# Speech Scrambling Using Multi-Stage Permutation with Filter Output

Ghassan M. Hassan
Al-Mustansiriyah University
Computer Department
Baghdad, Iraq
cs_gmhalsaddi@uomustansiriyah.edu.iq
gmhalsaddi@yahoo.com

## Abstract

The development of modern communications lead to discover a cipher systems to prevent the unauthorized listeners to steals the data (including speech), and became an important requirement. One of these systems is Speech Scrambler, which it applied to get a secured speech signal using for transmission. In this paper, we proposed speech scrambler algorithm based on shift register and permutation approach to scramble clear speech into unintelligible signal in order to avoid eavesdropping. The MATLAB software was used to simulate a proposed speech scrambler algorithm, which reduced the residual intelligibility. The experimental results demonstrate the high secure communication between two parts using proposed algorithm.

## المستخلص

تطور الاتصالات الحديثة ادى إلى اكتشاف أنظمة التشفير لمنع غير المصرح لهم من المستمعين بسرقة البيانات (بما في ذلك الكلام)، وأصبحت مطلبا مهما. احدى هذه الانظمه هو بعثرة الكلام، والتي تطبق للحصول على سرية الكلام المستخدم بالاتصالات. في هذا البحث، تم وضع خوارزمية مقترحة لبعثرة الكلام والتي تقوم على اساس مسجلات الازاحة والبعثرة والتي تقلل من الوضوحية المتبقية لمنع التنصت على المحادثات . تم استخدام برمجة MATLAB لمحاكاة الخوارزمية المقترحة لبعثرة الكلام. وانتائج التي تم الحصول عليها توضح الحصول على اتصال عالي الامنية بين جزئي الخوارزمية المقترحة.

## Keywords

Scramble, de-scramble, sampling, permutation.

## 1- Introduction

There has been an expected quickly increasing attention in, and progress of, secure communication algorithms with relation to the activities of military services, banking systems and other systems where degree of secured speech signal transmission plays a most important role. Scrambling is used to keep the confidentiality of speech signal over unauthorized listeners. It is simply disordering of the speech signal so that it is no longer intelligible. The original speech signal can be recovered by the intended receiver through appropriate descrambling technique. Among speech scramblers, analog speech scramblers are considered due to their wide applicability. The three most important criteria used to evaluate speech scramblers are[1]:

1. The scrambler’s ability to produce encrypted speech with low residual intelligibility;
2. The extent to which the encryption and decryption processes affect the quality of the speech recovered by the intended recipient;
3. The scrambler’s immunity to cryptanalytic attack.

## 2- Audio Scrambling

Scrambling of the audio signal can be done in analog and digital domain, but what are the difference between analog scrambling and digital encryption?, the answer is a digital encryption device convert the original voice waveform into a long sequence of 1s and 0s (a process called voice coding) and then uses a known algorithm to encrypt those 1s and 0s [2]. The digital cipher text is then modulated and transmitted. The receiving device demodulated, decrypts and converts this signal back into plain text voice signal [2]. There are advantages to both digital and analog scrambling. For example, analog scrambling can provide a more natural sounding voice and simple key management. Digital encryption can use a highly complex cipher, and can employ sophisticated techniques to reduce noise in weak signal areas [2]. Among speech scramblers, analog speech scramblers are considered due to their wide application [3]

## 3- Analog Audio Scrambling

Scrambling of the audio signal can be done in analog and digital domain. This section captures the classification of the analog audio scrambling techniques due to their wide applicability [3]. The taxonomy of analog audio scrambling algorithms is depicted in Figure 1.[4]

