

Ensuring dealer and participant truthfulness in the audio share generation and reconstruction processes for an audio secret sharing scheme

Guttikonda Prashanti ^{1*}, P Ashok Kumar ², Popuri Keerthika ³

¹ Department of Advanced Computer Science and Engineering, Vignan's Foundation for Science, Technology and Research, Vadlamudi, Guntur, AP, India

² Department of Chemical Engineering, Vignan's Foundation for Science, Technology and Research, Vadlamudi, Guntur, AP, India

³ Department of CSE, R.V.R. and J.C., College of Engineering, Chowdavaram, Guntur, AP, India

ABSTRACT

Polynomial-based secret sharing is a tool used to secure a secret that is being shared by a group of users. Dealer, through a private channel, distributes shadows of the secret to users in the group, and only the threshold number of users with their shadows can retrieve the secret. However, some users provide fake shadows so that the original secret cannot be retrieved. Identifying such cheating behavior is important while reconstructing the secret. This article introduces a novel method for audio-based secret sharing using polynomials. The proposed technique not only enables the creation of smaller-dimensional audio shares but also incorporates a mechanism to identify untrustworthy participants within the group. Our proposed method employs dual security measures to ensure the integrity and authenticity of the audio-sharing process. Firstly, our method includes a verification process to authenticate whether the dealer has indeed derived the audio share using the participant's true secret value. Through this approach, participants can ensure the integrity and authenticity of the audio shares published by the dealer. Secondly, another set of verification codes is generated to enable participants to validate each other's submitted secret values, preventing fraudulent submissions during the reconstruction process. By employing this dual approach, security is enhanced through the implementation of multiple layers of verification and authentication across the entire process.

Keywords: Checksum, Confidentiality, Discrete logarithms, Generator, Lagrange interpolation, Untrustworthy participants.

OPEN ACCESS

Received: July 12, 2024


Revised: December 23, 2024

Accepted: February 16, 2025

Corresponding Author:

Guttikonda Prashanti

drgp_acse@vignan.ac.in

 **Copyright:** The Author(s).

This is an open access article distributed under the terms of the [Creative Commons Attribution License \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted distribution provided the original author and source are cited.

Publisher:

[Chaoyang University of Technology](https://www.chaoyang.edu.cn/)

ISSN: 1727-2394 (Print)

ISSN: 1727-7841 (Online)

1. INTRODUCTION

Secret sharing emerged as an area of study within the science of information security to protect sensitive information, such as cryptographic keys, from being exploited by unauthorized parties. A threshold secret sharing consists of a dealer with a secret s , n participants called shareholders, and an access structure composed of subsets of shareholders that might cooperate to retrieve the secret. To tackle the secret sharing problem, Blakley (1979) employed the hyper plane geometry, while Shamir's (1979) solution was based on Lagrange polynomial interpolation. Threshold secret sharing is now a crucial foundation for delivering security services for several real-world applications, including cloud computing, sensor networks, IoT, Block chain etc. (Shamir, 1979; Shankar and Elhoseny, 2019; Parsa et al., 2021; Jeonghun et al., 2021).

In many secret sharing schemes, an assumption is made that participants will act honestly. However, this assumption often doesn't hold in real-world scenarios. Participants can be dishonest themselves, submitting altered or counterfeit shares instead of the original ones. This specific challenge has been tackled in the mentioned paper (Guttikonda and Mundukur, 2024).

The proposed scheme employs a method of generating audio shares that are more compact in size. These smaller shares offer advantages in terms of efficiency during storage and transmission. One of the crucial aspects of this scheme is its ability to validate whether participants have provided accurate or manipulated information even before the secret's reconstruction takes place. This pre-reconstruction verification is designed to identify dishonest behaviour at an early stage. Furthermore, the scheme adds an extra layer of security by allowing participants to confirm the legitimacy of their received shares. This process effectively eliminates the potential for the dealer to distribute deceptive or fake shares to any participant, thereby maintaining the integrity of the entire secret-sharing process (Prashanti and Nirupama, 2020).

The subsequent sections of this paper are structured as follows:

Section 1: Outlines relevant prior research concerning the proposed scheme.

Section 2: Outlines the steps of the proposed approach.

Section 3: A thorough analysis of security issues, experimental outcomes, the scheme's efficacy across various metrics, and a comparative analysis between our work and other related studies is carried out.

Section 4: Finally, encapsulates the concluding remarks and insights drawn from this study.

1.1 Related Work

Independently, Shamir (1979) and Blakley (1979) suggested a secret-sharing method to protect cryptographic keys. The secret is divided into shares while sharing a secret and distributed among a designated group of authorized individuals. The original confidential information can be reconstructed when a specified threshold of participants come to a consensus and collaboratively combine their respective shares. With s as secret and v_1, v_2, \dots, v_{t-1} as random numbers, the dealer generates a polynomial, as shown in Eq. (1). Next, the dealer evaluates the equation with identities $x_i \in [1, n]$ of members in the group to obtain shares $s_1, s_2 \dots s_n$ which are then assigned to the participants.

$$f(x) = s + v_1x + v_2x^2 + \dots + v_{t-1}x^{t-1} \text{ mod } q \quad (1)$$

Later, any t or more than t members with their shares and identities can retrieve the secret from Lagrange's interpolation equation.

Thien and Lin (2002) method is designed to securely distribute a secret image within a group while incorporating measures to reduce dimensions and add noise-like distortions to enhance security. This approach builds upon Shamir's method of secret sharing and introduces additional steps for increased confidentiality and robustness. The process begins with the dealer manipulating grayscale images to introduce noise-like patterns. This is achieved by truncating pixel values within the range of 0 to 250, and then subjecting them to a secret key-based permutation. As a result, the image takes on a noisy appearance. This noisy

image is subsequently divided into segments, each containing a specific number of pixels denoted as 't'. To generate image shares, Eq. (2) is evaluated. This equation considers the t pixels within a segment, represented as $(b_0, b_1, b_2, \dots, b_t)$, originating from the noisy image.

$$f(x) = b_0 + b_1x + b_2x^2 + \dots + b_tx^{t-1} \text{ mod } 251 \quad (2)$$

Notably, the shares that are created through this process are smaller in size due to the correspondence of t pixels to a single pixel in the share. To reconstruct the original secret image, a minimum of t shares is required. This reconstruction is facilitated by utilizing Lagrange interpolation in conjunction with the initial non-processed pixels from t distinct shares. By interpolating, the coefficients of Eq. (2) unveil the t pixel values forming the noisy image, which, after inverse permutation, restores the original image.

Zhao et al. (2009) took the Thien and Lin (2002) scheme a step further by extending it into a verifiable secret-sharing system designed to detect untrustworthy participants. Their approach utilized discrete logarithms to uncover fraudulent behavior. Notably, participants were empowered to select their individual secret shadows, eliminating the need for a secure communication channel between the dealer and participants. Vyavahare and Patil (2016) developed a method where shadows are generated from the original secret and no audio covers are required for preserving confidentiality. Verma et al. (2020) introduced a framework designed to counteract fraudulent behavior from dealers and shareholders. In order to mitigate the risk of dishonest tactics such as leaking confidential information through legitimate shares, they implemented the notion of dealer leakage resilience. This involves limiting the authority of dealers to independently select random values, thus reducing the potential for deceitful actions. Guttikonda and Mundukur (2020) introduced a novel technique for secure data sharing encompassing text, images, and audio content. This method involves the creation of shares, which are subsequently generated and assessed through the utilization of both constant and randomly assigned coefficients within the polynomial framework. Lein and Changlu (2010) expanded upon the fundamental concept of a (t, n) secret sharing scheme by providing a precise description of (n, t, n) secret sharing scheme, which involves multiple dealers. Massoud and Samaneh (2008) introduced two effective and verifiable multi-secret sharing schemes utilizing homogeneous linear recursion. The initial scheme offers improved performance, featuring a novel and straightforward construction along with diverse techniques for the reconstruction stage. The second approach is derived from the HC secret sharing method.

