Synchronization of Two Chaotic Stream Ciphers in Secure CDMA Communication Systems

Ahmed S. Alshammari
Department of Electrical Engineering
University of Hail
Hail, Saudi Arabia
ahm.alshammari@uoh.edu.sa

Abstract—In the basic processing of Code Division Multiple Access (CDMA) systems using chaotic code sequences, a pair of chaos generators in the transmitter and the receiver are used to generate the same sequence, in order to synchronize and retrieve the transmitted signals. In addition, a filter with a simple structure should be integrated into chaotic signals to achieve the maximum of the signal to noise ratio and mitigate the harmful effects of multipath. Another effective property of chaos signal is that a wireless multipath channel does not change the amount of contained information. Considering those issues, the present paper describes a practical system for synchronizing two chaotic generators used in a digital CDMA. Chaotic generators were used to spread the data and provide security against attack. Both receiver and transmitter were implemented using two separate Spartan 6 FPGA boards. Experimental results proved the robustness of the proposed method which could contribute towards the synchronization of chaotic signals in secure CDMA communication systems.

Keywords-synchronization; CDMA; chaotic; communication systems; FPGA

I. INTRODUCTION

During the last years, CDMA communication systems have been a much focused spot in modern secured communication systems technology [1-3]. CDMA is a multiplexing technique based on the spread spectrum principle [4, 5]. Its main advantage is that it allows the increase of the resistance to selective frequency fading, by spreading the power over a wide frequency band of a channel. In addition, CDMA gives the signal the ability to transmit noise of a form that makes it hardly detectable by unintended receivers [6]. Another advantage, due to the spread spectrum, is its resistance to jammers that may appear during transmission. The use of spreading sequences as codes distinguishes different users, giving the advantage of simultaneously exploiting the entire frequency band and time intervals [7], resulting in better utilization of the available resources. The conditions imposed by the orthogonality of code sequences reduce the interference between users [8]. Although CDMA has been successfully utilized in radio and optical communication systems, by either coherent or non-coherent approaches, many studies have focused on its application in other fields. In [9], an investigation was performed on induced random chip flipping used for multicarrier-based CDMA systems, securing multiple access. Researchers in [10] employed the Physical Layer Security (PLS) to protect confidential information in wireless CDMA, by proposing a binary signature design able to mitigate the reception of confidential messages by eavesdroppers. In [11], after evaluating the disguised jamming impacts on conventional CDMAs, a robust method was proposed using Advanced Encryption Standard (AES) to produce security-enhanced scrambling codes instead of conventional ones, to content disguised jamming using secure scrambling. Other researches contributed on CDMA applications in Collaborative Reader [12] and in Centimeter Accuracy Locating [13] in harmonic RFID systems. The detection of a received MC-CDMA signal and its time-delay estimation are very important in many applications, as multipath [14] and Multiple-Access Interference (MAI) can affect them. In this context, some approaches focused on mitigating the multipath and MAI impact, such as data-aided precoding [15], Reiterative Minimum Mean-Square Error (RMMSE) filters [16, 17] and Ultra-Wide Band (UWB) [18]. Atmospheric Optical (AO) communication emerged as a good candidate for broadband access environments, thanks to its ability to provide huge data rates. A suitable tool for the mathematical formulation of Bit-Error Rate (BER) on a secured relay-assisted AO/CDMA system in multiuser optical communications and especially over log-normal turbulence channel was deployed in [19]. Digital CDMA systems using chaotic signals for data spreading offer a high degree of security against unauthorized reception were reported in [20]. However, this technique adds an extra level of complexity regarding the synchronization between the transmitter and the receiver. The clock signal must be recovered, the two clocks must synchronize, and the receiver's digital chaotic generator must be synchronized with the transmitter's [21]. The design of a passband system requires a procedure for carrier recovery. A block diagram of a baseband system is shown in Figure 1.

This paper describes and validates experimentally an approach for synchronizing chaotic generators. Both transmitter and receiver chaotic generators use the same parameters, but they also need to start at the same time step in relation to the transmitted data, in order to recover them correctly. The chaotic generators were implemented with the Lorenz model [22].

Corresponding author: Ahmed S. Alshammari

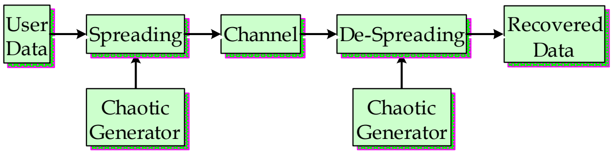


Fig. 1. Block diagram of the baseband system.

