I J C T A, 9(2) 2016, pp. 935-941
© International Science Press

An Efficient speech scrambling technique based on chaotic mapping and pseudorandom binary scrambling

Dhanya G.*, and J. Jayakumari**

Abstract: To enhance the information security in network communications, this paper suggests a new speech scrambling algorithm based on random permutation, chaotic mapping and pseudo random binary scrambling.Firstly random permutation algorithm is used to shuffle the rows of the original speech followed by shuffling the rows using chaotic Bernoulli mapping. This produces an intermediary scrambled speech. In the second step, pseudo random binary generator and chaotic encryption are utilized to make the final scrambled signal. Various analysis tests are then performed to determine the quality and intelligibility of the recovered speech. The suggested scheme for speech scrambling can resist traditional attacks and it indicates a good level of protection. Also, it can retrieve the original signal with excellent quality, quickly and efficiently.

Keywords: Speech scrambling, OFDM, Pseudo-random generator, random permutation, speech transmission index, common intelligibility scale

1. INTRODUCTION

In our daily life, speech communication is more common and the importance of offering a high level of security is increasing. Because of this reason a lot of speech scrambling techniques has been offered. Among which, analog scrambling is the most popular technique in speech communication. The commonly used cryptographic algorithms are Time domain scrambling, frequency domain scrambling and transform domain scrambling such as wavelet transform, discrete cosine transform, fast Fourier transform etc. [1]

The present work focusing on secured communication using scrambling, in which the data are converted to the intelligible form using scrambling operations at the sender. Data scrambling is mainly scrambling the data content to make the data unreadable during transmission. The unintelligible data is then transmitted through the channel to the destination. At the recipient side, the data are again converted back to an intelligible form by using descrambling operation and the data is conveyed securely. The scrambling and descrambling operations are performed by using a same key.[2]

The chaotic mapping has been employed in the scrambling algorithm. The chaotic map, which generates chaotic sequences and it is a pseudo random sequence which represents a good randomness, complexity and correlation. It delivers a complex system and difficult to predict and study. [1]

The advantages of chaos function is, it is secure, computationally faster and too it has simpler implementation. The early application of chaotic application sequences was to encrypt the text messages by using a key sequence which was generated by using a Bernoulli map. Of late, apart from the text messages, the Bernoulli map chaos functions are practiced to generate key sequences in encrypting the speech signals and images [3]. Hence the chaotic sequences can achieve cryptanalytically secured scrambling than other encryption methods.

* Research Scholar Noorul Islam University Kanyakumari, *Email: dhanyagnr@gmail.com*

** Head of the Department Noorul Islam University Kanyakumari

In this study, a combined approach of random permutations, chaotic Bernoulli map, pseudo random binary generator and chaotic encryption is used to get a number of sequences is proposed. The generated key sequences are applied for scrambling of speech signal.

This paper consists of five sessions. The scrambling operation is explained in 2nd sessions, while in session 3 comprise the proposed system. The performance analysis is presented in section 4 followed by conclusions in session 5.

2. FREQUENCY DOMAIN SCRAMBLER

The analog scrambling process can be described using matrix algebra. Let x represent a vector which contains speech, samples of length N and F represents the N*N Fast Fourier transform matrix [4].

Let U be FFT of the speech signal x is given by:

$$U = F.\, x$$

The Fourier transform results a new vector u. The $N*N$ permutation matrix P is applied to the speech vector u to produce a vector V.

$$V = P.\, u$$

The inverse transformation F^{-1} is applying on v gives a scrambled speech signal y [4].

$$y = F^{-1}.\, v$$

Table 1 and 2 shows the FFT speech scrambler performance analysis under PESQ and BER. The results do not show a good performance. Because of using four FFTs, the implementation of this scrambler is difficult. Consequently, we extend a secure method to provide better quality of the speech signal.

Table 1
FFT speech scramblers based on PESQ

Type of Scrambler	PESQ(AWGN)
FFT scrambler	4.02

Table 2
Evaluating random permutation with PRBS scrambling using different parameters

Type of scrambler	Eb/N0	BER
FFT scrambler with AWGN channel	10	0.6129

2.1. Permutation

The scrambling process does not increase the bandwidth of the system. Permutation is restricted to $M!$ FFT coefficients lying within the speech band 300-3000Hz. The possible number of permutations is $M!$ [5]. An efficient permutation method generates M! Permutations from a random number seed lying between 0 and 1. We can use this random number as a key in the scrambling process. Random numbers are generated using a pseudo random binary generator. This will reorder the speech segments and create the words unintelligible.

