SECURE SPEECH WITH LFSR

Arathi k Chandran[1], Sreela Sreedhar[2]

[1]PG Student, [2]Associate Professor, HOD, Department of Computer Science & Engineering, Toc H Institute of Science and Technology, Kerala, India

Abstract

Secure Speech with LFSR presents an encryption method for compressed and watermarked speech signal. There are several number of techniques available for watermarking, compression and encryption purpose, but there are various flaws in these techniques. Existing compression algorithms are very complicated and time consuming. Watermarking increases the size of the speech signal which in turn will affect the transmission of the speech signal. Previous encryption algorithms also increase the size of the signals, the security of the system can be easily compromised and these techniques are time consuming. Since the speech signals need to be transmitted and stored for future use, a good loss-less compression algorithm is needed to reduce the size of the speech signal and the lossless compression technique should be simpler and quicker. Because of compression, empty spaces are created within the speech signal. These empty spaces are used for embedding watermark signals into the speech signal. Then the compressed plus the watermarked signal is encrypted for making the signal more secure. Since the watermarked signal is encrypted, several attacks on the watermark signal can be reduced. Linear Feedback Shift Register is used for encryption purpose. Using Linear Feedback Shift Register the compressed plus watermarked signals are encrypted to form a cipher text and cipher text is transmitted .The transmitted cipher text is received by the receiver and decrypted using Linear Feedback Shift Register ,then the watermarked signal is extracted, the signal is decompressed and the speech is played back to the receiver.

Keywords: *Compression, Watermark, Encryption, Linear Feedback Shift Register and Cipher Text.*

----------***----------

1. INTRODUCTION

Secure speech communication is of great importance in civil, military and commercial field. Since speech communication is widely used, the importance of providing a high level of security becomes vital issue. As a result digital watermarking and encryption of speech signals were introduced.

Digital Watermarking is the process of adding unobtrusive content into the digital data. Unobtrusive content doesn't attract much attention of an attacker. Digital data can be of any form, it can be an image or an audio or a video etc.

Watermarking can be used for authentication purpose, integrity purpose and confidentiality purpose. Whenever integrity or confidentiality is concerned watermark can be extracted at that point of time.

In this paper a good encryption process is described after the compression and watermarking. The signal is compressed to produce space for watermarking. Then watermark is added to the signal.

A lossless compression technique is used to compress the signal. Speech compression involves compression of audio data in the form of a speech. Lossless technique is complement to lossy compression. For lossless compression technique compression ratio is only 3:1 where as in lossy compression technique compression ratio is 12:1. But as compression ratio increases the quality of the signal degrades. Lossy compression technique is not suitable for archiving or editing applications. Because once edited or archived, it affects the quality of the signal.

Secure speech or ciphony or secure voice is a term in cryptography for the encryption of a speech signal. Linear Feedback Shift Register is a widely used technique for speech encryption. LFSR is suitable because speech is a continuous stream of data.

2. MATEMATICAL BACKGROUND

Speech is read by the system as samples. The samples are converted into 8 bit PCM samples [1].Values of these samples range from -128 to +127. It is very rare to obtain a sample greater than 120.Since it is a speech signal, most values might be zero. Most of the samples have normal distribution as $\sigma = 6$ to 25.Formula for normal distribution is given below as equation 1.

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \quad (1)$$

Where, σ^2 = variance, μ = median. x = value of a sample.

The probability of obtaining 125 value for a sample is very rare. When a speaker is speaking at least 8000 samples are

produced in one second. In that 2 to 27 percentage will be zero. So at least 160 samples will be there to embed the watermark

Data encryption and decryption consist of XORing with pseudorandom number produced from a pseudorandom number generator.

Stream cipher is used here with the help of LFSR. Pseudorandom number is generated using LFSR. Let the generated numbers be $k_1, k_2 \ldots\ldots, k_n$. Plain text is in the form of $p_1, p_2 \ldots\ldots, p_n$. The output is the cipher text is in the form $c_1, c_2 \ldots\ldots, c_n$.

Encryption process is carried out as given in equation 2.

$$c_i = p_i \oplus k_i \quad (2)$$

Decryption process is carried out as given in equation 3.

$$p_i = c_i \oplus k_i \quad (3)$$

3. RELATED WORK

Digital watermarking is of three types: Robust, Fragile and Semi fragile.

