DDT-based Chaotic Interleaver Aided Cooperative OFDM System

Shahid Manzoor[1], Noor Shamsiah Othman[2], Muhammad Asif Khan[3] and Asim Ali[4]
[1,2]Department of Electrical and Electronics Engineering, Universiti Tenaga Nasional, Malaysia
[1]Department of Electrical and Electronic Engineering, UCSI University, Kuala Lumpur, Malaysia
[3]University of Engineering & Technology, Taxila, Pakistan, [4]University of Wah, Wah Cantt, Pakistan
[1]shahid@ucsiuniversity.edu.my, [2]Shamsiah@uniten.edu.my, [3]massif.khan@uettaxila.edu.my, [4]asim.ali@uow.edu.pk

***Abstract*—Typically, interleaver is used to recover information signal from outage where errors in burst form is transformed into single errors. The best interleaver should have the optimal properties of spread and dispersion. Therefore, this paper reports a method to design highly dispersive and systematic interleaver. The interleaver is designed using an incremental approach, which uses a Chaotic Logistic Map (CLM) to generate interleaver positions and utilizes the counter-based difference distribution table (DDT) that has been used in cryptanalysis, in order to achieve highly random and disperse interleaver positions by avoiding bad positions that produce repetitive pairs in the output. The proposed interleaver is implemented in single input single out (SISO) and cooperative Orthogonal frequency division multiplexing (OFDM) system. The performance of the proposed interleaver is evaluated in terms of spread, dispersion, bit error rate (BER) as a function of the burst error length and BER versus channel signal-to-noise-ratio (SNR). The performance of the proposed interleaver is compared with chaotic interleaver, block interleaver and with Matlab® random interlaever. The results show that the proposed interleaver outperforms all the interleavers considered in the simulations and there is 1 dB to 3.5 dB improvement in different scenarios of length of burst errors in terms of BER for proposed SISO OFDM systems. More specifically, the employment of the proposed interleaver in the cooperative OFDM system gives improvement of about 2.75 dB to 3.5 dB at BER = 10^{-2}, as compared to the non cooperative OFDM systems when having the burst error length of 5 bits, 10 bits and 15 bits.**

***Index Terms*—Chaotic Interleaver, Differential Distribution Table, OFDM, Cooperative Communication.**

I. Introduction

Wireless communication offers enormous advantages in terms of speediness, cost and mobility. Wireless LAN (WLAN) is not tangibly connected as a wired LAN and operates through the air. As a result, the reliability of the data is expected to be questionable due to the error-prone nature of the wireless channel which is caused by fading and multipath phenomena [1], [2]. In wireless channels, errors related to the demodulator have a tendency to occur in bursts which corresponds to deep channel fading [3], [4]. The use of interleaving greatly increases the capability of error protection codes to correct burst errors [5]–[10].

In orthogonal-frequency-division-multiplexing (OFDM) communication system, interleaver is invoked after channel coding to enhance the performance of channel coding and to enable it to use non-complex error correction codes for burst noise caused by intense fades. OFDM systems are observed to have have high correlation among their data frames, which results in high peak to average power ratio (PAPR). Thus, in order to mitigate this intense correlating problem, interleavers are being used in OFDM systems [10], [11].

There has been an increase interest on the design of interleaver that improves the properties of interleaver, namely, spread and dispersion. In [12], the author proposed an innovative chaotic interleaver based on baker map to randomize the data and decreased the effect of PAPR in OFDM. A unique scrambling of OFDM constellation symbols based on chaos is proposed in [5], [6], [13]. Chaos is also favorable because of its high nonlinearity which is the key to design interleaver [14].

Cooperative communication is a well-known approach to improve the system spectrum efficiency by exploiting spatial diversity. Cooperative diversity technique in OFDM system was proposed in [15], where a mobile station collaborates with other users jointly to emulate multiple-input-multiple-output (MIMO) communication system [16]. Whilst, in [17], [18], the authors proposed signal-to-noise-ratio (SNR) estimators that were invoked in an OFDM-based cooperative system, where it was observed that the OFDM-based cooperative system outperformed the single-input-single-output (SISO) system in terms of SNR and bit error rate (BER).

