International Journal of Networks and Communications 2016, 6(3): 49-56
DOI: 10.5923/j.ijnc.20160603.02

An Efficient Secured Turbo Codes for Long Term Evolution System Enhancement

M. E. Abd El-Hameed[1], Mohsen A. M. El-Bendary[2], I. O. Bekhiet[3], H. M. Abd El-Kader[3]

[1]Worker University, Egypt
[2]Department of Communication Technology, Faculty of Industrial Education, Helwan University, Egypt
[3]Department of Electonics and Communication, Faculty of Engineering, Banha University, Egypt

Abstract In this paper an efficient secured interleaver is utilized in Turbo codes for Long Term Evolution (LTE) system. The engine of the presented technique is the Baker formula; it works based on secret key. The proposed technique system improves the Bit Error Rate (BER) and the throughput as well as the security also. This scheme depends on chaotic Baker map encryption. A comparison study between the proposed chaotic interleaving scheme and the traditional block and convolutional interleaving schemes for LTE system transmission over an Additive White Gaussian Noise (AWGN) channel is presented. The simulation results show the superiority of the proposed scheme over the traditional schemes. It reveals also, the turbo codes perform better with the proposed technique compared to the internal block interleaver used in LTE system. The data ordering in the proposed scenario based on the determined key length, this key controls the power of data randomizing. It can be used as a secret key also, to enhance the LTE security, packet-by-packet protection.

Keywords LTE, Turbo codes, Interleaver, Baker map, Packet protection

1. Introduction

The company Long Term Evolution [1] has long been seen as the first advancement towards stronger, faster and more efficient 4G data networks. LTE has been developed to meet the requirements of this era and to realize the aim of achieving global broadband mobile communications. The objectives of this evolved system includes higher radio access data rates, improved system capacity, coverage, flexible bandwidth operations, improved spectral efficiency, low latency, reduced operating costs and seamless integration with the Internet and existing mobile communication systems [2]. The technology under LTE can currently reach downlink peak rates of 100Mbps and uplink speeds of 50Mbit/s. The LTE technology is also a scalable bandwidth technology for carriers operating anywhere from 20 MHz to 1.4 MHz. Long Term Evolution offers some excellent advantages over current 3G systems including higher throughput, plug and play compatibility, Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD), low latency and lower operating expenditures. It also offers legacy modes to support devices operating on General Packet Radio Service (GPRS) systems, while supporting seamless pass- through of technologies operating on other older cellular towers. The technologies put forth by LTE will not only be implemented over time, they are designed to be scalable. This scalability means can slowly introduce LTE technologies over time.

2. LTE Physical Layer

In the base station and one in the mobile station with a channel bandwidth is 20 MHz. One key feature of LTE systems is the support of a scalable channel bandwidth that ranges from 1.4 MHz up to 20 MHz, which makes its implementation more feasible to the service providers. As we see in Fig. 1 the LTE block diagram consist of:

A. *CRC*

A CRC (cyclic redundancy check) is used for error detection in transport blocks. The entire transport block is used to calculate the CRC parity bits. The transport block is divided by a cyclic generator polynomial to generate 24 parity bits. These parity bits are then appended to the end of transport block. The polynomial is as follows:

$$\begin{aligned} G(x) = {} & x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} \\ & + x^{7} + x^{6} + x^{5} + {}^{4} + x^{3} + x + 1 \end{aligned} \tag{1}$$

Segmentation and 2nd CRC: If the input block size is greater than 6144 bits, it is split in to smaller blocks. Again CRC is performed and redundant parity bits are appended to each resulting smaller block. Also, filler bits are added so the code block sizes match a set of valid block sizes input to turbo code.

* Corresponding author:

