Speech Encryption Techniques: A Selected Review

Jaspreet kaur[#1] , ER. Kanwal preet Singh[*2]

1. M. tech. Student, University College of engineering, Punjabi university Patiala.

2 Department of Computer Engineering, Assistant Professor, University College of engineering, Punjabi university Patiala, Punjab, India

1 Jaspreetkaur843@gmail.com

2 kanwalp78@yahoo.com

Abstract

Speech encryption is one of the key aspects in Computer Vision. From different point of views the problems of speech encryption have been resolved and the modification in the encryption technique is still going on. This is the main reason that speech encryption is used in a huge number of applications. In this paper a number of speech encryption techniques have been defined from which researcher can get an idea.

I. INTRODUCTION

A speech communications become more and more widely used and even more vulnerable, the importance of providing a high level of security is dramatically increasing. As such, a variety of the speech encryption techniques has been introduced. The analogue encryption has been one of the popular encryption techniques widely used in speech communication. Along this line, there are three main categories: frequency domain scrambling such as the frequency inverter and the band splitter, time domain scrambling such as the time element scrambling, and two-dimensional scrambling combining the frequency domain scrambling with the time domain scrambling . Besides, there is an amplitude scrambling technique, also known as the masking, which covers the speech signal by the linear addition of pseudo-random amplitudes.

Analogue speech encryption in the transform domain, e.g., fast Fourier transform, discrete cosine transform and wavelet transform, etc.] has also been developed. Recently, some new speech encryption methods have been proposed, e.g. chaotic cryptosystem [SI, encryption using circular transformations , etc. In this paper, we explore a four different hash based encryption algorithm to secure speech signals more advanced.

Encryption is necessary to ensure protection of data and watermark in the medium. Traditional symmetric key encryption algorithms like Data Encryption Standard (DES) use small blocks size with complex permutations process to give secure output cipher text .Public key algorithms are not suitable for large amount of data due its slow performance. AES was announced by National Institute of Standards and Technology (NIST) on 2001. AES is one of the most secure algorithms used in symmetric key cryptography. It uses complicate repeated steps to prevent analytic attacks that can discover weakness in the algorithm and so attack any encrypted data. AES use high diffusion to eliminate any prediction of key. AES algorithm is not appropriate for real time communication because of delay and interdependence of frames. If one frame is lost in AES next frames will be garbage to receiver.

Encryption of a signal consists in applying a completely reversible operation on a clear signal such that it is totally unintelligible to an unauthorized person. The need of encrypting signals finds its applications in Image, video and speech domains. Several methods of signal encryption are used such as time domain and frequency

domain techniques, chaos based methods. Segments or frequency bands are permuted in order to reduce the intelligibility of the signal. These methods are very vulnerable to cryptanalytic attacks and are replaced with transform based methods. .In these methods, we first sample the signal then the samples are partitioned into frames containing each sample. A transformation is then applied to obtain a transform vector with components. Encryption is done by permuting these components and the inverse transform is applied to obtain the encrypted signal in time domain. The encrypted signal is transmitted; the receiver performs the inverse operations in order to recover the original signal. The three most important criteria used to evaluate signal encryption algorithms are

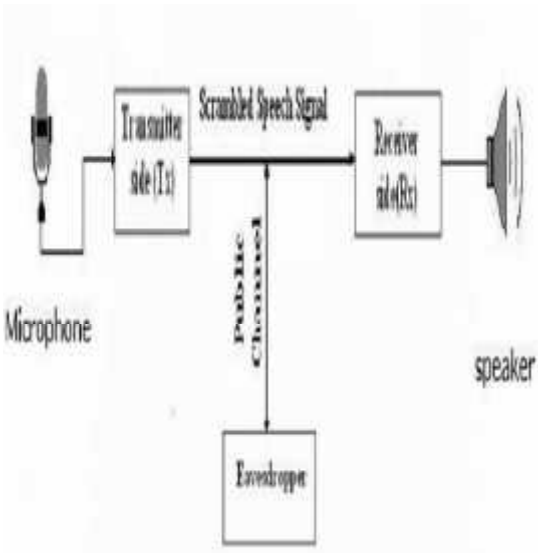
1) The ability of the algorithm to produce encrypted signal with very low residual intelligibility;

2) The extent to which the encryption and decryption processes affect the quality of the recovered signal and

3) The algorithm's security against cryptanalytic attack.