Fragile watermarking is used for tamper detection of original signal. The watermarked signal is added to the insignificant portion of data to provide imperceptibility. Watermarking is fragile if it fails to detect the slightest modification. They do not survive lossy transformation.

Robust watermarking provides a mark that can be removed only if the original signal is tampered. For security applications and copyright protections robust watermarking scheme is used.

Semifragile watermarking differentiates between the lossy transformation which is information altering and which is information preserving. Lossy transformation include signal processing steps which will alter the original signals.

The problem with digital watermarking is that when added it will increase the size of the original signal.

Speech being a one dimensional signal faces replacement attack, in which the watermarked block is replaced by yet another watermarked block [2], counterfeiting attack, in this type of attack a fake watermarked block is added to the original signal and copy and paste attack. Removing watermarked block from original signal is not a tedious task nowadays.

There are two types of compression techniques: lossy and lossless compression.

In lossy compression the decompressed signal will not be the exact replica of the original signal whereas in lossless compression the decompressed signal will be the exact replica of the original signal.

The purpose of the speech compression is to reduce the number of the redundancy bits. When speech signal is compressed it becomes easier for transmission and storing purpose.

There are three basic speech compression technique: waveform-based, parametric-based and hybrid coding techniques.

Waveform based compression technique minimise the error between the original signal and the reconstructed signal. This technique is mainly used to remove redundancy. Two main waveform based techniques are pulse code modulation and adaptive pulse code modulation.

Parametric based depends on how speech is produced. It differentiates between voiced and unvoiced speech. Based on this factor some parameters are calculated and then theses parameters are coded.

Hybrid based is a combination of parametric based and waveform based. Code Excitation Linear Prediction is a type of hybrid based coding.

In encryption technology voice encryptors and voice scramblers are used. The voice encryptors apply the cryptographic technique to the resulting bit stream from sampling.

There are two types of voice encryptors: hard encryptors and soft encryptors. Hard encryptors use hardware for encryption and soft encryptors use software for encryption.

Speech scramblers scramble the speech in many forms, one example is shown in the fig 1 below.

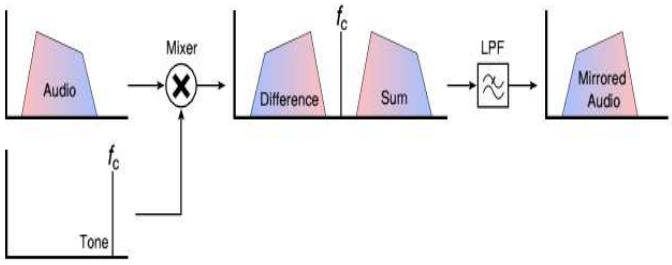

Fig -1: Voice scramblers

In the above figure the audio signal is mixed with a frequency as a result two forms of signals are produced that is difference and sum .The sum is filtered using a low pass filter and the resulting signal will be the mirror image of original signal.

4. METHODOLOGY

4.1 Linear Feedback Shift Register

Linear Feedback Shift Register (LFSR) is used to generate pseudo random numbers. LFSR has two main parts. They are shift register and feedback function [3].

The shift register can move its content in both direction. Either in left or in right direction. It shifts its content to adjacent positions and also shifts the content if the end position is vacant. During the shift the content of the end position bit is moved out and with the help of the feedback function the vacant position is filled. The result of the feedback function is inserted into the shift register during the shift, filling the position that is emptied as a result of the shift.

The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random with a very long cycle.

4.2 Gamma Distribution Function

Initial key is produced by math.random function in matlab to produce a random number which is sent to the receiver too. Then a chi square distribution is done to that random number and it is made as a seed to the LFSR. Chi square is a special case of gamma distribution function.

5. THE PROPOSED METHOD

In the proposed scheme watermarked signal is added to the space provided for watermarking after the compression. In earlier schemes adding watermark signal usually increases the size of the signal which in turn will affect the storage and transmission of the speech signal.

In this scheme watermarked signal is encrypted. Earlier watermarked signal might be present but encryption is usually absent. Since the watermarked signal is encrypted it provides an extra security to the signal and various attacks discussed above on watermarking can be avoided.

A lossless compression algorithm is used to compress the speech signal and to create space for watermarking. After creating space for watermarking, watermark signals are added in that space. In the next step speech plus the watermarked signal is encrypted.