Published online at http://journal.sapub.org/ijnc

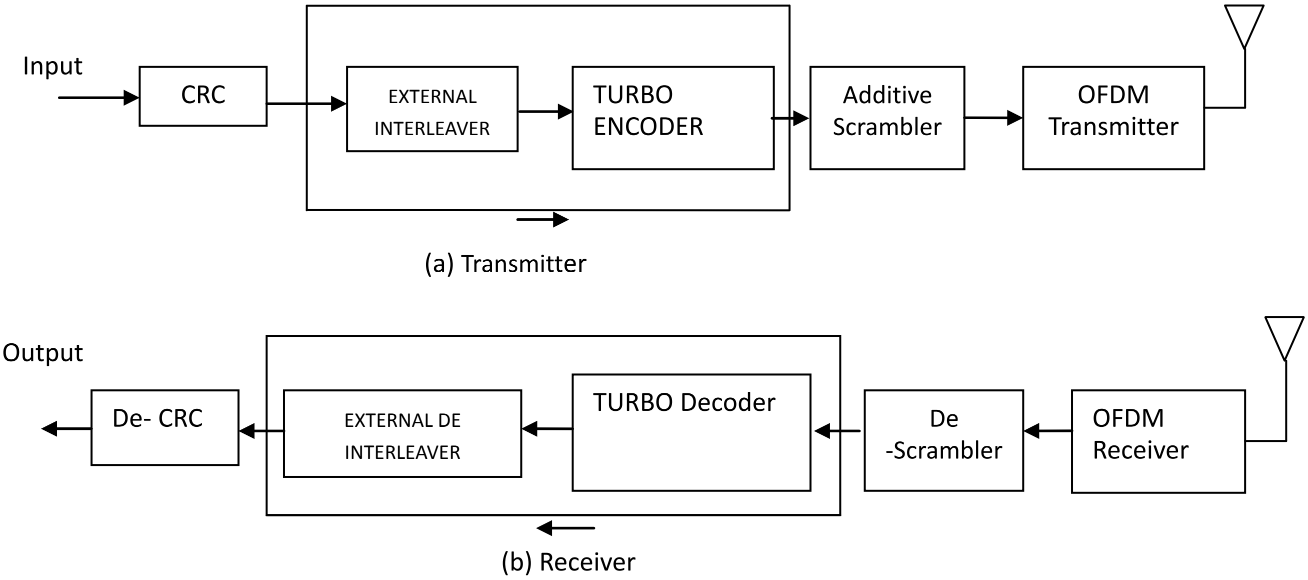


Figure 1. Block Diagram of LTE System

B. *Turbo coding and decoding*

Channel coding is used in most digital communication and especially in mobile communication to improve the error correcting capability. The LTE standards have adopted turbo coding. The scheme of the turbo encoder is a parallel-concatenated convolutional code with two 8-state convolutional encoders and one internal turbo code interleaver and a bit reordering block to reorder the coded bits. The performance of the turbo encoder depends critically on the interleaver structure [3], where the turbo coding interleaver vector (X) in LTE is set as follows:

$$xi = (f_1.i + f_2.i^2\ ) \bmod K \tag{2}$$

where f_2 and f_2 are chosen from the LTE specification depending on the frame size k.

C. *Scrambler*

Scrambling produces a block of scrambled bits from the input bits according to the relation given by the equation:

$$B^{\wedge} = b + c \bmod 2 \tag{3}$$

The B ^ symbol denotes the scrambled bits, b denotes the input bits, c denotes the scrambling sequence.

D. *OFDM System Block*

As we see in Fig. 2 Orthogonal Frequency-Division Multiplexing (OFDM) [4] is a multicarrier transmission technique that is used as the LTE downlink transmission scheme. In OFDM, the wide band frequency carrier is divided into narrow band subcarriers orthogonal to each other as in Fig. 3. Basically splits a high-rate data stream into a set of low-rate sub-streams that are transmitted simultaneously over a number of sub-carriers. Thereby, the bandwidth of the sub-carriers become small compared with the coherence channel bandwidth as in Fig.4.

This orthogonality in combination with an appropriate choice of subcarrier spacing (Δf) and the Cyclic Prefix (CP) length makes the OFDM system a robust transmission technique for frequency selective channels. The wide band frequency selective channel is converted into a group of narrow band flat fading channels at each subcarrier. Each subcarrier is modulated using one of Binary Phase-Shift Keying (BPSK). The Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM) schemes suggested by the LTE standards [6]. The OFDM modulator at the transmitter side is implemented using an N-point Inverse Fast Fourier Transform (IFFT) operation, where N denotes the total number of subcarriers. Using an IFFT reduces the implementation complexity significantly compared to using a bank of modulators for each sub-carrier. Each OFDM symbol in an LTE transmission frame consists of N subcarriers in the frequency domain with a frequency spacing Δf between each consecutive subcarrier. The choice of the proper Δf depends on the frequency selectivity of the channel and the maximum rate of channel variation, and the choice of the number of subcarriers depends on the assumed overall transmission bandwidth [7]. Not maintaining cyclic convolution for the OFDM subcarriers may lead to a loss of the subcarriers' orthogonality, which results in interference between adjacent subcarriers. To avoid that situation, an appropriate CP length is used. CP samples are chosen from the last part of the OFDM symbol, where a number of samples are copied and inserted at the beginning of the OFDM symbol. In LTE-OFDM based systems, the CP has two types: normal and long. The CP's length varies depending on the channel bandwidth used and the number of OFDM symbols. At the receiver side, the OFDM demodulator is implemented using an N-point Fast Fourier Transform (FFT) operation to convert the signal back to the frequency domain after removing the CP.