Difference distribution table (DDT) is a tool that is being used in differential cryptanalysis of block cipher. The differential cryptanalysis uses DDT to seek high probability of occurrences of output S-box differential pairs whose corresponding input pairs have difference [19]. DDT is used to measure output differentials and improve differential approximation probability in order to improve dispersion of interleaver [19], [20]. In [21] the author used DDT to construct S-Box for different cryptanalysis and to design a block cipher the main focus is to be able to start from desired DDT which assures high resistance against different kinds of differential cryptanalysis.

In this paper, DDT-based chaotic interleaver in cooperative OFDM system is presented which uses a chaotic map to generate interleaver positions and dynamically evaluates generated positions using the proposed criteria, namely in terms of spread and dispersion. Furthermore, the performance of the proposed interleaver is evaluated when it is employed after channel coding in an OFDM-based cooperative system.

978-1-7281-4737-6/19/$31.00 ©2019 IEEE

The rest of the paper is structured as follows. Section II presents the performance parameters used for evaluating the proposed interleaver, as well as, the proposed system that invokes the proposed interleaver. In Section III, the system overview and the algorithm of the proposed interleaver are presented. Section IV discusses the performance of the proposed interleaver, as well as the performance of the OFDM-based cooperative system that invokes the proposed interleaver, while our conclusions are offered in Section V.

II. Performance Parameters

The performance of the proposed interleaver is evaluated in terms of spread and dispersion. While, the performance of the OFDM-based cooperative system that invoked the proposed interleaver is evaluated in terms of BER versus burst error length, as well, as BER versus channel SNR. A good interleave must have the optimal properties of spread and dispersion [3]–[6], [14], [19].

A. Spread

Spread property is being used to handle the difference of the elements after permutation which initially are very closed to each other [5], [19]. Maximum value of spread, S is such that:

$$|p-q| < S \Rightarrow |\pi(p)-\pi(q)| > S, for 1 \leq S \leq N \quad (1)$$

Where $\pi()$ is a function that describes the mapping of an interleaver or permutation process of an interleaver, S is the spread factor and N is the total number of input symbols. In the above condition the first value shows the difference between the input symbols before interleaving and the second value shows the difference of the interleaved output symbols. Interleaver with large spread factor will spread the correlated bits far away from each other in the interleaved sequence.

B. Dispersion

The dispersion describes the randomness of the permutation of an interleaver [14], [19], which can be defined as:

$$D(\pi) = \{(q-p, \pi(q)-\pi(p)) | 0 \leq i < j < N\} \quad (2)$$

where N is the total number of input symbols, $D(\pi)$is dispersion pair, $(q-p)$ is the difference between the input symbols before interleaving and $\pi(q)-\pi(p)$ is the difference of the interleaved output symbols. The normalized dispersion is calculated as $(2|D(\pi)|)/(n(n-1))$. The dispersion of an interleaver is considered good if the normalized dispersion is near to 1 [4].

C. BER versus burst error length and BER versus SNR

Burst errors are converted to single errors by using an interleaver with robust spread and dispersion properties, which then can easily being corrected using error correcting codes. The proposed interleaver is evaluated and compared with Matlab® random interleaver [RANDINTL], chaotic interleaver [12] and block interleaver [10] when considering its performance in burst error environment for different values of channel SNR. BER is plotted against burst error length in order to analyze the performance of the proposed interleaver in converting burst errors into simple single errors, which are then corrected by single error correction code employed in the system. For a specific burst error length, the BER performance of the proposed interleaver is also evaluated as a function of channel SNR.

III. System and Proposed Interleaver Algorithm

A. System overview.

Figure 1 shows the proposed interleaver-aided SISO OFDM transceiver.

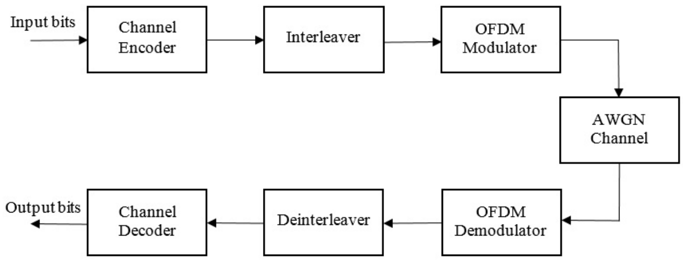

Fig. 1. Block diagram of the interleaver-aided SISO OFDM system.

