Multimedia Tools and Applications (2024) 83:403–423
https://doi.org/10.1007/s11042-023-15625-1

Cheating identifiable polynomial based secret sharing scheme for audio and image

Guttikonda Prashanti[1,2] · **Mundukur Nirupama Bhat**[1]

Received: 16 August 2021 / Revised: 24 December 2021 / Accepted: 22 April 2023 /
Published online: 17 May 2023

Abstract
Polynomial based secret sharing is the art of protecting information and a tool used in areas where a secret has to be distributed among multiple parties. In this method, secret is encrypted into noisy shares and transferred to participants in the group. Decoding of secret is possible only when sufficient number of authorized members in the group, stack their respective shares. In this article, polynomial based secret sharing for audio is proposed that computes a checksum to identify the dishonest participant and also the audio shares generated are of smaller dimension. To achieve this, a polynomial function is defined by considering amplitude values and random values as coefficients. Inclusion of random value as the coefficient of higher degree term in the polynomial makes the audio shares noisy and does not provide any information about the secret. This reduces the overhead of performing preprocessing on original audio before shares are generated. In addition, our proposed method can be used for multi secret sharing. Proposed scheme also facilitates identification of dishonest participant before reconstruction of secret through a trusted entity called combiner.

Keywords Polynomial · Secret sharing · Polynomial function · Coefficients · Discrete logarithms · Security channel · Verification · Dishonest participant · Multi secret · Encoding · Decoding

1 Introduction

With the growth of new network technologies, communication of multimedia files like audio, image, video over internet has increased. Audio data such as songs are transferred through internet by many commercial organizations such as iTunes, Spotify where many people can listen to their favorite music. Such organizations need to store huge audio data that require security aspects. Cloud is a place where many organizations can store their multimedia data securely. Due to security issues in single cloud,

✉ Guttikonda Prashanti
prashantiguttikonda77@gmail.com

[1] Vignan's Foundation for Science, Technology & Research, Vadlamudi, Guntur Dist., Andhra Pradesh, India

[2] Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

users are going for multi-clouds or inter-clouds. One technique for securing the data in multi-clouds is secret sharing algorithms [6, 10, 11, 14]. Not only in cloud computing, secret sharing scheme provides security services in other applications such as Internet of Things [7, 13] and sensor networks [19].

Secret sharing is used in situations where keeping a secret with one person is not reliable. Instead, the secret is split into shares and delivered to a group of authorized persons. Decryption of secret is achieved whenever threshold number of participants agrees and put together their shares. A threshold scheme based on polynomial interpolation has been introduced by Shamir [24] and Berkely [3] independently to protect cryptographic keys. Thien and Lin discussed an image secret sharing method that produces shares of reduced dimensions. The dimensionality reduction is based on threshold. Larger the threshold more reduced the dimensions of the shares [27].

In above schemes, it is supposed that the participants are honest, but in fact, it is impossible in the real world. Participant may himself be dishonest and may submit fake share or tampered instead of original share. This issue has been addressed in this paper. The aim of this work is to propose anew secret sharing scheme to identify cheating behavior of participants before reconstruction of secret and to protect audio and image data from hackers. Our scheme generates encoded shares of reduced size and also verifies whether the participants have submitted the true or fake information before reconstruction of the secret. This scheme consists of mainly three actors namely dealer, participants and combiner. Dealer is a secret holder and generates encoded shares of secret with reduced dimension. Dealer distributes these encoded shares to participants. Participants who want to reconstruct the secret have to submit their encoded shares to combiner. Combiner is a trusted entity or may be a trusted participant who reconstructs the secret after verifying the participant's information. The main goal of proposed method is to identify the cheating behavior and provide confidentiality to audio and image data.

Following are the main contributions of our proposed work from previous schemes:

i) Shorten share dimensions: Proposed secret sharing scheme that generates shares of smaller dimensions. Original audio can be reconstructed without any loss of information.
ii) Verifiable scheme: Proposed new scheme is able to identify if the participant is submitting genuine information or fake information before retrieving the secret.
iii) High security: Since participants possess encoded shares instead of original shares, it will be very difficult for adversary to gain original secret. Experimental result shows that the shares distributed to participants are completely noisy and provides no information about the secret. Thus, our proposed method provides high level security.

The rest of the paper is organized as follows: Some works related to proposed scheme are presented in Section 2. The three phases of proposed work are illustrated in Section 3. Section 4 discusses security analysis. Section 5 shows experimental results and strength of the scheme using different metrics. Section 6 presents advantage of our method. Comparison of our work with other related works are provided in Section 7. Conclusions are highlighted in Section 8.

2 Related work

In this section we illustrate some existing schemes related to our proposed method. Shamir [13] introduced the concept of sharing a secret among a group of n members, where any t members of the group can cooperate with each other to retrieve the secret. This is said to be *(t,n)* threshold scheme. Adapting Shamir's method, Thien-Lin et al. [19] proposed a method for sharing image among a group. Dealer truncates the pixel values of grey scale image to range 0–250 and then permutes them with a secret key so that the image becomes noisy-looking. This noisy image is divided into sections such that each section contains t pixels. Further, image shares are generated by evaluating Eq. 1 with t pixels of each section.

$$f(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_t x^{t-1} mod 251 \tag{1}$$

As t pixels of each section of original image correspond to one pixel in the share, shares generated are of reduced size. To reconstruct the secret, any t shares are required. Applying Lagrange interpolation along with first non-processed pixels of t shares, we can determine the coefficients. These coefficients are t pixel values of noisy image. To get the original image these pixels go through inverse permutation.

Lin and Tsai introduced a method that not only hides the shares into camouflage images but also furnished with the ability of authentication while reconstructing the secret. Disadvantage of this method is that shares constructed are of huge capacity [17]. Authentication ability of [17] has been improvised by Yang et al. [31] to prevent cheating by dishonest participant. Further, to achieve lossless secret sharing they applied Galois Field GF(2^8). Wang and Shyu introduced scalability method that requires all participants to put their shares for reconstruction of secret. Threshold number of participants can recover only partial secret. To get entire secret all participants in the group must combine. This method is limited to *(2,n)* scheme [28]. Yang and Huang [30] enhanced the *(2,n)* scheme to *(k,n)* secret scheme. Lein Harn [15] introduced a scheme against submitting a fake share by both inside and outside adversaries. Kanso [12] employed secret sharing scheme for securing medical images. They used run length encoding scheme for compressing medical images and then shares are generated with GF(31). In traditional secret sharing schemes, threshold t is fixed which may have some problems. So Xingxing Jia [29] proposed a scheme based on Chinese Remainder Theorem to change the threshold from t to t' without updating the shares. Dong Xie [5] adapted compressed sensing technique to generate shares of flexible sizes based on different applications. Their scheme also has addition capability of smooth scalability, noise-resilient capability, and high security. Abhishek Parakh et al. [2] presented a new scheme based on recursive polynomial interpolation for dividing a secret s into shadows of reduced size to achieve storage space efficiency. Noar and Shamir proposed visual secret sharing where decryption is done by simply stacking the shares [20].

Similar studies have also been done on audio known as audio secret sharing scheme (ASS). Desmedt et al. [32] proposed *(2,n)* ASS based on sound inference property, it requires *log2n* cover sounds to embed secret binary text. By simultaneous playing of audio shares and detecting changes in sound volume one can decrypt the secret text. Based on time division Lin et al. [16] developed framework that requires only single cover sound instead of *log2n* cover sounds. Daniel et al. [4] extended *(2,n)* ASS to *(k,n)* ASS by using flat frequencies instead of sound inference property. Huan et al. proposed a framework where the n audio shares generated from binary audio are embedded in n shelter audios which are pretreated by high dimensional matrix transformation [9]. Shivendra Shivani et al. presented a method to provide security to online song repositories. Their method

provided confidentiality to the songs stored in the repositories along with integrity verification and access control to the songs [25].