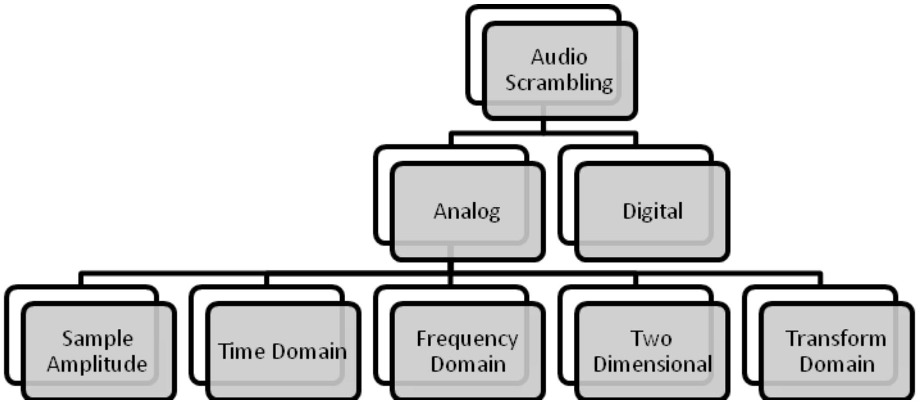


Figure -1- Taxonomy of analog audio scrambling algorithms

### 3-1 Review of the techniques

#### 3-1-1 Sample Amplitude Techniques

In the sample amplitude based technique, the amplitude samples of the original signals are taken up for scrambling [4][5]. Typical operations include interchange or permutation of speech samples [4][6], linear addition of pseudorandom noise amplitudes and non-linear modulo-arithmetic additions [4][7]. Two basic types of permutations available are Uniform (U) permutations and Shift-Register generated Pseudo-Random (PR) permutations. Some types of scramblers involve addition of masking signals to the amplitude samples, these masking signals can be a PR binary or modulo-arithmetic sequence.

#### 3-1-2 Time Domain Techniques

In time-domain scrambling, speech signals are divided into small time interval units (segments) and these units are permuted [3][5]. Main time domain techniques are Time-Inversion, Time Segment Permutation (TSP), Hopping-Window and Sliding Window TSP, Time Shifting of Speech Sub-bands, Reverberation [8] and time-domain based scrambler which does not need synchronization [9]

#### 3-1-3 Frequency Domain Techniques

In frequency-domain scrambling, speech signals are separated into several sub bands and these sub bands are then permuted.[3][5]. It ensures the original bandwidth is kept unchanged. In the frequency- domain, the first algorithms used were based on Fast Fourier Transform (FFT) technique, where the FFT coefficients are permuted frame to frame [3][10]. Techniques based on Discrete Cosine Transform [11][14], Wavelet Transform [12], Principal Component Analysis [13] etc.

#### 3-1-4 Two Dimension Techniques

In this class of scramblers the speech signal spectrum is divided into many sub-bands and the position of these sub-bands are then permuted[4][5]. Main frequency domain techniques are Frequency Inversion, Band-splitting, Band-splitting with Frequency Inversion and Frequency Inversion followed by Cyclic Band-shift [8].

### 3-1-5 Transform Techniques

This class of analog scramblers is based on operations performed on the linear transform coefficients of the audio samples [4]. Types of transforms used are Discrete Prolate Spheroidal Transform (DPST), Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Modified discrete cosine transform (MDCT), Hadamard Transform (HT), Circulant transformation, Wavelet Transform, parallel structure of two different types of wavelets with the same decomposition levels, combination of QAM mapping method and an orthogonal frequency division multiplexing (OFDM)[3][4].

## 4- Sampling

The analog signal (speech) is sampled every Ts seconds, where Ts is the sample interval. The inverse of sampling interval is called sampling rate or sampling frequency and denoted by fs, where fs=1/Ts, figure (2), [15]

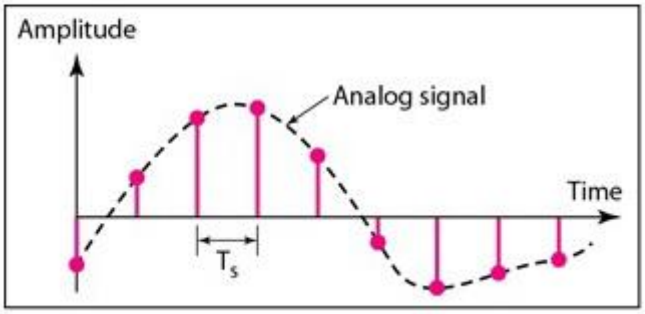


Figure -2- Speech sampling

The sampling rate is one important consideration. According to the Nyquist theorem, to reproduce the original analog signal, one necessary condition is that the sampling rate be at least twice the highest frequency in the original signal [15]. In this paper sampling rate was taken as fs=8000sampls/second.