Jani et al. (2015) proposed a method where images are encoded with DNA, then aggregated via DNA addition. Utilizing Lagrange interpolation and modular operations, shares are distributed and embedded securely for seamless reconstruction of multiple secrets. Bahman and Ziba (2019)

utilized collision-resistance and homomorphic properties to devise a threshold-verifiable secret-sharing scheme characterized by two notable features. Firstly, the scheme's security relies entirely on lattice problems. Secondly, participants can verify the consistency of their shares with the secret upon receipt, eliminating the need for communication. Arup et al. (2024) conducted an extensive review of various threshold secret-sharing schemes, examining key factors involved in designing secure and efficient methods. The study also explored different applications that utilize secret-sharing techniques. Additionally, the research outlined existing challenges in the field and provided insights into potential future directions for further advancements. Li et al. (2024) proposed a quantum secret-sharing scheme that supports a dynamic and adjustable threshold while incorporating cheating identification based on the Chinese remainder theorem. This approach allows participants to be updated dynamically without altering the shared secret or the private shares of the original members. Notably, it is the first scheme to introduce a flexible threshold in a quantum environment, greatly improving its practicality and adaptability.

1.2 Motivation

In today's digital age, audio content has become a critical component of multimedia, often containing confidential information. For instance, call centers frequently record customer interactions that may include sensitive details such as credit card numbers and addresses. These recordings are typically stored in cloud data centers. However, this presents a security risk, as unauthorized individuals or intruders at these cloud data centers could potentially exploit this sensitive information.

To address this risk, audio secret sharing schemes are employed to enhance the security of such sensitive audio data. Similar to the methods used for images, confidential audio can be encrypted and divided into multiple shares. These shares are then distributed across different cloud data centers. By requiring the simultaneous access and playing of a specific number of these shares, the original audio can be reconstructed. This approach ensures that unless a certain threshold of shares is compromised, the original audio remains secure.

In the area of secret sharing for audio, Desmedt et al. (1998) proposed a method for embedding secret binary text in audio data. Wang et al. (2015) proposed ASS based on fractal encoding and LSB technique. This method requires n audio covers to embed n parts of the original secret. Vyavahare and Patil (2016) developed a method where shadows are generated from the original secret, and no audio covers are required to preserve confidentiality. These existing audio secret-sharing methods have a limitation in assuming that participants are trustworthy, which is often an unrealistic assumption in real-world scenarios. Participants might act dishonestly by providing counterfeit shares or manipulated versions instead of the authentic ones. The

objective of this paper is to overcome this limitation by introducing a novel approach with the following aims:

Reduced dimensions of the shares: our new scheme aims to generate smaller-sized shares compared to the original secret. This aspect eases the storage and transmission burdens associated with handling shares.

Verification capability: Our approach aims to incorporate a verification mechanism to differentiate between legitimate and forged shares during the process of secret retrieval. This feature helps identify participants who attempt to submit fake data. Participants can also verify whether the dealer is publishing the true share or not.

High security: A key objective of our scheme is to produce shadows with minimal correlation to the original audio by incorporating randomized coefficients within the polynomial. As a result, our method substantially bolsters the security level, making it highly robust against potential breaches. Our proposed method can be applied in real-world scenarios such as healthcare, where audio recordings play a crucial role in patient consultations, medical histories, and treatment discussions. These audio files often contain sensitive medical information that must be securely stored and accessed only by authorized personnel to adhere to privacy regulations like HIPAA (Health Insurance Portability and Accountability Act) in the U.S. In this context, healthcare providers can use the proposed audio-based secret sharing method to safeguard these recordings. The dealer, typically a healthcare professional or administrator, generates shares of the audio data and distributes them to authorized medical staff members securely. Only a required number of medical professionals, such as a doctor, nurse, and medical administrator, can reconstruct the original audio recording using their shares. The dual verification mechanism ensures the authenticity of each participant's share, protecting against tampering or fraudulent data during the reconstruction phase.

Online music platforms that offer exclusive song releases, early access, or artist interviews could use the secret sharing method to securely distribute these files. Only a specific number of authorized participants (e.g., music reviewers, influencers, or premium subscribers) could reconstruct and access the full audio file.

2. PROPOSED SCHEME

The novel approach proposed in this paper offers the following functionalities:

- a) Division of the original secret audio A into n shares, each possessing smaller dimensions.
- b) Detecting dealer and participants who might engage in deceptive practices.

In our proposed approach, the dealer initiates by preprocessing a confidential audio file, producing corresponding audio shares denoted as A^i . Additionally, the dealer generates unique verification codes HS_i^{-1} for each participant. These codes serve the purpose of allowing

Table 1. Summarizes the notations used in the proposed scheme

Symbol	Description
D	Dealer
P	Participant
(t,n)	The t is threshold and n are the number of participants
($A^1, A^2, A^3 \dots A^n$)	Audio shares
($a_0, a_1 \dots a_{t-1}$)	Amplitude values of secret audio
x_i, R_i	The x_i is secret value and R_i is the public value of the i^{th} participant
($K_1, K_2, \dots K_n$)	Verification code for n participants to identify cheating behavior
HS_i	Verification code to authenticate dealer

participants to verify the authenticity of their respective audio shares, ensuring that they originate from their secret value x_i . Moreover, another set of verification codes K_i is generated, empowering participants to verify the authenticity of each other's submitted x_i values during the eventual reconstruction phase. The dealer disseminates these tuples (A^i, HS_i^1, K_i), ensuring transparency and integrity throughout the process. Prior to the reconstruction of the secret, participants utilize the HS_i^1 value to authenticate their audio shares, mitigating the risk of false shares being published by the dealer. Participants verify the pairs of x_i values utilizing K_i values to ensure that no fraudulent values are submitted by any participant. Upon confirming the validity of the audio shares A^i and x_i values, participants proceed with the reconstruction process.

2.1 Preprocessing of Audio and Share Construction

This module introduces a technique for audio-based secret sharing using polynomials. This method creates smaller-dimensional audio shares, offering advantages such as efficient storage utilization and minimized transmission overhead.

We must first convert the secret audio's amplitude samples from real to positive integer values. The amplitude samples that will be in the form of real numbers are initially rounded off during preprocessing by multiplying by 10^u , where u is an integer number. The bounds of the round off error are given by Eq. (3).

$$-\frac{1}{2} \times 10^{1-u} \leq \varepsilon \leq \frac{1}{2} \times 10^{1-u} \quad (3)$$

$$a' = ((a + \varepsilon) \times 10^u) + \gamma \quad (4)$$

Where u represents the rounding precision and ε represents the rounding error. Using the equation Eq. (4), each amplitude sample of secret audio is transformed to an integer and shifted to the first quadrant by a threshold γ to get positive sample values within Zp . The signal is not distorted when it is moved to first quadrant (Yakubu et al., 2015).

We have devised an innovative method of secret-sharing by leveraging the characteristics of polynomial functions. In this approach, a polynomial function is constructed by combining various terms, each consisting of a numerical

coefficient and the independent variable x of degree $t - 1$. Among these terms, the leading one holds the highest degree and thus the largest exponent. This leading term plays a crucial role in determining the behaviour of the polynomial. Its impact is significant because it grows at a faster rate compared to the other terms, owing to the highest exponent value it possesses. Our secret-sharing scheme revolves around this concept. A new dimension to secret sharing scheme is introduced by considering the coefficients of the polynomial's leading term as random values. Meanwhile, the coefficients of the remaining terms are derived from the amplitude values of a private audio source. This strategic inclusion ensures that the resulting audio shares remain obscured and devoid of any informative content about the secret. To generate n audio shares ($A^1, A^2, A^3 \dots A^n$) for n participants, each participant must compute their own secret value, x , and transmit it to the dealer. The process for computing the secret value, x , and conveying it to the dealer is outlined as follows:

1. To initiate the process, the dealer (D) selects two prime numbers, denoted as p and q . These primes are chosen with properties that mirror those used in the RSA cryptosystem. Subsequently, the dealer calculates the product $N = p \times q$.
2. The dealer proceeds to identify a value g from the interval $[N^{1/2}, N]$ that is also coprime with the previously chosen primes p and q . These values $\{g, N\}$ are then made public by the dealer.
3. Each participant, represented as $P_i \in P$, independently selects a substantial secret value x_i from the range $[2, N]$.
4. Subsequently P_i also selects $a_i \in [2, N]$ and calculates R_i from Eq. (5).

$$R_i \equiv g^{a_i} \text{mod} N \quad (5)$$

5. P_i computes x'_i, R'_i which is an encryption of x and R_i with the public key of dealer. P_i delivers $\{x'_i, R'_i\}$ to D .
6. D decrypts x'_i, R'_i with his private key and obtain x_i, R_i . D accepts x_i and publishes R_i only if x_i is relatively prime to N and $x_i \neq x_j$ and $R_i \neq R_j$ for all $P_i \neq P_j$. Otherwise, D insists P_i to choose new values.