Four methods have been proposed on the synchronization of analogue chaotic generators [23]. The first three methods, collectively known as continuous chaotic synchronization, are additive chaos masking, chaotic modulation and chaotic cryptosystem [24, 25]. The disadvantage of using these techniques is the requirement of large bandwidth due to continuous synchronization framework injection into the slave [26]. The fourth method, known as impulsive synchronization, overcame this issue consuming much less bandwidth [26]. Authors of [27] stated that impulsive and continuous synchronization are not reliable for chaotic communication systems, as both of them inject the drive signal into the slave system, which does not provide robust channel noise sensitivity. The method presented in [27] was based on an asynchronous serial communication protocol without the need of injecting signal into the dynamics of the slave system. Many researchers focused on the synchronization of chaotic generators. In [20], a novel detection method was proposed and was experimentally validated for weak sinusoidal signal that may exist in strong noise between two synchronization systems. In [28], a chaotic secure communication system was proposed, achieving significant improvement in the chaotic dynamic behavior by the application of phase modulation of the single loop feedback light.

In this paper, synchronization is based on sending a sync stream block used to trigger the receiver chaotic generator. When the sync stream is detected, the transmitter's chaotic generator output signal is identical to the receiver's, since both chaotic generators are also clock-synchronized. This synchronization method was implemented, tested and validated in hardware using two FPGA boards. The design procedure was based on different design tools: Matlab, Xilinx System Generator, ISE and the Hardware Description Language VHDL.

II. CLOCK RECOVERY

A. *Clock Recovery Based on a Simulink Model*

In serial digital data transmission, the local clock on the receiver must be adjusted in frequency and phase to the clock rate of the incoming signals [29]. The purpose of the recovered clock is to re-time the incoming serial data so that they can be received and processed synchronously, and the data transmitted can be properly retrieved [30]. The first step is to synchronize the clocks between the transmitter and receiver. Figure 2 shows that the clock is missing from the random data. The first step of the clock recovery process is to detect the rising and falling edges, and then recover the clock based on a band-pass filter. Figure 3 shows the SIMULINK model of the clock recovery. Figure 4 shows the detected rising and falling edges. The FFT function shows the clock signal and its harmonics that appear in the signal, as shown in Figure 5.

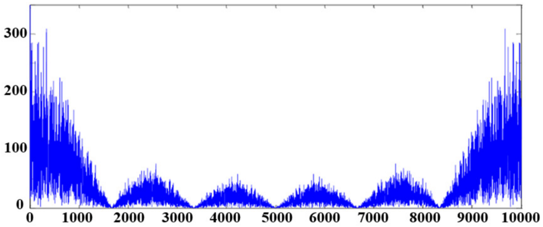


Fig. 2. Clock is missing from the data transmitted.

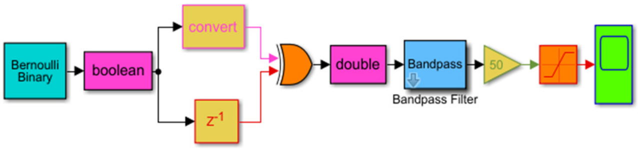


Fig. 3. Clock recovery Simulimk model.

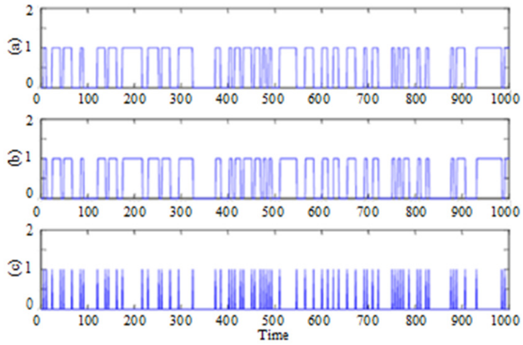


Fig. 4. Simulated results: (a) Binary random generator (Bernoulli), (b) delayed data by one sample, (c) rising and falling edge detections.

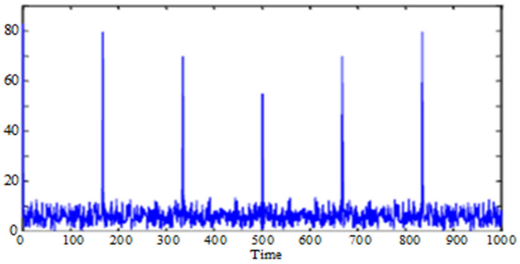


Fig. 5. Clock frequency of the random data.