## 5- Algorithm

The main aim of this algorithm is to establish the secure communication channel in order to secured speech signal transmissions. In this section, we describe the main steps of the proposed speech scrambling and descrambling procedures. All scramble and de-scramble methods done by using MATLAB programming. The flow chart of the proposed speech scrambler algorithm is presented in figure(3),

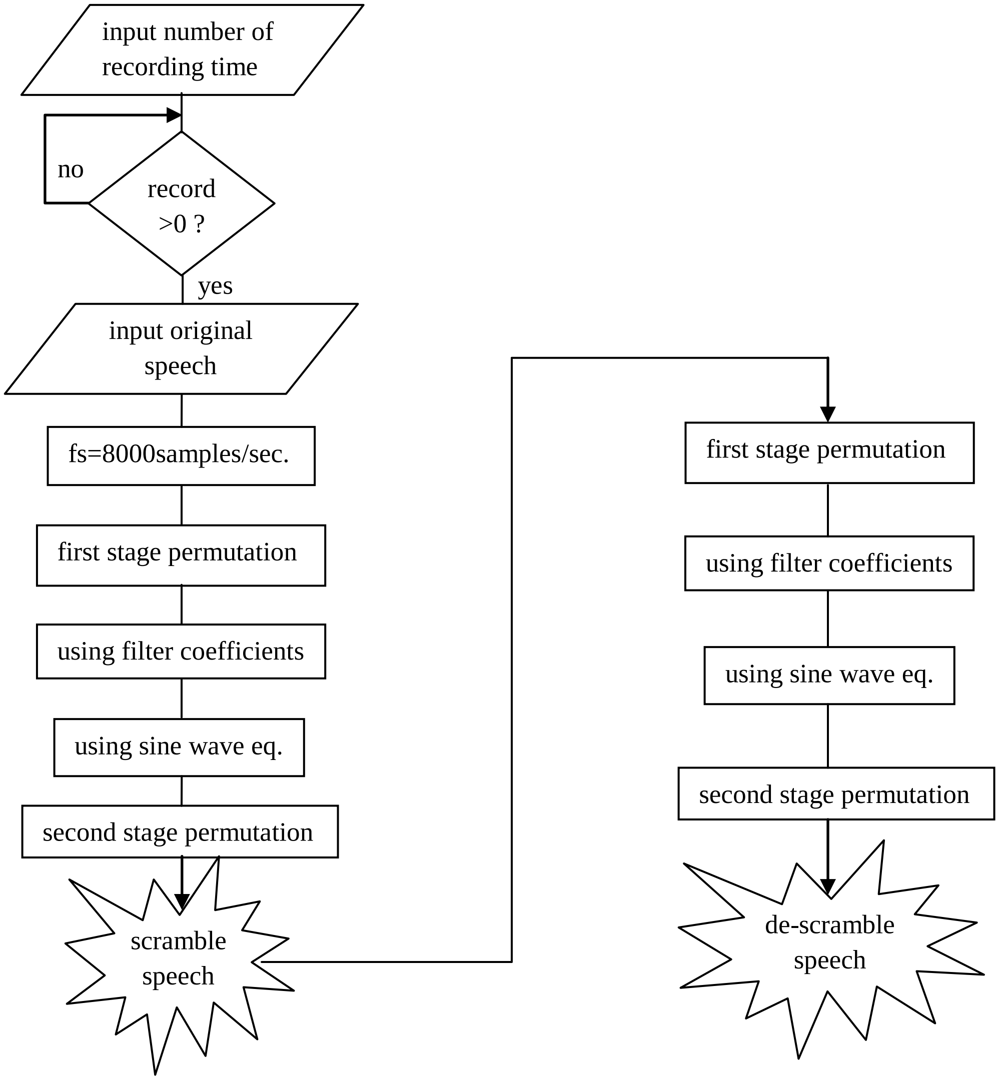


Figure -3- flowchart of scramble and de-scramble speech

### 5-1 Scrambler

The algorithm of proposed speech scrambler algorithm is as shown below:
**Input:** Clear speech signal**,** Number of seconds
**Output:** Scrambled speech signal
Step1)Input how many seconds of speech recording.
Step2)The analog signal (speech) is sampled at Nyquist rate (8000samples/second)

Step3) Using shift register to re-ordered the samples (first step scramble).