For secret audio A and x_i values of the participants $P_i \in P$, dealer follows subsequent steps to generate n audio shares ($A^1, A^2, A^3 \dots A^n$) of smaller dimensions.

1. Read the secret audio file.

2. Preprocess the secret audio's amplitude samples, converting real values to positive integer values as mentioned in Eq. (3) of section 2.1,

2.1 Transform the amplitude samples of A using Eq. (6):

$$A = \text{round}((A + \varepsilon) \times 10^u) \quad (6)$$

2.2 Apply the adjustment to the transformed amplitude using Eq. (7):

$$A' = A + m' \quad (7)$$

Where m' is the absolute of the minimum value of A .

3. Determine the greatest amplitude value in A' , and then take into consideration the first prime number (Q) that exceeds this maximum.
 4. Divide the array A' into sections, each comprising $(t-1)$ audio samples.
 5. Form an array of random values designated as 'r'. The dimension of this array should correspond to the count of sections established in step-4.
 6. The audio samples $(a_0, a_1 \dots a_{t-1})$ from a specific segment (step-4) are used as coefficients for terms of lower degrees. Additionally, the random number r_j generated in step-5 is adopted as the coefficient for the leading term. This yields a polynomial function represented as:
- $$h_j(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-2} + r_jx^{t-1} \text{ mod } Q \quad (8)$$
7. To produce the share A^i for participant P_i , compute Eq. (8) as $o_j = h_j(x_i)$ for every segment and allocate the resulting o_j value to A^i . each segment. Subsequently, assign the resultant value as o_j to A^i . In this context, x_i represents a confidential value disclosed by participant P_i to the designated entity, denoted as D .
 8. Iterate through steps 6 and 7 for each of the n participants to acquire the shares $(A^1, A^2, A^3 \dots A^n)$.

2.2 Generation of Verification Code for Identifying Dishonest Participant

Dealer generates verification codes $(K_1, K_2, \dots K_n)$ for each participant $(P_1, P_2, \dots P_n)$ and publishes them. This enables each participant to validate whether other participants are providing their true x_i values during the reconstruction process. The steps followed by the dealer to compute the verification code K_1 , are as follows:

1. D finds an integer $e \in [2, N]$ that is coprime with $\phi(N)$. Subsequently, D computes value of d such that $e \times d \equiv 1 \text{ mod } \phi(N)$, where $\phi(N)$ represents Euler's totient function applied to N .
2. D computes $K_i = R_i^{e/x_i} \text{ mod } N$ where $\frac{1}{x_i}$ is multiplicative inverse of x_i in $\text{mod } N$.
3. D publishes $\{d, K_i\}$. For $i = 1, 2, 3 \dots n$.

2.3 Creating Verification Code to Authenticate Dealer

In our proposed scheme, participants have the capability to verify whether the audio share generated by the dealer corresponds to their secret x_i value. This verification process involves the generation of a verification code. The code serves to authenticate whether the dealer has indeed derived the audio share using the participant's true x_i value. Through our proposed methodology, participants can ensure the integrity and authenticity of the audio shares published by the dealer. For this, entity D produces a pseudo-random sequence denoted as RN_i Eq. (10). This is accomplished by employing a pseudo-random function termed as PRNG driven by a seed value derived from x_i of participant P_i and d value of the dealer Eq. (9).

$$\text{seed}_i = (x_i \| d) \quad (9)$$

$$RN_i = \text{PRNG}(\text{seed}_i) \quad (10)$$

Subsequently, RN_i undergoes an XOR operation in combination with an audio share denoted as A^i . This leads to the creation of the arbitrary share AS_i as outlined in Eq. (11). The dealer then proceeds to compute the verification code HS_i^1 by employing Eq. (12). This computation involves the application of a hash function h to RN_i .

$$AS_i = A^i \oplus RN_i \quad (11)$$

$$HS_i^1 = h[AS_i] \quad (12)$$

Dealer publishes (A^i, HS_i^1) . The utilization of the hash function h and the pseudorandom function PRNG remains confidential, known solely to the dealer and participants.

2.4 Dealer Verification Phase

In our proposed method, participants have the capability to verify the audio shares published by the dealer. During the share construction, the audio shares $(A^1, A^2, A^3 \dots A^n)$ are derived from the secret values $(x_1, x_2, \dots x_n)$ of the participants $(P_1, P_2, \dots P_n)$. Therefore, it is imperative for participant P_i to confirm whether the dealer has generated the audio share A^i using their specific value x_i and not any alternate value. To achieve this, participant P_i calculates the seed_i value by applying Eq. (9) and then computes RN_i value using Eq. (10).

The participant subsequently produces an arbitrary share AS_i from the audio share A^i being disseminated by the dealer using Eq. (11) and then generates verification code with Eq. (13).

$$HS_i^2 = h[AS_i] \quad (13)$$

P_i then verify's if $HS_i^2 = HS_i^1$?. Here, HS_i^2 is derive from Eq. (13) and HS_i^1 from Eq. (12). If verification is successful, P_i believes that the share A^i that is published is derived from his secret value x_i and is valid. This is

necessary for preventing the dealer from publishing a fake share.

2.5 Participant Verification Phase

Before the reconstruction process, each participant can verify whether the other participant is providing true x_i value or not. To decrypt secret, a pooled approach utilizing t or more shares is utilized, with $P' = (P_1, P_2 \dots P_t)$ representing the group reconstructing the secret.

- Members belonging to P' are required to furnish their respective x_i values.
- Any participant in P' can verify the x_i value submitted by P_i , from K_i and d values by computing Eq. (14).

$$V_i = K_i^{x_i d} \bmod N \quad (14)$$

- If $V_i = R_i$ then P_i is a true participant. Otherwise P_i may be dishonest participant.

2.6 Secret Reconstruction Phase

With their t pairs of (x_i, A^i) , the participants within the P' group follows the subsequent steps for the secret reconstruction process:

- Retrieve the initial untapped amplitude values from all the t audio shares $(A^1, A^2, A^3 \dots A^t)$. These initial sampled values are denoted as $(a_0^1, a_0^2, a_0^3 \dots a_0^t)$.
- By inserting $(a_0^1, a_0^2, a_0^3 \dots a_0^t)$ values and x_i values into Eq. (15), the following expression is obtained.

$$f(x) = a_0^1 \frac{(x-x_2)(x-x_3)\dots(x-x_t)}{(x_1-x_2)(x_1-x_3)\dots(x_1-x_t)} + a_0^2 \frac{(x-x_1)(x-x_3)\dots(x-x_t)}{(x_2-x_1)(x_2-x_3)\dots(x_2-x_t)} + \dots + a_0^t \frac{(x-x_1)(x-x_2)\dots(x-x_{t-1})}{(x_t-x_1)(x_t-x_2)\dots(x_t-x_{t-1})} \bmod Q \quad (15)$$

- Upon simplification of Eq. (15), we arrive at a polynomial function $f(x)$ characterized by a degree of $(t-1)$. The constituents within $f(x)$ are systematically organized in an ascending manner from left to right. The resulting form of $f(x)$ can be expressed as:

$$f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-2} + r_jx^{t-1} \bmod Q \quad (16)$$

The $t-2$ coefficients derived from the Eq. (16) are stored within an array denoted as array B' .

