

Original Research Article**A real time Secured Voice Framework using the totally reconstructed Discrete Wavelet Transformation****Abstract**

In our daily today and with the upraise of the mobile computation and mobile phones we are using more voice applications. The voice application could then send voice information with different information over different communication channels. To protect this voice information we encrypt it. In this paper we are proposing a Framework using the totally reconstructed Discrete Wavelet Transformation (DWT) to encrypt the voice information in real time with where the sample rate of the encrypted voice signal is equal to the original voice signal sample rate.

Keyword: Discrete Wavelet Transformation, Sound/ Voice Encryption, Real time application

1. Introduction

There has been increasing interest in research involving the security of information systems. In recent years the number of computer attacks increased dramatically. With the use of the internet and smart mobile devices there is a need to secure the communication channels against possible threats. Securing voice communication became a very important Challenge to information technology researchers to find suitable ways in protecting this type of information.

In the world of new technologies we have more and more applications depending on sounds/voices. A variety of modern applications are taking sounds/voices as input, storing, processing and transferring it over different communication channels. The new era with the mobile computing gives us many challenges to handle the different multimedia elements. With sounds and voices as a major and important input to these devices there is a need to develop the right applications for it. This shows us the need for fast applications if applied on mobile devices, and then the user of a mobile device should not wait when doing the application. This means that there is a need of a real time applications and application processing. Therefore if we develop application for such type of devices or other devices we need not only to think about the application itself but also about the processing speed of the developed application. In real time application we have to develop the application with results appearing to the user or other systems without any delay. Therefore for we have to choose carefully the algorithm with a minimum time complexities and fast execution times. Another point of view we are considering is that the sound or voice we are using is transferred over different communication channels, therefore we using these channels we are facing different threads, we give us the need of securing the sound/voice over these channels. In our paper we

will use a methodology of encrypting/ decrypting the sound/voice, we the property of having all things done in real time.

The rest of this paper is organized as follows: literature review and related work is described in Section 2. Section 3 describes the Mechanism of the proposed method. In section 4 a Sample encryption of the proposed method is shown. Finally, Conclusions and future Work are drawn in section 5.

2. Related Works

Secure voice/ sound has been studied in many published papers; those papers discussed many secured methods, technologies and challenges. The encryption mechanism of voice / sound building up the different filter banks as keys for the different stages of the filtering process to encrypt the voice signal.

There are many ways to secure voice, one of these methods is to scramble the voice [1][2], where one have to transpose or invert the voice signal. Another way is to make the so called Base band inversion [3] or phase inversion, with it the spectrum is inverted at a single preset never changing frequency. One further way to deal with secure voice is the Amplitude modification [3], where it is not really change the original signal. Among further methods is the use of the linear predictive coding (LPC) [4]. The application of the cryptographically algorithm to the voice parameters results as clearly encrypted voice signal.

One of the pioneered concepts to secure voice was the SIGSALY System (X System, Project X, Ciphony I) developed by Bell Labs[5]. It was a secure voice system used in second World War for the highest-level Allied .This concept was built by adding noise to voice signals to prevent listening to the original voice signals by the enemy forces.

After that the United States Department of Defense uses the MELP or enhanced-MELP (Mixed Excitation Linear Prediction). The MELP is a voice/speech coding standard [5].Another standard for speech coding was created by Texas Instruments known as MIL-STD-3005 [5].

Many Encryption Systems based on hardware were built, where they are voice encryption schemes that use hardware to encrypt the speech without the use of a computer. They are used in Cell phones and radio to make them more secure. Hardware encryption systems are relatively expensive and difficult to acquire.

Hemlata Kohad et al[6] discussed in their work the different methods used for the encryption and decryption of the speech signals. Among the discussed methods are the Time Domain Scramblers, the Frequency Domain Scramblers and the Pseudo Noise Sequences Encryption. They showed also the different modes of encryption systems. They concluded that the Speech encryption using a method called the Kasami sequence is better with the time domain and frequency domain as they compared with the other pseudorandom noise methods. They showed also that enhancement of the security of Speech encryption is possible using the kasami method.