Step4) After re-ordering, the samples multiplied by filter coefficients of large period (ten numbers), and get filter output.

Step5) Multiply the filter output by the equation of sin wave.

Step6) Apply another step for permutation by using shift register again to get the final result.

Step7) End.

### 5-2 De-Scrambler

Step1)Specify sample rate (take the same sample rate as in scramble “8000samples/second”)

Step2)Using shift register to re-ordered the samples (first step descramble).

Step3)After re-ordering, the samples multiplied by filter coefficients of large period (the same ten numbers), and get filter output.

Step4)Multiply the filter output by the equation of sin wave.

Step5)Apply another step for permutation by using shift register again to get the final result (original speech).

## 6- Design of the Scrambler

### 6-1 Entity of the Frame

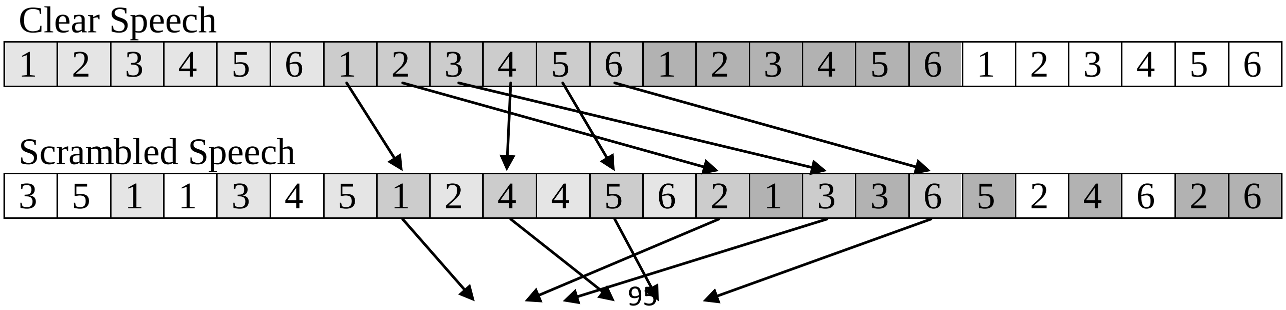
The size of scrambler which it is used in this algorithm is n X m (n- is the number of filter coefficients, while m is the length of speech’s file).

### 6-2 Specifications

The analog signal (speech) was sampled at 8000 samples/seconds. The speech signal is processed at the band width of 3KHz (300~3300Hz), while the channel of transmission at the band width of 4KHz(0~4000Hz)

### 6-3 How Algorithm Works

Figure (4) shows how it works. Speech was break into small segments and scrambled with another segments to change order, (even with first or second scramble and de-scramble).



Clear Speech

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 |

Scrambled Speech

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 5 | 1 | 1 | 3 | 4 | 5 | 1 | 2 | 4 | 4 | 5 | 6 | 2 | 1 | 3 | 3 | 6 | 5 | 2 | 4 | 6 | 2 | 6 |

De-Scrambled Speech

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 |

delay

Figure (4) Permutation of segments

## 7- Experimental Results

When the algorithm applied for different kinds of results, it seems like;

- Result of pronounced digits in Arabic language, figure (5)

