# Analysing Secret Sharing Schemes for Audio Sharing

Seema Vyavahare
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune-44

Sonali Patil, PhD
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune-44

## ABSTRACT
In various applications such as military applications, commercial music systems, etc. audio needs to be transmitted over the network. During transmission, there is risk of attack through wiretapping. Hence there is need of secure transmission of the audio. There are various cryptographic methods to protect such data using encryption key. However, such schemes become single point failure if encryption key get lost or stolen by intruder. That's why many secret sharing schemes came into picture.

There are circumstances where an action is required to be executed by a group of people. Secret sharing is the technique in which secret is distributed among n participants. Each participant has unique secret share. Secret can be recovered only after sufficient number of shares (k out of n) combined together. In this way one can secure secret in reliable way.

In this paper we have proposed Audio Secret Sharing based on Li Bai's Secret Sharing scheme in Matrix Projection. Then the proposed scheme is critically analysed with the strengths and weaknesses introduced into the scheme by comparing it with existing schemes.

## Keywords
Audio Secret Sharing, Matrix Projection, Secret Sharing.

## 1. INTRODUCTION
Digitization of information has increased the sharing of personal information over internet. Storage and transmission of the information attracts many intruders. In the internet savvy world it is very essential to keep confidential information secure. While storing the information, it is necessary to keep information without tampering. Also information should not be lost. In the commercial business applications where multiple users need to access some secure resources there is always the risk of the unauthorized access, modification or destruction of the information. Hence there is need of information security for protecting the confidentiality, integrity and availability of the information. The information can be in form of text data, pictures, audio or video and so on. There are various techniques for providing the security to the information. Figure 1 shows the hierarchy of the security system.

The most popular method to protect information is using encryption and decryption methods [1]. Encryption and decryption methods involve lot of computations and increase the complexity. Also, if the encryption key is lost then there is no way to make information available for the use. Visual cryptography [2] is the method in which the information is decoded using human eyes. Similarly, audio cryptography [3] is the method in which audio is divided into the number of parts. While reconstructing the audio, calculations are not required. Only playing of the audio shares simultaneously, with human ears one can reveal the original audio information. Steganography is the method of hiding data inside other data. Steaganography is often prone to attacks in which if cover data is attacked then the private data which is hidden may also lost.

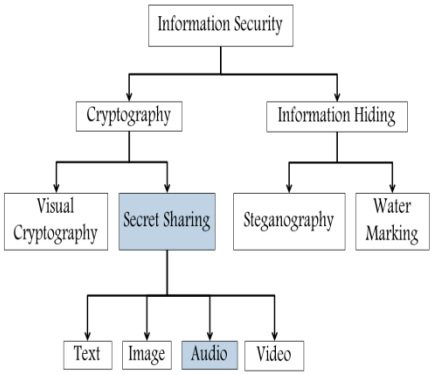


**Fig.1 Information Security System**

Secret sharing scheme (SSS) [4] is the method of sharing secret information in scribbled shares among number of partners who needs to work together. No partner individually can use that scribbled share to reconstruct original secret data. Only sufficient number of partners can come together to disclose the secret. Audio secret sharing (ASS) [5, 6] is the method of dividing the audio secret into number of pieces. Sufficient number of pieces can be combined together to get the original audio secret. In the military applications, audio surveillance, audio needs to be transmitted over the network. During transmission, there is risk of attack through wiretapping. Hence there is need of secure transmission of the audio. Using audio secret sharing, one can send the audio in the form of shares. At the receiver end, sufficient shares are combined to regenerate the original audio data. No audio share will reveal any of the information about the audio. Hence during transmission even though attack happens, intruder will not get any information about secret audio. Basic concept of secret sharing is shown in Figure 2.

The remaining part of the paper is organized in different sections as follows. The literature survey is given in Section II. In Section III the description of the proposed technique is given. Section IV discusses observations. Conclusion and future work is given in Section V.