Zhao et al. [23] extended Thien-Lin scheme to verifiable secret sharing scheme to identify dishonest participant. They used discrete logarithms to identify cheater. Participants choose their own secret shadow and hence no security channel required for communication between dealer and participant. Ma et al. [18] scheme is capable of identifying cheaters when k participants involve in reconstruction. The cheating identification ability and size of shadow in the proposed scheme are improved from the previous cheating identifiable secret image sharing scheme. For cheating detection, some secret sharing schemes [21, 26] adopted a trusted third entity called combiner to verify the participants.

In this paper, we proposed a new secret sharing scheme that generates shares of reduced size and capable of identifying cheaters. Using proposed scheme, dealer generates encoded shares and distributes them to the participants. Since the shares are encoded participants cannot gain any information about the secret. Also, dealer generates verifiable code using one-way hash functions. Combiner uses this code to authenticate the information provided by the participants. Experimental results and statistical analysis show that encoded shares generated are noisy and secret can be reconstructed without any loss of information.

Proposed method is to safe guard audio and image data that can be used in following applications:

Call centers stores call recordings of their customers in servers. Some call recordings contain sensitive information which cannot be accessed by single person. Our proposed work *(t,n)* audio secret sharing can be used to protect such sensitive audio messages. The General Manager (dealer) of call center generates encoded shares of secret audio data and distributes among n supervisors (participants). Only when at least t or more number of supervisors submit their true encoded shares to the branch manager (combiner), secret audio data can be retrieved.

In medical applications some patient's medical conditions and their images has to be kept secret. Disclosing entire condition of some important patient to one doctor is not reliable. In such scenarios, our proposed secret sharing scheme on image can be used which divides medical image into encoded shares that are distributed among a group of doctors and a threshold number of doctors under a trusted entity can retrieve the image for diagnosis.

Military communications include transmission of secret image such as military map along with audio signals that contain sensitive messages. Providing the entire sensitive information to single commander is not secure as he may compromise. In such conditions proposed multi secret sharing scheme can be applied. The secret (audio and image) at a time can be distributed among a group of commanders in the form of encoded shares. Secret can be retrieved only by combiner when sufficient number of commanders comes together.

3 Proposed scheme

The proposed method allows the secret audio A to be divided into n shares with smaller dimensions, and identify dishonest participant before secret reconstruction. Dealer D is a trusted entity and a secret holder, generates shares from the secret and distributes them to the participants. To reconstruct the secret, threshold number of participants has to come together. They have to submit their shares to the combiner C. Combiner is a trusted third

party whose role is to verify whether the participants have submitted true information. If the information submitted by the participants is true than combiner reconstructs the secret and reveals the secret to the participants. This section is divided into three phases: Initialization phase, share construction and distribution phase, verification and secret reconstruction phase. The notations of variables used in the proposed work is provided in Table 1.

In initialization phase, dealer generates values (N, g, e, d) with the properties of RSA algorithm and transmits *(e,d)* value to combiner through secure channel. In share construction and distribution phase, dealer computes *ID* value by choosing a unique value for each participant. Then using ID_i value and secret audio A, dealer generates shares A^i from proposed share generation procedure. Dealer encodes ID_i to EID_i using discrete logarithms, A^i to ES_i with pseudo random sequence and generates a verifiable code HS_i from one way hash function. The values (EID_i, ES_i, HS_i) are distributed to the participant$_i$, for $i \ \varepsilon \ [1,n]$ instead of original ID_i and A^i.

In verification and reconstruction phase, any t or more number of participants have to come together to retrieve the secret. Each participant has to submit their (EID_i, ES_i, HS_i) to the combiner. Combiner reconstructs the original A^i and ID_i and checks its authenticity with the verification code HS_i. If found authentic, means participant$_i$ has provided true information. After authenticating all the t participants and obtaining valid information, combiner reconstruct the secret audio A using Lagrange's interpolation and reveals the secret to t participants. Figure 1 shows three phases of proposed method.

Table 1 Notations of variables used

Variable	Definition
D	Dealer
C	Combiner
t	Threshold for deriving original secret
n	Number of participants
$P=(P_1, P_2, .. P_n)$	Set of n participants
A	Original secret audio
$(A^1, A^2, A^3 \ldots A^n)$	n audio shares for n participants
a_i	Original secret audio sample $(a_i \in A)$
a_0^i	First audio sample of audio share A^i
e, d	Secret values of dealer and combiner
ID_i, EID_i	Identity and encoded identity of participant i
g	generator
h	Hash algorithm
$PRNG$	Pseudo random number generator
ES_i	Encoded audio share of i participant
HS_i	Verifiable code of i participant
$P^{'}=(P_1, P_2 \ldots . P_t)$	Threshold number of participants
r	Array of random numbers
I	Original secret Image
$I^{'}$	Encrypted secret Image
b_i	i^{th} Pixel of secret image I
$b_i^{'}$	i^{th} Pixel of encrypted secret image $I^{'}$
r_j	j^{th} Random number in array r

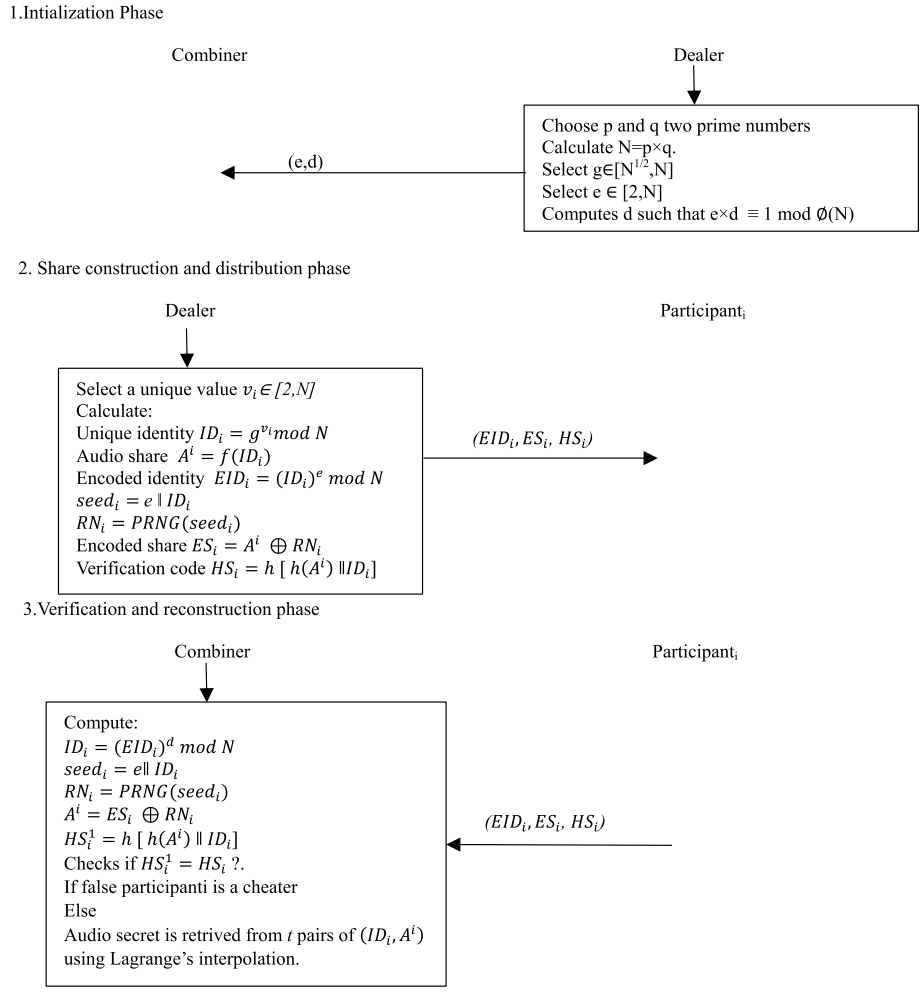

Fig. 1 Proposed method

3.1 Initialization phase

This module deals with computation of (N, g, e, d) values by the dealer. Considering the properties of RSA algorithm, dealer chooses p and q two prime numbers and calculates $N=p\times q$. Finds generator $g\in[N^{1/2},N]$ and also relatively prime to p and q. Finds an integer $e \in [2,N]$ in a way that e is relatively prime to $(p-1)$ and $(q-1)$ and then computes d such that $e\times d\equiv 1 \bmod \varnothing(N)$ where $\varnothing(N)$ is Euler phi function. Then sends (e,d) to the combiner through secure channel.

