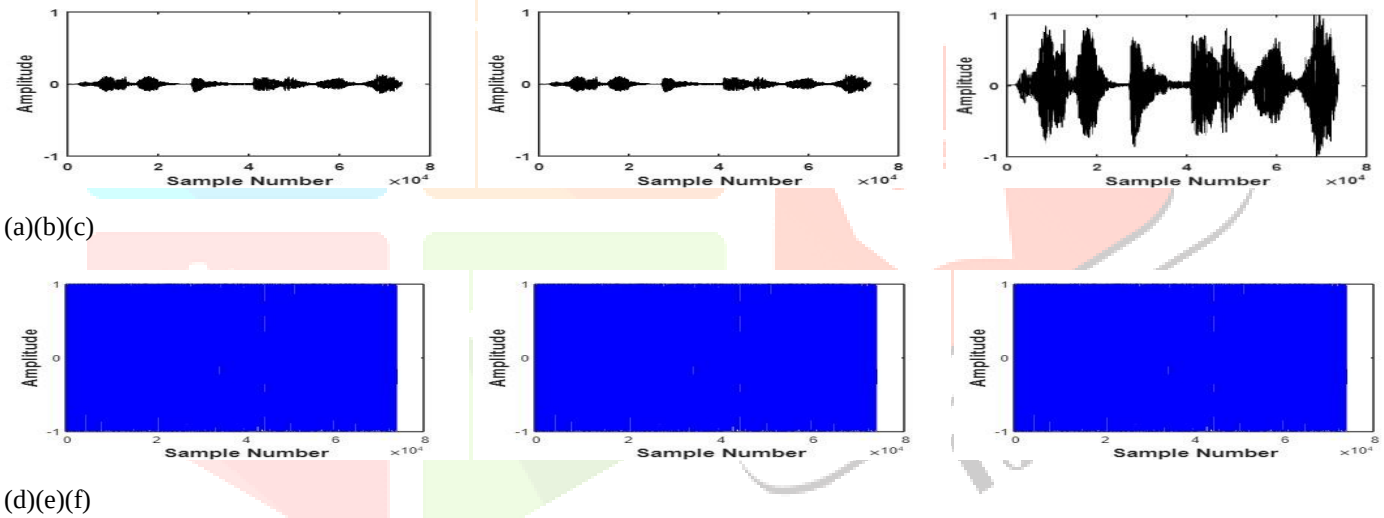
Metric	Value	Description
MSE	0.1360	Measures the average squared difference between original and encrypted signals.
SNR	8.6640	Evaluates the quality of encrypted audio relative to the original.
PSNR	-23.8661	Assesses the amount of noise introduced by hybrid encryption.

Table 5 :Entropy and Correlation Analysis of Hybrid Encrypted Audio Data.

Metric	Original Audio	Encrypted Audio	Description
Information Entropy	2.3838	3.9857	It shows that you have some randomness, and the higher we have encrypted data, the more secure itis.
Correlation Analysis	1.000	0.444	This computes similarity a low value for encrypted data gives state of high security.

Table 6 : Texture analysis for Hybrid encryption

Metric	Original Audio	Encrypted Audio	Description
Contrast	8.1382e-05	5.7060	Displays intensity variation within audio data frames.
Homogeneity	1.000	0.7350	Correspondence with uniformity; low values for encrypted data mean randomness.

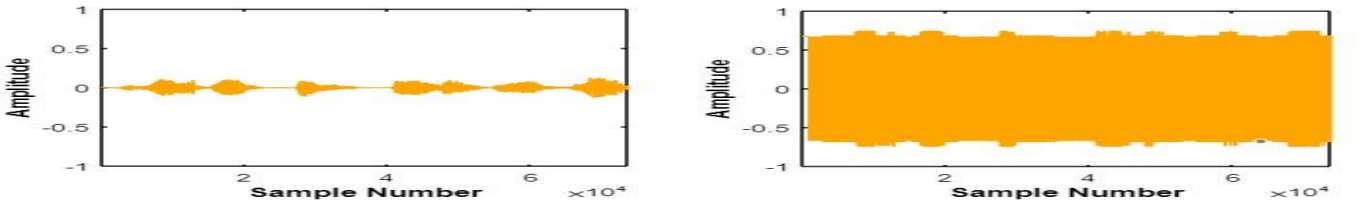


(a)(b)(c)

(d)(e)(f)

Figure 1 : Visualization of Audio Data Encryption Using Chaotic Maps

(a) Logistic Map : Original Audio Data (b) Modified Logistic Map : Original Audio Data (c) Henon Map : Original Audio Data
(d) Logistic Map : Encrypted Audio Data (e) Modified Logistic Map : Encrypted Audio Data (f) Henon Map: Encrypted Audio Data



(a) (b)

