ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

Contemplating Audio Secret Sharing Schemes

Prof. Sonali Patil[1], Tejal Chavan[2], Priyanka Sangwan[3], Vinay Shastri[4], Akash Sunthwal[5]

Pimpri Chinchwad College of Engineering, Nigdi, Pune India[1]

Students, Pimpri Chinchwad College of Engineering, Nigdi, Pune, India[2,3,4,5]

Abstract: The methodology of secret sharing involves the ownership of the key by the dealer which would give access to the original secret that has been divided into shares. This concept has been applied similarly onto an audio message that has to be conveyed over a network. The Audio Data is divided into multiple shares which would be collated later on in order to get the original audio message. The failure to meet the condition would render the entire message useless that is to say that all the shares are essential for the reconstruction of the original audio message. The intent of this paper is to study and analyse the audio secret sharing schemes. The comparative analysis of different audio secret sharing schemes that have been proposed in the past has been put forth.

Keywords: Cryptography, Audio Secret Sharing, Masking, Security

I. INTRODUCTION

The knowledge of secret sharing [1] is generally applicable in the military and corporate environments. These areas require the transmission of highly sensitive data that if trampled with, may have a direct and drastic impact over the existence of integrity of the entire nation or institution.

Previously the method of cryptography was used which resulted into the formation of cipher text or encrypted text that would provide a means of obscuring the original data to be communicated. This method provided the means of revealing the original data by using the secret key only. That is only the participants who have been privileged with the key would have the access to the complete data. If such a key is inappropriately handled and is lost, the original data too would be deemed inaccessible.

In order to compensate for this fatal drawback, audio secret sharing was introduced. Perception of the original audio data is achieved through human audibility so as to decrypt it. Audio secret sharing is an example of secret sharing whose decryption can be performed by human ears. In audio secret sharing formation of incomprehensible shares from the original audio file(data) takes place. These shares would then be transmitted over the network to the participants. These separate shares would be collated from the participants so as to get the original audio data. Various extended capabilities [2] are required to fulfil the need of applications.

II. LITERATURE SURVEY

A. Audio cryptography: A(2,2) secret sharing for wave file [3]

In this scheme (2,2) Audio Cryptography Scheme is being used in which the original digital secret message is being concealed into two specified cadences. The original secret message will be perceived only by playing the two cadences simultaneously.

Share construction algorithm
The pre-requisite for this algorithm is a two channel wave file whose length has to be calculated using the header information, using the formula:

*Number of seconds= number of samples / (Number of tracks * Sample per second)*

Now, depending upon the length, the wave file will be divided into *n* parts. Two share files are generated from the original file. The header information will be replicated, as it is, in these two files.

The first part of the first channel will be copied into both the channels of the first share and first part of the second channel into both the channels of the second share, and the process will be repeated for rest of the parts of the two shares, only by interchanging the channels. All the parts will be copied into the shares using these steps.

Reconstruction algorithm
There is no specific requirement of an algorithm to reveal the original audio message, as the message will be revealed by playing the shares simultaneously.

B. Reinforcement of VoIP Security with Multipath Routing and Secret Sharing Scheme [4]

A technique for enhancement of the vocal communication's security over a network has been proposed. Secret sharing scheme along with the multipath routing techniques have been combined and for conveying the information for one end to another Shamir's secret sharing [1] scheme is used. Lagrange's interpolating polynomial is used in Shamir's scheme.

In [1] a unique (k, n) threshold-based secret sharing scheme is proposed in which *k* points in the two-dimensional plane with distinct x_i s are identified, with q(x) being the only polynomial of degree $k-1$ such that

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

$q(x_i) = y_i$ for all i. The data D, is divided into n numbers $D_i(i = 1; : : : ; n)$ by selecting a random $k - 1$ degree polynomial $q(x) = a_0 + a_1x_1 + : : : + a_{k-1}x_{k-1}$ in which $a_0 = D$, and is evaluated as $D_1 = q(1); D_2 = q(2); : : : ; D_n = q(n)$. Given any subset of k of these values and their indices, coefficients of $q(x)$ can be derived through interpolation and $D = q(0)$ can thus be evaluated. Otherwise, no chance to calculate D exists.