3.2 Share construction and distribution phase

In this phase, dealer generates shadows of the shares along with verification code that are distributed among the participants $P=(P_1, P_2, .. P_n)$.

3.2.1 Identity generation

For each participant $P_i \in P$, D randomly selects a unique value $v_i \in [2,N]$ and calculates ID_i using Eq. 2.

$$ID_i = g^{v_i} mod\ N \tag{2}$$

3.2.2 Share generation

In this module, polynomial based Secret sharing scheme of *(t,n)* threshold for secret audio A is proposed that generates n audio shares $(A^1, A^2, A^3 \ldots A^n)$ of smaller dimensions. D generates a polynomial function of *(t-1)* degree. The secret audio is read with a sample depth of 8 bits so that the sampled values $(a_0, a_1, a_2 \ldots)$ are in range 0–255. These are further divided into portions such that each portion consists of *(t-1)* audio samples. While defining the polynomial function, *(t-1)* audio samples of a given portion are considered as coefficients for lower degree terms. Random number is generated and is taken as coefficient for leading term. Then polynomial function is evaluated for n participants to obtain n shares with x value defined by the participant**.**

Since *(t-1)* sampled values of a given portion are evaluated to one sampled value of audio share, we obtain shares whose dimensions are diminished to *1/t-1* of confidential audio. The subsequent steps followed by D for constructing audio shares are given below:

1. Let the secret audio be A. Scan the audio data from A and write into y.
2. For each value a_i of y

   2.1 If $a_i < 250$ then store a_i value in array B
   2.2 If $a_i \geq 250$ then store a_i in B as two values first 250 and then $(a_i\text{-}250)$

3. Divide the array B into portions such that each portion has *t-1* values.
4. Generate an array of random numbers r, of size equal to the number of portions.
5. For each portion j and random value r_j, we define polynomial function as Eq. 3.

$$f(x) = a_0 + a_1 x + \cdots . + a_{t-1} x^{t-2} + r_j x^{t-1} mod 251 \tag{3}$$

   To generate share A^i for the P_i participant where $i \in [1, n]$, evaluate above equation as $q_j = f(ID_i)$ for each portion and assign the corresponding q_j value to A^i. ID_i is a unique value computed by D for participant P_i.
6. Repeat step 5 for all n participants to get shares $(A^1, A^2, A^3 \ldots A^n)$.

3.2.3 Share encoding and distribution

Before distributing the shares, dealer encodes ID_i and audio shares A^i of the participants.

Dealer computes encoded identity EID_i from ID_i along with secret value e using Eq. 4.

$$EID_i = \left(ID_i\right)^e \ mod\ N \tag{4}$$

To encode the audio share, pseudo random sequence is generated using pseudo random function PRNG that takes a seed value. Seed value is generated from Eq. 5 with secret entity e and ID_i of the participant,

$$seed_i = e||ID_i \tag{5}$$

$$RN_i = PRNG\left(seed_i\right) \tag{6}$$

Pseudo random sequence RN_i generated from Eq. 6 is XORed with audio share A^i, to obtain encoded share ES_i as shown in Eq. 7.

$$ES_i = A^i \oplus RN_i \tag{7}$$

Dealer computes verification code HS_i from Eq. 8, by applying hash function h on original audio share A^i and identity ID_i.

$$HS_i = h\left[h\left(A^i\right)||ID_i\right] \tag{8}$$

Dealer sends (EID_i, ES_i, HS_i) to participant P_i. Hash function 'h' and pseudo random function PRNG is private between dealer and combiner.

3.3 Verification and reconstruction phase

Decipherment of secret is done by pooling t or more encoded shares. Consider $P^{'} = (P_1, P_2 \ldots . P_t)$ be group of members who want to reconstruct the secret.

3.3.1 Verification process

Members of $P^{'}$ have to submit their (EID_i, ES_i, HS_i) values to the combiner. Combiner decodes audio shares and identities with secret pair (e, d). First ID_i is decoded from EID_i using Eq. 9.

$$ID_i = \left(EID_i\right)^d \ mod\ N \tag{9}$$

Next, for decoding audio share A^i from ES_i, combiner creates Eqs. 4 and 5 from e and ID_i as mentioned below

$$seed_i = e||ID_i$$
$$RN_i = PRNG\left(seed_i\right)$$

Original share A^i is acquired from Eq. 10, where pseudo random sequence RN_i is XORed with audio share ES_i

$$A^i = ES_i \oplus RN_i \tag{10}$$

From A_i and ID_i, combiner computes $HS_i^1 = h\left[h\left(A^i\right)||ID_i\right]$ and checks if $HS_i^1 = HS_i$?. If 'yes' information submitted by participant P_i is true else P_i is dishonest.

3.3.2 Reconstruction of secret

The members in the group $P^{'}$ can reconstruct the secret with their t pairs of (ID_i, A^i). The following steps are to be proceeded for reconstruction of secret:

1. Extract the first unused amplitude values from each of the t audio shares $(A^1, A^2, A^3 \ldots A^t)$. Let the first sampled values of t audio shares be $\left(a_0^1, a_0^2, a_0^3 \ldots a_0^t\right)$.
2. Substituting these t values and ID_i as x_i values of $P^{'} = (P_1, P_2 \ldots P_t)$ in Eq. 11.

$$\begin{aligned} f(x) = & a_0^1 \frac{(x-x_2)(x-x_3)\ldots(x-x_t)}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_t)} \\ & + a_0^2 \frac{(x-x_1)(x-x_3)\ldots(x-x_t)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_t)} + \ldots \\ & + a_0^t \frac{(x-x_1)(x-x_2)\ldots(x-x_{t-1})}{(x_t-x_1)(x_t-x_2)\ldots(x_t-x_{t-1})} \end{aligned} \tag{11}$$

3. Simplifying Eq. 11, we obtain a polynomial function *f(x)* (Eq. 12) of degree *(t-1)*. The terms in *f(x)* are arranged from left to right in ascending order.

$$f(x) = a_0 + a_1 x + \cdots . + a_{t-1} x^{t-2} + r_j x^{t-1} mod 251 \tag{12}$$

The *t-1* coefficients of above equation are stored in array *B*.

4. Repeat steps from 1 to 3, until all sampled values of audio shares are processed.
5. For each element o_i of *B*

5.1 If $o_i < 250$ then store o_i into *A'* and sequentially read the next value in *B*.
5.2 If $o_i = 250$ then read immediate next value o_{i+1} and store $(o_i + o_{i+1})$ value in *A'*. As o_{i+1} has been used, we read the next value o_{i+2}.