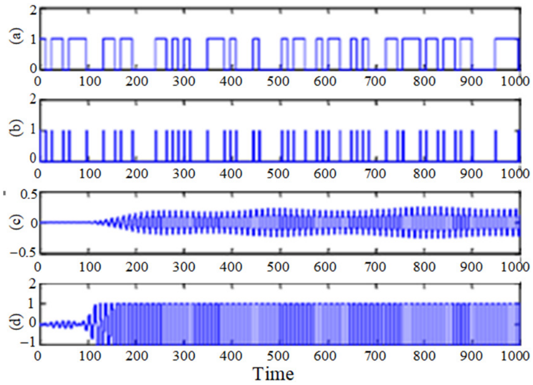


Fig. 6. Simulated test of clock recovery: (a) Binary random generator (Bernoulli), (b) rising and falling edges, (c) bandpass filter response, (d) recovered clock.

Figure 6 shows the simulated results of the clock data recovered from the random transmitted data.

B. Clock Recovery based on System Generator ® model

Figure 7 shows the clock recovery model based on System Generator. The FIR filter is able to recover the desired frequency from the random data generator. Figure 8 shows that the clock is recovered from the random data generator.

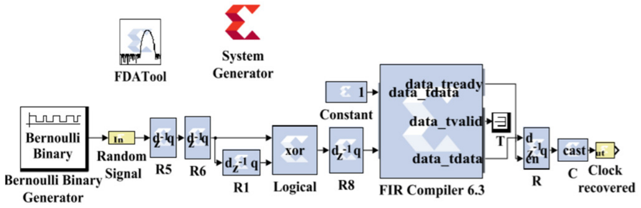


Fig. 7. Clock recovery as visualized by the oscilloscope.

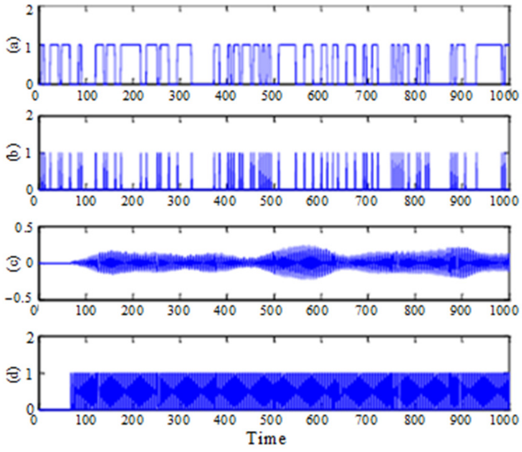


Fig. 8. Simulated results, (a) Binary random generator (Bernoulli), (b) rising and falling edges, (c) FIR filter, and (d) recovered clock.

III. SYNCHRONIZATION METHOD

At first, the receiver recovers the master clock of the digital system. The second process is to synchronize the transmitter's and receiver's chaotic generators. The principle scheme of the synchronization is presented in Figure 9.

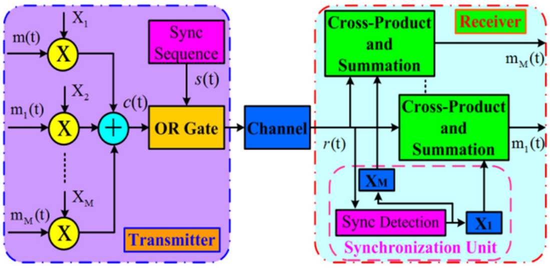


Fig. 9. The DS-CDMA digital communication system-based chaotic signal with the synchronisation unit.

When the sync stream block transmits the 32-bit stream, a known constant delay is added before the Lorenz generator starts generating the signal at the transmitter. The receiver's synchronization unit uses the received signal *r(t)* to generate the de-spreading signal, which is identical to the Lorenz chaotic generator at the transmitter *c(t)*, and they are both clocked at the same clock rate. For data recovery, the received signal is multiplied with the chaotic signal, which is synchronized with the received signal, and then it is accumulated. The cross-product and summation process consist of the product block and the accumulator, the accumulator, and the rational block which compares the threshold with the accumulated value.