Figure 2 : Visualization of DNA-Based Audio Data Encryption Using Chaotic Maps

(a) Original Audio Data Encoded in DNA Encoding(b) Encrypted Audio Data Represented in DNA Encoding

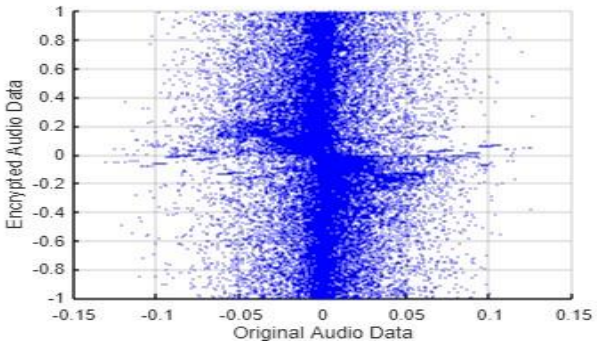
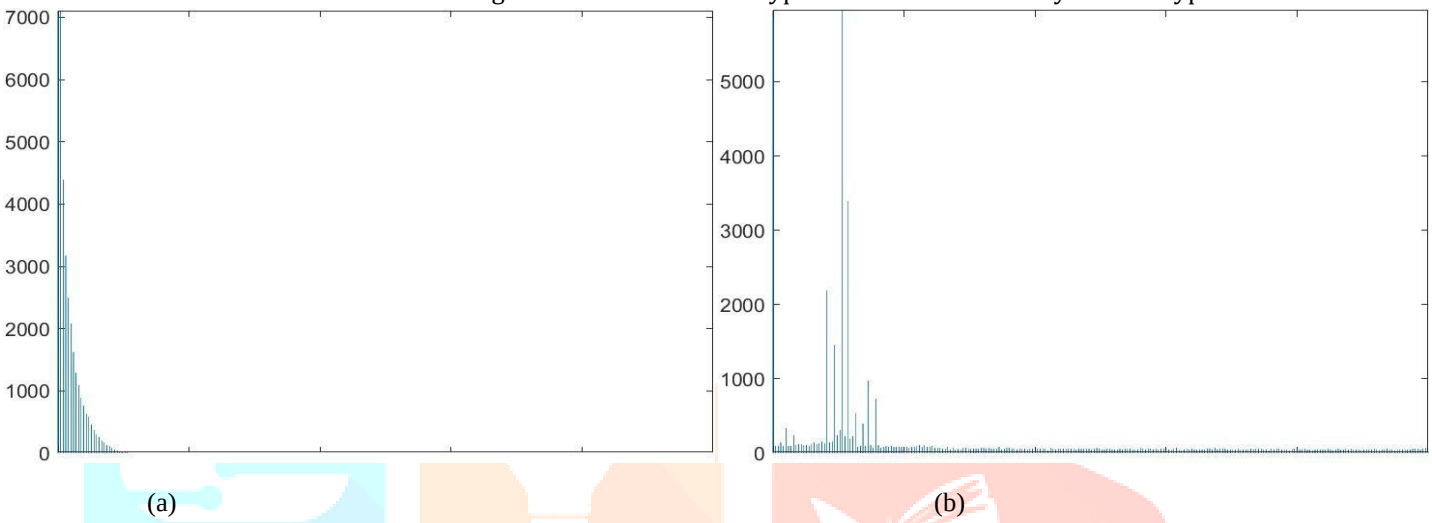
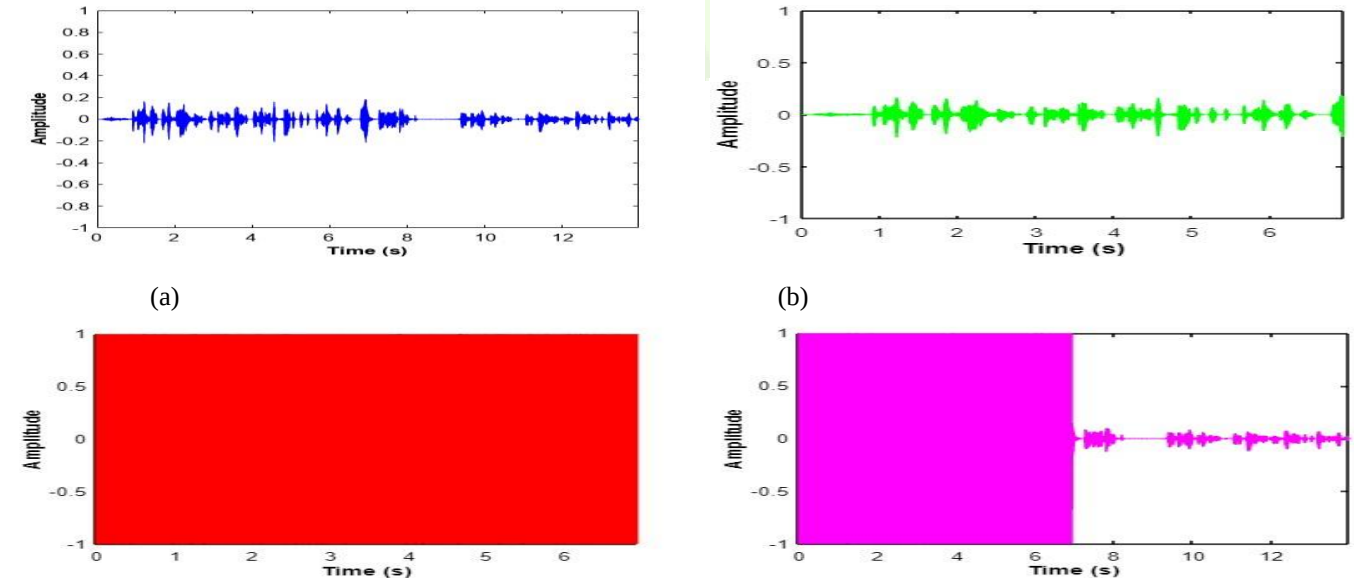