Jay M. Joshi et al[7] added in their work another security level to the existing security standard for mobile communication. This added security level was done using the Discrete

Wavelet Transformation. They showed a comparison between their approach and existing approaches for mobile communication. They also suggested a Hardware implementation of their approach. They showed that their proposed method with the allowed mobile communication delay standards and their method need only 20% of CPU load, a maximum size of about 15k bytes, a minimum size of about 13k bytes and other capacity results.

Siddeeq Y. Ameen et al [8] showed in their work that using segmental spectral signal-to-noise ratio to test the performance of their proposed system. They concluded that the built system have a high security performance with a distinguish between male and female speakers.

Another related work is the work of Tin Lai Win and co. [9]. They presented in their work an overview of the symmetric cryptography. They used the Linear Feedback Shift Register (LFSR) to examine the Voice over IP Security. They found that the Linear Feedback Shift Register (LFSR) algorithm is suitable for encrypting/decrypting of streams of data.

3. The Mechanism of the proposed method

A wavelet is from its name a small wave, which oscillates beginning at the zero value amplitude, then increasing and at the end decreasing towards zero value. Wavelets are considered as functions, which can act as a bandpass filters with a variations between high frequency and low frequency[10].

The wavelet Ψ has the following property:

$$\int_{-\infty}^{+\infty} \Psi dt = 0$$

There are many types of commonly used wavelets, among them the Haar wavelet, Daubechies wavelets, Symlets and many others [11].

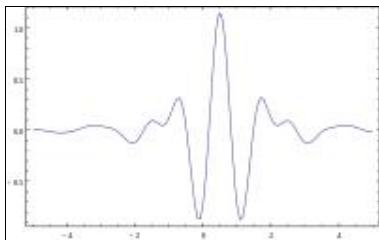


Figure 1: Wavelet example

The Discrete Wavelet Transform (DWT) is a wavelet transform, where the wavelets are discretely used, with the advantage that it can capture the frequency information and the time information of the signal (location information)[12].

The multiscale decomposition analysis is composed of a discrete time low pass and band pass filter banks. It divides the discrete time signal into a high band and a low band one. The signal x is down sampled by the factor of two, figure 2.

$$y_{low} = (x * g) \downarrow 2$$

$$y_{\text{high}} = (x * h) \downarrow 2$$

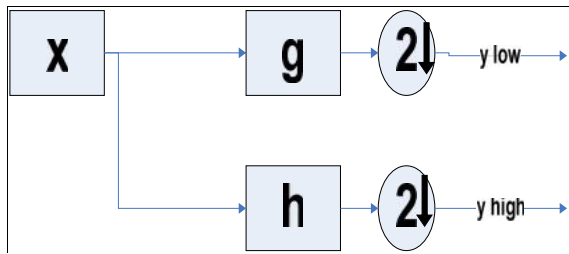


Figure 2: The multiscale decomposition analysis with DTW

This process is repeated with the low band output, where the fast discrete wavelet transform produces a stream of samples octaves. Half the sampling rate, such a one again halved sampling rate for the 1 octave lower lying bound.

The proposed voice encryption method steps are shown in figure 3.