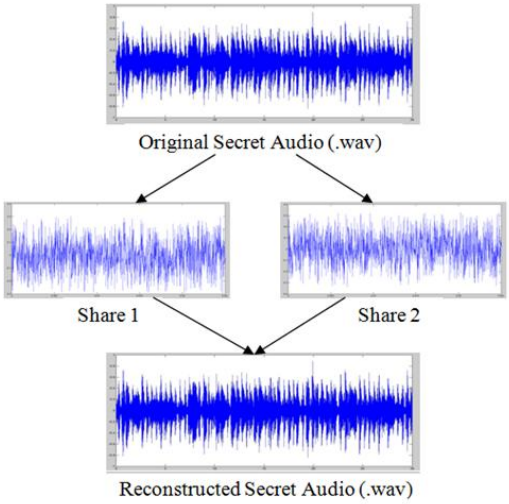


**Fig. 2Concept of Audio Secret Sharing**

## 2. LITERATURE REVIEW

In the area of audio secret sharing, many authors have contributed. Firstly, audio secret sharing was proposed by Desmedt, Hou, and Quisquater [3] in 1998. To embed a message into a stanza of cover sounds is the basic idea of the scheme. For enhancing the security of vocal communication, multipath routing [7] with secret sharing is proposed in 2010. In this technique, multiple network paths are used for transferring the data and it is mainly developed for sharing load and improving reliability. Shared cryptography based on embedding of the session key is proposed in 2011 [8]. The scheme is developed to overcome the limitation of single point failure of encryption key. Scheme used the graphical masking method by performing simple AND operation for share creation and OR operation on sufficient number of shares for secret reconstruction. For providing security to the audio secret sharing schemes, [9] proposed a scheme in 2012. In this paper, a novel scheme for evaluation is stated which uses the mutual information between secret and the shares.

### *A. A Strong Ramp Secret Sharing Scheme Using Matrix Projection*

Li Bai proposed a strong (k, n) threshold based ramp secret sharing scheme [10] in 2006. It is based on matrix projection technique. For square image of m × m, this scheme reduces share size to m × 1. It works as follows for secret image of size m × m. Image must be square image.

**Share Construction:**

i. For m × m image take random matrix A of m × k of rank k.
ii. Choose n random k × 1 vectors out of which any k vector must be independent.
iii. Shares calculated as,
$$v_i = (A \times x_i)\ mod\ p\ ,\ 1 \le i \le n\ .$$
iv. Compute projection matrix $.
$$\$ = A \times \left(A^{'} \times A\right)^{-1} \times A'$$
v. Compute remainder (public) matrix.
$$R = (S - \$) mod\ p$$
vi. Destroy matrix A, vectors $x_i$, projection matrix $ and secret S.
vii. Distribute n shares $v_i$ among shareholders. Make remainder matrix R public.

**Secret Reconstruction:**

i. Select any k shares and combine them to form matrix B.
$$B = [v_1\ v_2\ \dots\ v_k]$$
ii. Compute projection matrix $.
$$\$ = B \times (B' \times B)^{-1} \times B'$$
iii. Compute secret image S.
$$S = (R + \$) mod\ p$$

### *B. A Reliable (k, n) Image Secret Sharing Scheme*

In previous Strong Ramp method there is one public matrix with same size as secret image. But it may lead to single point failure. If we lost public matrix or it get corrupted, we cannot reconstruct the secret image. To overcome this problem, Li Bai suggested a reliable scheme [11] incorporating with it Thien and Lin's [12] image SSS. It increases share size but still it is less than secret image size. It works as follows.

**Share Construction:**

First five steps are same as previous strong ramp scheme.

i. For m × m image take random matrix A of m × k of rank k.
ii. Choose n random k × 1 vectors out of which any k vector must be independent.
iii. Shares calculated as,
$$v_i = (A \times x_i)\ mod\ p\ ,\ 1 \le i \le n\ .$$
iv. Compute projection matrix $.
$$\$ = A \times \left(A^{'} \times A\right)^{-1} \times A'$$
v. Compute remainder (public) matrix.
$$R = (S - \$) mod\ p$$
vi. Now, instead of making R matrix public secretly share it using Thien and Lin's image SSS.
It will give n shadow images of R of size m × (m/k).
$G_1, G_2, \dots, G_n$ are shadow images of R image.
vii. To get image share, combine shares v and shadow image G such as ,
$Sh_i = [v_i G_i]$
viii. Destroy matrix A, vectors $x_i$, $v_i$, projection matrix $, remainder matrix R ,$G_i$ and secret S.
ix. Distribute n shares $Sh_i$ among shareholders.

**Secret Reconstruction:**

i. Select any k shares and take first column of each share to form matrix B.
$$B = [v_1\ v_2\ \dots\ v_k]$$
ii. Compute projection matrix $.
$$\$ = B \times (B \times B)^{-1} \times B'$$
iii. Using Thien and Lin's image SSS reconstruct R matrix.
iv. Compute secret image S.
$$S = (R + \$) mod\ p$$

### *C. Reduced share size audio secret sharing*

In reduced share size audio secret sharing [5], (t, n) audio secret sharing scheme is proposed. This method is based on Li Bai's scheme [10]. During share construction audio data is read and its frequency samples are calculated. Then audio data is represented in matrix form and Li Bai's SSS is applied to generate shares. During share generation public matrix is obtained. That public matrix and frequency samples are made public. Shares are distributed among n participants. In secret reconstruction phase, any t shares are collected and using matrix projection method secret is generated.