At the SISO OFDM transmitter, the source bits are encoded using Hamming code (7,4), which are then interleaved using the proposed DDT-based chaotic interleaver prior to OFDM modulation. The Hamming code (7,4) has a minimum hamming distance of 3, thus, it has capability to correct a single error. The interleaved bit stream is then modulated using N sub-carriers OFDM, and transmitted over Additive White Gaussian Noise (AWGN) channel. At the receiver, the reverse process occurs. More specifically, the received OFDM signal will be demodulated, de-interleaved and channel decoded.

Figure 2 shows the Cooperative OFDM System, where the source node, S, relay node, R and destination node, D employ the proposed interleaver-aided SISO OFDM transceiver of Figure 1. In this work, the Decode-and-Forward (DAF) collaborative protocol is used between the source, relay and destination nodes. More specifically, the source node, S transmits the OFDM signal to the relay node, R and the destination node, D. At receiver of the relay node, R, the received OFDM signal is demodulated, de-interleaved and decoded, and then, re-encodes it and finally transmits it to the destination node, D. In this work, the signal transmission over AWGN channel between the nodes is assumed.

At the destination node, D, the received OFDM signal from the source node, S is combined with the OFDM signal from the relay node, R using Maximum Ratio Combiner (MRC) prior to the demodulation, de-interleaving and decoding process.

B. DDT-based Chaotic Interleaver Algorithm

The proposed interleaver adopts similar approach as the S-Box algorithm that was designed for multimedia encryption [19]. More specifically, the proposed interleaver exploits

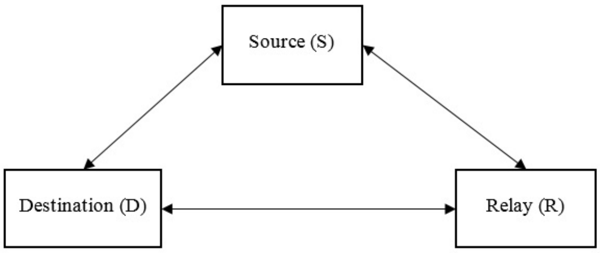

Fig. 2. Block diagram of the cooperative OFDM system.

TABLE I
SIMULATION PARAMETERS FOR OFDM MODULATION

Parameters	Value
IFFT Size	2 56
Sampling Frequency = F_s	20 MHz
Sub Carrier Spacing = $\Delta f = F_s/IFFT$	1×10^5
Symbol Time = $T_b = 1/\Delta f$	1×10^{-5}
Guard Interval Time = $T_g = G \times T_b$, where $G = 1/4$	2×10^{-6}
OFDM symbol Time = $T_s = T_b + T_g$	1.25×10^{-5}

Chaotic Logistic Map (CLM) to generate the interleaver positions and utilizes counter-based DDT to optimize the interleaver, in such that the value of the differential approximation probability (DP) is low.

The proposed interleaver aims for high level of randomness that invokes an incremental design approach with the aid of counter-based DDT. In other words, there should be distinct difference between positions in the interleaver, which is indicated by having the minimum occurrence frequency of output difference of 2.

DDT is generated using the interleaver's output difference, Δz for all possible interleaver's input differences, Δx. The main steps of the DDT-based chaotic interleaver are as follows:

1) At the initialization stage, the CLM is used to generate two initial interleaver positions, namely, z_1 and z_2, and these positions are placed in a position vector, P. Meanwhile, the initial value of variables are set, namely, the input difference $\Delta x = 1$, and $R = 2$, where R denotes the occurrence frequency of Δz. Then, the output difference between (z_1, z_2) is determined using $\Delta z = x_1 \bigoplus x_2$ and placed in DDT.
2) Then, the positions are generated incrementally, one by one. More specifically, the next interleaver position is generated using CLM, namely, z_3. Subsequently, DDT entries are generated by computing Δz for all possible $\Delta x = [2, 3, ..., 2^n]$, where n is the interleaver length.
3) If the criteria of having $R = 2$ is met then the position z_3 is added in position vector P.
4) If the criteria $R = 2$ is not met then, the position z_3 is ignored and a new interleaver position is generated using CLM, where the Step (2) is repeated and tested against the criteria of $R = 2$ until all the interleaver positions are generated.
5) If the interleaver positions cannot be improved further, the value of R is incremented by 2. Then, the remaining interleaver positions are generated using Step 2 and Step 3 and if necessary the value of R is incremented by 2.