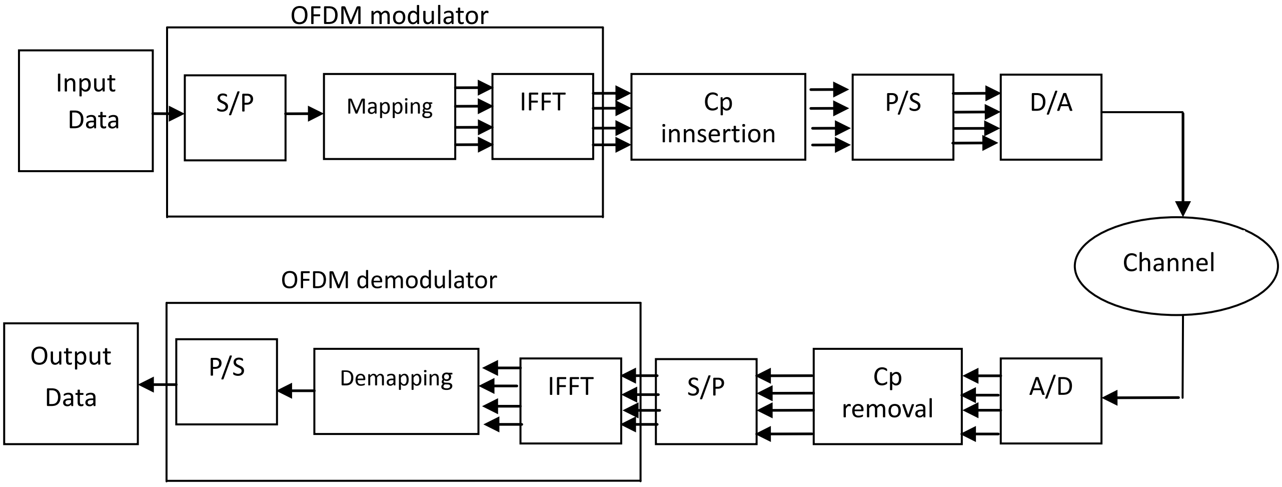


Figure 2. OFDM Transmitter and Receiver

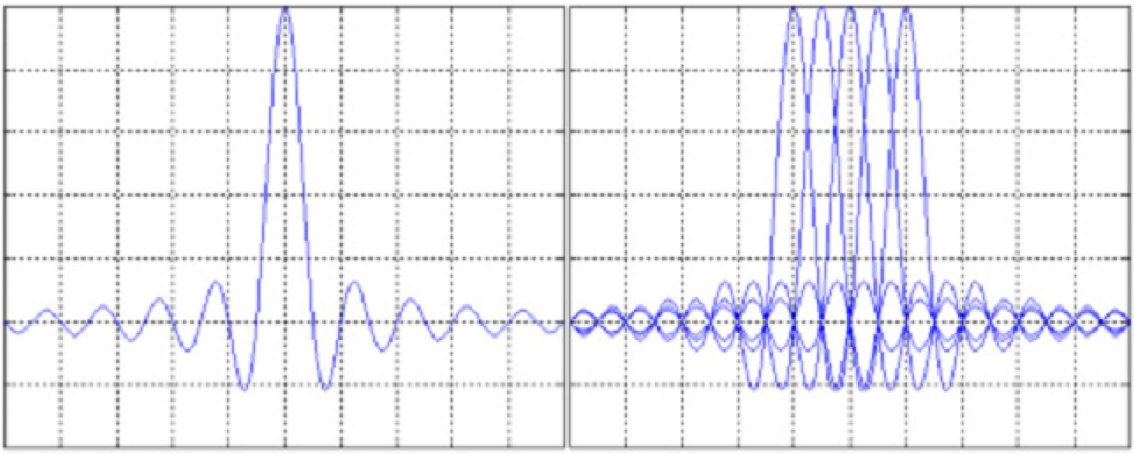
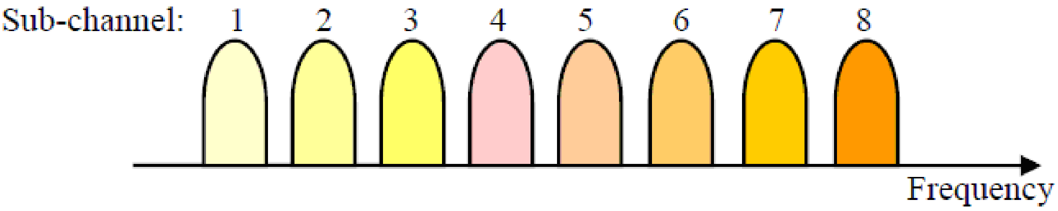
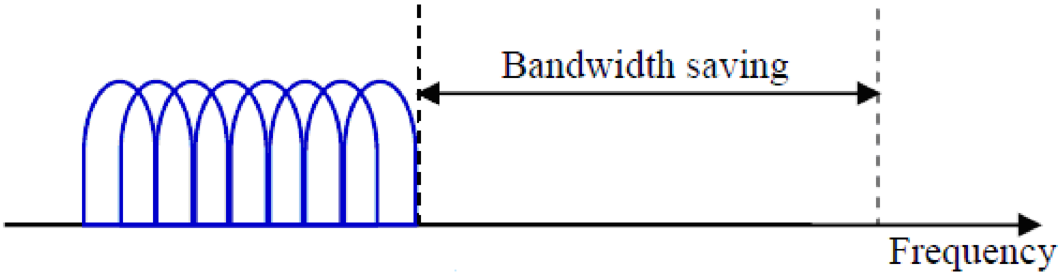