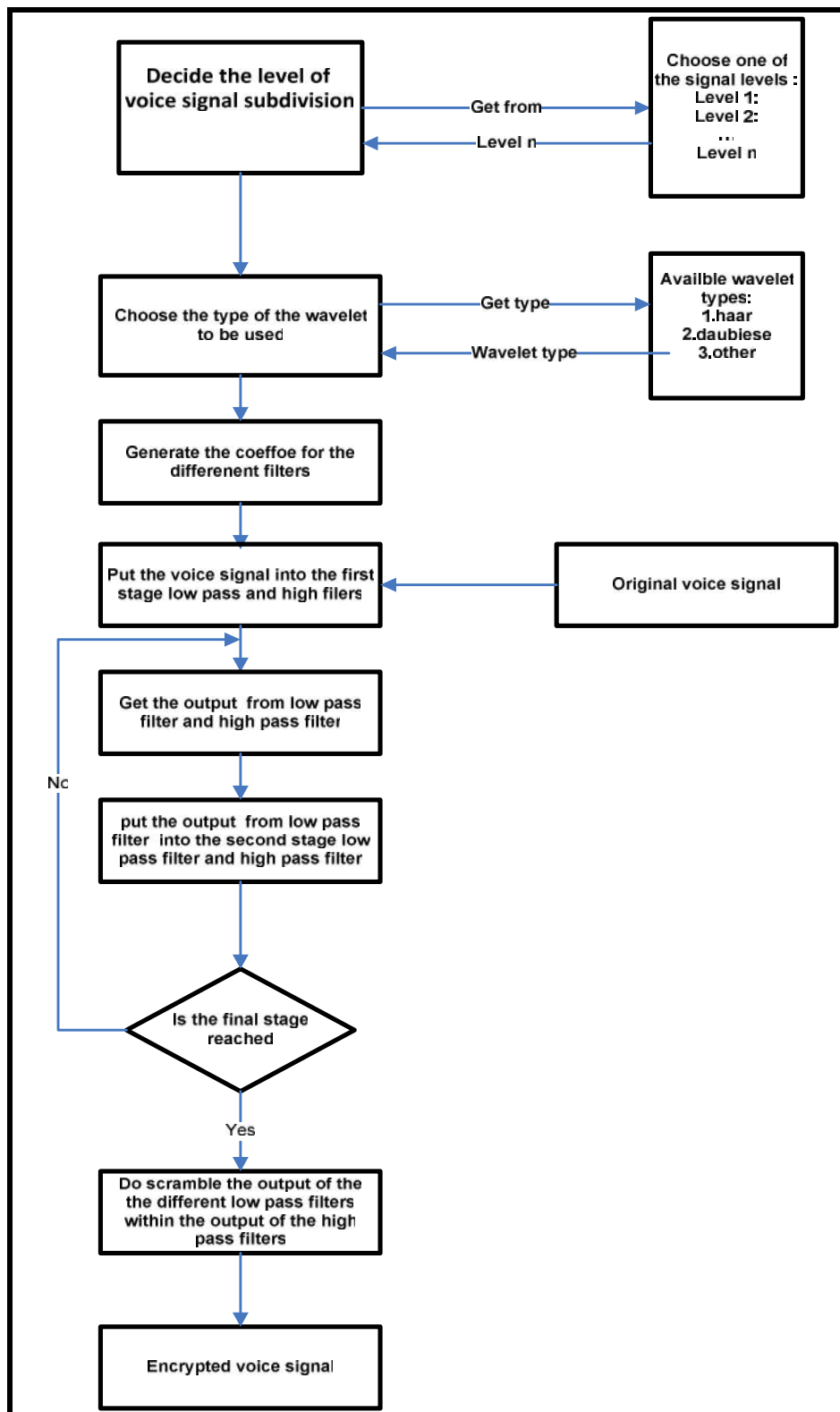


Figure 3: The proposed voice encryption method.

At the first step of the proposed method one decides about the level of voice signal subdivision which means the number of octaves to be used (which is equal to n). At this step the voice signal is divided in different sub signals, where the signals level should be selected from the available signal levels (namely n levels). The more the value of this selection is, and then more sub signals are produced, which makes the encryption more efficient.

The next step is to choose the type of the wavelet to be used for the discrete wavelet transformation from a given list of the available wavelet types like the Haar wavelet, Daubechies wavelets, etc. For more encryption complexity one can develop his own wavelets and then add them to the available wavelet list.

After this step the generation of the coefficients for the different filter banks is done. These coefficients are stored as a vector for further processing.

We put then the original voice signal into the first stage of the low pass and high filters.

At the next step we get the output from low pass filter and high pass filter, where the output of the high pass filter is stored.

The output from low pass filter is putted again like the original voice signal into the second stage low pass filter and high pass filter. The last two steps are repeated until the required level of sub signals is reached.

If the final stage reached then we do scramble the output of the low pass filter within the output of the different high pass filter. After all we have the encrypted voice signal with the same sample rate as the original voice signal. This encrypted voice signal is then transmitted through an appropriate transmission channel.

The different parameters (n levels, type of the wavelet, filter banks parameters) are acting as the key for this encryption method.

4. A Sample encryption of the proposed method

As a sample of the model we will use the following

At the production of the voice signal we have a continuous representation of the voice signal with a common sampling rate like 8 kHz, see figure 4.