IV. SYNCHRONIZATION OF CHAOTIC SIGNALS

A. Transmitter System

The transmitter system includes the Lorenz generator, a spreading block, and a block generating the sync stream which is shown in Figure 10. The Lorenz generators are represented by 32-bit fixed point with 20 fractional bits. The chaotic signals are then serialized by using a parallel to serial convertor. The sync stream generates 32-bit length known data. The bit sequence [1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1, 1,1,1,1,1,1] was used for this purpose. The sync stream block contains a counter, a ROM, a comparison block, an accumulator block, a register, and a convert block. Figure 11 shows the simulated signals of the sync sequence block.

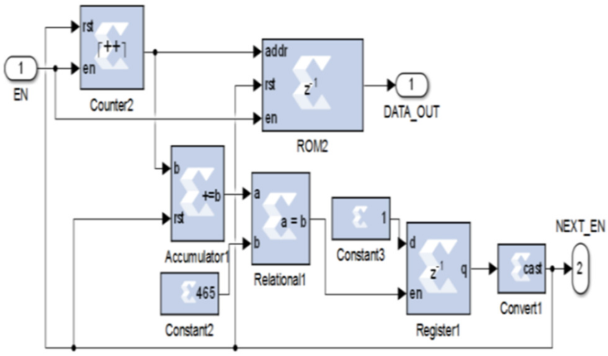


Fig. 10. Sync sequence block using the Xilinx System Generator.

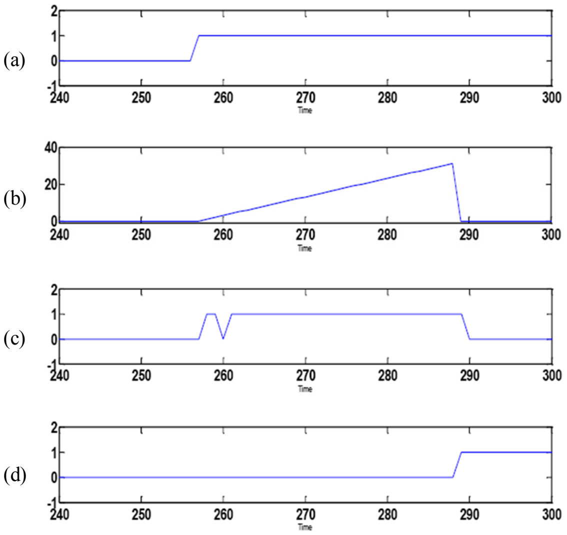


Fig. 11. Simulated test of the synch stream module: (a) Enable signal, (b) counter, (c) 32-bit ROM, and (d) enable signal for the next subsystem to start.

B. Receiver System

The receiver system includes a Lorenz generator identical to the transmitter's, and a sync detector block. The sync detector was deployed by using a Finite State Machine based on VHDL. When the 32-bit sequence is received, the finite state machine is able to detect it and enable a signal for chaotic generators. Figure 12 shows the receiver's sync detector and Figure 13 shows the simulated signal of the sync sequence block at the receiver system. It is clear that the desired sync signal is detected perfectly and stays at one constantly.

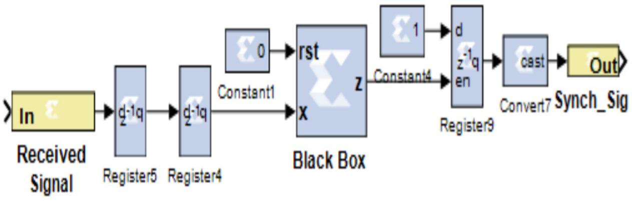


Fig. 12. Sync detector, as views using the Xilinx System Generator.

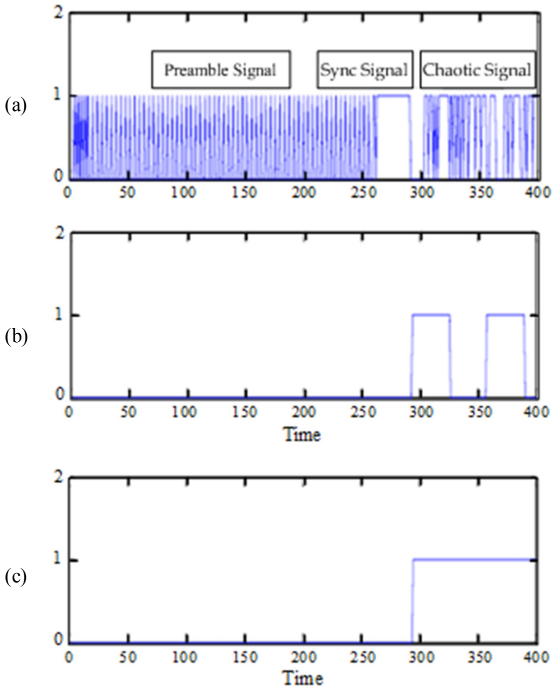


Fig. 13. Simulated test of the sync stream module: (a) Preamble data, sync data, and chaotic signal, (b) synch signal is detected, (c) sync signal is constant.

