APTIKOM Journal on Computer Science and Information Technologies
Vol. 2, No. 1, 2017, pp. 20~25
ISSN: 2528-2417
DOI: 10.11591/APTIKOM.J.CSIT.43

Speech Scrambling Based on Chaotic Mapping and Random Permutation for Modern Mobile Communication Systems

Dhanya G*[1], J Jayakumari[2]
Noorul Islam University, Kanyakumari, India
*Corresponding author, e-mail: dhanyagnr@gmail.com

Abstract

The expanding significance of securing data over the network has promoted growth of strong encryption algorithms. To enhance the information protection in network communications, this paper presents a Random permutation, chaotic mapping and pseudo random binary scrambling. It involves transforming the intelligible speech signal into an unintelligible form to protect it from interrupters. In this report, suggest a simple and secure procedure to secure the speech signal. The speech scrambling process makes use of two Permutations. In the first step, Random permutation algorithm is used to swap the rows of the original speech followed by swapping of rows using chaotic Bernoulli mapping. This produces an intermediary scrambled speech. In the second measure, pseudo random binary generator is used to make the final scrambled signal. Various analysis tests are then executed to determine the quality of the encrypted image. The test results determine the efficiency of the proposed speech scrambling process.

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

1. Introduction

Now a day's transfer of information is essential for communication in everyday life. Today the vast sum of multimedia data such as video, text and image is exchanged over various networks. Which contains much more secret information that will have high risk [1]. The security techniques provide a major function in maintaining integrity or authentication and privacy of data from unauthorized peoples. The encryption techniques transform the original signal into another form to protect it from unauthorized listeners by using a private key. AES, RSA and DES are the available encryption algorithms, which involves a great number of computations. [1-2]. Chaos theory is a study of mathematics and it is practiced in many of the emerging areas like cardiology, EEG analysis, communication and weather prediction. Chaos is extremely sensitive to initial conditions and it means a state of disorders. Many of the researchers are applied chaos sequences for encryption of the speech signals. One of the chaos function is the Bernoulli function generates an unpredictable non periodic pseudo random sequence. 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. [1].

In this study, a combined approach of random permutations, chaotic Bernoulli map and pseudo random binary generator 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 [3-5]. 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

Received December 15, 2016; Revised February 11, 2017; Accepted February 22, 2017

vector V: V= P. u. The inverse transformation $F^{-1}$is applying on v gives a scrambled speech signal y [5]: $y= F^{-1}. v$

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! [6]. 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 transmission 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.

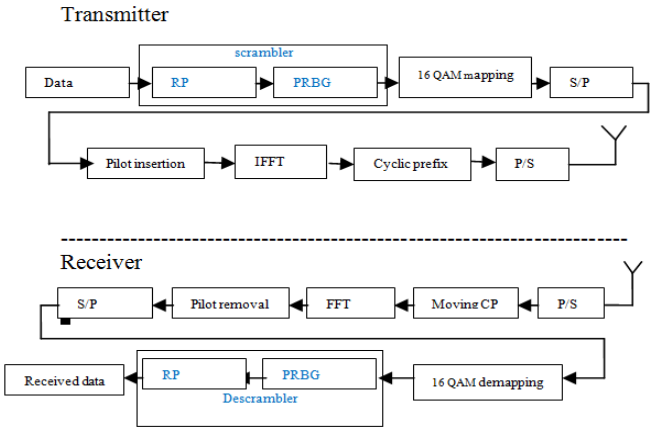

Figure 1. Proposed OFDM Based Speech Scrambler Block Diagram

The proposed scheme is based on the combination of three permutations, random permutation(RP), chaotic Bernoulli mapping (CM) and pseudo random binary scrambling (PRBS). 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 output of the PRBS 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. 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 in Table 3.

Table 3. Parameters of Proposed OFDM Based Speech Scrambler

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

$$q_k = \begin{cases} P_{k+1} & \text{if } 1 \le k \le t-1 \\ P_1 & \text{if } k=t \end{cases} \quad (1)$$

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

$$RR_k = f^{-1} q_k \quad (2)$$

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

$$X'(k) = Xq_k \quad (3)$$

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).

$$X''(k) = X'(t-k+1) \quad (4)$$

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.

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

Round function rounds to the nearest whole number. 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. Here two types of permutations are used to seed and key. Therefore, it is more crypt analytically secured scrambling based on OFDM system.

$$X''(k) = X'''(k) \text{ XNOR round } (R'_k) \quad (6)$$

$$X'(k) = X''(t-k+1) \quad (7)$$

$$P_k = \begin{cases} q_{k-1} & \text{if } 2 \le k \le t-1 \\ q_t & \text{if } k=1 \end{cases} \quad (8)$$

$$X_k = f^{-1}(Pk) \quad (9)$$

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 [8]

Table 4. Comparison of OFDM Speech Scramblers Based on PESQ

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: (1). Speech Transmission Index (STI), (2) 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 [9]. Speech transmission index computes all the factors in the speech transmission path, affects intelligibility in Table 5.