5.1 Sampling the Signal

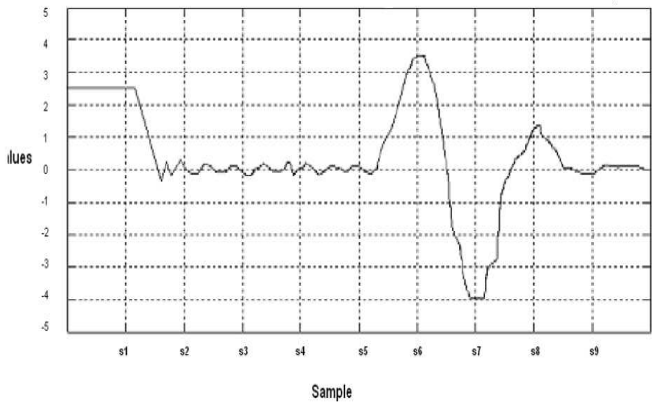

Fig -2: Sampling of speech signal

The speech signal should be read and then sampled. Sampling is periodic measurement of an analog signal and changes a continuous-time signal into a discrete-time signal. Figure 2 shows an analog signal, the signal is sampled after a given interval Ts which is the sampling period.. s1, s2, s3……., are the samples obtained from this analog signal.

5.2 Compress and Create Space for Watermark

Consider speech signal in fig 2. Let's say after sampling the speech signal is in the form s1=3, s2=0, s3=0, s4=0, s5=0, s6=0, s7=-1 [1].

After compression the samples will become s1=3, s2=0, s3=125, s4=5, s6=pw, s7=-1.

Here s3=125 means s2 is repeated and 125 is an identifier bit for repetition. s4=5 means s2 is repeated 5 times. Now s6 is free so that position can be considered for adding the watermarked signal.

If in any case the sampled value is 125 then change the value to 126. And if the repetition is more than 255, then write as s1=3, s2=0, s3=125, s4=255……so the 4th position is given 255 value which tells the algorithm that next position is also for the repetition.

5.3 Add Watermark Signal

In the next step watermark signal is added to the space pw which was created by the lossless compression. The advantage of this method is that it doesn't increase the size of the speech signal.

The phone number or terminal number and speaker's ID will be saved. When it is used in voice chat using computer, watermark will save computer's MAC address and IP address.

After the parameters are saved the parameters are coded. This coded form is then embedded to the places ready for watermark and then sent to encryption.

5.4 Encryption

After watermarking, the signal is to be encrypted for secure transmission or storage. LFSR is used for encryption.

The sender will obtain a random number using matlab and that random number is sent to the receiver. Receiver receives the random number. Sender and receiver will perform a chi square distribution of that number and will feed to LSFR.

The sender and the receiver side encryption should take place together.

Once the voice is produced, it is sampled, compressed, watermarked .Then the signal is converted to the binary form for bit by bit XORing with the LFSR.

5.5 Decryption

The received signal is decrypted by XORing with the LFSR again to produce the compressed and watermarked signal. Then through the reverse method of the compression algorithm the watermark is extracted. That is when it sees 125 it knows that the samples are going to get repeated and the watermark signal is also embedded. So first watermark signal is extracted then the signal is decompressed

Below in fig 3 find the overall system design of the process.