IV. SIMULATION RESULTS

In this section we characterize the behaviour of the proposed interleaver in terms of spread and dispersion. We also evaluate the performance of the proposed interleaver-aided SISO OFDM scheme, as well as, the cooperative OFDM system using the BER as a function of the channel SNR and burst error length. The simulations and analysis of the simulation results are performed using Matlab®. In our simulation, the interleaver length $n = 256$ and OFDM symbol length $N = 256$ were employed. Table I shows the OFDM parameters used in the simulations.

A. Analysis of Spread

Figure 3, 4 and 5 show the histogram of the interleaver achieved spread when the value of spread, in Equation 1 are $S{<}2$, $S{<}3$ and $S{<}4$, respectively. More specifically, Figure 3 illustrates the interleaver achieved spreads as a function of the locations of the interleaver input elements, when the distance between the input elements before interleaving and after interleaving are one symbol apart. Meanwhile, Figure 4 and Figure 5 illustrates the achieved spread when the distance between the input elements before interleaving and after interleaving are two and three symbols apart.

The results show that the proposed interleaver achieved high spread, where the average achieved spread $> \sqrt{n/2}$, where $n = 256$ is the interleaver length.

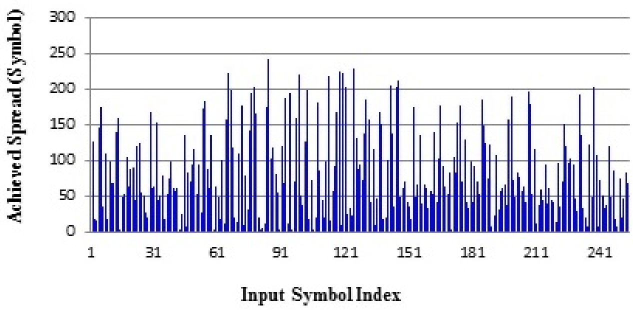

Fig. 3. Spread histogram of proposed interleaver with S $<$ 2.

B. Analysis of Dispersion

The randomness of an interleaver is described by dispersion parameter, where the maximum normalized dispersion value is 1. Thus, the proposed random interleavers in [4], [11] which have value of normalized dispersion approaching 0.8 are considered good. Whilst, the proposed algebraic interleavers in [5] have dispersion approximately 0.5. The dispersion is determined by using Equation 2 as presented in Section II-B. Our proposed interleaver has normalized dispersion of about 0.78, which indicates that the proposed interleaver permutes the input elements efficiently with high randomness.

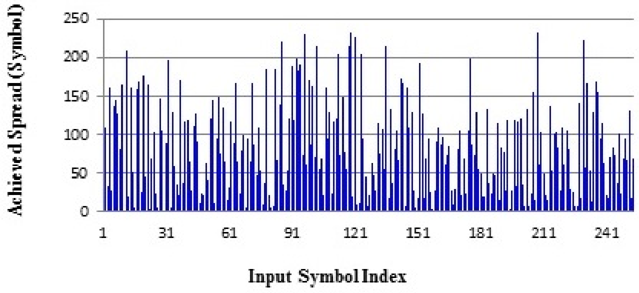

Fig. 4. Spread histogram of proposed interleaver with S < 3.

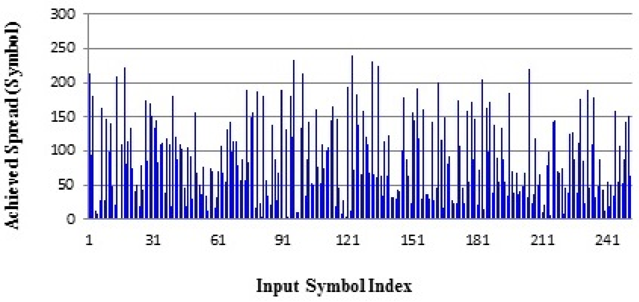

Fig. 5. Spread histogram of the proposed interleaver with S < 4.