Speech encryptions systems are mainly are of two types:

- Hardware based speech encryption systems.
- Software based speech encryption systems.



II. LITERATURE REVIEW

In this section, we are presenting the research work of some prominent authors in the same field and explaining a short description of various techniques for speech encryption

A. Atef Mermoal " An Iterative speech Encryption scheme based on subspace technique"

Among the cryptographic approaches, signal processing techniques has become recently an interesting one. Blind source separation (BSS)-based encryption schemes have been built up using the intractability of the under determined BSS problem. In this paper, we propose a new encryption method. The proposed approach is iterative and based on the subspace concept together with the use of nonlinear functions and key signals. The proposed technique represents an interesting feature: only a part of the secret key parameters used during encryption is necessary for decryption. Furthermore, the iterative encryption algorithm will provide no contents if no plain-text is fed in the input.

B. G. Ramesh & Prof. Dr. R. UMARANI:- "UMARAM: A Novel Fast Encryption Algorithm For Data security In Local Area Network"

Symmetric encryption algorithms, are UMARAM .IMA key Algorithm. The IMA Key is a key generation algorithm based on random extraction of data from an image file. The algorithm is demonstrated in MATLAB and tested for key randomness and effect of image size on key generated. It is used for generating 1st key in the AES encryption process. The results for same plaintext input and different keys are obtained and analyzed. The new algorithm is applied successfully on both text file, voice message, And Image File.

C. Md. Abdul Matin & Imranul Kabir Chowdhury "Watermarking with Fast and Highly Secured Encryption for Real-time Speech Signals"

Watermarking technique with fast encryption and compression. Recently a number of algorithms exist for watermarking and encryption. The drawbacks are size, security and time for execution .Compression is necessary to maintain size small where bandwidth and storage capacity is limited. A loss-less compression technique is used to compress speech signal. Due to compression, vacant places are created. These vacant places are used for watermark. In the proposed

encryption technique size of encrypted data is increased by only 12.5%.Execution of encryption is faster than present unbreakable algorithms. The proposed encryption is also highly secured and can be used for real-time application and saving signal. Watermark will exist even signal cropping.

D H. Peyvandi & S._J. Park ." Security in Data Communication and Privacy in Converstions for Underwater Wireless Networks using Scrambled Speech Scheme".

In this paper, a secure scheme for under water telecommunication networks has been proposed. The main idea stems from the fact that all telecommunication networks. , including underwater networks, have been basically prepared to transfer speech and voice. In our proposed scheme, the input voice is transformed to the bit stream using a low bit rate encoder. Then, the whole bits are mapped to the predefined symbols, which have been originally designed using hi-fi speech records. Symbols are stored in a lookup table in the both sides of channel. At transmitter side, the prepared signal is windowed, filtered and shaped to transfer over underwater link. The overall bit error rates are as low as that have not any significant effect on quality of speech while, on the other hand, the output noises are quite unintelligible for intruders who try to access to the conversations through the channel of telecommunication network. Produced noises are signals including random scrambled speech-based symbols in which make no any sense to the listener. The simulated system was considered to transfer speech to obtain results in an experimental state. The results show that the proposed scheme for underwater telecommunication is reliable.

E. B. Putra & Suyanto "Implementation of Secure Speaker Verification at Web Login Page Using Mel Frequency Cepstral Coefficient-Gaussian Mixture Model (MFCC-GMM) Comparisons analysis of various technique"

The need of security for web page was increased as the development of online activity especially trading or banking .Speaker recognition can be used to secure the web page which need highly security level. In this research ,the speaker recognition system at web page was successfully built for login authentication security. For enrolment and verification need, speech signal from clients was recorded in 35 seconds for enrolment and 10 seconds for verification then transferred to server by network. Then this signal will be processed with sampling. frame blocking, windowing hamming and discrete Fourier transform. The signal in frequency domain will be filtered by nonlinear power spectral subtraction to reduce the backgrounds noise. For identification ,the system extracts the feature of Mel frequency Cepstral coefficient (MFCC), and to build the model of these feayures uses Gaussian mixtures model.(GMM).To improve the security level ,the system uses Secure socket layer(SSL) with 1024 bits RSA encryption .From this research we have succeeded in optimizing the signal quality up to 5 db SNR ,the mean error recognition level of FAR is about 23.3% and for 27.5 and the maximum accuracy of the recognition system is around 88% when the quality of speech signal is clean. The computation time for enrolment is about 552573,5 milliseconds for verification is about 129062,6 milliseconds.