On the receiver side, the same key and the pseudo random binary generator are used to recover the original language.The speech scrambler based on Fast Fourier Transform retains a considerable protection in the data transmittal and the system is more complex by the function of four FFTs.

3. ANALYSIS OF THE PROPOSED SYSTEM

To get rid of the drawbacks of the existing system, proposed a new technique OFDM-based speech scrambler. The block diagram of the proposed system is shown in figure (1).

The proposed scheme is based on the combination of four permutations, random permutation, chaotic Bernoulli mapping, pseudo random binary encryption and chaotic encryption. The random permutation reorders the speech segments in time, which is performed by a seed. It produces a scrambled data, which is unintelligible to others. The Bernoulli chaotic mapping is used to generate a random number for scrambling. This is the intermediate scrambled output, which is fed to the pseudo random generator. The pseudo random binary scrambling is done by using a pseudorandom binary generator along with a key. The PRBS performs an XOR operation with the outputs of PRBG and the chaotic function. The PRBS output is fed to the Chaotic Bernoulli encryption, it also performs another XOR operation with the outputs of PRBS and random data. The output of the chaotic mapping is a scrambled output, which has not any similarity with the original signal, it takes in an unintelligible signal. This data is transmitted through the channel. It is crypt analytically secured algorithm and it produces low residual intelligibility. [6]

At the receiver side, descrambling is performed by using the same seed and key in the transmitter side. For analyzing the system the following parameters are used.

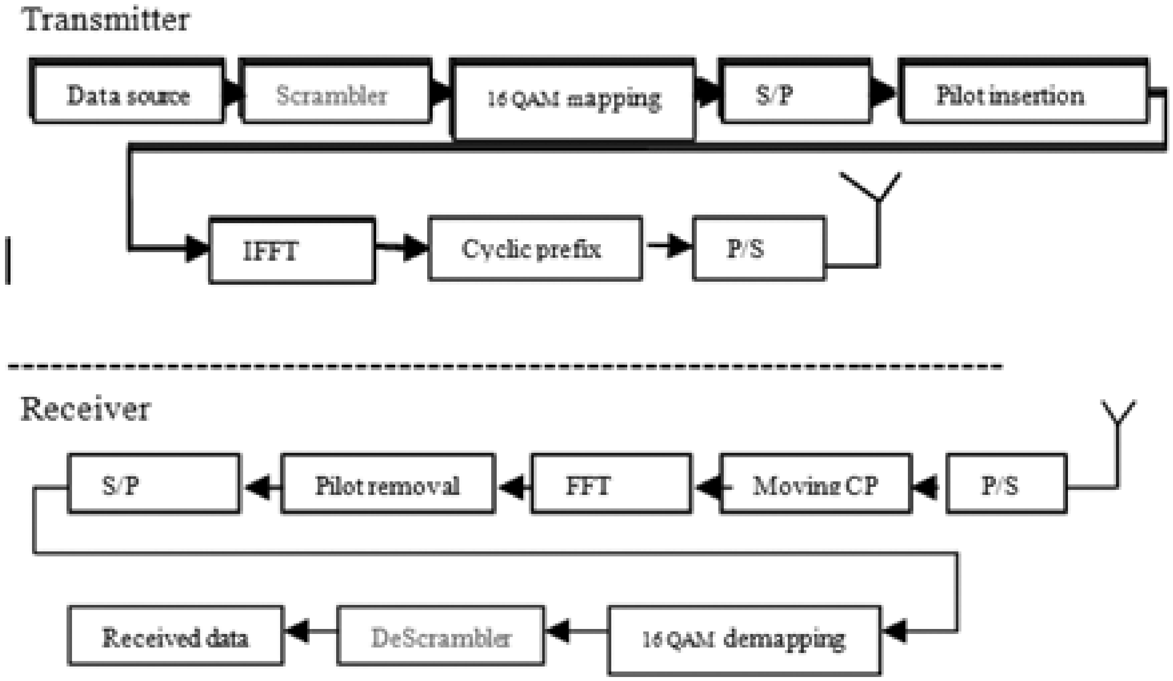


Figure 1: Proposed OFDM based speech scrambler block diagram [6]

Table 3
Parameters of proposed OFDM based speech scrambler [6]