6. *A'* is the reconstructed audio which is obtained without any loss of information.

For example, in a (3, 4) scheme, let the first two amplitude values in the audio are $(a_0, a_1) = (78, 241)$ and random value 92. Let the participant's identities are 50, 60, 150, 160 for shares 1, 2, 3 and 4 respectively. Then first amplitude values for four shares are obtained using Eq. 3 in Section 3.2:

$$\begin{aligned} a_0^1 &= 78 + 241 \times 50 + 92 \times 50^2 mod\ 251 = 164 \\ a_0^2 &= 78 + 241 \times 60 + 92 \times 60^2 mod\ 251 = 111 \\ a_0^3 &= 78 + 241 \times 150 + 92 \times 150^2 mod\ 251 = 87 \\ a_0^4 &= 78 + 241 \times 160 + 92 \times 160^2 mod\ 251 = 51 \end{aligned}$$

Repeating the above procedure for all amplitude values creates four audio shares. For decoding, any three participants have to submit their identities. Suppose we have (50, 164), (60, 111), (150, 87). We could gain *f(x)* from Eq. 11 in Section 3.3 as follows:

$$f(x) = 164\frac{(x-60)(x-150)}{(50-60)(50-150)} + 111\frac{(x-50)(x-150)}{(60-50)(60-150)} + 87\frac{(x-50)(x-60)}{(150-50)(150-60)}$$
$$f(x) = 78 + 241x + 92x^2 mod 251$$

Finally, 78 and 241 are the two amplitude values of original audio that are recovered.

4 Security analysis

In this section we have analyzed the recoverability and confidentiality of shares generated through our proposed scheme. We also discussed how cheaters can be identified efficiently.

Theorem 1 *Any (t-1) or fewer participants cannot gain any information about the secret.*

Proof Suppose *(t-1)* participants cooperate together, with *(t-1)* encoded shares they can construct *(t-1)* polynomials equations and has to solve these set of equations.

$$f(ID_1) = a_0 + a_1 ID_1 + \cdots . + a_{t-1} ID_1^{t-2} + r_1 ID_1^{t-1} mod\ 251$$
$$f(ID_2) = a_0 + a_1 ID_2 + \cdots . + a_{t-1} ID_2^{t-2} + r_2 ID_2^{t-1} mod\ 251$$
$$\vdots$$
$$f(ID_{t-1}) = a_0 + a_1 ID_{t-1} + \cdots . + a_{t-1} ID_{t-1}^{t-2} + r_j ID_{t-1}^{t-1} mod\ 251$$

Since the amplitude values of audio shares are in range 0 to 250. The possibility of guessing each a value is $\frac{1}{251}$. For a secret audio of size 91240×1, there are $91240 \times 1/(t\text{-}1)$ polynomials. The possibility to achieve the secret audio is

$$\left(\frac{1}{251}\right)^{91240\times 1/t-1}$$

As this is a very small number, there is a very little chance of getting the secret audio. Further, the participants have the encoded version of shares $ES_i$and identities EID_i, rather than original shares and identities. Decoding them by participants requires secret entity e, d of the combiner. Thus, it is difficult for the participants to gain the original identities and shares from (ES_i, EID_i). Therefore, any *(t-1)* participants cannot recover the secret by pooling their information.

Theorem 2 *Having t or more true encoded shares, the retrieval of secret is realizable only by the combiner rather than the participants.*

Proof As mentioned in Section 3.2, each participant holds encoded shares (EID_i, ES_i) generated with secret entity e of the combiner. Since, $EID_i = g^{v_i e} mod\ N$. From this deriving ID_i is difficulty as the adversary do not having any information about values (v_i, e) and it requires solving discrete logarithms which is NP problem. Further, computation of A^i from ES_irequires $seed_i$ derived from (e, ID_i) pair. Thus, the participants cannot retrieve the secret.

As the secret values *(e,d)* are known to the combiner, the following operations are performed to get (ID_i, A^i).

Computes ID_i with d value: $\left(EID_i\right)^d = g^{v_i ed} = g^{v_i} mod\ N = ID_i$.

Achieving ID_i and knowing e value, compute share A^i as follows:

$$seed_i = e||ID_i$$
$$RN_i = PRNG\left(seed_i\right)$$
$$ES_i \oplus RN_i = A^i \oplus RN_i \oplus RN_i = A^i$$

Thus, combiner successfully decodes the information of participant$_i$ as (ID_i, A^i). Likewise, after decoding information of all participants, combiner applies Lagrange's interpolation and retrieves the secret.

Theorem 3 *Combiner can successfully identify the dishonest participant*

Proof To retrieve the secret, at least t participants must submit (ES_i, EID_i, HS_i) to the combiner. Let participant$_j$ submit $\left(EID'_j, ES'_j\right)$ instead of (EID_j, ES_j) then combiner with his secret value e and d computes

$$\left(EID'_j\right)^d = ID'_j\ different\ from\ ID_j$$
$$e||ID'_j = seed'_j$$
$$RN'_j = PRNG\left(seed'_j\right)$$
$$ES'_j \oplus RN'_j = A^{j'} \neq A^j$$
$$HS'_j = h\left[h\left(A^{j'}\right)||ID'_j\right]$$

As HS'_j is different from HS_j, participant$_j$ is marked as 'dishonest'. It is very hard for participant$_j$ to change the values of (ES_j, EID_j) such that it matches HS_j.

5 Experimental analysis

5.1 Feasibility of our method for (3, 4) threshold scheme

As mentioned in Section 3.1, dealer computes secret pair *(e,d)* and sends to combiner through secure channel. With 4 participants and 3 as threshold, dealer generates 4 shares such that any 3 participants can retrieve the secret. For this, initially dealer chooses 4 distinct values for 4 participants and computes 265, 584, 78, 815 as ID_i for each participant using Eq. 2.

For secret audio A, dealer generates shares A^i by evaluating Eq. 3. Results of audio sharing process is shown in Fig. 2a is the secret audio of dimension 91,240 × 1; (b)-(e) are the audio shares of dimension 45,620 × 1 generated for four participants with ID values (265, 584, 78, 815); f) is the lossless reconstructed audio constructed with (265, 584, 78).

Dealer encodes the identities ID_i of the participants with secret value e (Eq. 4) and also audio shares A^i with pseudo random sequence generated from the seed value (Eqs. 5, 6 and 7). Figure 3 shows the encoded shares that are distributed to the participants.