- Continue with steps 1 through 3 until all audio share samples have been processed.
- Compute audio A using Eq. (17).

$$A = \frac{B' - m'}{10^u} \quad (17)$$

- A represents the regenerated audio, achieved with complete preservation of information.

3. RESULTS AND DISCUSSION

Shamir's approach, which has been shown to be secure, forms the foundation for our suggested method for creating the shares. Our method also verifies the legitimacy of the participant which is analyzed in this section. We have used MATLAB R2022B to implement the suggested algorithms to validate our proposed strategy.

3.1 Security Analysis

In this section, we conducted a security analysis of our proposed scheme with respect to thwarting dishonest participants and preventing the distribution of counterfeit shares by the dealer among the participants.

Theorem 1: It is impossible for a coalition of $(t-1)$ participants to acquire any information regarding the secret.

Proof: Let's consider the scenario where $(t-1)$ participants collaborate and possess $(t-1)$ shares. In this situation, they can generate $(t-1)$ polynomial equations as follows:

$$f(x_1) = a_0 + a_1x_1 + \dots + a_{t-1}x_1^{t-2} + r_1x_1^{t-1} \bmod Q$$

$$f(x_2) = a_0 + a_1x_2 + \dots + a_{t-1}x_2^{t-2} + r_2x_2^{t-1} \bmod Q$$

$$f(x_{t-1}) = a_0 + a_1x_{t-1} + \dots + a_{t-1}x_{t-1}^{t-2} + r_jx_{t-1}^{t-1} \bmod Q$$

Now, we have $(t-1)$ equations with $(t-1)$ unknowns (the coefficients $a_0, a_1 \dots a_{t-1}$). However, this system of equations is not sufficient to solve for all the unknowns. This is because polynomials of degree $t-1$ require at least t distinct points to fully determine all the coefficients of the polynomial (via interpolation methods) and with only $(t-1)$ points, the system of equations is underdetermined because there are more unknowns than equations.

Attempting to solve this system of equations becomes an intricate task unless the term corresponding to the i^{th} participant is guessed. Consequently, a minimum of t points is required to accurately interpolate the polynomial. Thus, due to the need for the i^{th} term for solving the equations and the lack of correlation between polynomials, it becomes evident that any attempt by $(t-1)$ participants to pool their information cannot lead to the recovery of the secret.

Theorem 2: Participant P_i can successfully check the validity of his/her share that is published by the dealer.

Proof: Let P_i receives fake share $A^{i'}$ instead of correct share A^i . To verify the validity of the share received, P_i follows these steps:

Step 1: P_i computes a seed value $seed_i$ Eq. (9) using their secret value x_i and the dealer's public value d .

Step 2: Using the computed $seed_i$, P_i generates a random number RN_i Eq. (10) using a Pseudo-Random Number Generator (PRNG).

Step 3: P_i computes the expected share AS_i' , with the received fake share $A^{i'}$ and the generated random number RN_i as shown in Eq. (18).

$$A^{i'} \oplus RN_i = AS_i' \quad (18)$$

Step 4: P_i computes the hash of the expected share AS_i'

from Eq. (19).

$$HS'_i = h[AS'_i] \quad (19)$$

The computed hash HS'_i does not match the hash HS_i published by the dealer as mentioned in Eq. (12) of section 2.3, it confirms that the received share $A^{i'}$ is invalid.

The use of a PRNG with a unique seed for each participant ensures that different participants generate different random numbers, making it difficult for an adversary to manipulate the shares without being detected. The hash function provides an additional layer of security by making it computationally infeasible for an adversary to forge a valid share without knowing the secret value x_i .

Theorem 3: Dishonest participant can be identified by computing $K_i^{x_i d} \equiv R_i \bmod N$.

Proof: Let P_i be a participant holding the secret x_i and the corresponding value R_i the dealer generates a verification code K_i derived from x_i and R_i as described in section 2.2., to verify that P_i has provided the correct secret x_i during reconstruction process, any other participant can compute $K_i^{x_i d} \bmod N$ where d is the public value of the dealer and checks that this computed value is equal to $R_i \bmod N$. This verification holds because, according to Section 2.2, K_i is defined as $K_i = R_i^{\frac{e}{x_i}} \bmod N$ substituting this to $K_i^{x_i d}$ yields.

$$K_i^{x_i d} = (R_i^{\frac{e}{x_i}} \bmod N)^{x_i d} = R_i^{\frac{e}{x_i} x_i d} \bmod N \quad (20)$$

Since the dealer ensures that $e \times d \equiv 1 \bmod \phi(N)$, By properties of modular arithmetic the Eq. (20) further simplifies to,

$$R_i^{\frac{e}{x_i} x_i d} \bmod N = R_i \bmod N \quad (21)$$

Thus, if P_i is honest and provides the correct secret x_i , the computed value $R_i \bmod N$ obtained from Eq. (21) matches the $R_i \bmod N$ value computed from Eq. (5). However, if P_i is dishonest and provides a false value x'_i the computation becomes,

$$K_i^{x'_i d} = (R_i^{\frac{e}{x_i}} \bmod N)^{x'_i d} = R_i^{\frac{e}{x_i} x'_i d} \bmod N = R_i^{\frac{x'_i}{x_i}} \bmod N \quad (22)$$

The value $R_i^{\frac{x'_i}{x_i}} \bmod N$ computed from Eq. (22) is compared with $R_i \bmod N$ value obtained from Eq. (5). In this case $R_i^{\frac{x'_i}{x_i}} \bmod N \neq R_i \bmod N$. This is because $x_i \neq x'_i$ and the modular exponentiation will not yield $R_i \bmod N$. This indicates that the provided x'_i is incorrect. Thus, the computation $K_i^{x_i d} \equiv R_i \bmod N$ acts as a test for honesty. If the result holds true, P_i has provided the correct secret value. If it does not hold, then P_i is identified as dishonest or a

potential cheater.

Theorem 4: Knowing the public values K_i and d , deriving the secret x_i of participant P_i by adversary is difficult.

Proof: As discussed in section 2.2 K_i can be expressed as $R_i^{\frac{e}{x_i}} \bmod N$.

Where $R_i = g^{a_i} \bmod N$ derived from section 2.1. The public values available to an adversary are K_i and d . Using these, the adversary can compute,

$$K_i^d = (R_i^{\frac{e}{x_i}})^d \bmod N = R_i^{\frac{e}{x_i} d} \bmod N = R_i^{\frac{1}{x_i}} \bmod N \quad (23)$$

Here, the property $e \times d \equiv 1 \bmod \phi(N)$ ensures that $\left(\frac{e}{x_i}\right) \times d = 1/x_i$. Substituting the value of R_i Eq. (5) in Eq. (23) we get,

$$K_i = (g^{a_i})^{\frac{1}{x_i}} \bmod N \quad (24)$$

To derive x_i from Eq. (24), the adversary must solve for x_i given g , a_i , K_i , N . This involves solving a discrete logarithm $\frac{a_i}{x_i} = \log_g(K_i) \bmod N$ which is hard. Even if the adversary were to compute $\frac{a_i}{x_i}$, isolating x_i would require further steps. Specifically, they would need to invert $\frac{a_i}{x_i}$, which introduces additional mathematical challenges since a_i is a randomly chosen secret, independent of x_i . Thus, deriving x_i from K_i is infeasible, ensuring the security of the scheme.

3.2 Experimental Analysis for (3,4) Threshold Scheme

A (3,4) scheme ensures robustness by requiring at least 3 participants for reconstruction, which is a reasonable trade-off between security and practicality (ensuring accessibility to the secret when required). The $n = 4$ offers a small yet realistic group size to demonstrate feasibility while reducing computational overhead compared to schemes with larger n . In real-world applications, a (3,4) scheme is particularly suitable for scenarios like a board of directors needing a quorum to access confidential information, or a cryptographic key shared among four devices, where at least three are required to unlock or use the key. Fig. 1 demonstrates the viability of the proposed (3,4) secret-sharing scheme by visualizing the plain audio signal and the distinct audio shares generated for four participants. The subfigures provide insights into the time-domain representation of the plain audio, its frequency-domain characteristics, and the unique noisy behaviors of the generated shares. Fig. 1 (i), displays the plain audio signal as a waveform in the time domain. The waveform exhibits natural fluctuations in amplitude, characteristic of raw audio signals. This serves as the base signal before preprocessing and share generation. Fig. 1 (ii), the amplitude spectrum of the plain audio is visualized here, showing how the energy of the signal is distributed across different frequencies.