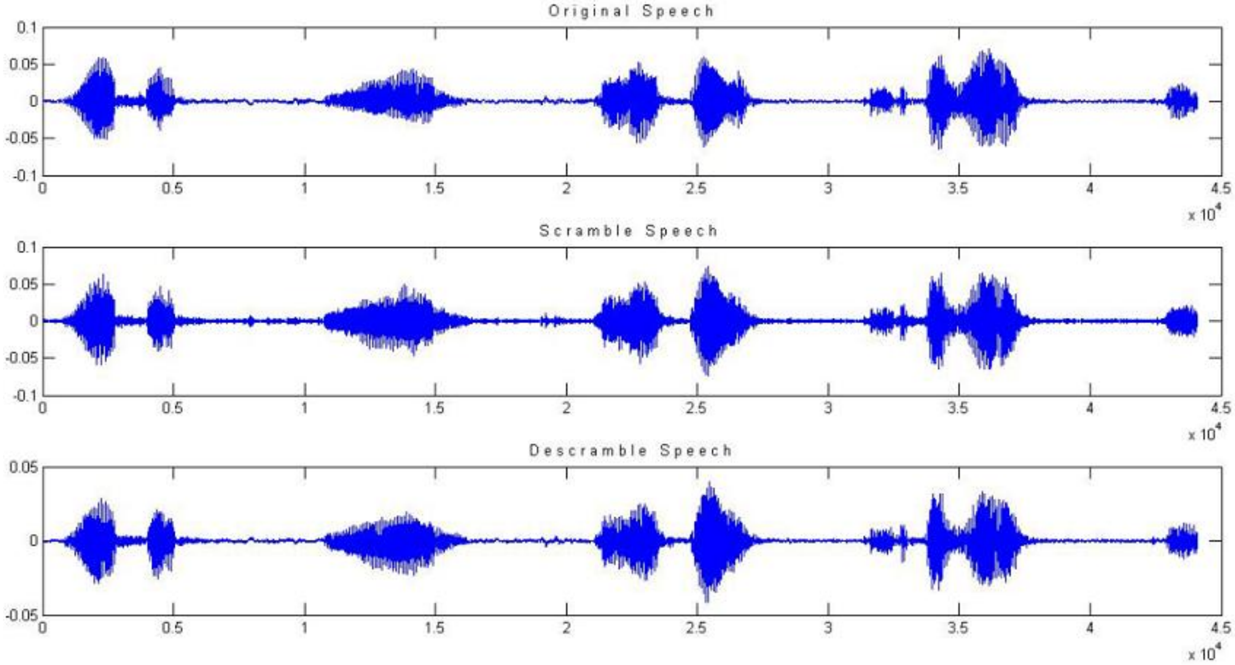


Figure -5- result of pronounced digits in Arabic

- Result of pronounced digits in English language, figure (6)