C. Bit Error Rate (BER) as a Function of Burst Error Length

The proposed interleaver-aided SISO OFDM and the interleaver-aided cooperative OFDM system are evaluated in terms of BER versus burst error lengths for three different of channel SNR, namely, channel SNR of 5dB, 10 dB and 15 dB. The proposed interleaver is compared with conventional Matlab® random interleaver [RANDINTL], the proposed block interleaver in [10], and the proposed chaotic interleaver in [12] when each of these interleaver is invoked in the SISO OFDM system.

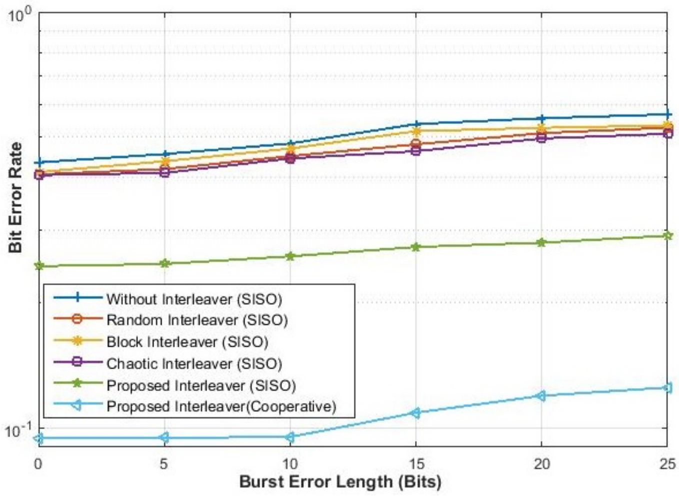

Fig. 6. BER versus burst error length when channel $SNR = 5dB$

Figure 6, 7 and 8 illustrates the BER performance against

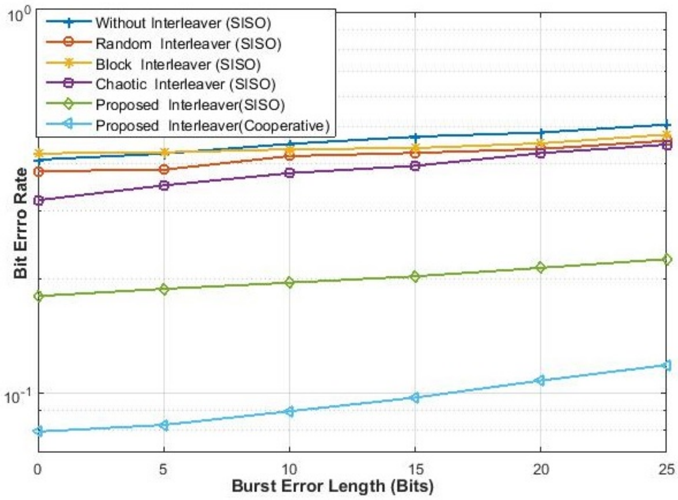

Fig. 7. BER versus burst error length when channel $SNR = 10dB$

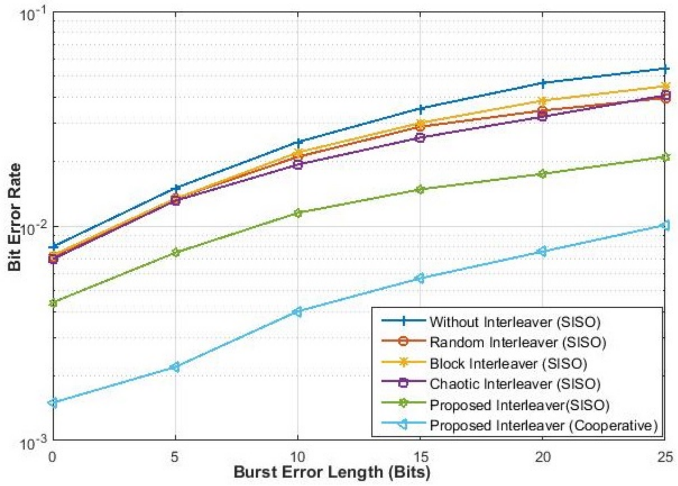

Fig. 8. BER versus burst error length when channel $SNR = 15dB$

burst error length of 5, 10, 15, 20 and 25 bits length, which are introduced manually and XORed with modulated data. The results show that the proposed interleaver-aided SISO and cooperative OFDM system outperform the other benchmarks scheme. More specifically, it is observed that as the channel SNR increased, the BER decreased. Therefore, it is evident that proposed interleaver inherent with near optimal dispersion can convert longer burst of errors into simple single errors that can easily recovered with single error correcting codes.

D. Bit Error Rate (BER) as a Function of Channel SNR

The performance of the proposed interleaver is also evaluated in terms of BER as a function of channel SNR when considering different burst error length of 5, 10 and 15 bits as shown in Figure 9, 10 and 11, respectively. It can be seen that the proposed interleaver outperforms all other interleavers. The proposed interleaver is also invoked in OFDM-based cooperative system and it can be seen that the proposed interleaver that is invoked in the OFDM-based cooperative system performs even better as compared to the proposed OFDM SISO that invoked the proposed interleaver. More specifically, in the case when the burst error length is 5 bits, the proposed interleaver-aided cooperative OFDM system outperforms the proposed non-cooperative OFDM system by about 3.5 dB, as shown in Figure 9. Furthermore, at BER = 10^{-2} the proposed interleaver outperforms the chaotic interleaver by about 1.9 dB, random interleaver by about 2.5 dB and block interleaver by about 3.2 dB in the SISO OFDM system when the burst error length is 5 bits, as shown in Figure 9.