Peaks in the spectrum indicate dominant frequency components in the plain audio. Fig. 1 (iii), illustrates the amplitude spectrum of the first share generated for P_1 with $x = 50$. The frequency-domain representation ensures that this share alone provides no meaningful information about the plain audio signal. The amplitude spectrum of the second share, created for P_2 with $x = 120$, is shown in Fig. 1 (iv), the spectral pattern differs from the plain audio, ensuring unique and secure representation. Fig. 1 (v), depicts the amplitude spectrum of the third share, derived using $x = 30$ for P_3 . Like other shares, it ensures that the plain signal's original properties are obscured, safeguarding against unauthorized reconstruction. The fourth share's amplitude spectrum, generated using $x = 100$ for P_4 , is visualized in Fig. 1 (vi), together with at least two other shares, this share can help reconstruct the original audio signal as per the (3,4) scheme. It's important to note that, in accordance with the procedures outlined in section 2.1, the signals have been subjected to preprocessing, leading to the conversion of the negative values of the plain signal into positive integers.

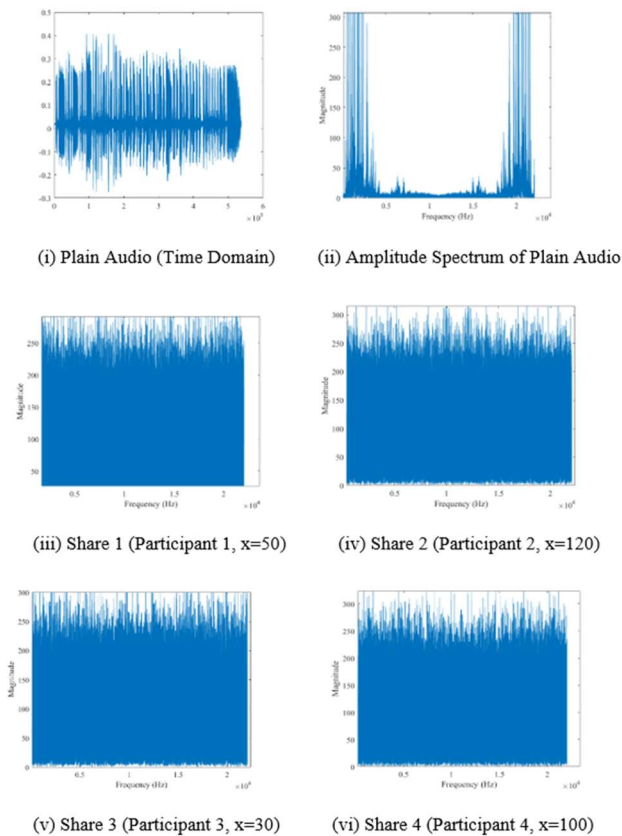


Fig. 1. Time and frequency domain representation of plain audio and audio shares

Spectrogram analysis provides valuable insights into the spectral characteristics of the audio, revealing information about the distribution of energy across different frequencies and how it evolves over time. In the spectrogram of the

original audio shown in Fig. 2 (i), shows clear patterns and recognizable frequency components corresponding to the original sounds. Fig. 2 (ii), presents the spectrogram of the first audio share generated for participant 1, where the spectral content is notably scrambled when compared to the original audio. Fig. 2 (iii), presents the spectrogram of the second audio share, generated for participant 2, which also shows a random and distorted frequency pattern. Fig. 2 (iv) displays the spectrogram of the third audio share, created for participant 3, where the spectral components remain scrambled, with no identifiable structure from the original audio signal.

This proves that our proposed method can mask the original signal by introducing randomness or altering the frequency distribution in a way that makes it difficult to discern the original content.

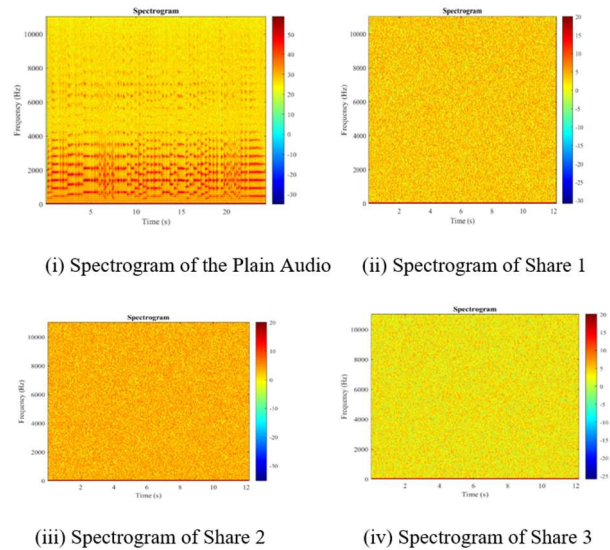


Fig. 2. Spectrograms of plain audio and audio shares

3.2.1 Correlation Analysis

The Pearson correlation coefficient, which is represented by the formula defined in Eq. (25), was used to evaluate the similarity between audio shares and the original audio.

$$r = \frac{\sum_{i=1}^m (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{(\sum_{i=1}^m (X_i - \bar{X})^2)(\sum_{i=1}^m (Y_i - \bar{Y})^2)}} \quad (25)$$

The results of the similarity computation between the original audio represented by $(Y_i)_{i=1}^m$ and the four shares $(X_i)_{i=1}^m$ are 0.0023, 0.0020, 0.0018, -0.0036, its corresponding plot is shown in Fig. 3. Notably, it becomes evident from these results that the similarity score between the shares and the secret audio approaches zero. This observation leads to the conclusion that there is a lack of similarity between the original audio and the shares. The original audio and the rebuilt audio have a high similarity score of 1.000, indicating a successful audio reconstruction technique with minimal information loss.