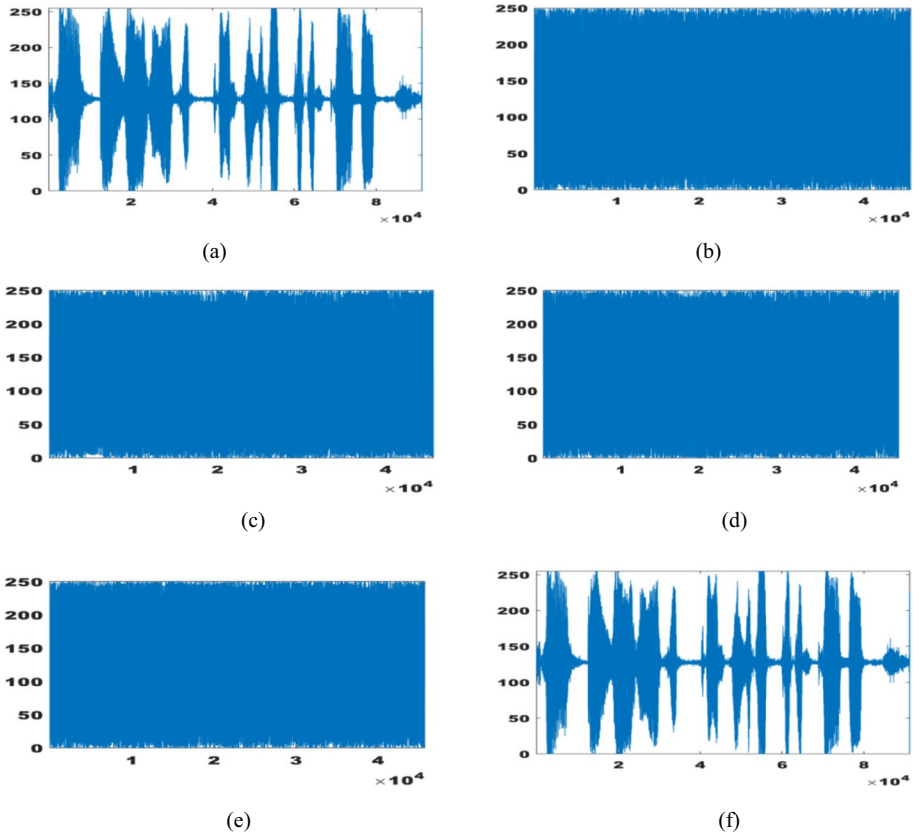

Fig. 2 **a** to **f** are audio plots related to share construction and reconstruction of secret

5.2 Correlation analysis

The proposed method generates shares of smaller dimensions provided that they are noisy for concealing information. In audio data the adjacent amplitude values are correlated. To eliminate the correlation between audio samples, our proposed method includes a random coefficient for higher degree term as a blinding factor and other lower terms takes amplitude values as given in Eq. 3.

To compute similarity among audio shares and original audio, we used Pearson correlation coefficient represented by Eq. 13.

$$r = \frac{\sum_{i=1}^{m}\left(X_i - \overline{X}\right)\left(Y_i - \overline{Y}\right)}{\sqrt{\left(\sum_{i=1}^{m}\left(\left(X_i - \overline{X}\right)\right)^2\right)\left(\sum_{i=1}^{m}\left(\left(Y_i - \overline{Y}\right)\right)^2\right)}} \tag{13}$$

Here m is total number of audio samples in audio share. $\left(X_i\right)_{i=1}^{m}$ are the first m adjacent sampled values of the original audio. $\left(Y_i\right)_{i=1}^{m}$ are the adjacent audio samples of audio share. Results are shown in Table 3. For shares as the correlation coefficient is less, we can say that original audio and shares are dissimilar. The relation between the sampled

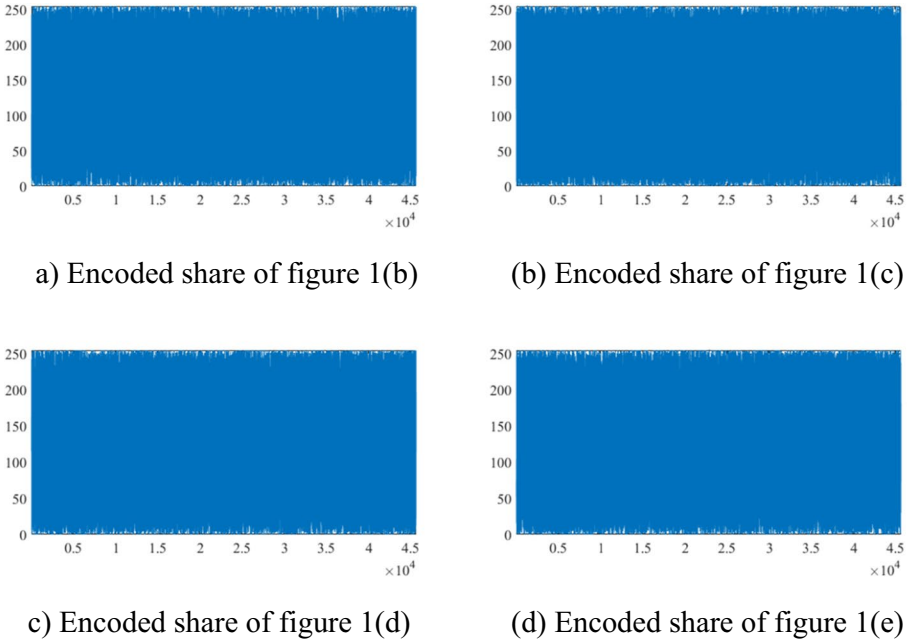

Fig. 3 Encoded shares distributed to the participants

values present in original audio is eliminated in the shares thereby providing no information about the secret. Similarity score is about 1 between original audio and reconstructed audio which shows that audio is reconstructed without any loss of information. Figure 4 shows plot of randomly selected 3000 adjacent sampled values of original audio and shares generated. Figure 4a shows the plot of adjacent sampled values of original audio which are

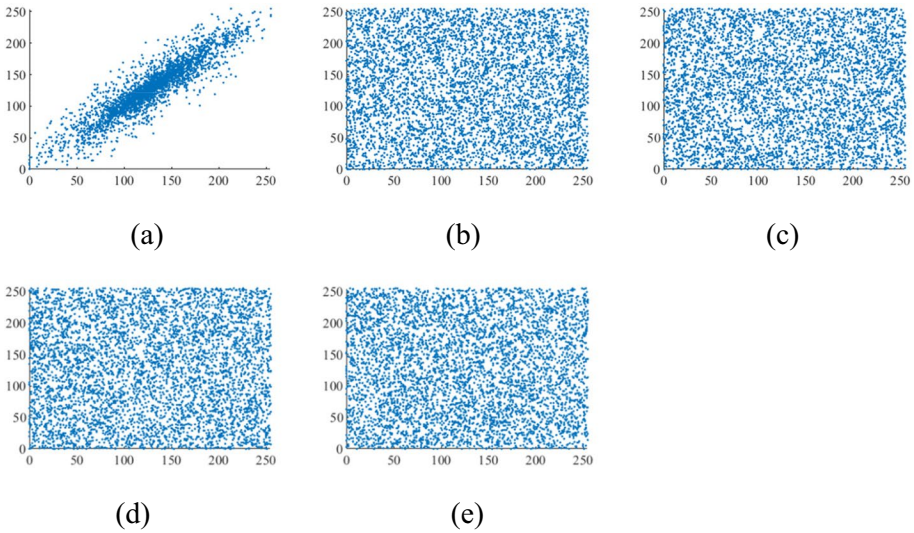

Fig. 4 Plot for 3000 random horizontal adjacent sampled values of original audio and encoded shares