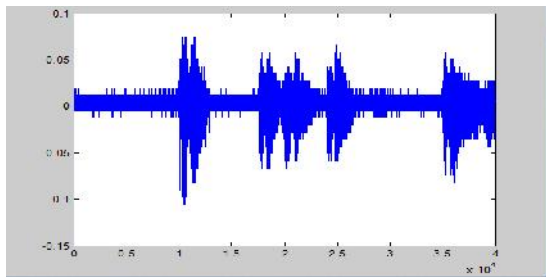


Figure 4: original voice signal

At the first step we have to choose the level of voice signal subdivision which means the number of octaves to be used (namely n). In this example we will choose n equal to three, therefore we should have 4 different signals outputs like in figure 5:

The next step is to choose the type of the wavelet to be used for the discrete wavelet transformation from the given list of the available wavelet. For this example we choose a Daubechies wavelet.

the output from low pass filter is putted into the second stage filtering repeatedly until we reach the final level having the following outputs shown in figure 6:

[illegible]

If we have an original voice signal with the sample rate $k = 8\text{ kHz}$ then we have then the output signals having the following sample rates: h_1 with the sample rate $k/2 = 4\text{ kHz}$, h_2 with the sample rate $k/4 = 2\text{ kHz}$, h_3 with sample rate $k/8 = 1\text{ kHz}$ and $h_4 = 1\text{ kHz}$ with the sample rate $k/8$. Adding all the sub signals sample rates together gives the original sample rate, namely 8 kHz .

h1h2h1h3,h1h2h1h4,h1h2h1h3,h1h2h1h4,h1h2h1h3,h1h2h1h4,h1h2h1h3,...

This is then the final scrambled signal with the originals sampling rate to be transmitted.

5. Conclusion and future Work

In this work we proposed a new framework for the real time encryption and scrambling of speech signals. The new framework gets the original signal with the original sample rate and gives this signal as a scrambled one using Discrete Wavelet Transformation (DWT).

The proposed method is implemented using standard available software with the feature that the encrypted signal is retrieved in real time. The method is a good way to encrypt voice for real time applications. The original voice signal is preserved and totally reconstructed.

For future work there will further experimental comparison to measure the different performance levels compared with other voice encryption methods

References

- [1] B. Goldburg, S. Sridharan, and E. Dawson, "Design and cryptanalysis of transform-based analog speech scramblers", IEEE Communication, Vol. 11, No. 5, 1993.
- [2] A. Matsunaga, K. Koga, and M. Ohkawa, "An analog speech scrambling system using the FFT technique with high-level security", IEEE Communication., Vol. 7, No. 4, 1989.
- [3] H. J. Beker and F. C. Piper, "Secure Speech Communications" Academic, London, UK, 1985.
- [4] Jeremy Bradbury, "linear Predictive Coding", 2000.
- [5] William R. Bennett, "Secret Telephony as a Historical Example of Spread-Spectrum Communications", IEEE Transactions on Communications, Vol. 31, No. 1, 1983.
- [6] Hemlata Kohad, V.R. Ingle, M. Gaikwad, "An Overview of Speech Encryption Techniques", International Journal of Engineering Research and Development, Volume 3, Issue 4, 2012
- [7] Jay M. Joshi, Upena Dalal, "Hardware Implementation of Wavelet Based Speech Encryption for End-to-end Security in Mobile Communication System", Int. J. of Recent Trends in Engineering and Technology, Vol. 4, No. 4, 2010.
- [8] Siddeeq Y. Ameen, Abbas A. Al-Shalchi, Muhanad D. Al-Bayati, "Design and Hardware Implementation of a Speech Cipher System", Journal (NUCEJ), Vol. 10, No. 1, 2007.
- [9] Tin Lai Win, Nant Christina Kyaw, "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)", World Academy of Science, Engineering and Technology, Vol. 2, 2008.
- [10] Paul S. Addison, "The Illustrated Wavelet Transform Handbook", Institute of Physics, ISBN 0-7503-0692-0, 2002.
- [11] Martin V., Herley C., "Wavelets and filter banks: Theory and design", Signal Processing, IEEE Transactions, 1992.
- [12] Stephane M., "A wavelet tour of signal processing", 1998.