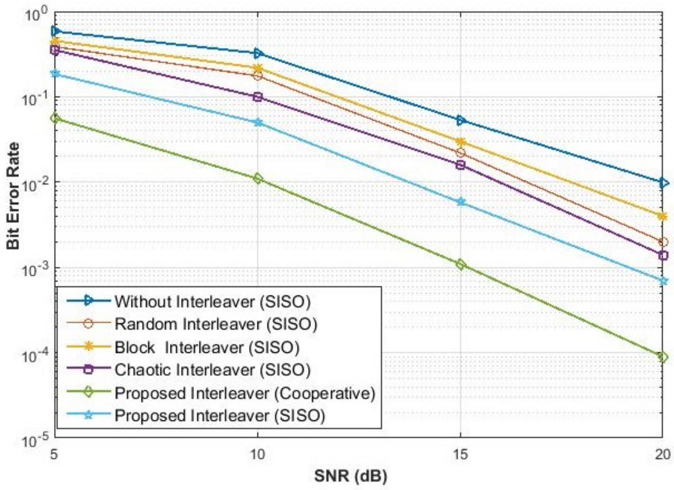

Fig. 9. BER versus channel SNR when burst error length = 5 bits

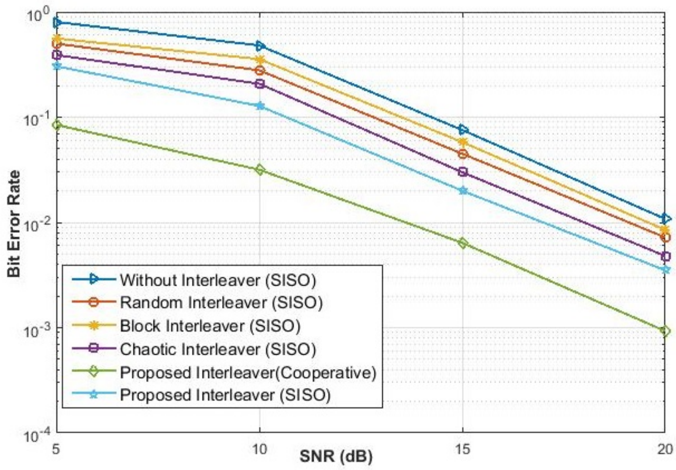

Fig. 10. BER versus channel SNR when burst error length = 10 bits

It can be seen from Figure 10 that the cooperative OFDM system that invokes the proposed interleaver outperforms the proposed non-cooperative OFDM system by about 2.75 dB at BER = 10^{-2}. Figure 10 compares the performance of the proposed interleaver that is employed in the SISO OFDM system and of its corresponding SISO OFDM system that invokes other interleavers when the burst length is 10 bits. More over, the employment of the proposed interleaver outperforms the chaotic interleaver by about 1.2 dB, Random interleaver by about 2.3 dB, block interlever by about 2.5 dB at BER = 10^{-2}, as shown in Figure 10.

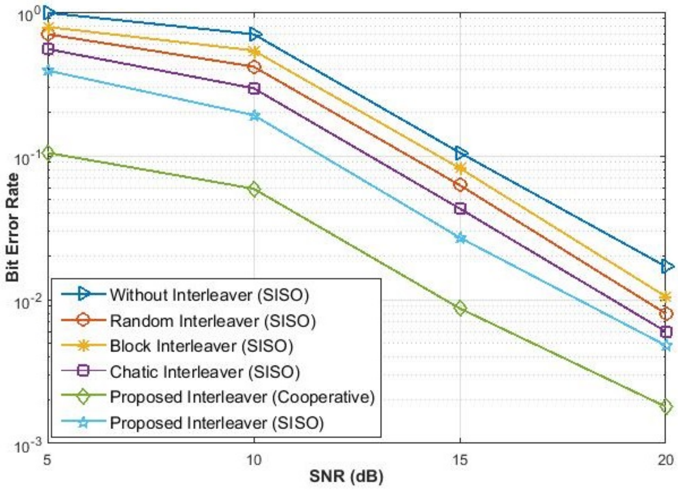

Fig. 11. BER versus channel SNR when burst error length = 15 bits

Similarly, in Figure 11, the proposed interleaver-aided cooperative OFDM system outperforms the proposed non-cooperative OFDM system by about 2.75 dB at BER = 10^{-2}. The proposed interleaver-aided non cooperative OFDM outperforms the chaotic interlever by about 1 dB, Random interleaver by about 2 dB, block interlever by about 2.5 dB at BER = 10^{-2}, when the burst error length is 15 bits, as observed in Figure 11.

V. Conclusions

In this paper, the DDT-based chaotic interleaver aided cooperative OFDM system is presented. It has been demonstrated that the proposed system achieved a significant BER performance improvement compared to that of the non cooperative OFDM system. The