Figure 3. Spectra of (a) an OFDM sub-channel and (b) and OFDM signal



(a) Conventional multicarrier technique



(b) Orthogonal multicarrier modulation technique.

Figure 4. Representation of OFDM signal [5]

3. Turbo Coding in LTE

Turbo codes were first introduced by Berrou, Glavieux and Thitimajshima in 1993 and have Performances within a few tenth of a dB from the Shannon limit. The Turbo encoder in LTE [9] is a code Parallel Concatenated Systematic Convolutional (PCCC) with two 8-state constituent encoders the same as in Universal Mobile Telecommunications Service (UMTS) and one Turbo code contentions free internal interleaver (different from UMTS). The encoders are based on RSC (Recursive Systematic Convolution) codes and their generator polynomial is given by G=[1, g_0/g_1], where g_0=[1011] (Feedback) and g_1=[1101] (feed forward).

The structure of the Turbo encoder used in LTE is shown in Fig.5, the output of the LTE Turbo encoder consists of three parts, a systematic bit and two parity bits. The systematic bit (X_k) is the untouched input bit. The first parity bit (Z_k) is the output of the first convolutional encoder with the original input (C_k) input and the second parity bit ($Z0_k$) is the output of the second convolutional encoder after interleaving (by the Turbo code internal interleaver) of the input bit ($C0_k$) as its input For trellis termination the tail-bits $X0_k$ are inserted [8] [9].

A. *Interleaver role in turbo code*

Interleaver size and structure considerably affect turbo code error performance [10]. Turbo codes consist of a parallel concatenation of two Recursive Systematic Convolutional (RSC) coders in conjunction with an interleaver and associated decoder as shown in Fig.4. Interleavers in Turbo code can be categorized as traditional and random types. Traditional interleavers consist mainly of a block interleaver and a convolutional interleaver [1]. Currently, the random interleaver attract much attention since it can contribute not only to correct abrupt errors occurred in signal transmission but also to enhance the randomness of code sequences resulting in lowering the BER and frame error rate (FER) of the communication system. However, it’s difficult in practice to realize the pure randomness in interleaver’s design based on current techniques. As regard to the implementation of the Turbo codes, there are two main obstacles including algorithm complexity and system delay for the Turbo codes being employed into digital communication system in the near future. The main contribution for performance on Turbo codes in system is interleaving and decoding.