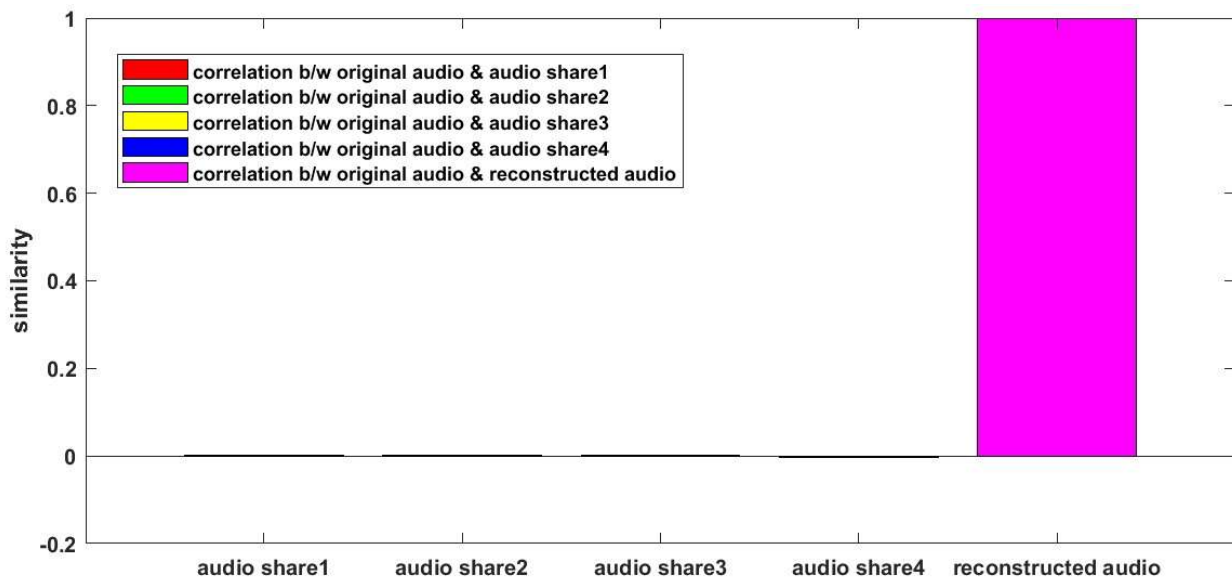


Fig. 3. Similarity plot

To mitigate the inherent correlation present in adjacent amplitude values of audio data, a strategic approach was adopted involving the introduction of a random coefficient as a component of higher degree terms in a polynomial function. This introduced random coefficient effectively functions as a blinding factor during the generation of noisy shares. The rationale behind this process was to break down the existing correlation among adjacent audio data points. Fig. 4 is the evidence of the noisy shares generated through this process. Fig. 4 (i), showcases the plot of the of 5000 Sampled values from original audio with the values represented as real numbers. Fig. 4 (ii), shows the plot of 5000 sampled values from the first audio share, generated for participant 1. This share exhibits a noisy, irregular pattern, differing significantly from the original audio. Fig. 4 (iii), presents the plot of 5000 Sampled values from the second audio share, created for participant 2. The transformation into positive integers is evident, and the randomness introduced in the share ensures that it bears no direct resemblance to the original audio. Fig. 4 (iv), illustrates the plot of 5000 Sampled values from the third audio share, generated for participant 3. This share continues to show a distorted and random pattern, with no clear correlation to the original signal. Fig. 4 (v), depicts the plot of 5000 Sampled values from the fourth audio share, created for participant 4. The plot displays the noisy, random behavior as the other shares. Fig. 4 (vi), shows the plot of reconstructed audio which closely resembles the original audio signal.

It's worth noting that the sampled values of the shares are transformed into positive integer values as part of the audio preprocessing, a procedure expounded upon in section 2.1 of the discussion. An essential outcome of this generation process is the elimination of the inherent correlation

between sampled values within the shares. This achievement stems from the deliberate incorporation of the random coefficient. This innovative approach not only preserves security but also introduces a discernible separation between the shares and the original audio.

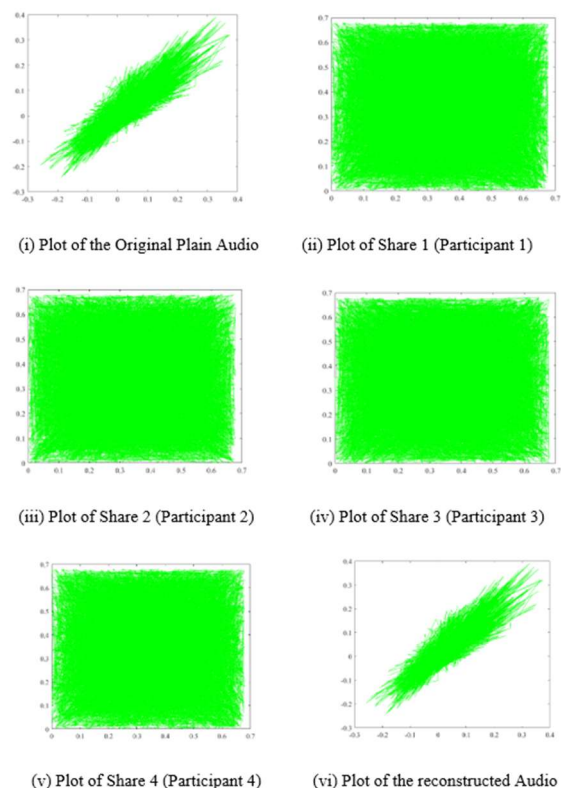


Fig. 4. Plot containing 5000 sequentially adjacent sampled values of plain audio, audio shares and reconstructed audio

Table 2. Average processing time and applications of proposed method

Threshold (k,n)	Execution time (s) for share generation	Execution time (s) for generating Pseudo random values and hash values	Execution time (s) for secret reconstruction	Share size (bytes)	Applications
3,4	0.551328	0.273188	1.747383	2152400	Suitable for small groups or teams. Examples: Family financial documents, team passwords, small project keys.
11,50	5.240862	0.184833	8.058767	430480	Best for medium-sized organizations where you need to balance security and complexity. Examples: Secure access in departments, corporate secure voting systems, or employee shared credentials.
21,300	26.155568	0.563324	17.277989	215240	Ideal for large-scale systems requiring high security and fault tolerance. Examples: Distributed cloud storage systems, blockchain networks, or national secure voting.

The proposed secret-sharing scheme presents an innovative approach to enhancing security in distributed systems by leveraging cryptographic primitives such as pseudo-random number generation, modular arithmetic, and hash functions. While the method inherently involves complex mathematical operations, these steps ensure robust protection against unauthorized access and tampering. The inclusion of performance benchmarks in Table 2, such as execution times and share sizes for a secret audio of size 538100, demonstrates the scheme's feasibility across varying threshold setups, making it suitable for diverse applications ranging from small teams to large-scale systems.

3.2.2 Comprehensive Storage Analysis

In a simple secret sharing scheme, each participant's share is the size of the secret S , and with k participants, the total storage required is $k \times S$. Additionally, $k-1$ random coefficients are used to generate the polynomial (e.g., in Shamir's scheme), and while these coefficients are stored internally by the dealer and are not required for reconstruction process, they do not contribute directly to participant storage. Therefore, the total storage required for shares per participant is S , and for k participants, it totals $k \times S$.

In our proposed scheme, the storage requirements are significantly optimized. Only the highest-degree term coefficient is random, while the remaining $k-2$ coefficients are derived from the secret. So, the size of each participant's share is reduced to $\frac{S}{k-1}$. For k participants, the total storage

for shares becomes $k \times \frac{S}{k-1}$, which is smaller than the $k \times S$ required in a simple secret sharing scheme.

Moreover, to enhance security, a random array of size $\frac{S}{k-1}$ is generated for each participant using a seed value, and XORed with the participant's share. The hash value (SHA-256, 32 bytes) for each share is then stored for verification. Since the random array is derived by the receiver using the seed value, there is no need to store it. These random values are generated dynamically and used internally by the dealer or participant to generate the shares or perform the XOR operation and are not transferred. As a result, no additional storage cost is incurred for these random values. Thus, for k participants, the share storage requirement is $k \times \frac{S}{k-1}$ and the hash storage requirement is $32 \times k$. This results in a total storage requirement of $k \times \frac{S}{k-1} + 32 \times k$.

Compared to the $k \times S$ storage requirement of simple secret sharing, our scheme is more storage-efficient, especially for larger k . The reduction in share size outweighs the additional overhead of storing hash values, making the scheme scalable and efficient for scenarios involving a large number of participants.

3.2.3 Histogram Analysis

Histogram analysis is employed to visually depict the distribution of signals in audio data. Fig. 5 (i), presents the histogram of the original audio signal, illustrating its distribution. The histogram for share 1, shown in Fig. 5 (ii), reveals no clear pattern or clustering of values, highlighting