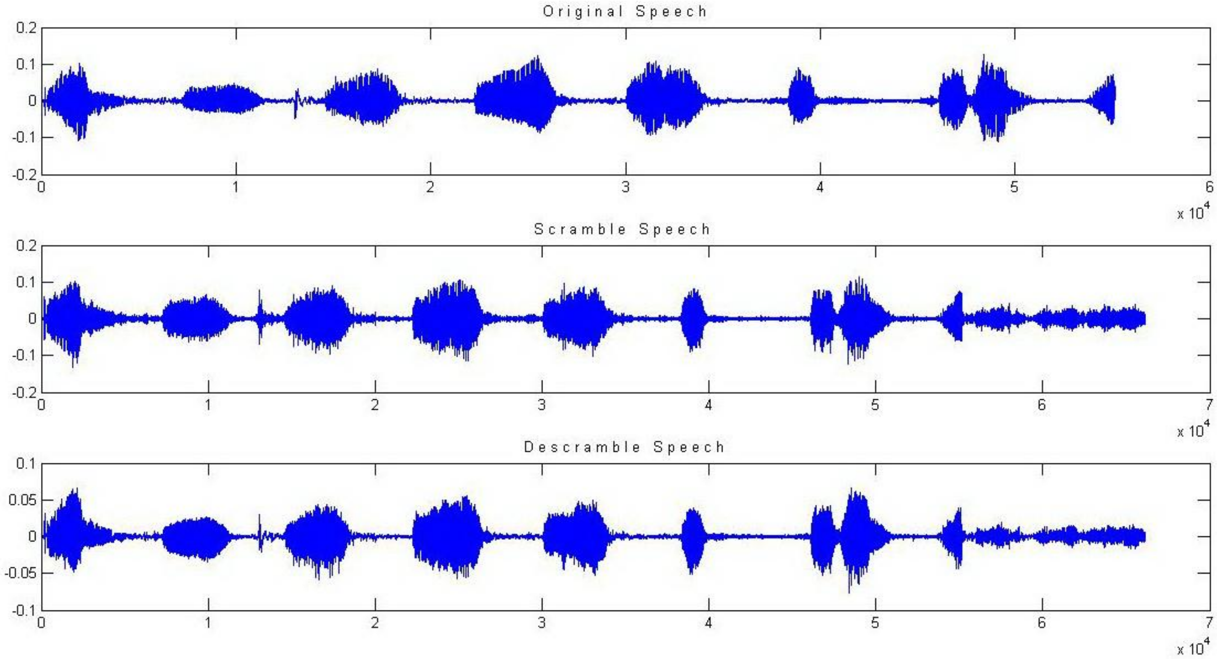


Figure -6- result of pronounced digits in English

- Result of pronounced one sentence in English language, figure (7)

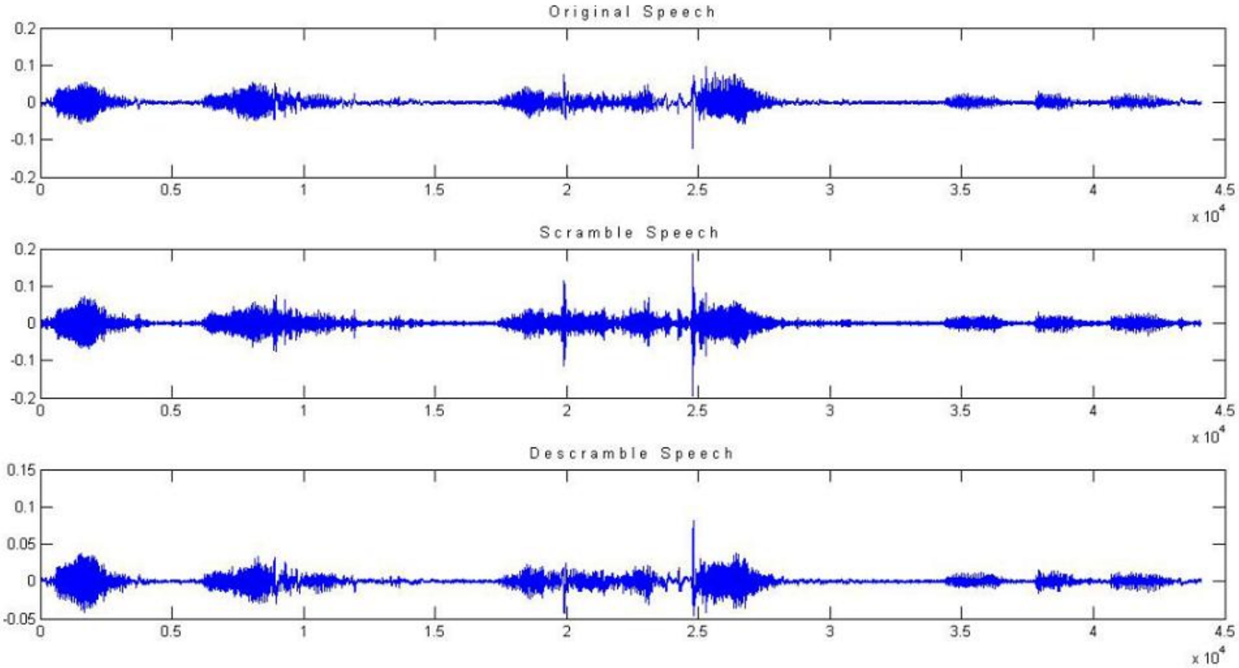


Figure -7- result of pronounced one sentence in English

- Result of conversation between two person in English language, figure (8)