Figure 3 : Visualization of Hybrid Encryption Applied to Audio Data
Scatter Plot of Original Audio Data vs Encrypted Audio Data After Hybrid Encryption.



(a) (b)

Figure 4 : Histogram Analysis of Audio Data Before and After Hybrid Encryption
(a)Histogram of Original Audio (b) Histogram of Encrypted Audio



(a) (b)

(c) (d)

Figure 5: Waveform Comparison of Original and Selectively Encrypted Audio Signals.
(a) Shows the original audio waveform, serving as the baseline for the encryption process. (b) Illustrates the extracted audio segment before encryption, which is the focus of the selective encryption technique. (c) The extracted segment is encrypted using a chaotic map, demonstrating the transformation into a random waveform. (d) Shows the complete audio, where the encrypted segment is merged with the unaltered portion of the original signal.

VII. RESEARCH FINDINGS AND DISCUSSION

This study investigates two distinct methods of audio encryption: **whole audio encryption** and **selective audio encryption**. Both techniques were evaluated based on their effectiveness in maintaining data integrity, ensuring security, and optimizing computational efficiency.

A. Whole Audio Encryption

The entire sound encryption approach includes encoding the whole sound sign, offering a hearty answer for getting all parts of the information. By scrambling the full sign, this technique guarantees that no part of the sound can be gotten to or messed with, consequently giving an elevated degree of safety. The encryption was done utilizing a turbulent guide to produce pseudo-irregular successions, which were then joined with the sound information through XOR tasks. This strategy ensures that the whole sound sign is consistently encoded, upgrading generally speaking insurance against unapproved access.

However, one disadvantage of this approach is the expanded computational expense. Encoding the whole sign requires really handling time and assets contrasted with strategies that emphasis on unambiguous sections. Notwithstanding this, the entire sound encryption strategy performed well in the NIST measurable tests, demonstrating that the encoded sound sign displayed a serious level of irregularity and unusualness, which is basic for security. This affirms that the strategy is viable in forestalling likely assaults.

B. Selective Audio Encryption

Interestingly, the particular sound encryption strategy targets just a particular piece of the sound sign, normally the part with the most noteworthy plentifulness or other basic highlights.

This strategy essentially decreases the computational above, as it centers around encoding just the most touchy fragments of the sound. The pinnacle location system recognizes the piece of the sign that ought to be scrambled, guaranteeing that the main pieces of the sound are secured.

Although, particular encryption lessens handling time, it may not offer a similar degree of security as entire sound encryption, as parts of the sound sign remain decoded. Nonetheless, the outcomes from the NIST test suite showed that the specifically scrambled sections actually showed an elevated degree of irregularity, exhibiting that the encryption really upset the construction of the sign while keeping up with information honesty. This particular methodology finds some kind of harmony between computational proficiency and security, making it a reasonable arrangement in situations where handling time is a worry yet security can't be compromised.

C. Comparison and Implications

Both entire and specific sound encryption strategies enjoy their separate benefits. Entire sound encryption gives uniform insurance across the whole sound sign, making it reasonable for situations where most extreme security is expected, in spite of the greater computational expense. Then again, specific sound encryption offers an additional productive other option, especially in situations where asset requirements are a worry, as it centers encryption endeavors around basic pieces of the sign.

In down to earth applications, the decision between these two strategies relies to a great extent upon the particular necessities of the framework. For example, continuously correspondence frameworks or distributed storage, where computational assets might be restricted, particular encryption might offer a decent harmony among security and effectiveness. Be that as it may, for applications managing delicate or high-esteem sound information, entire sound encryption might be the favored choice because of its extensive security.