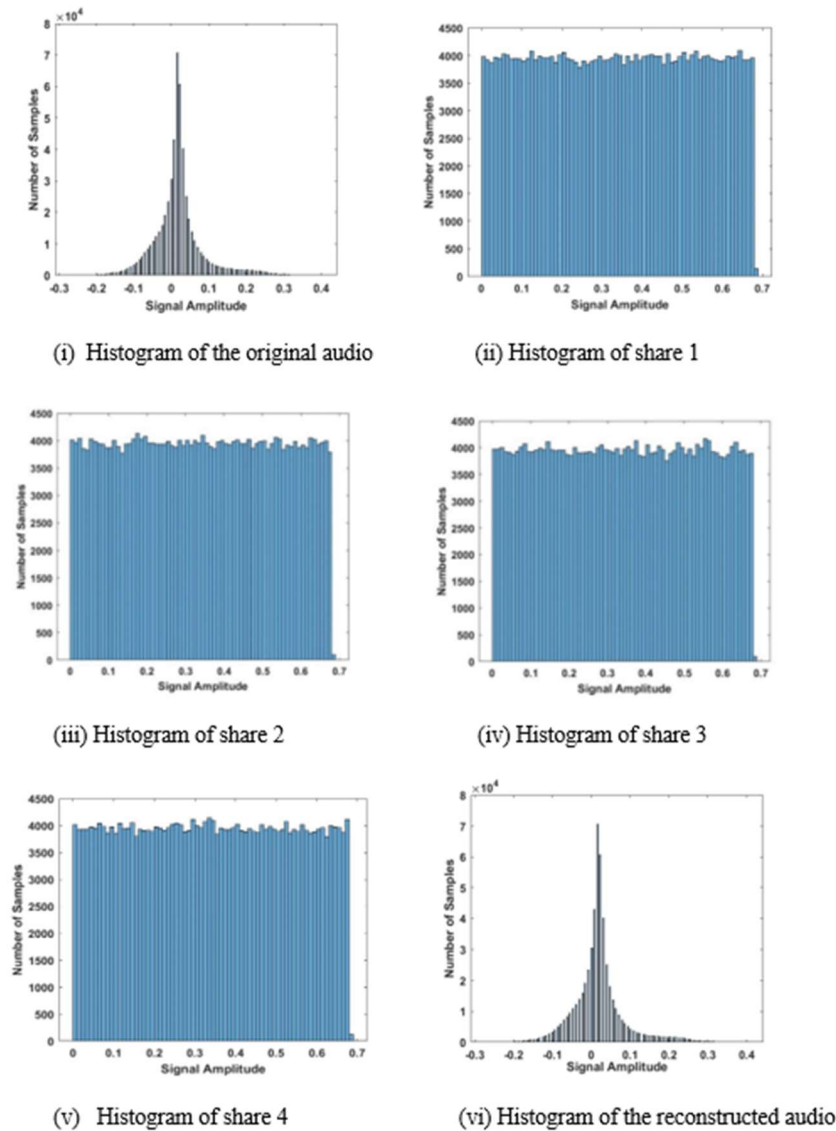


Fig. 5. Amplitude distribution of original audio, generated shares and reconstructed audio

the noisy nature of the share, which is characteristic of a secret-sharing scheme intended to conceal the original signal. Fig. 5 (iii), shows the histogram of share 2, where the absence of significant peaks or concentrations further indicates that this share is highly randomized, with no direct correlation to the original audio. The histogram of share 3, presented in Fig. 5 (iv), demonstrates that the amplitude values are spread across a wide range, ensuring that the original audio's characteristics remain hidden. Finally, the Fig. 5 (v), displays the histogram for share 4, where the lack of any distinct structure in the amplitude values further reinforces the effectiveness of the secret-sharing method in obscuring the original audio signal.

In contrast, the histogram of the reconstructed audio showcased in Fig. 5 (vi), perfectly aligns with the histogram of the original audio depicted in Fig. 5 (i). This compellingly establishes that the proposed methodology excels in

faithfully reconstructing the secret audio, managing to preserve the amplitude values seamlessly

3.2.4 Number of Samples Change Rate (NSCR) and UACI (Unified Average Changing Intensity)

In the realm of quantitative analysis, two essential metrics, namely NSCR and UACI, play a pivotal role. NSCR, akin to the concept of Number of Pixel Change Rate (NPCR), is determined as outlined in Eq. (26) and UACI is in Eq. (27),

$$NSCR = \frac{\sum_i D_i}{L} \times 100 \quad (26)$$

$$UACI = \frac{1}{N} \sum_i \frac{|S_1(i) - S_2(i)|}{2^Q - 1} \quad (27)$$

In Table 3, the NSCR and UACI values are both validated to be zero, affirming the flawless reconstruction of the

original audio. This outcome serves to affirm the flawless reconstruction of the original audio, reinforcing its lossless nature. These results align with recent advancements in secret sharing scheme by Parihar et al. (2024), that utilizes lightweight Boolean and additive modulo operations for share generation and reconstruction.

3.2.5 Peak Signal-to-Noise Ratio (PSNR)

PSNR stands as a widely adopted metric for signal quality assessment. In the context of two distinct audio signals, the PSNR values are determined using Eq. (28):

$$PSNR = 10 \times \log_{10} \frac{MAX^2}{MSE} \text{ (dB)} \quad (28)$$

Table 3, showcases an infinite PSNR value for the original audio in comparison with its reconstructed counterpart. This observation provides compelling evidence supporting the lossless reconstruction of the original audio. The result clearly indicate that the reconstruction process is lossless, which aligns with the findings of prior research by Parihar et al. (2024). Additionally, this finding is consistent with the work of Abbasi et al. (2024), who demonstrated an audio watermarking scheme with secret sharing in the transform domain, achieving high fidelity and secure data embedding.

3.3 Comparison with Different Secret Sharing Schemes

Our proposed technique has a few notable advantages over current secret sharing schemes, shown in Table 4. The distinctive features of our scheme are as follows:

- 1) Our scheme empowers each participant to validate their

own share. This crucial feature acts as a safeguard against any attempts by the dealer to distribute counterfeit shares among participants. Moreover, any participant can scrutinize the authenticity of another participant's information during the secret reconstruction phase. This validation is facilitated through the utilization of equation $K_i^{x_i^d} = R_i \text{ mod } N$, elaborated upon in section 2.3.

- 2) Our scheme capitalizes on the fact that shares are derived from participant-specific secret values, allowing the dealer to distribute encrypted shares via public channels.
- 3) Our novel secret sharing scheme stands out by allowing (t-1) chosen secret audio values per section to form a unified share audio sample, reducing share size to just the 1/(t-1) of the original audio.
- 4) One of the remarkable aspects of our scheme is the elimination of the need for permutation and inverse permutation operations to enhance security. The introduction of a random coefficient as a component of higher degree terms in a polynomial function serves as a blinding factor during the generation of noisy shares, thus significantly augmenting the overall security of the scheme.

Table 5, presents a comparison of audio secret sharing schemes, showcasing the performance of our proposed method alongside the approaches of Yakubu et al. (2015) and Guttikonda and Mundukur (2020). To demonstrate the adaptability of the proposed method, two distinct audio samples were chosen. The first audio file (Counting.wav) has a sampling rate of 44,100 Hz, which is the standard for CD-quality audio. This high sampling rate is widely used in

Table 3. Metrics for assessing the quality of original and reconstructed audio

Metrics	Original audio and reconstructed audio
Correlation coefficient (<i>r</i>)	1
Peak Signal-to-Noise Ratio (PSNR)	∞
Number of Samples Change Rate (NSCR)	0
Unified Average Changing Intensity (UACI)	0

Table 4. Comparison of proposed method with others work

Schemes	Verification of any participant against cheating	Dealer-participant communication channel	Dealer verification against share distribution	Smaller share size	Use of permutation key
Shamir (1979)	No	Secure channel	No	No	No
Thien and Lin (2002)	No	Secure channel	No	Yes	Yes
Zhao et al. (2009)	Yes	No channel	No	Yes	Yes
Zuquan et al. (2024)	Yes	Secure channel	No	Yes	No
Shyamalendu and Bibhas (2020)	Yes	Any channel (secure or no secure channel)	No	No	No
Alam et al. (2024)	Yes	No channel	Secure	Yes	No
Our scheme	Yes	No channel	Secure	Yes	No

Table 5. Comparison of audio processing methods in terms of execution time

Methods	Length (s) of audio	Bits/sample of audio	Sampling frequency of audio (Hz)	Total samples	Share creation (s)	Share reconstruction (s)	Share size
Yakubu et al. (2015)	15.534	16	44100	685056	0.2484	0.1105	Equal to the size of secret
Our scheme	15.5341	16	44100	685056	0.1261	1.9331	Reduced by $1/k-1$ of secret
Guttikonda and Mundukur (2020)	24.4036	8	22050	538100	0.3728	0.0608	Equal to the size of secret
Our scheme	24.4036	8	22050	538100	0.2937	1.5248	Reduced by $1/k-1$ of secret

Table 6. Impact of audio duration and sampling rate on processing times

Audio file	Duration (s)	Sample rate	Total samples	Share construction (s)	Share reconstruction (s)
TrainWhistle.wav	9.3344	22050	211660	0.200275	0.067173
preamble10.wav	9.5991	44100	411648	0.241592	0.087305
FlagRaising.wav	24.4036	22050	538100	0.293719	1.524882
Turbine.wav	22.4305	44100	989184	5.793718	2.778

consumer formats, providing rich and detailed sound. The audio has a duration of 15.5341 s with a bit depth of 16 bits per sample. However, the increased sampling rate and total number of samples introduce greater computational complexity. The second audio file (*FlagRaising.wav*) has a sampling rate of 22,050 Hz, which is half the standard CD-quality rate. This lower sampling rate is often used in applications where reduced file sizes are prioritized over the highest audio fidelity, such as voice recordings or certain streaming services. With a duration of 24.4036 s and a bit depth of 8 bits per sample, this sample provides insights into the method's efficiency and less resource-intensive conditions.