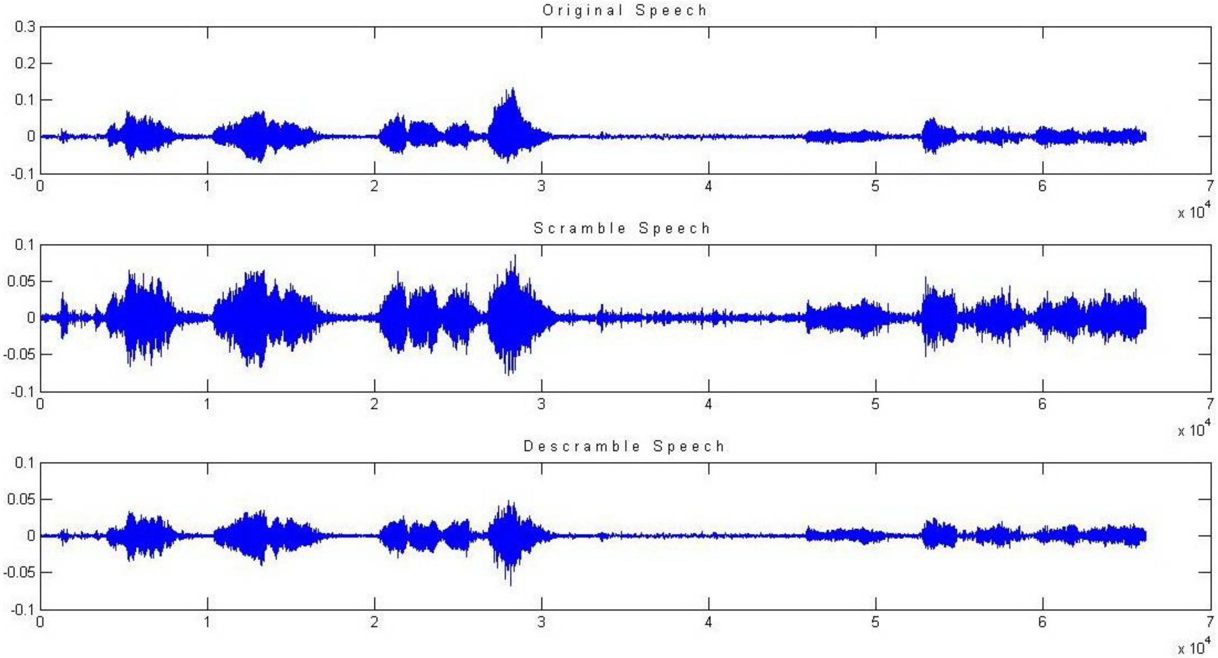


Figure -8- result of conversation between two person in English

## 8-Tests for Good Scrambling

There are many tests done to exam the scramble algorithm to introduce a perfect method. Some of tests are:[4]

1-Residual Intelligibility

The amount of redundant information in the scrambled signal is termed as residual intelligibility, which helps in easier recovery of the original information. [4]

2-Encoding Delay

The amount of time taken per unit by the scrambling algorithm to complete the scrambling operation is termed as encoding delay; in general the unit is taken as block or segment. The encoding delay is directly proportional to the number (N) of units, length (L) of each unit and the number of samples (S) present in one unit. When N, L, and S increases the recovered speech quality increases because of the availability of more number of permutable samples, but the encoding delay also increases.[4]

3-Key-space

The procedure used for transforming the signal is commonly called as Key. The level of security offered by an analog scrambling algorithm is a complex function of the number of usable keys called as key-space, length, rate of change of the key, properly selected limited key dictionary, proper time variation and distribution of the keys.[4]

4-Bandwidth Expansion

When the speech signal is scrambled, discontinuities are introduced in the scrambled signal, which results in an increase in the scrambled signal bandwidth. For higher scrambling effectiveness, larger amount of discontinuities are introduced, which in turn increases the bandwidth.[4]