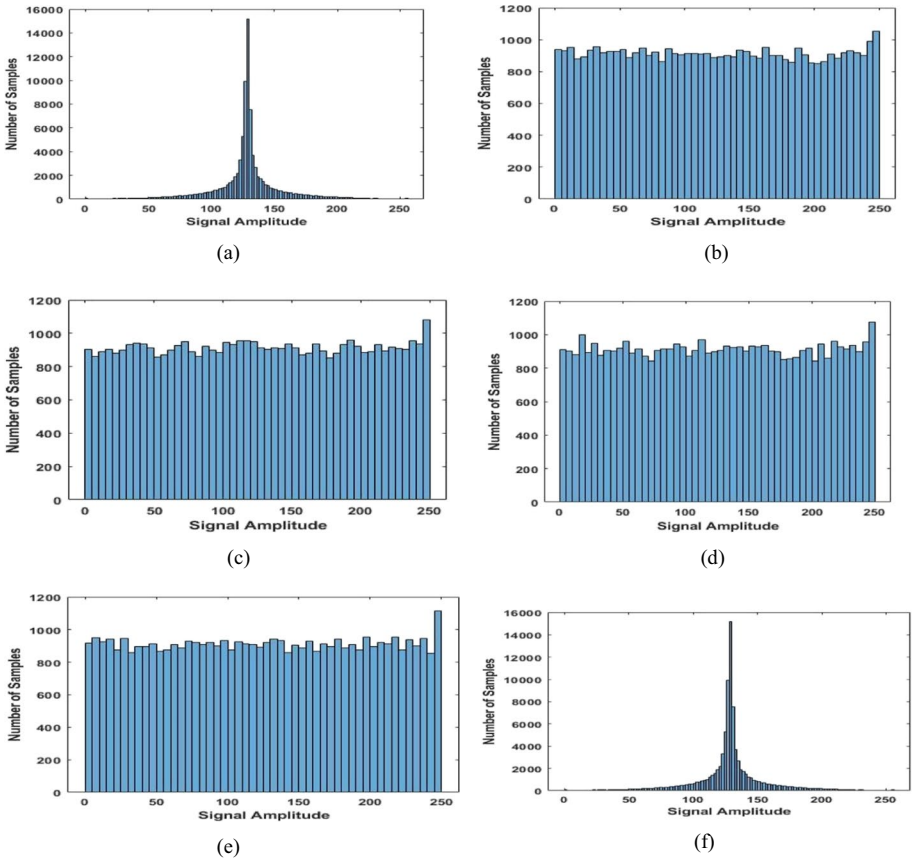

Fig. 5 Histogram analysis

in diagonal line that indicates close similarity between them, (b) to (e) are plots of encoded shares where the correlation between sampled values are eliminated thereby showing random pattern. For horizontal adjacent pairs we get the correlation coefficient values for original audio and encoded share as 0.95, −0.0075, 0.00101, −0.00109, 0.0033.

5.3 Histogram analysis

Histogram for audio provides visual representation of signal distribution. Figure 5a, b, c, d, e shows histogram of original audio, its encoded shares and reconstructed audio. Histograms of encoded audio shares shows that the amplitude values are distributed

Table 2 UACI values obtained between the encoded shares

	Encoded share 1	Encoded share 2	Encoded share 3	Encoded share 4
Encoded share 1	0	33.8404	33.8872	33.8161
Encoded share 2	33.8404	0	33.8085	33.8567
Encoded share 3	33.8872	33.8085	0	34.0655
Encoded share 4	33.8161	33.8567	34.0655	0

Table 3 PSNR, NSCR and correlation coefficient for original and audio shares

Audio files	Correlation coefficient (r)	PSNR	NSCR
Original audio & audio share 1	−0.0049	10.0590	99.6519
Original audio & audio share 2	0.0054	10.1256	99.6431
Original audio & audio share 3	−0.0017	10.0795	99.6412
Original audio & audio share 4	0.0028	10.2588	99.6213
Original audio & reconstructed audio	1	∞	0

nearly flat which indicates that they are noisy and have no statistical relation with original audio samples. Histogram of reconstructed audio in Fig. 5e is identical to the histogram of original audio shown in Fig. 5a. This proves that proposed method can successfully reconstruct the secret audio without any loss of amplitude values.

5.4 Number of samples change rate (NSCR)

One important requirement of secret sharing process is that the shares should be totally different from the original secret. Number of samples change rate (NSCR) is a test that computes the difference between the two audio segments and can be calculated using Eq. 14.

$$NSCR = \frac{\sum_i D_i}{L} \times 100 \tag{14}$$

Where D_i is 1 if corresponding samples of two audios are different, otherwise D_i is 0. Table 3 shows the NSCR test results between original audio and audio shares. Obtained NSCR values for audio shares and encoded shares are listed in Table 4. NSCR values in both tables are high, indicating that two audios are significantly different from one another. In Table 3, last row indicates NSCR value for original audio and reconstructed audio which is zero. This shows that our proposed scheme is lossless secret sharing scheme.

5.5 UACI (Unified Average Changing Intensity)

One test to measure similarity between two noisy signals is UACI (Unified Average Changing Intensity). Suppose S_1 and S_2 are two noisy signals of length N. UACI value can be calculated using Eq. 15.

$$UACI = \frac{1}{N} \sum_i \frac{| S_1(i) - S_2(i) |}{255} \tag{15}$$

Table 4 PSNR, NSCR, UACI and correlation coefficient for audio shares and encoded audio shares

Audio files	Correlation coefficient (r)	PSNR	NSCR	UACI
audio share 1 & encoded share 1	−0.0053	7.6377	100	33.5310
audio share 2 & encoded share 2	0.0013	7.6813	100	33.5149
audio share 3 & encoded share 3	−0.0011	7.6675	100	33.5603
audio share 4 & encoded share 4	−0.0066	7.6272	100	33.4947

Table 2 shows UACI values obtained between the encoded shares that are distributed to participants. According to literature [1, 8], it can be observed that the values are higher than ideal value (33.46%) which shows the proposed scheme is resistive to different attacks. In Table 4, UACI values are nearer to ideal value which shows that there is no similarity between the audio shares and its respective encoded shares.

5.6 Peak signal-to-noise ratio

PSNR is most commonly used to test quality between original image and reconstructed image. The PSNR value for original audio with reference to obtained audio shares, along with reconstructed audio are listed in Table 3. Smaller PSNR values in Table 3, shows that shares are noisy which means that signals are almost destroyed and does not provide any information about the secret audio. PSNR value between original and reconstructed audio is ∞. This proves the lossless reconstruction of secret audio. In our proposed method, participants are provided with encoded audio shares instead of original audio shares and PSNR values between these two are shown in Table 4. These values shows that audio shares distributed to participants are dramatically randomized and are resistant to attacks.

5.7 Results of proposed method for images

As grayscale images carry pixel values in range 0–255, so our proposed scheme is applicable to images also. To generate image shares, D will execute steps 1 to 6 of Section 3.2 with pixels of the secret image instead of sampled values of secret audio. Experimental results of our proposed scheme on images are shown in Fig. 6a secret image; (b) to (e) are encoded shares; (f) shows reconstructed secret image.

6 Benefit of our proposed scheme

One benefit of our scheme is that it supports multi secret sharing. Suppose the dealer want to share a secret image along with secret audio that is two secrets during one secret sharing process. Initially the dealer truncates the values in range 251–255 in audio and image to 250. Dealer then encrypts the image with symmetric key k so the correlation between pixels can be eliminated. The encryption process is as follows:

1. With k as seed value, generate an array r of random numbers. The size of this array is equal to the size of image I.
2. Every pixel in the image I is treated with Eq. 16 to get the encrypted image I'

$$b'_i = b_i + r_i + b'_{i-1} mod\ 251 \tag{16}$$

Where b_i is i^{th} pixel of image I, r_i is i^{th} random value in array r, b'_i and b'_{i-1} are i^{th} and $(i\text{-}1)^{th}$ pixel of image I'. Initially b'_{i-1} is 0.

After encryption of image, shares are generated using the proposed secret sharing process in Section 3.2 where the lower degree terms of the polynomial Eq. 3 have truncated sampled values of audio as coefficients and pixels of encrypted image as coefficient of higher degree term instead of random numbers.