V. FPGA IMPLEMENTATION AND RESULTS

A. Design Process

The architecture of the studied system is summarized in the following stages:

- Simulink was used for designing, testing and analyzing all integrated subsystems: the Lorenz chaotic generator, its analogue-to-digital signal convertor, the scrambling scheme of Lorenz signals, the four-user digital communication system based on a Lorenz stream cipher, the user data spreading based on Lorenz system, the bipolar encoding, the de-spreading blocks using cross-correlation, cross product, dot product and summation, the data extraction process, the user data threshold tracking value, and the Lorenz stream cipher for four users with and without added noise. Repetitive tests and comparisons between transmitted and recovered data were conducted for all Simulink models, using the Error Rate Calculation to evaluate the system performance and obtain the desired results. It is important to note that many Simulink blocks, not available in the library, were designed in order to ensure compatibility with Xilinx blocks. Xilinx blocks, such as buffers, were designed in the Xilinx System Generator.
- Consequently, the chaotic signal synchronization, the Lorenz system, the data and clock recovery, and their VHDL code were generated using System Generator.
- Afterwards, the synthesis and the configuration of the target device were ensured via the Integrated System Environment (ISE), and a program file, dedicated to a specific device, was generated before being downloaded to the FPGA card. The results were viewed using an oscilloscope.
- The final step included the testing of the system and the comparison between experimental and simulation results.

Table I shows the digital communication system specifications, and Figure 14 summarizes the design procedure of the studied system implementation using an FPGA board (Spartan 6).

TABLE I. PARAMETER SUMMARY

Main clock frequency	20MHz oscillator
Modulation	Spread Spectrum (SS)
Spreading code	32-bit
Spreading user data frequency	64MHz
User data frequency	2MHz
Data rate	2Mbps
FPGA development board	SP605
FPGA family	Xilinx® Spartan 6
FPGA (IC) model number	xc6slx45t-3fgg484
Number of user data streams generated and encrypted	One
Method of user data stream production	Linear Feedback Shift Register (LFSR)

B. Test and Results of the System

The Lorenz equations where x, y and z are state variables, while A, B and C are parameters, are:

$$x = A(y - x) \quad (1)$$

$$y = B.x - y - x.z \quad (2)$$

$$z = x.y - C.z \quad (3)$$

In hardware implementation, the chaotic signal was digitized to 32-bit with 25 fractional bits. Figure 15 shows the real time results, as visualized by the oscilloscope.

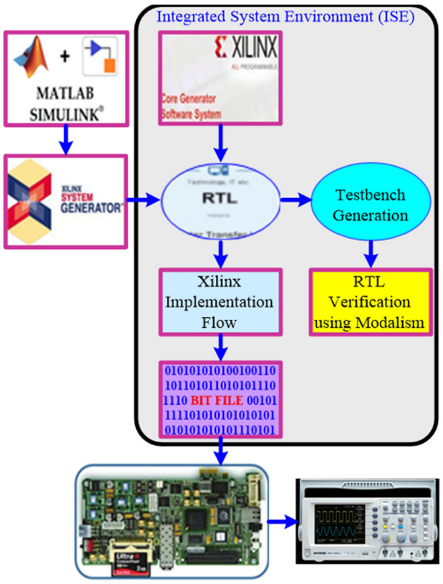
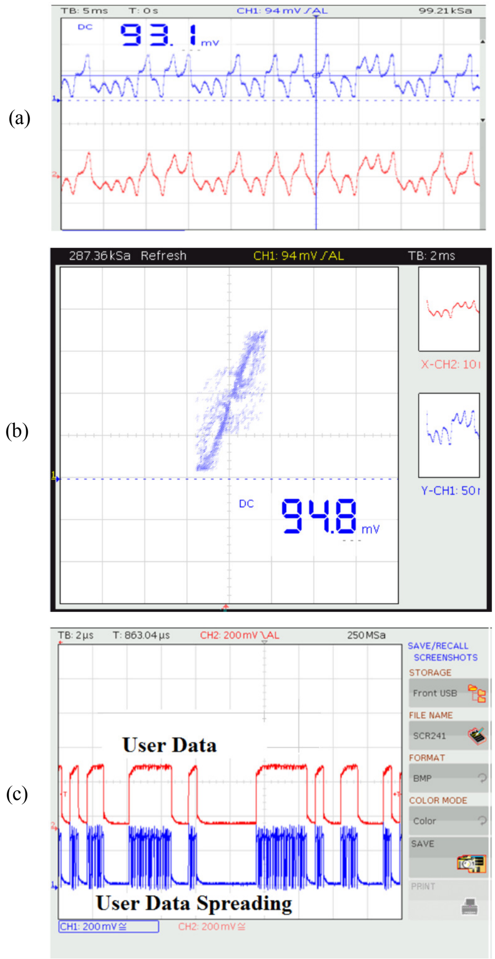