Parameter	*Value*
FFT size(IFFT)	64
Bandwidth of transmission channel	300-3400Hz
Bandwidth of the input speech channel	0-3000Hz
Number of subcarriers	52
Sampling frequency	8kHz
Subcarrier spacing	312.5 kHz
Data symbol duration Td	3.2μs
Cyclic prefix duration Tcp	0.8 μs
Total symbol duration Ts (TD + Tcp)	4 μs
Mapping and demapping schemes	16 QAM

Let X is the input data be an array of t elements, k denotes the position of an array. X_k be the value of the k^{th} position element of permuted data array. R denotes the random data and P_k is the position of the random data. The position change of the random data is expressed as q_k. It will obtained by the expression

$$q_k = \begin{cases} P_{k+1} & if\, 1 \le k \le t-1 \\ P_1 & if\;\; k = t \end{cases} \tag{1}$$

The scrambled random data after applying q_k is expressed as RR_k. f is the position function.

$$RR_k = f^{-1}\, q_k \tag{2}$$

The scrambled output after first permutation can be denoted as $X'(k)$

$$X'(k) = Xq_k \tag{3}$$

This is the output of the first scrambler.

The output of the first scrambler is given to the Bernoulli chaotic mapping. It generates an intermediate scrambled output. It is represented by $X''(k)$.

$$X''(k) = X'(t – k + 1) \tag{4}$$

This is the output of the second scrambler.

This scrambled output is fed to the pseudorandom binary generator and applying a pseudo random binary scrambling. In this scrambler XOR operation is done with a random key (K). The output of the third permutation is $X'''(k)$. It is obtained by XOR the output of the first permutation and the output of PRBG. R'_k is the random binary data generated by PRBG.

$$X'''(k) = \text{round}\ (R'_k\,)\ \text{XOR}\ X''_k \tag{5}$$

Round function rounds to the nearest whole number.

The output of the fourth permutation is denoted as $X''''(k)$. It is obtained by XOR the output of the third permutation and the random data generated by chaotic mapping.

$$X''''(k) = \text{round}\ (Z'_k\,)\ \text{XOR}\ X'''_k \tag{6}$$

$Z'(k)$ is the random binary data generated by chaotic mapping.

$X''''(k)$ is given as the input of the QAM mapping. The QAM mapped output is then changed to parallel form. After inserting pilots, data are given to the IFFT operation. The cyclic prefix is added to the output of IFFT and the data is converted back to serial form for transmitting. AWGN channel is utilized for transferring the information.

At the recipient side, inverse operations are performed.

$$X'''(k) = X''''(k)\ \text{XNOR round}\ (Z'_k) \tag{7}$$

$$X''(k) = X'''(k)\ \text{XNOR round}\ (R'_k) \tag{8}$$

$$X'(k) = X''(t - k + 1) \tag{8}$$

$$P_k = \begin{cases} q_{k-1} & if\, 2 \le k \le t-1 \\ q_t & if\;\; k = 1 \end{cases} \tag{9}$$

$$X_k = f^{-1}\,(Pk) \tag{10}$$

Here four types of permutations are used, therefore it is more crypt analytically secured scrambling based on OFDM system.

4. PERFORMANCE MEASUREMENT

The quality and intelligibility of speech were evaluated by a perceptual evaluation of speech quality (PESQ), speech transmission index (STI) and common intelligibility scale (CIS). The noise performance is measured by signal to interference plus noise ratio (SINR) and Bit error rate (BER).

4.1. Perceptual Evaluation of Speech Quality (PESQ)

PESQ is used to compare an original speech signal with the received speech signal. The received speech signal is recognized as "degraded signal" and the original speech signal is known "reference signal" [9]. The Perceptual evaluation of speech quality (PESQ), it calculates the quality of a speech signal by a 5-point scale. The 5 corresponds to the excellent speech quality, 4 for sound, 3 for fair, 2 for poor and corresponds to bad or unsatisfactory speech quality, is demonstrated in table 4 [7]

Table 4
Comparison of OFDM speech scramblers based on PESQ [6]

Type of OFDM	PESQ(AWGN)
OFDM with RP	4.3
OFDM with RP & PRBS	4.4
OFDM with CS &PRBS	4.5