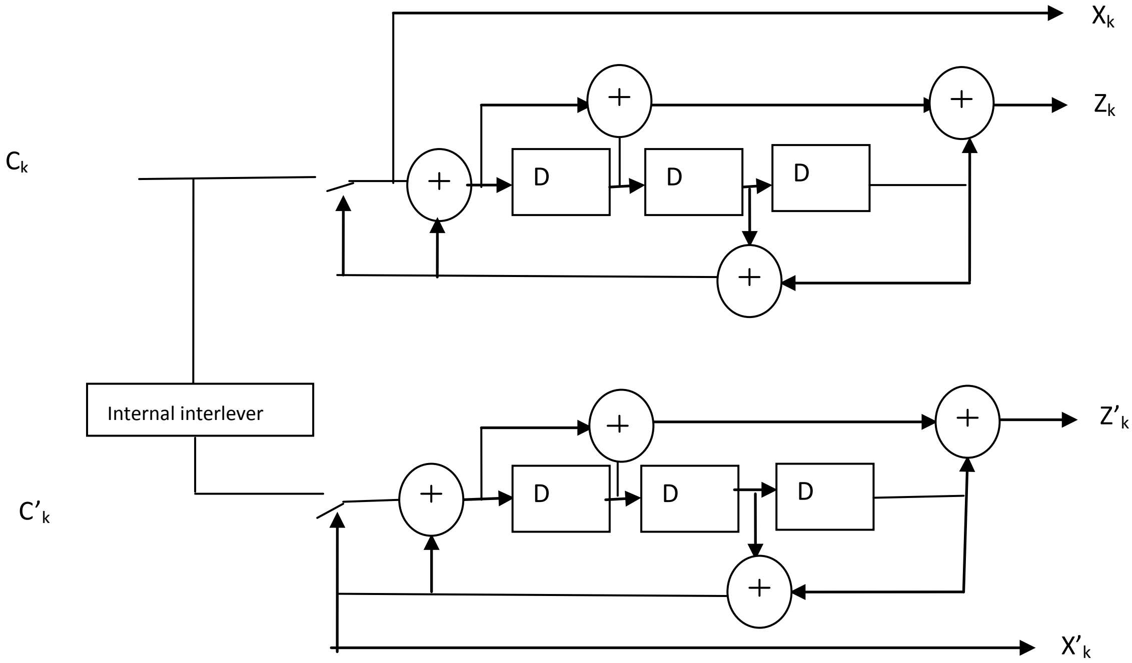


Figure 5. Structure of the LTE Turbo Encoder

4. Proposed Modifications

We study the feasibility of data interleaving prior to transmission over LTE system. The paper presents a new chaotic interleaver and compares to the traditional block and convolutional interleavers.

A. *Block Interleaver Scheme*

The block interleaving is used with turbo decoder in LTE system, the data is rearranged into a matrix in a row-by-row manner, and then read from the matrix in a column-by-column manner.

B. *Convolutional Interleaver Scheme*

A convolutional interleaver [4] [11] consists of N rows of shift registers, with different delay in each row. In general, each successive row has a delay which is J symbols duration higher than the previous row as shown in Fig.6. The code word symbol from the encoder is fed into the array of shift registers, one code symbol to each row. With each new code word symbol the commutator switches to a new register and the new code symbol is shifted out to the channel. The i-th (1 ≤ i ≤ N-1) shift register has a length of (i-1)J stages where J = M/N and the last row has M-1 numbers of delay elements.

C. *Chaotic Interleaver Scheme*

As mentioned in the previous subsection, the block interleaver is not efficient with 2-D error bursts. As a result, there is a need for an advanced interleaver for this task. As we see in Fig.7 the 2-D chaotic Baker map [12] [13] in its discretized version is a good candidate for this purpose. After rearrangement of bits in to a 2-Dformat, the chaotic Baker map is used to randomize the bits. The discretized Baker map is an efficient tool to randomize the items in a square matrix. Let $B(n_1, . . . , n_k)$, denote the discretized map, where the vector, $[n_1, . . . n_k]$, represents the secret key, S_{key}. Defining N as the number of data items in one row, the secret key is chosen such that each integer n_i divides N, and $n_1+. . . ,+n_k$ = N. Let $N_i = n_1+. . . ,+n_{i-1}$. The data item at the indices (r, s), is moved to the indices:

$$B(r,s) = [\frac{N}{n_i}(r - N_i) + s \bmod(\frac{N}{n_i}), \\ \frac{n_i}{N}(s - s \bmod(\frac{N}{n_i})) + N_i] \tag{4}$$

Where $N_i \le r \prec N_i + n_i, 0 \le s \prec N, \textit{and } N_i = 0.$

In steps, the chaotic permutation is performed as follows:

1. An N×N square matrix is divided into N rectangles of width ni and number of elements N.
2. The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from left to right beginning with upper rectangles then lower ones.
3. Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