The data would be revealed using the Lagrange's interpolation formula:

$$d_0 = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \le j \le t, t \ne j} \frac{x_{i_t}}{x_{i_t} - x_{i_j}} \right) \bmod p$$

In this scheme the number of necessary data amongst n data has to be greater than k so as to reconstruct the original data.

Shamir's (t, n) threshold scheme is based on Lagrange's Interpolating polynomial and the scheme is information-theoretically secure. By using Shamir's threshold scheme concept we can get a very robust key management scheme.

C. *Graphical Masking Method [5]*

In this method shares are generated and reconstructed by ANDing and ORing, respectively the predefined minimal number of shares. Each share that has been generated will have only a subset of the original data (bits) available in it and these missing bits would replenished by exactly (*k-1*) other shares but not less than that.

Share construction algorithm

During the share construction phase of the algorithm, n masks will be formed for n individual shares using the mask generation algorithm. For the generation of the masks individual masks will be ANDed with the secret.

Secret reconstruction algorithm

With the condition that less than k shares will not reveal any data, OR any k number of shares in order to obtain the original secret back.

Mask generation algorithm

A matrix will be formed with the dimension ${}^{n}C_{k-1} \times n$ by arranging rows of size n. These rows will have (*k-1*) numbers of *0*'s and (*n-k+1*) numbers of *1*'s.

A new matrix will be generated by transposing the original one generated. The dimension of this matrix is $n \times {}^{n}C_{k-1}$. Each row of this matrix will form the individual mask for n shares. Each mask has the size of ${}^{n}C_{k-1}$ bits.

This algorithm uses ANDing and ORing operation which provides the advantage of less computational complexity.

III. TABLE I COMPARATIVE ANALYSIS

Author	Technique used	Threshold	Reliability	Computational Complexity	Share Size	Security	Extended Capabilities
Amresh Nikam et al [5]	(2,2) Secret Sharing for wave file	(2,2)	No	Less	Same as Secret	Low	No
Nobuyuki Enomoto et al [2]	Shamir's Secret Sharing Scheme	(k,n)	Yes	More	Same as Secret	High	No
Prabir Kr. Naskar et al [3]	Graphical Masking Method	(k,n)	Yes	Less	Same as Secret	Low	No
Yoshida. K.[7]	Shamir's Secret Sharing Scheme	(k,n)	Yes	Less	More than size of original secret	High	To some extent

IV. APPLICATIONS

The audio secret sharing provides security to plans/strategies of financial groups related to projects involving client's assets. The military applications involving sending messages over communication devices/ networks also use the scheme. It can also be used to provide security for voice communication in VoIP methodology.

V. CONCLUSION

Various extended capabilities are not considered in Audio Secret Sharing scheme. Various audio secret sharing schemes have been studied and analysed in this paper. The comparative study shows that there is a need for more robust audio secret sharing techniques in near future.

REFERENCES

[1] Shamir : " How to share a secret ?" , comm. ACM, 22 (11) : 612-613, 1979.
[2] Sonali Patil, Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications (0975 – 8887) Volume 46– No.19, May 2012
[3] Amresh Nikam, Poonam Kapade, Sonali Patil, "Audio Cryptography: A (2, 2) Secret Sharing for Wave File" International Journal of Computer Science and Application Issue 2010.
[4] 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.
[5] 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.
[6] 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.
[7] Yoshida. K, Sch. of Comp. Sci. & Eng., Univ. of Aizu, Aizu-Wakamatsu, Japan, "Security of Audio Secret Sharing Sheme encrypting Audio Secrets", Internet Technology And Secured Transactions, 2012 International Conference.