4.2. Speech Intelligibility Measurement

Two parameters are applied for measuring speech intelligibility

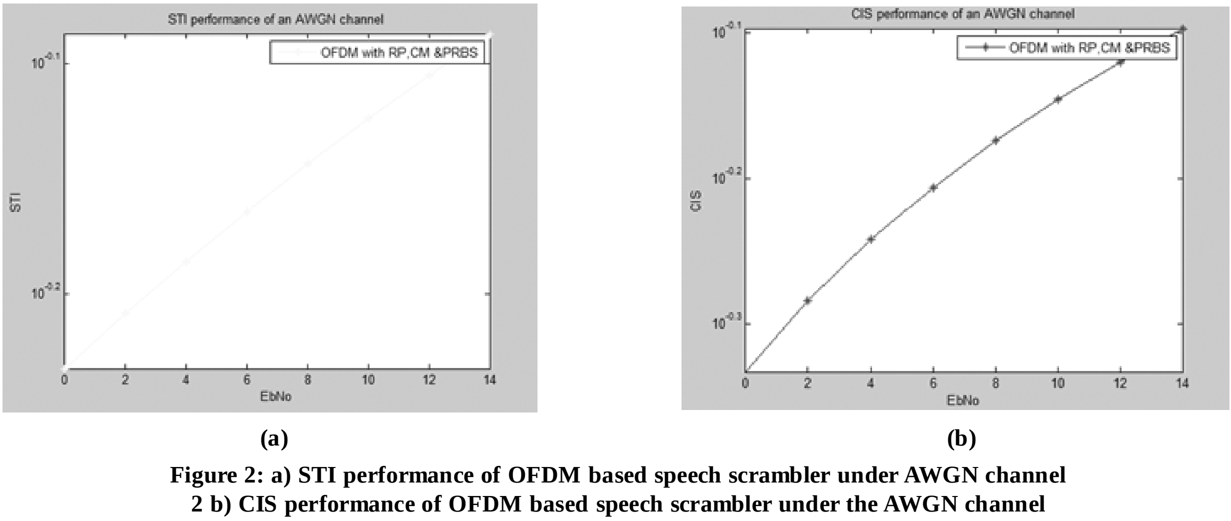
Speech Transmission Index (STI)

Common Intelligibility Scale (CIS)

The range of the speech transmission index lies between 0 and 1. The 0 indicates bad and the 1 indicates excellent. The weighted sum of Modulation transfer function (MTF) is applied to measure speech transmission index (STI). Modulation transfer index (MTI) is derived from a modulation transfer function (MTF). Here STI is calculated for a band of frequencies. SNR ranges are limited from +15db to -15db [8]. Speech transmission index computes all the factors in the speech transmission path, affects intelligibility.

Table 5
Relation between STI and speech intelligibility [7]

STI	.00–.30	.30–.45	.45– .60	.60–.75	.75–1.00
Speech intelligibility	Bad	Poor	fair	Good	Excellent



(a) **(b)**

Figure 2: a) STI performance of OFDM based speech scrambler under AWGN channel 2 b) CIS performance of OFDM based speech scrambler under the AWGN channel

The simulation results show that, the quality of the speech and the intelligibility of the speech are excellent, also the noise performance is low in this scrambler. Thus, the proposed scrambler RP with PRBS is the best scrambling technique in future communication.

Table 6
Evaluating random permutation with PRBS scrambling using different parameters

Type of OFDM	Eb/N0	BER	SINR	STI	CIS
OFDM with RP, CM & PRBS (AWGN)	12	0.210	0.1415	.7883	.7683

The simulation results show that, in table 6, the quality of the speech and the intelligibility of the speech are excellent, also the noise performance is low in this scrambler. Therefore, the proposed scrambler RP, CM& PRBS is the best scrambling technique in future communication.

4.3. Noise Performance

The SINR and BER performance of OFDM based CM & PRBS scrambler under the AWGN channel is shown in table 6. The Signal to Interference plus Noise Ratio is defined as the ratio between Signal power (Ps) and Interference power (PICI) plus noise power (N0) [8].

$$\text{SINR} = \text{PS} / \text{PICI} + \text{N0} \tag{7}$$

The speech.wav was given as the input signal. BER is calculated using the parameter Eb/N0. The random permutation with PRBS scrambling shows better performance and it has a low bit error rate when compared with the others under the AWGN channel. [8]

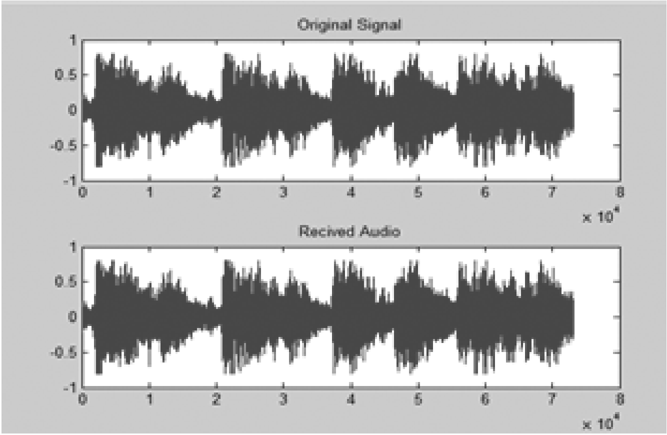


Figure 3: Original and reconstructed speech waveform [6]