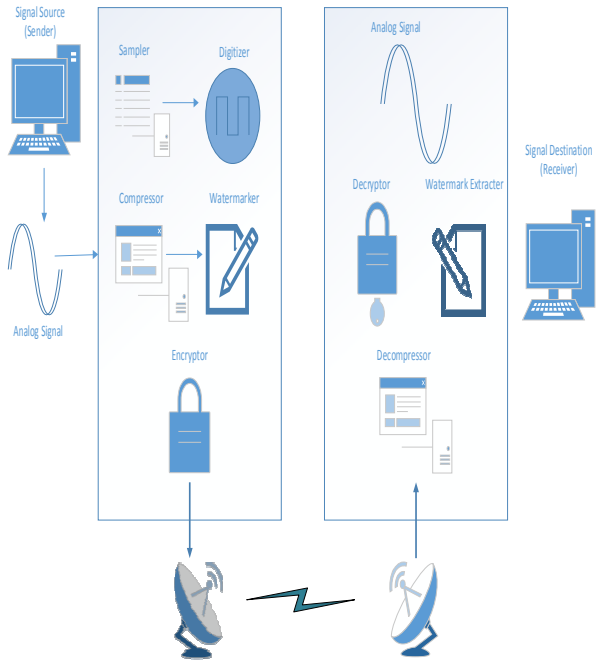

Fig -3: Overall System Design

5.6 Block Diagram

Before encryption as shown in fig 4 the original signal is sampled by PCM method and the output of the sampling is 8 bit PCM .Once the signal is sampled it is compressed using loss less compression .Once the samples are compressed it creates space for the watermark. Watermark signal is added to the created space. Then encryption is performed by XORing with the pseudorandom number which is generated by pseudorandom number generator. Then the encrypted signal is the output of the system. The signal is then transmitted by the sender.

After the signal is received by the receiver the encrypted signal is decrypted as shown in fig 5 by XORing it with the pseudorandom number. After decrypting the watermark signal is extracted from the signal by the method of decompression. After decompression the original signal is produced.

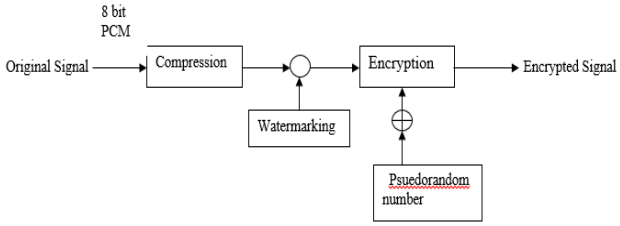

Fig -4: Block Diagram of operations before transmission

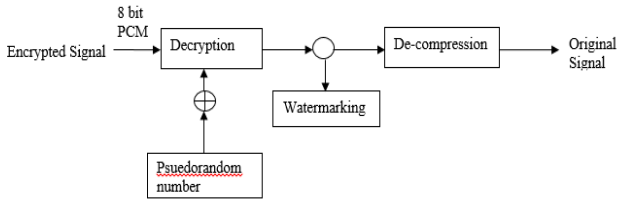

Fig -5: Block Diagram of operations after reception.

6. CONCLUSIONS

Secure speech with LFSR represents a watermarking scheme for identification, verification and authentication of real-time speech signal. The watermark is not easily detectable as the size of the frame is not increased. If the there is any attempt to change the content of the signal in the transmission channel, proposed scheme can detect it and return noise at the end. However, if any other decryption algorithm other than LFSR is used, it also returns just noise at the end. Thus it prevents eavesdropping, man-in-the-middle attack and provides security of the stored speech signal. It is only possible for someone who has the possession of watermarking algorithm scheme to get the speech signal meaningful. Finally, the user or administrator doesn't require additional memory space because of watermarking and encryption

REFERENCES

[1]. H. M. D. Kabir, S. Bahauddin, M. I. Azam, et. al.,"A Theory of Loss-less Compression of High Quality Speech Signals with Comparison" in European Modelling Symposeum (EMS 2010), 17-19 Nov. 2010.

[2]. Hussain Mohammed Dipu Kabir, Saeed Anwar, Syed Bahauddin Alam, K. M. Sabidur Rahman, Md. Abdul MatinI, Imranul Kabir Chowdhury. "Watermarking with Fast and Highly Secured Encryption for Real-time Speech Signals" 2010 IEEE

[3]. Tin Lai Win, and Nant Christina Kyaw. "Speech Encryption and Decryption using Linear Feedback Shift Register" Proceedings of World Academy of Science: Engineering & Technology; Dec2008, Vol. 48, p1293

BIOGRAPHIES

Arathi K Chandran received B.Tech Degree in Computer Science from Toc H Institute of Science and Technology. She has 2 years of experience at Mphasis an HP company. Her domain at Mphasis was Lotus Notes. She is currently pursuing M.Tech Degree at Toc H Institute of Science and Technology specialization in Data Security (Computer Science).

Assoc. Prof. Sreela Sreedhar received her B.Tech degree from Government Engineering College Palakad and her M.Tech Degree from Dr. M.G.R educational and research institute. She is currently serving as HOD in Computer Science Department at Toc H Institute of Science and Technology. Presently author is also doing her Ph.D. at Anna University. Her area of interest is Data Security.