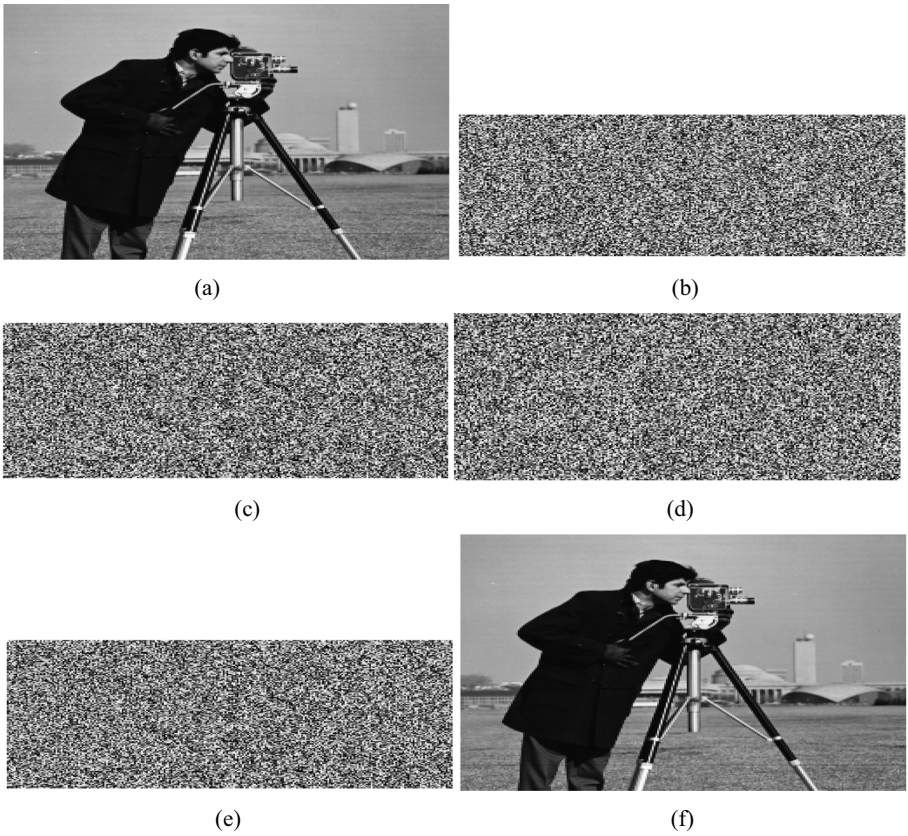

Fig. 6 Experimental results for image

Secrets are reconstructed by executing the steps 1 to 3 in Section 3.3, whereby the polynomial of degree *(t-1)* is built. The *(t-1)* coefficients of the polynomial are extracted and stored as audio values and the coefficient of leading term is stored as pixel value of image. Image obtained is an encrypted image I' which requires decryption. Using key k as seed value, random numbers equal to number of pixels in encrypted image are generated and stored in array r. The pixels of image I is obtained from the Eq. 17.

$$b_i = \left(b'_i - r_i - b'_{i-1}\right) mod\ 251 \tag{17}$$

Finally obtained audio data and pixels of the image carry values less than 250. They are restored to range 251–255 by executing step 5 in Section 3.3 so as to obtain lossless secret audio and image. Experimental results for sharing both audio and image in one secret sharing process is shown in Fig. 7. Results shows that shadows for image are not generated because the pixel values are combined with audio samples of audio shares. So, the dealer can use this method for watermarking purpose also. The present method of multiple secrets is performed using audio and image. It can also be extended to text [22] using ASCII values.

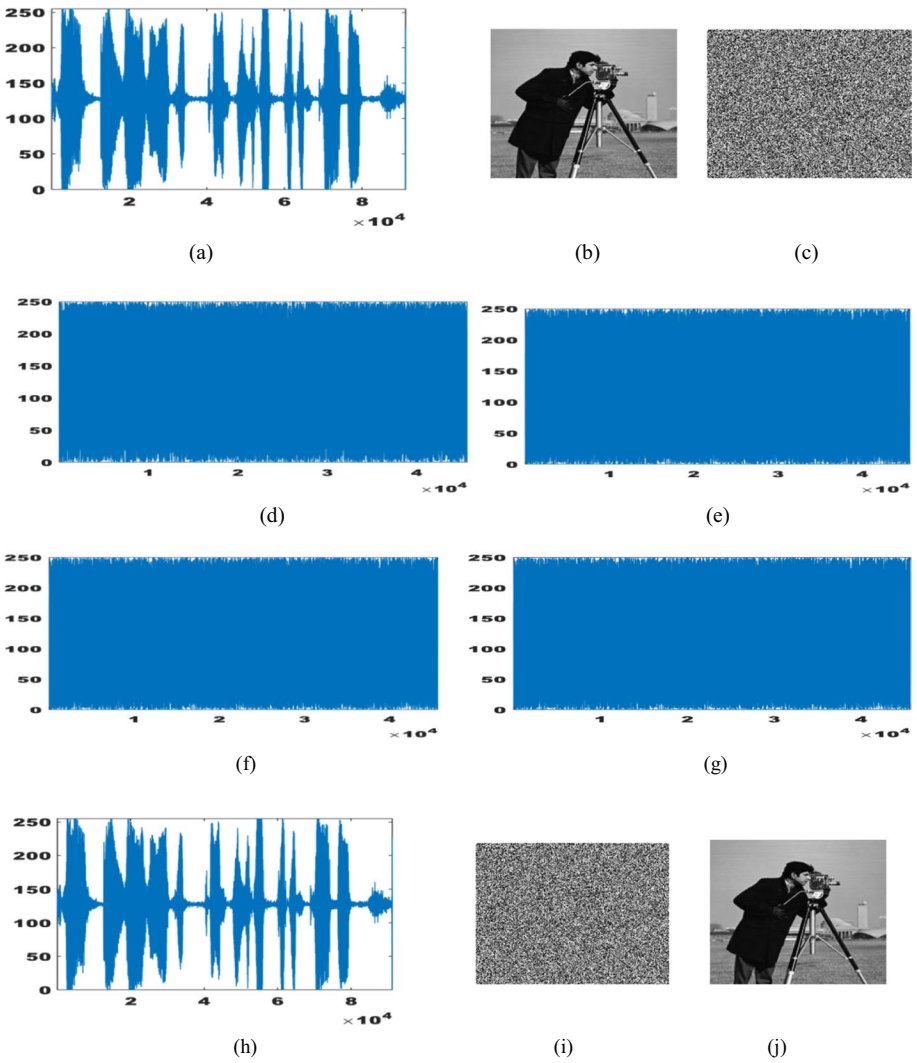

Fig. 7 **a** secret audio; **b** secret image; **c** encrypted image of **b**; **d** to **g** are generated shares; **h** reconstructed secret audio; **i** reconstructed image; **j** decrypted image of **i**

7 Comparison

When compared to existing secret sharing scheme our new scheme has some important properties which are summarized in Table 5. Our scheme has following properties:

1) Combiner can successfully verify any participant whether he/she is providing true information before reconstructing the secret.
2) As shares are encrypted with the secret pair *(e,d)* in Section 3.1, dealer can use either secure channel or public channel to distribute the encrypted shares to the participant.

Table 5 Comparison of proposed method with other works

Capability	[24]	[27]	[23]	Our scheme
Verification of any participant against cheating	no	no	yes	yes
Communication channel between dealer and participant	Secure channel	Secure channel	Public channel	Through any channel
Combiner verification	no	no	no	yes
Multi-secret sharing	no	no	no	yes
Use of permutation key on secret to get noisy shares	no	yes	yes	no
Smaller share size when compared to original secret	no	yes	yes	yes

3) In our proposed secret sharing scheme, *(t-1)* sampled values of the secret audio for a given section of original audio is evaluated to one audio sample of the share. Hence the size of the shares is reduced to *1/t-1* of the original image.
4) Our scheme does not require any permutation operations before construction of shares. Having random number as the leading coefficient of polynomial Eq. 2 in Section 3.2, itself is sufficient for generating noisy shares. Further noisy shares are encrypted thereby increasing the security of the scheme.
5) Experimental results in Section 6 shows that in one secret sharing process, we can share two secrets. So, our method can be used for multi secret sharing.