proposed interleaver achieved optimal values of spread, where the average achieved spread is greater than 11 and the normalized dispersion value of about 0.78. The performance of the proposed interleaver was also evaluated in terms of BER as a function of burst error length, as well as, BER as a function of channel SNR. The simulation results showed that the performance of the proposed interleaver provides a significant improvement when compared with other interleavers, namely, the chaotic interleaver, the random interleaver and the block interleaver. More specifically, the proposed interleaver is at least 1 dB better than the chaotic interleaver when the burst error length is 15 bits in the SISO OFDM system. Moreover, the employment of the proposed interleaver in the cooperative OFDM system gives improvement of about 2.75 dB to 3.5 dB at BER = 10^{-2}, as compared to the non cooperative OFDM systems when having the burst error length of 5 bits, 10 bits and 15 bits.

Acknowledgement

This research is supported by Universiti Tenaga Nasional Internal Grant 2018 (UNIIG 2018) under grant J510050800.

References

[1] E. Krouk and S. Semenov, *Modulation and Coding Techniques in Wireless Communications*. John Wiley & Sons, 2011.

[2] H. Yang and G.-P. Jiang, "High-Efficiency Differential-Chaos-Shift-Keying Scheme for Chaos-Based Noncoherent Communication," *IEEE Trans. Circuits and Systems—Part II: Express Briefs*, vol. 59, no. 5, pp. 312–316, May 2012.

[3] G. Forney, "Burst-Correcting Codes for the Classic Bursty Channel," *IEEE Transactions on Communication Technology*, vol. 19, no. 5, pp. 772–781, Oct 1971.