Table 5. Relation between STI and speech intelligibility

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

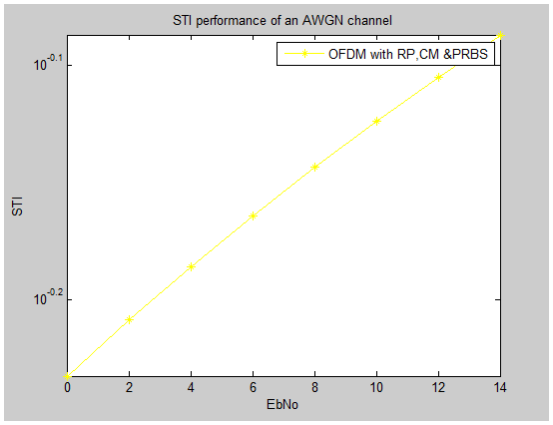

Figure 2(a)

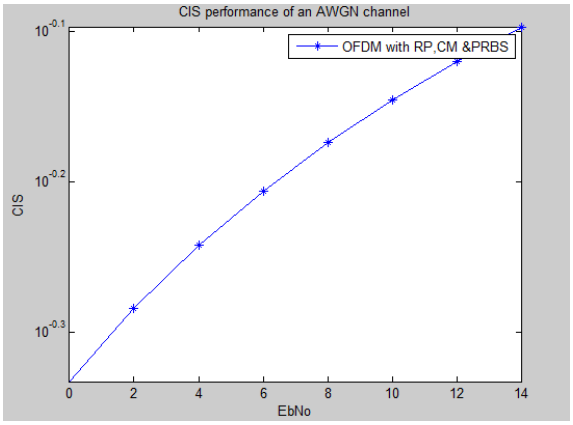

Figure 2(b)

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. 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.

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

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) [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:

$$SINR = PS / PICI + N0 \quad (7)$$

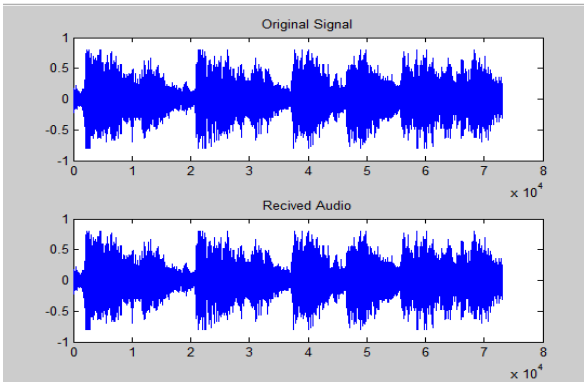

Figure 3. Original and Reconstructed Speech Waveform

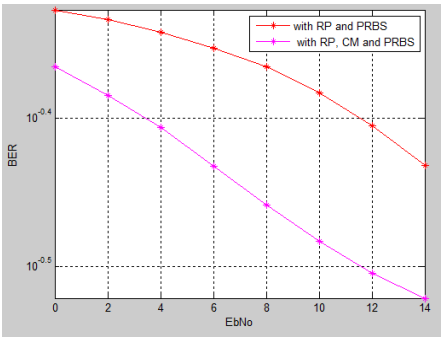

Figure 4. BER Performance of OFDM Based Speech Scrambler under AWGN Channel

Table 7. Comparison of Different Types of OFDM Speech Scramblers Based on a BER under the AWGN Channel

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 speech scrambling and descrambling is performed utilizing a key sequence generated from a sequence of Bernoulli map and Pseudo random binary generator is offered. The proposed system is compared with the speech scrambler using the FFT method. To test the efficiency of the proposed system various analysis tests are done. According to the survey comparison from proposed algorithm and previous technique shows that the suggested algorithm is more effective in terms of intelligibility and quality. The algorithm employed is too flexible in the sense that they can be utilized for several applications. The results obtained verify that the scrambled speech obtained is less prone to various cryptanalytic attacks.

References:

[1] Rohith S, K N Hari Bhat, A Nandini Sharma, *Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift Register*, International conference on advances in electronics, computers and communication, 2014

[2] Mina Mishra1 and V. H. Mankar2, Review on Chaotic Sequences Based Cryptography and Cryptanalysis, *International Journal of Electronics Engineering*, 3 (2), 2011, pp. 189– 194

[3] Eng. Sattar B. Sadkhan, N. H. Kaghed, *Design and Evaluation of Transform – Based Speech Scramblers using different Wavelet Transformations*, Fifth International Symposium. (CSNDSP), Communication Systems, Networks and Digital Signal Processing. Volume: fith – 2006

[4] D. C. Tseng, J. H. Chiu "An OFDM Speech Scrambler without Residual Intelligibility"TENCON 2007-2007IEEE Region10conferenceDOI:10.1109/TENCON.2007.4428903, Publication Year:2007, Pages:1-4

[5] 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

[6] 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

[7] 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.

[8] Tiago H. Falk1 andWai-Yip Chan2, 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.

[9] 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.