8 Conclusion

We proposed a method for deriving audio shares from the secret audio characterized by dimensionality reduction and noisiness. Dimension of individual share is diminished to *1/t-1* of the secret audio by having the coefficient of the polynomial as amplitude values in conjunction with random values. Inclusion of random numbers creates noise audio shares thereby reducing the burden of performing permutations before share generation process. Additionally, another method is also proposed where the participants are verified by the combiner before secret reconstruction against cheating. Experimental results show that our scheme is applicable to image files and also supports multi secret sharing scheme. Proposed system ensures that the shares generated are noisy and can be reconstructed without loss of information along with a verification mechanism to identify dishonest participant.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflicts of interest/competing interests The authors declare they have no conflicts / competing interests.

References

1. Abdelfatah RI (2020) Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. IEEE Access 8:69894–69907. https://doi.org/10.1109/ACCESS.2020.2987197
2. Abhishek P, Subhash K (2011) Space efficient secret sharing for implicit data security. Inf Sci 181:335–341. https://doi.org/10.1016/j.ins.2010.09.013
3. Blakley GR (1979) Safeguarding cryptographic keys. In: Proceedings of the AFIPS National Computer Conference, vol 48, pp 313–317
4. Daniel S, Spyros SM (2005) General access structures in audio cryptography. IEEE International Conference on Electro Information Technology, Lincoln, NE, USA, pp 6. https://doi.org/10.1109/EIT.2005.1627018
5. Dong X, Lixiang L, Haipeng P, Yixian Y (2017) A secure and efficient scalable secret image sharing scheme with flexible shadow sizes. PLoS One 12:1–17. https://doi.org/10.1371/journal.pone.0168674
6. En Z, Ming L, Siu-Ming Y, Jiao D, Jun-Zhe Z, Gang-Gang J (2021) Fair hierarchical secret sharing scheme based on smart contract. Inf Sci 546:166–176. https://doi.org/10.1016/j.ins.2020.07.032
7. Harkeerat K, Pritee K (2020) Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. Future Gener Comput Syst 102:30–41. https://doi.org/10.1016/j.future.2019.07.023
8. Hu W, Wu T, Chen Y, Shen Y, Yuan L (2021) A lossless secret image sharing scheme using a larger finite field. Multimed Tools Appl 80:28731–28743. https://doi.org/10.1007/s11042-021-11104-7

9. Huan L, Zheng Q, Xuanping Z, Xu W (2011) Auditory cryptography security algorithm with audio shelters. Adv Control Eng Inf Sci-Procedia Eng 15:2695–2699. https://doi.org/10.1016/j.proeng.2011.08.507
10. Jeonghun C, Sushil KS, Tae WK, Jong HP (2021) Blockchain-empowered cloud architecture based on secret sharing for smart city. J Inf Secur Appl 57:102686. https://doi.org/10.1016/j.jisa.2020.102686
11. Jian S, Dengzhi L, Xingming S, Fushan W, Yang X (2020) Efficient cloud-aided verifiable secret sharing scheme with batch verification for smart cities. Future Gener Comput Syst 109:450–456. https://doi.org/10.1016/j.future.2018.10.049
12. Kanso A, Ghebleh M (2018) An efficient lossless secret sharing scheme for medical images. J Vis Commun Image Represent 56:245–255. https://doi.org/10.1016/j.jvcir.2018.09.018
13. Lake B, Mihailo I, Michel AK (2019) A secure and robust scheme for sharing confidential information in IoT systems. Ad Hoc Netw 92:101762. https://doi.org/10.1016/j.adhoc.2018.09.007
14. Lakshmi VS, Deepthi S, Deepthi PP (2021) Collusion resistant secret sharing scheme for secure data storage and processing over cloud. J Inf Secur Appl 60:102869. https://doi.org/10.1016/j.jisa.2021.102869
15. Lein H, Changlu L, Yong L (2015) Fair secret reconstruction in (t, n) secret sharing. J Inf Secur Appl 23:1–7. https://doi.org/10.1016/j.jisa.2015.07.001
16. Lin CC, Tsai WH (2003) Secret image sharing with capability of share data reduction. Opt Eng 42:2340–2345. https://doi.org/10.1117/1.1588661
17. Lin CC, Tsai WH (2004) Secret image sharing with steganography and authentication. J Syst Softw 73:405–414. https://doi.org/10.1016/S0164-1212(03)00239-5
18. Ma Z, Ma Y, Huang X, Zhang M, Liu Y (2020) Applying cheating identifiable secret sharing scheme in multimedia security. J Image Video Proc 2020:42. https://doi.org/10.1186/s13640-020-00529-z
19. Na W, Junsong F, Jiwen Z, Bharat KB (2018) Source-location privacy full protection in wireless sensor networks. Inf Sci 444:105–121. https://doi.org/10.1016/j.ins.2018.02.064
20. Naor M, Shamir A (1995) Visual cryptography. In: De Santis A (ed) Advances in cryptology-EUROCRYPT'94, Lecture notes in computer science, vol 950. Springer, Berlin, pp 1–2. https://doi.org/10.1007/BFb0053419
21. Phiri KK, Ali P, Eneya L, Kim H (2018) Linear (t, n) secret sharing scheme based on single polynomial. Int J Appl Eng Res 13:11600–11605
22. Prashanti G, Nirupama BM (2020) Polynomial-based secret sharing scheme for text, image and audio. J Inst Eng (India): B 101:609–621. https://doi.org/10.1007/s40031-020-00475-4
23. Rong Z, Jian JZ, Fang D, Feng QZ (2009) A new image secret sharing scheme to identify cheaters. Comput Stand Interfaces 31:252–257. https://doi.org/10.1016/j.csi.2007.10.012
24. Shamir A (1979) How to share a secret. Commun ACM 22:612–613. https://doi.org/10.1145/359168.359176
25. Shivendra S, Shailendra T, Krishn KM, Zhigao Z, Arun KS (2018) Providing security and privacy to huge and vulnerable songs repository using visual cryptography. Multimed Tools Appl 77:11101–11120. https://doi.org/10.1007/s11042-017-5240-6
26. Shyamalendu K, Bibhas CD (2020) A verifiable secret sharing scheme with combiner verification and cheater identification. J Inf Secur Appl 51:102430. https://doi.org/10.1016/j.jisa.2019.102430
27. Thien CC, Lin JC (2002) Secret image sharing. Comput Graph 26:765–770. https://doi.org/10.1016/S0097-8493(02)00131-0
28. Wang R, Shyu S (2007) Scalable secret image sharing. Signal Process Image Commun 22:363–373. https://doi.org/10.1016/j.image.2006.12.012
29. Xingxing J, Daoshun W, Daxin N, Xiangyang L, Jonathan ZS (2019) A new threshold changeable secret sharing scheme based on the Chinese remainder theorem. Inf Sci 473:13–30. https://doi.org/10.1016/j.ins.2018.09.024
30. Yang C, Huang S (2010) Constructions and properties of k out of n scalable secret image sharing. Opt Commun 283:1750–1762. https://doi.org/10.1016/j.optcom.2009.12.077
31. Yang CN, Chen TS, Yu KH, Wang CC (2007) Improvements of image sharing with steganography and authentication. J Syst Softw 80:1070–1076. https://doi.org/10.1016/j.jss.2006.11.022
32. Yvo D, Shuang H, Jean JQ (1998) Audio and optical cryptography. Springer-Verlag Berlin Heidelberg 1514, pp 392–404