Our scheme significantly reduces share creation time compared to Yakubu et al. (2015) and Guttikonda and Mundukur (2020), making it more efficient in generating shares. However, this comes at the cost of a higher share reconstruction time, which is considerably longer than the other methods. Additionally, our scheme improves storage efficiency by reducing the share size to $1/k-1$ of the original secret, whereas the other methods maintain a share size equal to the original secret. This analysis highlights a clear trade-off: while our approach optimizes storage and share creation speed, it increases the time required for reconstruction, while also highlighting the method's adaptability to different audio qualities.

As the duration increases, or the sampling rate increases, the total number of samples increases proportionally. This affects the computational load for processing and storage of the audio data. The effect of these factors on the proposed method is demonstrated in Table 6. For shorter audio durations (9.334 and 9.5991), the share construction and reconstruction times are lower, with increased sampling rates (e.g., 44,100 Hz compared to 22,050 Hz) slightly raising the processing times due to the higher number of

total samples. For longer audio durations (22.4305 and 24.4036 s), the impact of both duration and sampling rate becomes more pronounced, with significantly higher construction and reconstruction times observed, particularly at 44,100 Hz. These results highlight the trade-off between processing time and audio quality, as well as the scalability of the proposed method for diverse audio scenarios.

4. CONCLUSION

The audio shares produced by our proposed method exhibit dimensionality reduction and noisiness. These shares are created by employing the amplitude values of the secret audio as coefficients in a polynomial. As a result, the resultant audio shares are only $1/t-1$ the size of the original secret audio. Using random numbers results in noisy audio shares, obviating the necessity for intricate operations like permutations or complex encryption procedures. Moreover, an additional mechanism is outlined wherein participants working in collaboration possess the capability to validate the integrity of any fellow participant's actions, specifically in cases of potential dishonest behavior. Our method ensures not only the injection of controlled noise into the shares for enhanced security but also guarantees that the shares can be reconstructed comprehensively without information loss, and it also includes two verification methods one to detect dishonest participants and second to ensure the integrity and authenticity of the audio shares published by the dealer. In real-world scenarios, participants may join or leave, which could lead to a change in the threshold value t . In these situations, the dealer would need to reconstruct the polynomial equation to accommodate the new threshold and regenerate the corresponding shares and verification codes. To overcome this limitation, the proposed method could be extended to an adaptable threshold secret sharing scheme.

This would enable the inclusion or exclusion of participants without the need to regenerate or redistribute shares, thereby improving the system's flexibility and minimizing the operational burden associated with participant changes.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- Abbasi, A.T., Miao, F., Islam, M.S. 2024. A secure and robust audio watermarking scheme using secret sharing in the transform-domain. *Circuits Syst Signal Process*, 44, 1274–1307.
- Arup, K.C., Sanchita, S., Amitava, N., Sukumar, N. 2024. Secret sharing: A comprehensive survey, taxonomy and applications. *Computer Science Review*, 51, 100608.
- Alam, I., Alali, A.S., Ali, S., Asri, M.S.M. 2024. A verifiable multi-secret sharing scheme for hierarchical access structure. *Axioms*, 13, 515.
- Bahman, R., Ziba, E. 2019. A verifiable threshold secret sharing scheme based on lattices. *Information Sciences*, 501, 655–661.
- Blakley, G.R. 1979. Safeguarding cryptographic keys. In *proceedings of the AFIPS National Computer Conference*. IEEE Computer Society, 48, 313–317.
- Desmedt, Y.G., Hou, S., Quisquater, J.J. 1998. Audio and optical cryptography. In *International Conference on the Theory and Application of Cryptology and Information Security*. Berlin, Heidelberg, 1514, 392–404.
- Guttikonda, P., Mundukur, N.B. 2020. Polynomial-based secret sharing scheme for text, image and audio. *Journal of the Institution of Engineers (India): Series B*, 101, 609–621.
- Guttikonda, P., Mundukur, N.B. 2024. Cheating identifiable polynomial based secret sharing scheme for audio and image. *Multimedia Tools and Applications*, 83, 403–423.
- Jani, L.A., Anandha, G.S.M., Modigari, N. 2015. DNA based multi-secret image sharing. *Procedia Computer Science*, 46, 1794–1801.
- Jeonghun, C., Sushil, K.S., Tae, W.K., Jong, H.P. 2021. Blockchain-empowered cloud architecture based on secret sharing for smart city. *Journal of Information Security and Applications*, 57, 102686.
- Li, F., Wu, Q., Lin, C., Zhu, S. 2024. A threshold changeable dynamic quantum secret sharing scheme with cheating identification. *Quantum Inf Process* 23, 358.
- Lein, H., Changlu, L. 2010. Strong (n,t,n) verifiable secret sharing scheme. *Information Sciences*, 180, 3059–3064.
- Massoud, H.D., Samaneh, M. 2008. New efficient and practical verifiable multi-secret sharing schemes. *Information Sciences*, 178, 2262–2274.
- Parihar, B., Deshmukh, M., Rawat, A.S. 2024. A framework for counting based secret sharing scheme for images. *Multimedia Tools and Applications*, 83, 86757–86790.
- Parsa, S., Shabir, A.P., Mohiuddin, G.B., Ali, A.H., Khan, M. 2021. Secret sharing-based personal health records management for the internet of health things. *Sustainable Cities and Society*, 74, 103129.
- Prashanti, G., Nirupama, B.M. 2020. Secret sharing with reduced share size and data integrity. *Ingénierie des Systèmes d'Information*, 25, 227–237.
- Shyamalendu, K., Bibhas, C.D. 2020. A verifiable secret sharing scheme with combiner verification and cheater identification. *Journal of Information Security and Applications*, 51, 102430.
- Shamir, A. 1979. How to share a secret. *Communications ACM*, 22, 612–613.
- Shankar, K., Elhoseny, M. 2019. Optimal lightweight encryption based secret share creation scheme for digital images in wireless sensor networks. *Secure Image Transmission in Wireless Sensor Network Applications*, 564, 115–129.
- Thien, C.C., Lin, J.C. 2002. Secret image sharing. *Computer Graphics*, 26, 765–770.
- Verma, O.P., Jain, N., Pal, S.K. 2020. A hybrid-based verifiable secret sharing scheme using chinese remainder theorem. *Arabian Journal for Science and Engineering*, 45, 2395–2406.
- Vyavahare, S., Patil, S. 2016. Analysing secret sharing schemes for audio sharing. *International Journal of Computer Applications*, 137, 39–42.
- Wang, J.N., Wu, T.X., Sun, T.Y. 2015. An audio secret sharing system based on fractal en-coding. In: *Proceedings of 49th International Carnahan Conference on Security Technology*, 211–216.
- Yakubu, M.A., Namunu, C.M., Pradeep, K.A. 2015. Audio secret management scheme using Shamir's secret sharing. *International Conference on Multimedia Modeling*, 8935, 396–407.
- Zhao, R., Zhao, J.J., Dai, F., Zhao, F.Q. 2009. A new image secret sharing scheme to identify cheaters. *Computer Standards and Interfaces*, 31, 252–257.
- Zuquan, L., Guopu, Z., Yu, Z., Hongli, Z., Sam, K. 2024. An efficient cheating-detectable secret image sharing scheme with smaller share sizes. *Journal of Information Security and Applications*, 81, 103709.