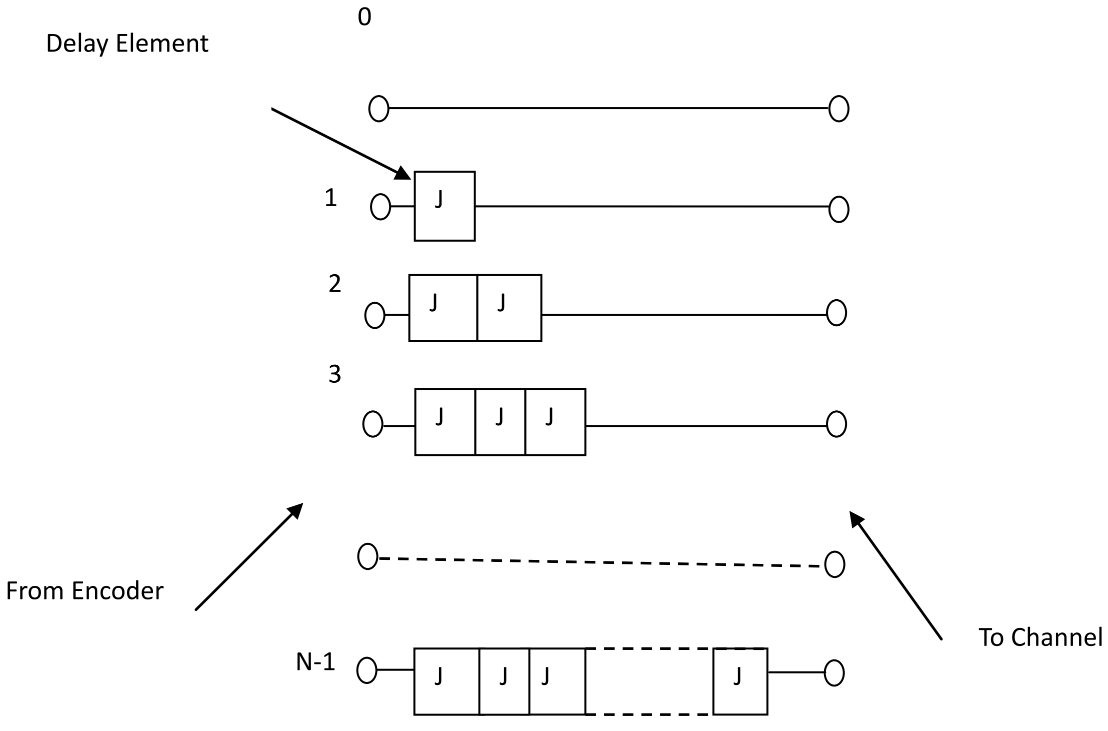
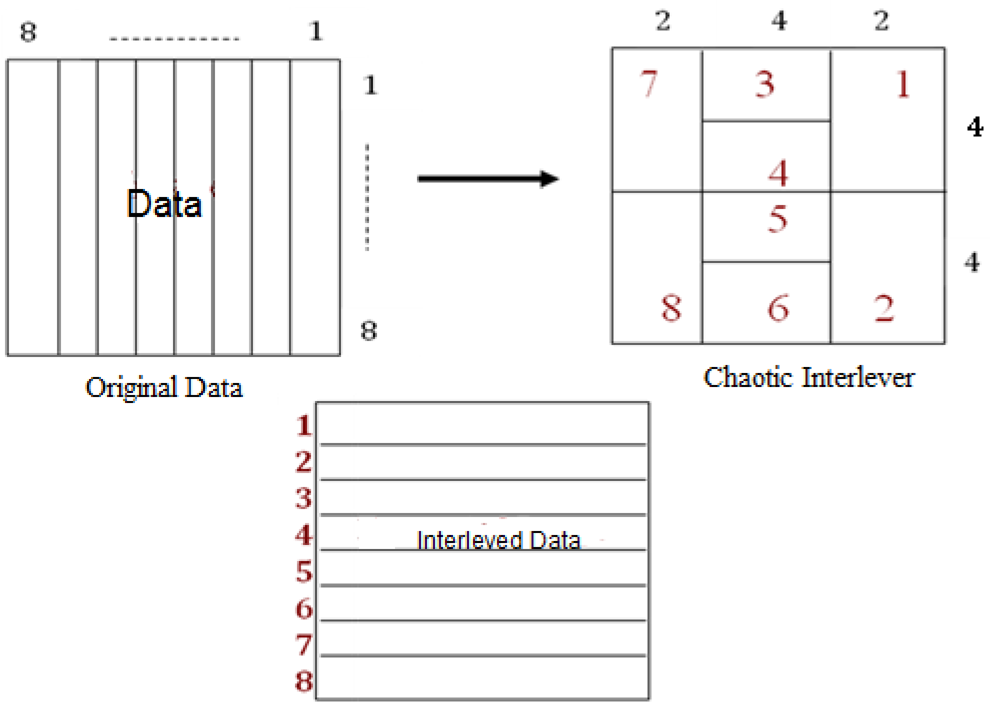


Figure 6. Convolutional Interleaver



B_{1}	B_{2}	B_{3}	B_{4}	B_{5}	B_{6}	B_{7}	B_{8}
B_{9}	B_{10}	**B_{11}**	B_{12}	B_{13}	B_{14}	B_{15}	B_{16}
B_{17}	B_{18}	B_{19}	B_{20}	B_{21}	B_{22}	B_{23}	B_{24}
B_{25}	B_{26}	**B_{27}**	B_{28}	B_{29}	B_{30}	**B_{31}**	B_{32}
B_{33}	B_{34}	B_{35}	B_{36}	B_{37}	B_{38}	B_{39}	B_{40}
B_{41}	B_{42}	**B_{43}**	B_{44}	B_{45}	B_{46}	B_{47}	B_{48}
B_{49}	B_{50}	B_{51}	B_{52}	B_{53}	B_{54}	B_{55}	B_{56}
B_{57}	B_{58}	**B_{59}**	B_{60}	B_{61}	B_{62}	**B_{63}**	B_{64}