F. Lei, Insu Song, and Shah Atiqur RahmanJames Cook " Optimal Watermarking Scheme for Breath Sound

In this paper, a new watermarking scheme for breath sound based on lifting wavelet transform (LWT), discrete cosine Transform (DCT), singular value decomposition (SVD)and dither modulation (DM) quantization is proposed to embed encrypted source and identity information, and medical conditions, such as cold and flu symptoms in breath sound while preserving important biological signals for detecting breathing patterns and breathing rates. In the proposed scheme, LWT is first carried out to decompose the signal followed by applying DCT on the approximate coefficients. SVD is then performed on the LWT-DCT coefficients to get the singular values. The novelty of our proposed method includes the introduction of the particles warm optimization (PSO) technique to optimization the quantization steps of the DM approach too. Simulation

results show that our watermarking scheme achieves good robustness against common signal processing attacks and maintains the imperceptivity. The comparison results also show good performance of our scheme.

.

Table 1. Comparative Analysis of Various Techniques

S.NO	Paper name	Author name	Technique used	Application area
1.	An Iterative speech Encryption scheme based on subspace technique	Atef Mermoal	Subspace technique	Mainly used for speech and image security
2.	UMARAM: A NOVEL FAST Encryption Algorithm For Data security In Local Area Network	G. Ramesh & Prof. Dr. R. UMARANI	UMARAM AND IMA KEY algorithm.Based on random extraction of data from an image file	Provide security in local area networking
3.	Watermarking with Fast and Highly Secured Encryption for Real-time Speech Signals"	Md. Abdul Matin & Imranul Kabir Chowdhury	Watermarking technique	Authentication ,verification& identification of a real signal
4.	Security in Data Communication and Privacy in Conversations for Underwater Wireless Networks using Scrambled Speech Scheme.	H. Peyvandi & S._J. Park	Scrambled Speech Scheme	Underwater telecommunication networks.
5.	Implementation of Secure Speaker Verification at Web Login Page Using Mel Frequency Cepstral Coefficient-Gaussian Mixture Model (MFCC-GMM)Comparisons analysis of various technique:"	E. B. Putra & Suyanto	Mel Frequency Cepstral Coefficient(MFCC), Gaussian Mixture (GMM) Models	Online activity especially trading or banking.
6.	Optimal Watermarking Scheme for Breath Sound	Lei, Insu Song, and Shah Atiqur RahmanJames Cook	Optimal Watermarking Scheme	Medical Science, such as to detect cold and flu symptoms in breath sound

III. CONCLUSION

This paper presents a short description of various speech encryption techniques to make familiar with different ways of transferring audio data securely on a network.

IV. REFERENCES

[1] Atef Mermoul "AN ITERATIVE SPEECH ENCRYPTION SCHEME BASED ON SUBSPACE TECHNIQUE ", 2011 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA)

[2] G. Ramesh & Prof. Dr. R. UMARANI:-"UMARAM: A Novel Fast Encryption Algorithm For Data security In Local Area Network", 2010 IEEE.

[3] Md. Abdul Matin & Imranul Kabir Chowdhury "Watermarking with Fast and Highly Secured Encryption for Real-time Speech Signals", 2010 IEEE.

[4] H. Peyvandi & S.J. Park " Security in Data Communication and Privacy in Converstions for Underwater Wireless Networks using Scrambled Speech Scheme". 2011 MTS.

[5] B. Putra & Suyanto "Implementation of Secure Speaker Verification at Web Login Page Using Mel Frequency Cepstral Coefficient-Gaussian Mixture Model (MFCC-GMM) Comparisons analysis of various technique:, 2011 2nd International Conference on Instrumentation Control and Automation

15-17 November 2011, Bandung, Indonesia

[6] Lei, Insu Song, and Shah Atiqur Rahman James Cook " Optimal Watermarking Scheme for Breath Sound , WCCI 2012 IEEE World Congress on Computational Intelligence June, 10-15, 2012 - Brisbane, Australia

[7]Q.-H. Lin, and E-L. Yin "Blind source separation appliedto image cryptosystems with dual encryption ,"in Electronics Letters, vol. 38, no. 19, pp. 1092-1094,

September 2002.

[8] Q.-H. Lin, E-L. Yin, and Y-R. Zheng "Secure image communication using blind source separation ,"in IEEE 6th CAS Symp. On Emerging Technologies:

Mobile and Wireless CO. Shanghai, China, May 31-June 2,2004.