Fig. 14. Block diagram of the design procedure.


(a)
TB: 5ms T: 0s CH1: 94 mV 99.21kSa
DC 93.1 mV
(b)
287.36kSa Refresh CH1: 94 mV TB: 2ms
X-CH2: 10
Y-CH1: 50
DC 94.8 mV
(c)
TB: 2µs T: 863.04µs CH2: 200mV 250MSa
User Data
User Data Spreading
CH1: 200mV CH2: 200mV

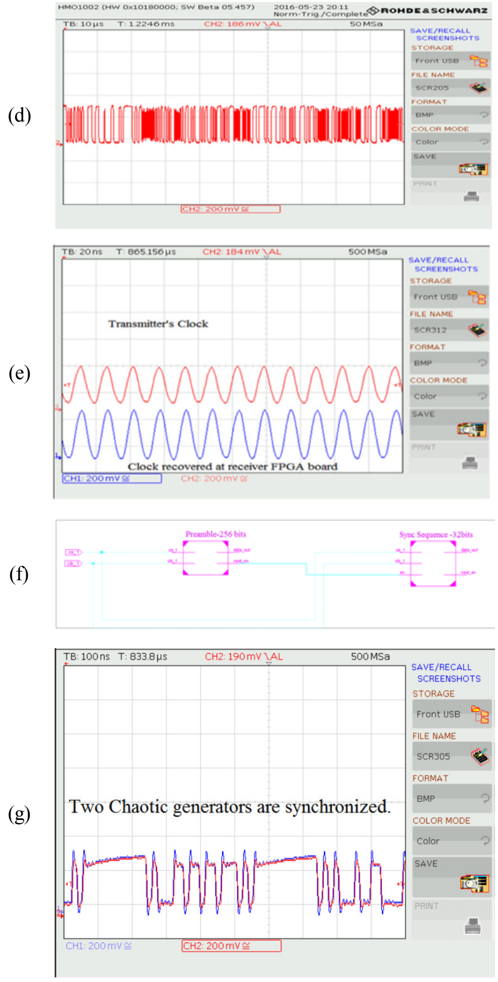

(d)
ROHDE&SCHWARZ
TB: 10µs T: 1.2246ms CH2: 186mV 50MSa
CH2: 200mV
(e)
TB: 20ns T: 865.156µs CH2: 184mV 500MSa
Transmitter's Clock
Clock recovered at receiver FPGA board
CH1: 200mV CH2: 200mV
(f)
Preamble-256 bits
Sync Sequence -32bits
(g)
TB: 100ns T: 833.8µs CH2: 190mV 500MSa
Two Chaotic generators are synchronized.
CH1: 200mV CH2: 200mV

Fig. 15. Implementation results: (a) Analogue representation of the Lorenz generator for of x-state and y-state signals, (b) Lorenz attractor, (c) user data spreading for ones, (user data are represented by the red signal, user data spreading by 32-bit are represented by the blue signal), (d) user data spreading for ones and zeros combined. (e) transmitter clock (red) and recovered clock at receiver side (blue), (f) RTL schematic of the preamble and sync sequence of 32-bits, and (g) two chaotic generators are synchronized perfectly at the slave system/receiver.

C. System Performance Analysis

The system bit rate achieved was 2Mbps. However, this data rate could increase by using one modulation scheme, such as BPSK (Binary Phase Shift Keying). The synchronization technique is robust against channel noise and it does not affect the efficiency of channel usage.