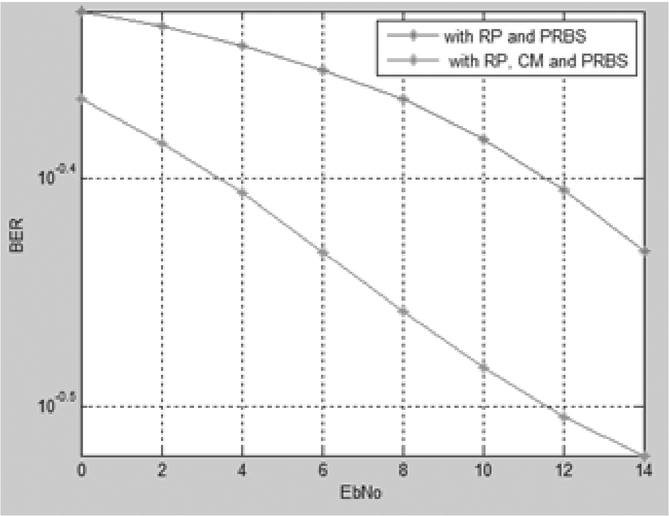


Figure 4: BER performance of OFDM based speech scrambler under AWGN channel

Table 7
Comparison of different types of OFDM speech scramblers based on a BER under AWGN channel [6]

Type of OFDM	Eb/N0	AWGN
OFDM with RP & PRBS	10	0.4101
OFDM with RP, CM & PRBS	10	0.32663

The comparison table 7 shows that the suggested method (RP, CM & PRBS scrambling) gives better performance than other methods.

5. CONCLUSION

In this paper proposed a new speech scrambling algorithm based on random permutation, Bernoulli chaotic mapping and PRBS. Firstly used a random permutation to disorder the segments of speech signal. Then used a PRBG followed by Bernoulli chaotic mapping. Thus obtain a scrambled speech. The suggested system is compared with the speech scrambler using the FFT method. To prove the efficiency of the proposed system various analysis tests are done. The simulation results indicate that the proposed system is secure and more efficient and it is crypt analytically more secured algorithm for the 4th generation of mobile communication.

REFERENCES

[1] Huan Zhao, Shaofang He, Zuo Chen, and Xixiang Zhang "Dual key speech encryption algorithm based undetermined BSS" The Scientific World Journal, Volume 2014, Article ID 974735, 7 pages.

[2] Shahram Etemadi Borujeni and Mohammad Eshghi "Chaotic image encryption design using Tompkins page algorithm" Mathematical Problems in Engineering, Volume 2009, Article ID 762652, 22 pages.

[3] Senk, V., Delic, V.D. ; Milosevic, V.S. "A new speech scrambling concept based on Hadamard matrices" Signal Processing Letters, IEEE (Volume: 4, Issue: 6), DOI:10.1109/97.586036, pages: 161–163, June 1997.

[4] Sridharan, S., Dawson, E.; Goldburg, B. "Fast Fourier transform based speech encryption system" Communications, Speech and Vision, IEEE Proceedings I (Volume:138, Issue: 3), DOI:10.1049/ip-i-2.1991.0029, pages: 215–223, June 1991.

[5] Borujeni, S.E. "Speech encryption based on fast Fourier transform permutation" Electronics, Circuits and Systems, 2000. ICECS 2000. The 7th IEEE International Conference on (Volume:1), 10.1109/ICECS.2000.911539, pages: 290-293 vol. 1,2000

[6] Dhanya G., Dr. J. Jayakumari, "Optimal speech scrambling technique for OFDM based system", *International Journal of Applied Engineering Research,* ISSN 0973-4562 Volume 9, Number 24 (2014) pp. 28871-28878.

[7] Tiago H. Falk1 and Wai-Yip Chan 2, "Performance Study of Objective Speech QualityMeasurement for ModernWireless-VoIP Communications", *EURASIP Journal on Audio, Speech, and Music Processing*, Volume 2009, Article ID 104382, 11 pages.

[8] Jianfen Ma, Yi Hu and Philipos C. Loizou, "Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions", *Acoustical Society of America*, May 2009.