[9] Q.-H. Lin, E-L. Yin , T-M. Mei and H.-L. Liang, "A speech encryption algorithm based on blind source separation," in Proc. Int. Conf. Commun., Circuits

Syst.: Signal Process., Circuits Syst., 2004, vol. II, pp.1013-1017.

[10] Z.M. Lu and S.H. Sun, "Digital Image Watermarking Technique Based on Vec [1] William Stallings, "Network Security S. Boussakta, and H.G.J. Holt; "New two dimensional transform;"*Electronic letters*; vol. 29, n° 11, pp. 949 – 950, 27 May 1993.

[11] O. Nibouche, S. Boussakta, and M. Darnell, "Pipeline Architectures for Radix-2 New Mersenne Number Transform" *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 56, n° 8, pp. 1668 – 1680, Aug. 2009.

[12] M. Stojanovic, "Underwater wireless communication current achievements and research challenges", IEEE OES Newsletter, Nov.2006.

[13] M. Stojanovic, "Design and capacity analysis of cellular type under water acoustic networks," IEEE J. Oceanic Engineering, vol.33, pp.171-181,Apr. 2008.

[15] J. M. Peterson, J. Kursoe and B. N. Levine, "A survey of practical issues in underwater networks", Wireless Underwater Network (WUWNet'06),USA, Sep. 2006.

[16] J. H. Goh, A. Shaw and A. Al-Shamma, "Underwater wireless communication system", Journal of Physics: Conference Series178012029, 2009.

[17] H. Peyvandi, B. Fazaeefar and H. R. Amindavar, "Determining class of underwater vehicles in passive SONAR using Hidden Markov Modelwith Hausdorff similarity measure," IEEE OES Symposium on Underwater Technology (UT'98), Apr. 1998.

[18] M.Farrokhrooz and M. Karimi, "Ship noise classification usingprobabilistic neural network and AR model coefficients," IEEE Oceans Conference-Europe (Oceans'05), vol.2, pp.1107-1110, 2005.

[19]H. Shahbazi and M. Karimifard, "Design and analysis of low frequency communication system in Persian Gulf", MTS/IEEE Oceans Conference, Canada, Sep. 2008.

[20] H. Peyvandi, "A novel approach for data transmission over voice dedicated channel of worldwide telecommunication networks," The 8th IEEE Symposium on Wireless Telecommunication (WTS'09), Czech Republic, Apr. 2009.

[21] H. Peyvandi and A. R. Ebrahimi, "A Neural Approach for Compensation of Nonlinear Distortion Effect in up to 1600bps Data Communication over Voice-Dedicated Channels", 17th IEEE Conference on Telecommunication (ICT'10), Qatar, Apr. 2010

[22] Besacier, Laurent dkk. 2004. "Voice Biometric Over the Internet In The Framework Of COST Action 275". Eurasip Journal on Applied Signal Processing 2004.

[23] Jain, K Anil, dkk. 2008. "Biometric Template Security, Review Article". Eurasip Journal on Applied Signal processing 2008

[24] Gilmore, William, dkk. 2008. 'The Future of Online Internet Marketing: A Solution To behavioral Marketing using Biometrics".

Journal of Bussines & Economic Research February 2008.

[25] Wayman, James. 2005. "Biometrics Systems, Technology Design and Performance Evaluation". Italy, USA: Springer

[26]Bimbot, Frederic dkk.2004."Tutorial on Text Independent Speaker Verification". EURASIP Journal on Applied Signal Processing. Hindaw Publishing Corporation.

[27] Kinnunen, Tomi H.2005. "Optimizing Spectral Feature Based Text Independent Speaker Recognition", Dissertation. Department Computer Science and Engineering, University of Jouensuu, Jepang, unpublished.

[28] Houtarnaki, Rosa Emilia Gonzales. 2005. "Fundamental Frequency Estimation and Modeling for Speaker Recognition", Master's thesis. Department of Computer Science, University.

[29]W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, pp. 313-36, 1996.

[30] J. Huang, Y. Wang, and Y. Q. Shi, "A blind audio watermarking algorithm with self-synchronization," in Proceedings of IEEE International Symposium on Circuits and Systems, 2002, pp. 627-630.[3] X.-Y. Wang and H. Zhao, "A 6

Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT," IEEE Transactionson, Signal Processing,vol.54,pp.4835-4840,200