VI. Conclusion

This paper described a practical system for synchronizing two chaotic generators used in a digital CDMA. The method based on a sync stream transmitted to the receiver in order to trigger the Lorenz chaotic generator in the same time step. Thus, the chaotic synchronization was maintained and it was not affected by channel noise. Both the receiver and transmitter were implemented using two separate Spartan 6 FPGA boards. The proposed technique was validated experimentally, and the obtained results demonstrate the robustness of the system. The advantage of a synchronization method is that there is no need to inject a signal into the dynamics of the slave system, which affects the channel efficiency. In addition, this method is not affected by high noise. However, the disadvantage of this method is that when the synchronization signal is affected, the synchronization between the two systems will be lost.

REFERENCES

[1] J. A. Awokola, O. N. Emuoyibofarhe, A. Omotosho, J. O. Emuoyibofarhe, and J. O. Mebawondu, "Perspectives of Threat Modeling of a Secure Cloud Picture Archiving and Communication System," *Engineering, Technology & Applied Science Research*, vol. 9, no. 5, pp. 4859–4862, Oct. 2019.

[2] A. A. Eyadeh and M. N. Al-Ta'ani, "Performance Study of Wireless Systems with Switch and Stay Combining Diversity over α-η-μ Fading Channels," *Engineering, Technology & Applied Science Research*, vol. 9, no. 6, pp. 5047–5055, Dec. 2019.

[3] B. Pranitha and L. Anjaneyulu, "Performance Evaluation of a MIMO based Underwater Communication System under Fading Conditions," *Engineering, Technology & Applied Science Research*, vol. 9, no. 6, pp. 4886–4892, Dec. 2019.

[4] M. Marey and H. Mostafa, "Iterative Channel Estimation Algorithm For Downlink MC-CDMA Systems With Two-Path Successive Relaying Transmission," *IEEE Communications Letters*, vol. 23, no. 4, pp. 668–671, Apr. 2019, doi: 10.1109/LCOMM.2019.2901878.

[5] P. Pan and L. Yang, "Spatially Modulated Code-Division Multiple-Access for High-Connectivity Multiple Access," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4031–4046, Aug. 2019, doi: 10.1109/TWC.2019.2920644.

[6] G. Song, X. Wang, and J. Cheng, "Signature Design of Sparsely Spread Code Division Multiple Access Based on Superposed Constellation Distance Analysis," *IEEE Access*, vol. 5, pp. 23809–23821, 2017, doi: 10.1109/ACCESS.2017.2765346.

[7] F. Molina, J. Villares, F. Rey, and J. Sala-Alvarez, "Decentralized Random Energy Allocation for Massive Non-Orthogonal Code-Division Multiple Access," *IEEE Communications Letters*, vol. 23, no. 12, pp. 2306–2310, Dec. 2019, doi: 10.1109/LCOMM.2019.2945710.

[8] W. Liu, Y.-C. Liang, Y. Li, and B. Vucetic, "Backscatter Multiplicative Multiple-Access Systems: Fundamental Limits and Practical Design," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 5713–5728, Sep. 2018, doi: 10.1109/TWC.2018.2849372.

[9] J. Choi and E. Hwang, "Secure Multiple Access Based on Multicarrier CDMA With Induced Random Flipping," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5099–5108, Jun. 2017, doi: 10.1109/TVT.2016.2623791.

[10] M. Li, G. Ti, X. Tian, and Q. Liu, "QoS-Based Binary Signature Design for Secure CDMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10011–10023, Nov. 2017, doi: 10.1109/TVT.2017.2743042.

[11] T. Song, K. Zhou, and T. Li, "CDMA System Design and Capacity Analysis Under Disguised Jamming," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2487–2498, Nov. 2016, doi: 10.1109/TIFS.2016.2585089.

[12] X. Hui and E. C. Kan, "Collaborative Reader Code Division Multiple Access in the Harmonic RFID System," *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 2, pp. 86–92, Jun. 2018, doi: 10.1109/JRFID.2018.2852484.

[13] X. Hui, Y. Ma, and E. C. Kan, "Code Division Multiple Access in Centimeter Accuracy Harmonic RFID Locating System," *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 51–58, Mar. 2017, doi: 10.1109/JRFID.2017.2745898.