The advantage of this scheme is that reduced share size. As compared to original secret size, the share size is reduced

remarkably. But the failure of this scheme is in public matrix. If public matrix is lost or gets corrupted, then secret reconstruction fails.

**Table I: Comparison Between Existing And Proposed Audio Secret Sharing**

| Scheme / Parameter | Prabir's ASS | Patil's ASS | Proposed Scheme |
|---|---|---|---|
| Underlying Technique | Graphical Masking | Matrix Projection | Matrix Projection and Polynomial |
| Share size | Varies with n and k | m | (m x m) / k + m |
| Renewal of Shares | No | Yes | Yes |
| Verifiability | No | Yes | Yes |
| Cheater Identification | No | No | Yes |

Table (1) shows the comparative study of existing schemes and proposed scheme based on different parameters. First parameter shows that which technique is used for secret sharing. Next parameter is individual share size. For share size calculation it is assumed that, audio data is a square matrix of size m x m. Based on that secret size share size is computed. From Table (1), we can see that, proposed scheme has share size greater than Patil's ASS, but it is less than original secret size.

Remaining parameters are extra functionalities that can be added to secret sharing. In many circumstances secret sharing has to provide additional capabilities to satisfy certain requirements. Such capabilities include proactive redistribution of shares, verifiability of the shares, and robustness against cheating shareholders. Proactive Secret Sharing Scheme (PSSS) is a scheme that allows generating new set of shares for the same secret from the old shares without reconstructing the secret. Using PSSS, all the shares Table 1 shows a study of papers related to focused web crawler.

are refreshed so that old shares become useless.Concept of PSS is proposed by Herzberg et.al. in [13]. In this paper they give general idea of proactive secret sharing and how to manage information leakage. Li Bai [14] proposed a proactive scheme in matrix projection secret sharing scheme. As proposed scheme is based on Li Bai's Reliable scheme, we can also add this feature to our scheme.

Next feature is verifiability. Verifiable schemes seek to prevent individuals from lying about their share in order to obtain information about the other shares. Benaloh [15] introduced verifiable secret sharing first time in 1986. S. Patil, P. Deshmukh [16] proposed a scheme to verify reconstructed secret. This scheme is based on Li Bai's reliable image secret sharing scheme. Therefore, this feature can be extended in our proposed work.

Cheater identification scheme is used to identify the cheater among several participants. There may be possibility that shares will get changed during transmission or get changed by someone purposely. So, we need to identify who is cheater? S. Patil and P. Deshmukh [17] proposed new approach to identify cheaters in matrix projection based secret sharing. This feature is also supported in proposed scheme. No one has proposed extra functionalities for Prabir's ASS.

existing scheme. It also supports extended capabilities like proactive features, verifiability of reconstructed secret and cheater identification.

# 3. PROPOSED ARCHITECTURE

In this work, a novel audio secret sharing scheme is proposed. The scheme is based on Li Bai's [11] reliable secret sharing. There are two main phases.

1. Share construction
2. Secret reconstruction

Figure 3 shows the steps of share construction. Detailed steps of share construction are given below.

**Share construction:**

i. Read secret audio data.

ii. Calculate frequency samples for input secret audio data.

iii. Represent audio data in square matrix form. Add padding zeros if necessary.

iv. To generate shares, apply Li Bai's reliable secret sharing scheme on audio data which is represented in matrix form. Here we get shares in matrix form.

v. Convert shares into sequential data which is already in matrix form.

vi. Using frequency samples convert sequential shares into audio data.

vii. Distribute audio shares among authorised *n* participants.

Figure 4 shows the steps of secret reconstruction. Detailed steps of secret reconstruction are given below.

**Secret reconstruction:**

i. Collect any distinct *k* shares.

ii. Represent each share into matrix form.

iii. Apply Li Bai's reliable scheme to reconstruct secret. Obtained secret will be in matrix form.

Convert matrix data into sequential Using frequency samples, obtained sequential data is converted back into audio data. The audio which is achieved is nothing but secret audio data.