[4] C. Avenacio-Leon, "Analysis of the Dispersion and Spreading Properties of Interleavers for Turbo Codes," in *Computing Research Conference*, 2004.

[5] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "A Novel Seed Based Post Modulation Interleaver: Design and Analysis," in *International Conference on Intelligent and Advanced Systems*, 2010, pp. 1–6.

[6] ——, "Chaos Based Constellation Scrambling in OFDM Systems: Security & Interleaving Issues," in *International Symposium on Information Technology*, vol. 4, 2008, pp. 1–7.

[7] K. Xie, W. Wang, and J. Li, "On the Analysis and Design of Good Algebraic Interleavers," in *4th International Symposium on Turbo Codes & Related Topics; 6th International ITG-Conference on Source and Channel Coding*, 2006, pp. 1–6.

[8] F. J. Escribano and A. Tarable, "Interleaver Design for Parallel Concatenated Chaos-based Coded Modulations," *IEEE Communications Letters*, vol. 17, no. 5, pp. 834–837, 2013.

[9] M. A. Khan, V. Jeoti, and R. S. Manzoor, "Secure Interleaving-Physical Layer Security Enhancement of OFDM Based System," in *International Conference on e-Technologies and Networks for Development*, 2011, pp. 349–361.

[10] Y. Gagiev, A. Trushanin, R. Maslennikov, A. Lomayev, and A. Kostin, "Block Interleaver Design for the Single Carrier Modulation in IEEE 802.11 ay," in *2018 24th Asia-Pacific Conference on Communications (APCC)*, 2018, pp. 57–61.

[11] N. R. Raajan, B. Monisha, P. Vishnupriya, N. Rangarajan, G. N. Jayabhavani, and C. Nishanthini, "Chaotic Interleaving for Secure OFDM," *Research Journal of Information Technology*, vol. 5, no. 3, pp. 449–455, 2013.

[12] M. E. Abd Elhameed, M. A. M. El-Bendary, E. O. Begheet, and H. M. Abd Elkader, "An Efficient Chaotic Interleaving with Convolution Encoder and Decoder for Simplicity in LTE System," *International Journal of Networks and Communications*, vol. 8, no. 1, pp. 1–9, 2018.

[13] A. Nair and K. Kiasaleh, "Chaotic Circle Map Interleaver for OFDM," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, 2016, pp. 1–5.

[14] A. Shukla, A. Bansal, V. K. Deolia, and K. Veer, "MMSE Equalization Based Performance of Chaotic Interleaving Scheme for Iterative IDMA System," *International Journal of Sensors, Wireless Communications and Control*, vol. 9, pp. 1–10, Nov 2018.

[15] Z. Lin, *Cooperative Communication in OFDM-based Systems*. MS Thesis, University of Wollongong, 2013.

[16] Z. Chen, W. Zheng, and X. Chen, "Convolutional Interleaver Used for OFDM-based Cognitive Radio Systems in Severely Fading Channel," in *4th IEEE International Conference on Information Science and Technology*, 2014, pp. 184–187.

[17] S. Manzoor and N. S. Othman, "Signal to Noise Ratio Estimation in OFDM Based Cooperative Communication System," in *IEEE 13th Malaysia International Conference on Communications (MICC)*, 2017, pp. 84–89.

[18] ——, "Signal to Noise Ratio Estimation Using CAZAC Time Synchronization Preamble in Cooperative Communication System," in *IEEE 4th International Symposium on Telecommunication Technologies (ISTT)*, 2018, pp. 1–6.

[19] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, "A Chaos-based Substitution Box (S-box) Design with Improved Differential Approximation Probability (DP)," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 42, no. 2, pp. 219–238, 2018.

[20] O. Dunkelman and S. Huang, "Reconstructing an S-box from its Difference Distribution Table," *IACR Transactions on Symmetric Cryptology*, pp. 193–217, 2019.

[21] C. Boura, A. Canteaut, J. Jean, and V. Suder, "Two Notions of Differential Equivalence on Sboxes," *Designs, Codes and Cryptography*, vol. 87, no. 2-3, pp. 185–202, 2019.