All the above factors are applied for testing the algorithm of this paper, by using **digits only, sentence, and conversation between two persons**. The results in the table(1) for the intelligibility of the speech, by applied the algorithm for 27 time ;

| Intelligibility<br>Type of speech | original speech | scramble speech | descramble speech |
|---|---|---|---|
| **Digits** | 100% | 3.2% | 94.7% |
| **Sentence** | 100% | 2.9% | 95.5% |
| **Conversation** | 100% | 2.6% | 95.2% |

Table -1- Results of intelligibility for average of 27 time

Also, the algorithm applied for different size segment of speech 10-bit, 16-bit, 32-bit, and 256-bit. The result as shown in table (2);

| size of segment | security | intelligibility |
|---|---|---|
| **10-bit** | medium | medium |
| **16-bit** | better | low |
| **32-bit** | high | low |
| **256-bit** | very high | very low |

Table -2- Security and intelligibility for different segments

## 9- Conclusions and Future Work

In this paper, we have proposed a watermarking speech scrambler algorithm based on shift register and permutation approach which can be used for secure communication. Experimental results show that the security of proposed algorithm is very high and provides high-quality encryption of speech signal with much less intelligibility at the output signal. After applied this algorithm for multi times, and get different results, the algorithm may enhanced by removing the silent period between the words, which appear in figures 5 to 8. One method of doing this, by permuted the segments of silent period with the segments of the vocalized words to get the final result of segments.

## 10-References

[1]Bruce Goldburg, S. Sridharan, Ed Dawson, “Design and Cryptanalysis of Transform-Based Analog Speech Scramblers”, IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, June 1993.

[2]Jeanen France, “Basic Scrambler Information”, Account Manager, North America, Transcrypt International.

[3]Anjana D. S., Minu Kuriakose, “Frequency Speech Scrambler based on Hartley Transform and OFDM Algorethm”, International Journal of Computer Applications(0975-8887), vol. 61, no. 8, January 2013.

[4]A. Srinivasan, P. Arul Selvan, “A Review of Analog Audio Scrambling Methods for Residual Intelligibility”, Innovative Systems Design and Engineering, ISSN 2222-1727(Paper), vol. 3, no. 7, 2012.

[5]Maysaa abd ulkareem, Iman Qays Abduljaleel, “Speech Encryption Using Chaotic Map and Blowfish Algorithms”, Journal of Basrah Researches (Sciences), vol. 39, no. 2, 2013.

[6] J. Phillips, M. H. Lee, J. E. Thomas, ” Speech Scrambling by The Re-Ordering of Amplitude Samples”, Radio and Electronic Engineer 41, pp.99-112, March 1971

[7] S. C. Kak, et al, “On Speech Encryption Using Waveform Scrambling”, The Bell System Technical Journal 56, pp.781-808, May-June 1977.

[8] N. S. Jayant, “Analog Scramblers for Speech Privacy”, Computers and Security, North-Holland Publishing Company pp.275-289, 1982.

[9] F. Huang, E. V. Stansfield, ”Time Sample Speech Scrambler Which Does Not Require Synchronization”, IEEE Transactions on communications 41, pp.1715-1722, November 1993.

[10]Ehsani, M. S. and Borujeni, S. E. , “Fast Fourier Transform Speech Scrambler”, Proceedings of The First International IEEE Symposium on Intelligent Systems, vol. 1, pp. 248 – 251, 2002.

[11]Dawson, E. , “Design of a Discrete Cosine Transform Based Speech Scrambler”, Electronics Letters, vol. 27, pp. 613 – 614, 1991.

[12]Ma, Fulong , Cheng, Jun and Wang, Yumin, “Wavelet Transform-Based Analogue Speech Scrambling Scheme”, Electronics Letters, vol. 32 , pp.719-721, 1996.

[13]Nidaa A. Abbas, “Speech Scrambling Based on Principal Component Analysis”, Journal of Computing, vol. 1, no. 3, pp. 452-456, 2009.

[14]B. Goldburg, E. Dawson, S. Sridharan, “A Secure Analog Speech Scrambler Using The Discrete Cosine Transform”.

[15]Behrouz A. Forouzan, “Data Communications and Networking”, Fourth Edition, McGraw-Hill International Edition, 2007