Figure 7. Mechanism operation of the proposed interleaver with 8 × 8 matrix data size

Fig. 7 shows an example for chaotic interleaving of an 8 × 8 square matrix (i.e., N = 8). The secret key, $S_{key} = [n_1, n_2, n_3] = [2, 4, 2]$. Note that, the chaotic inter-leaving mechanism has a better treatment to both 1-D and2-D error bursts than the block interleaving mechanism. Errors are better distributed to bits after de-interleaving in the proposed chaotic interleaving scheme. This S_{key} controls the matrix segmentation and the interleaved data arranging. This key can be changeable and long to enhance the security. So, the Turbo code performance will be developed with security bonus [14].

5. Simulation Results

After the Baker map chaotic interleaving implemented by the step 1 to step 3 and as can be seen from the algorithm steps, it's easy to design the interleaver in practice. And the overall performance for Turbo codes will be enhanced significantly Another advantage of the proposed interleaver is that during the chaotic mapping only a few parameters are needed being transferred from transmitter to receiver, thus not only we can save channel volume for transmitting more source data on the one hand, but also decrease the probability of data error occurred in the signal transmission on the another.

To verify the effectiveness of the proposed interleaver, BER performance compared with other interleavers from the simulation results are given as curves shown in Figs. 8 and 9 respectively. As can be clearly seen from the curves shown in the figure, with reducing the computation complexity the proposed interleaver exhibits a high BER performance than other random interleavers. From the Figs 8 and 9, we found that the throughput also improved from the other interleavers.

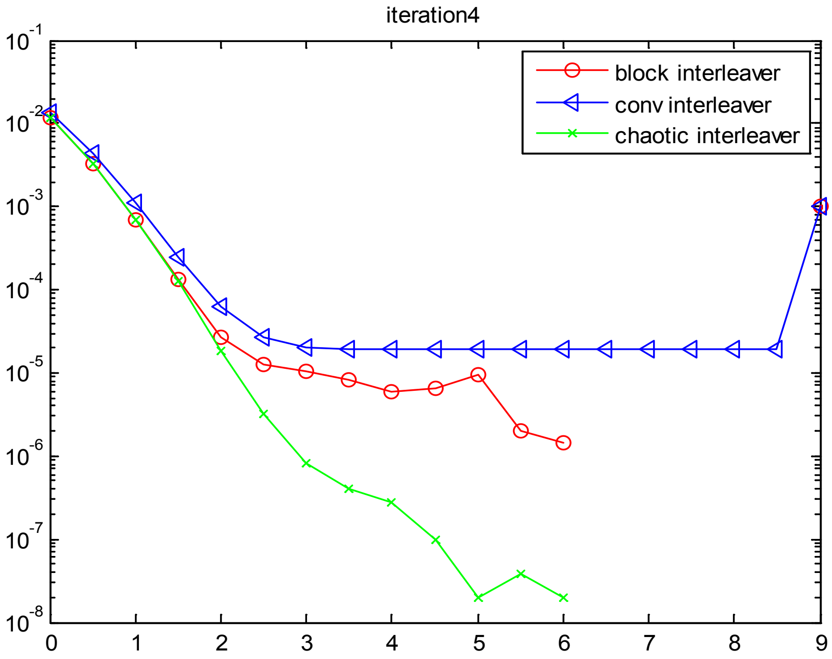


Figure 8. BER versus SNR for LTE system with chaotic interleaver on AWGN Channel techniques