D. Future Directions

While the two strategies show solid execution, future exploration could investigate advancing the specific encryption strategy to improve its security further without compromising productivity. Furthermore, examining the capability of mixture models that consolidate the advantages of the two methodologies could prompt considerably more compelling encryption arrangements.

CONCLUSION AND FUTURE DIRECTIONS

This research presents a fresh strategy for protecting audio using chaotic maps paired with DNA schemes. It also focuses on locking key parts of audio data to keep a good balance between top-notch safety and speedy processing. The randomness from chaotic maps and the intricate design of DNA schemes make it tough for unwanted listeners to crack into the system. Tests using stuff like entropy and the links between data bits show this method can keep audio safe without messing up the quality when you listen to it after unlocking.

What to look into next for this study includes : Real-Time Encryption: Upgrading the system to handle live audio getting encrypted needs super fast and smart processing. **Hybrid Security Models:** Putting this way of doing things together with different encrypting strategies to build stronger systems with many levels of protection.

Broader Applications: Looking into how well this method works for keeping other digital stuff like pictures and clips safe to use it in all sorts of areas.

REFERENCES

1. Liu, W., & Kadir, Z. (2018). An Audio Encryption Algorithm Based on DNA Encoding and Chaotic Maps. *International Journal of Network Security, 20(4)*, 703-710.
2. Pueyo, E., Muñoz, F., & Gómez, J. (2013). Audio Encryption Using Chaotic Maps and Variable Parameters. *Signal Processing: An International Journal, 7(2)*, 15-24.
3. Roy, M., Chakraborty, S., & Mali, K. (2024). Audio encryption framework based on chaotic map and DNA encoding. *Applied Acoustics, 224*, 110152.
4. Gnanajeyaraman, R., &Prasadh, K. (2009). Audio encryption using higher dimensional chaotic map. *International Journal of Recent Trends in Engineering*, *1*(2), 103.
5. Kumar, A., & Dua, M. (2023). Audio encryption using two chaotic map based dynamic diffusion and double DNA encoding. *Applied Acoustics*, *203*, 109196.
6. Alawida, M. (2024). Enhancing logistic chaotic map for improved cryptographic security in random number generation. *Journal of Information Security and Applications*, *80*, 103685.

7. Demirtas, M. (2024, May). A Sound Encryption Method Based on Feature Extraction and a Novel Chaotic Map. In *Proceedings of the 2024 10th International Conference on Computer Technology Applications* (pp. 303-309).
8. Shah, D., Shah, T., & Jamal, S. S. (2020). Digital audio signals encryption by Mobius transformation and Hénon map. *Multimedia systems*, *26*(2), 235-245.
9. Thanikaiselvan, V., Abilash, P., Lingeswar, C., Sathya, P., Kaviya, K., Subashanthini, S., &Amirtharajan, R. (2024, June). Chaotic Audio Encryption and Decryption Using Logistic Map. In *2024 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)* (pp. 346-351). IEEE.
10. Sheela, S. J., Suresh, K. V., & Tandur, D. (2017, February). Chaos based speech encryption using modified Henon map. In *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1-7). IEEE.
11. Umar, T., Nadeem, M., &Anwer, F. (2024). Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. *Expert Systems with Applications*, *257*, 125050.
12. Aly, R. (2024). Hyperchoatic Chen System Based Audio Signal Encryption.
13. Akhtar, M. M., Singh, M., Kadyan, V., & Due, M. Enhancing Time Efficiency in Audio Encryption: A Novel Approach Leveraging Double DNA Operations within Chaotic Map-Based Schemes. *Available at SSRN 4963758*.
14. Hansen, J. H., Radhakrishnan, V., & Arehart, K. H. (2006). Speech enhancement based on generalized minimum mean square error estimators and masking properties of the auditory system. *IEEE Transactions on Audio, Speech, and Language Processing*, *14*(6), 2049-2063.
15. Pauletto, S., & Hunt, A. (2005, July). A comparison of audio and visual analysis of complex time-series data sets. In *Proceedings of ICAD 05-Eleventh Meeting of the International Conference on Auditory Display* (pp. 6-9).
16. El Hanouti, I., & El Fadili, H. (2021). Security analysis of an audio data encryption scheme based on key chaining and DNA encoding. *Multimedia Tools and Applications*, *80*(8), 1207712099.
17. Streijl, R. C., Winkler, S., & Hands, D. S. (2016). Mean opinion score (MOS) revisited: methods and applications, limitations and alternatives. *Multimedia Systems*, *22*(2), 213-227.
18. Kim, S. J., Umeno, K., & Hasegawa, A. (2004). Corrections of the NIST statistical test suite for randomness. *arXiv preprint nlin/0401040*.
19. Marton, K., & Suciu, A. (2015). On the interpretation of results from the NIST statistical test suite. *Science and Technology*, *18*(1),