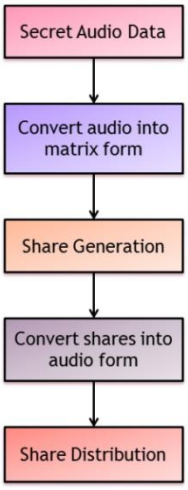


**Fig. 3Share Generation in Audio Secret Sharing**

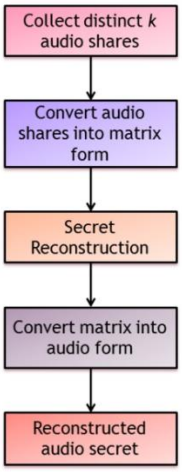


**Fig. 4Secret Reconstruction in Audio Secret Sharing**

## 4. CONCLUSION

As the use of internet has been increased tremendously in recent years, most of people transmit their data through internet. There is possibility that the data may get hacked and get misused. To protect such data many security systems are proposed.

In many circumstances, secret sharing has to provide more flexibility and functionality. The requirements for different extra functionalities of SSS are often contradictory to each other which make construction of a SSS with several additional features a challenge. In many circumstances secret sharing has to provide additional capabilities to satisfy certain requirements. Such capabilities include proactive redistribution of shares, verifiability of the shares, and robustness against cheating shareholders.

In this paper, we have introduced new approach for audio secret sharing.It will also remove single point of failure in existing scheme. It also supports extended capabilities like proactive features, verifiability of reconstructed secret and cheater identification.

## 5. REFERENCES

[1] Douglas R. Stinson, "Cryptography: Theory and Practice", Third edition.

[2] M. Naor and A. Shamir, "Visual cryptography," Advance in Cryptology: Eurpocrypt'94

[3] Lecture Notes In Computer Science, Springer Verlag, Germany, Vol. 950, pp. 1–12, 1995.

[4] AmreshNikam, Poonam Kapade, SonaliPatil, "Audio Cryptography: A (2, 2) Secret Sharing for Wave File" International Journal of Computer Science and Application Issue 2010.

[5] A. Shamir, "How to share a secret" Communication of the ACM, vol. 22,no. 11, pp.612-613, Nov 1979.

[6] SonaliPatil, P. R. Deshmukh, TejalChavan, Vinay Shastri, Priyanka Sangwan, AkashSunthwal, "Reduced share size audio secret sharing", International Conference on Pervasive Computing (ICPC), pp.1-4, IEEE, 2015.

[7] Sagar A. Yashwantrao, Prof. Vilas J. Jadhav, Prof.Pravin S. Rahate, "Shared Cryptographic Scheme with Efficient Data Recovery and Compression for Audio Secret Sharing" International Journal of Emerging Technology and Advanced Engineering", ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014.

[8] Ryouichi Nishimura, Shun-ichiro Abe, Norihiro Fujita and Yoiti Suzuki, "Reinforcement of VoIP Security with Multipath Routing and Secret Sharing Scheme", Journal of Information Hiding and Multimedia Signal, Volume 1, Number 3, July 2010.

[9] Prabir Kr. Naskar, Hari Narayan Khan, Ujjal Roy, Ayan Chaudhuri , Atal Chaudhuri, "Shared Cryptography with Embedded Session Key for Secret Audio", International Journal of Computer Applications (0975 – 8887) Volume 26– No.8, July 2011.

[10] Yoshida. K. Sch. , "Security of Audio Secret Sharing Scheme encrypting Audio Secrets", Internet Technology And Secured Transactions, 2012.

[11] Li Bai, "A Strong Ramp Secret Sharing Scheme Using Matrix Projection", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006.

[12] Li Bai, "A Reliable (k, n) Image Secret Sharing Scheme", IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006.

[13] Thien and Lin, "Secret image sharing", Computers & Graphics, vol. 26, no.5, pp. 765-770, 2002.

[14] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, "Proactive Secret Sharing Or: How to Cope with Perceptual Leakage", Springer- Verlag, 1998.

[15] Li Bai, XuKai Zou, "A Proactive Secret Sharing Scheme in Matrix Projection Method", International Journal of Security and Networks, Volume. 4, No. 4, PP. 201-209, 2009.

[16] J. C. Benaloh, "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Proceedings of CRYPTO86 Springer, Berlin, PP. 251260, 1986.

[17] SonaliPatil, P. Deshmukh, "Verifiable Image Secret Sharing in Matrix Projection Using Watermarking", International conference on Circuits, Systems, Communication and Information Technology Applications, IEEE, 2014.

[18] the 14th International World Wide Web Conference. 2005, pp. 1190-1191.