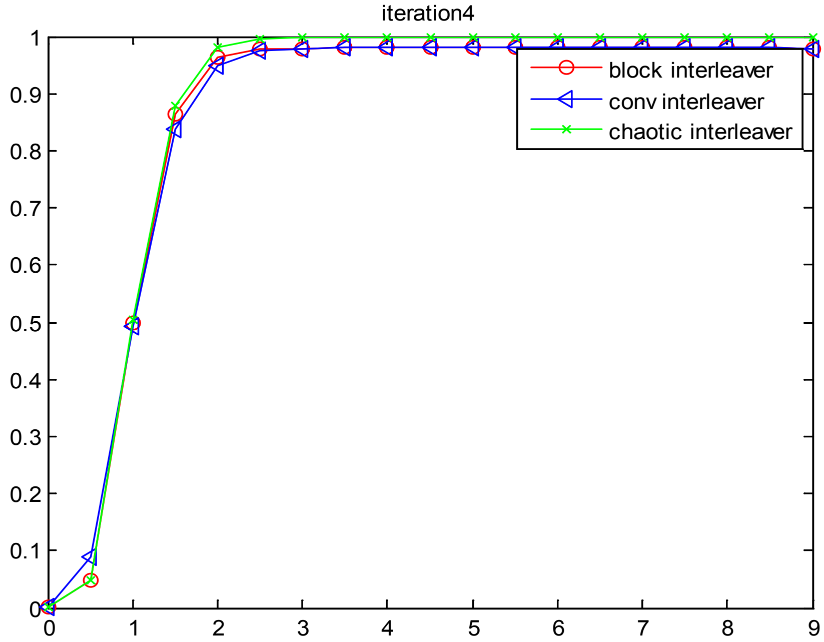


Figure 9. Throughput of LTE System with Chaotic Interleaver on AWGN Channel Techniques

6. Conclusions

This paper presented a simple and efficient novel chaotic interleaver for the transmission of data over LTE system. A comparison study between the proposed interleaver and the conventional interleavers has been presented. The computer simulation results have revealed the effectiveness of the proposed interleaver at medium and high SNR values. Also, the proposed interleaver enhanced the security level as it is based on chaotic map encryption.

REFERENCES

[1] A Chaotic Interleaver Used in Turbo Codes Hongyu Zhang Lin Wang Qingsheng Yuan, Hongxia Wang Juebang Yu (School of Electronic Engineering UESTC, Chengdu, 610054, China. Diksha

[2] Duggal and Jyoteesh Malhotra "Performance analysis of Long Term Evolution Physical Channels" International Journal of Future Generation Communication and Networking Vol. 9, No. 3 (2016), pp. 269-278.

[3] W. C. Jakes, Microwave Mobile Communication, Wiley, New York, 1974

[4] J. Yuan, B. Vucetic, W. Feng, "Combined turbo codes and interleaver design" IEEE Trans. Comm., vol.47, No.4, pp.484-487, Apr. 1999

[5] H. Schulze and C. Luders, "Theory and Application of OFDM and CDMA Wideband Wireless communication," John Wiley, 2005

[6] Manjunatha K N, Kiran B, Prasanna Kumar. C/''Design and ASIC Implementation of a 3GPP LTE –Advance Turbo Encoder and Turbo Decoder" International Journal of Engineering Research and Applications (IJERA) ISSN:2248-9622 www.ijera.com Vol.2, Issue 4, July-August 2012, pp.006-010.

[7] R. V. Nee and R. Prasad, OFDM for Wireless Multimedia Communications, Artech House, 2000. Terrestrial Radio Access (EUTRA)" Multiplexing and Channel Coding", Jan. 2012.

[8] Emilia Käsper, "Turbo Codes",www.tkk.fi/~pat/coding/essays/turbo.pdf, cited 15 June, 2012.

[9] Patel Sneha Bhanubhai, Mary Grace Shajan, Upena D. Dalal "Performance of Turbo Encoder and Turbo Decoder for LTE"IJEIT Vol2, Issue6, Oct 2012

[10] R.V. BANDGAR, S.N. WAR, A.K, S. SHETH, "Performance Analysis of Turbo Coded OFDM Over Uncoded & Convolutional Coded OFDM", International Journal of Industrial Electronics and Electrical Engineering, Volume-3, July-2015

[11] Prabhavati D. Bahirgond, Shantanu k. Dixit "Ber Analysis of turbo code interleaver" International Journal of Computer Applications (0975-8887)Vol.126-No.14,September2015

[12] V. Murugan, D. Sivakumar, "Non-Coherent Bit Interleaving Coded Scheme for PAPR Reduction of OFDM Signal", 4th National Conference on Advanced Computing, Applications & Technologies, May 2014

[13] An Efficient Chaotic Interleaverfor Image Transmissionover IEEE 802.15.4 Zigbee Network Mohsen A. M. M. El-Bendarya, Atef Abou El-Azmb, Nawal El-Fishawyb, Farid S. M. Al-Hosareyb, Mostafa A. R. Eltokhya, Fathi E. Abd El-Samieb, and H. B. Kazemianc

[14] M.A.M ElBendary "Mobility Effects Combacting through Efficient Low Complexity Technique" CiiT, Vol5, No12, December 2013. 3GPP TS 36.212 v10.4.0: "Evolved Universal"

[15] John G. Proakis, Digital Communications, Mc-Graw-Hill: International Editions, 4th ed.

[16] Ausgewählte Kapitel der Nachrichtentechnik, WS 2009/2010LTE: Der Mobilfunk der Zukunft Channel Coding and Link Adaptation Shahram Zarei 16. December 2009