[14] A. Scaloni, P. Cirella, M. Sgheiz, R. Diamanti, and D. Micheli, "Multipath and Doppler Characterization of an Electromagnetic Environment by Massive MDT Measurements From 3G and 4G Mobile Terminals," *IEEE Access*, vol. 7, pp. 13024–13034, 2019, doi: 10.1109/ACCESS.2019.2892864.

[15] Y. Choi, J. Lee, M. Rim, and C. G. Kang, "Constructive Interference Optimization for Data-Aided Precoding in Multi-User MISO Systems," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1128–1141, Feb. 2019, doi: 10.1109/TWC.2018.2890059.

[16] Y. Shen and Y. Xu, "Multiple-Access Interference and Multipath Influence Mitigation for Multicarrier Code-Division Multiple-Access Signals," *IEEE Access*, vol. 8, pp. 3408–3415, 2020, doi: 10.1109/ACCESS.2019.2962633.

[17] Y. Shen, Y. Wang, Z. Peng, and S. Wu, "Multiple-Access Interference Mitigation for Acquisition of Code-Division Multiple-Access Continuous-Wave Signals," *IEEE Communications Letters*, vol. 21, no. 1, pp. 192–195, Jan. 2017, doi: 10.1109/LCOMM.2016.2625298.

[18] S. Wang, G. Mao, and J. A. Zhang, "Joint Time-of-Arrival Estimation for Coherent UWB Ranging in Multipath Environment With Multi-User Interference," *IEEE Transactions on Signal Processing*, vol. 67, no. 14, pp. 3743–3755, Jul. 2019, doi: 10.1109/TSP.2019.2916016.

[19] H. T. T. Pham, P. V. Trinh, N. T. Dang, and A. T. Pham, "Secured relay-assisted atmospheric optical code-division multiple-access systems over turbulence channels," *IET Optoelectronics*, vol. 9, no. 5, pp. 241-248, Oct. 2015, doi: 10.1049/iet-opt.2014.0148.

[20] G. Li and B. Zhang, "A Novel Weak Signal Detection Method via Chaotic Synchronization Using Chua's Circuit," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 3, pp. 2255–2265, Mar. 2017, doi: 10.1109/TIE.2016.2620103.

[21] T. Wang, D. Wang, and K. Wu, "Chaotic Adaptive Synchronization Control and Application in Chaotic Secure Communication for Industrial Internet of Things," *IEEE Access*, vol. 6, pp. 8584–8590, 2018, doi: 10.1109/ACCESS.2018.2797979.

[22] D. Brown, A. Hedayatipour, M. B. Majumder, G. S. Rose, N. McFarlane, and D. Materassi, "Practical realisation of a return map immune Lorenz-based chaotic stream cipher in circuitry," *IET Computers & Digital Techniques*, vol. 12, no. 6, pp. 297-305, Nov. 2018, doi: 10.1049/iet-cdt.2018.5005.

[23] T. Yang, "A Survey of Chaotic Secure Communication Systems," *International Journal of Computational Cognition*, vol. 2, no. 2, pp. 81–130, Jun. 2004.

[24] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 626–633, Oct. 1993, doi: 10.1109/82.246163.

[25] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 634–642, Oct. 1993, doi: 10.1109/82.246164.

[26] S. Sadoudi, M. S. Azzaz, and C. Tanougast, "Novel experimental synchronization technique for embedded chaotic communications," in *2014 International Conference on Control, Decision and Information Technologies (CoDIT)*, Metz, France, Nov. 3-5, 2014, pp. 669–672, doi: 10.1109/CoDIT.2014.6996976

[27] A. De Marcellis *et al.*, "Impulse-Based Asynchronous Serial Communication Protocol on Optical Fiber Link for AER Systems," in *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, Genoa, Italy, Nov. 27-29, 2019, pp. 370–373, doi: 10.1109/ICECS46596.2019.8964829

[28] S. Cui and J. Zhang, "Chaotic Secure Communication Based on Single Feedback Phase Modulation and Channel Transmission," *IEEE Photonics Journal*, vol. 11, no. 5, pp. 1–8, Oct. 2019, doi: 10.1109/JPHOT.2019.2931615.

[29] T. Zhou, Z. Zuo, and Y. Wang, "Quantizer-Based Triggered Control for Chaotic Synchronization With Information Constraints," *IEEE Transactions on Cybernetics*, vol. 48, no. 8, pp. 2500–2508, Aug. 2018, doi: 10.1109/TCYB.2017.2741103.

[30] L. Yin, Z. Deng, B. Huo, and Y. Xia, "Finite-Time Synchronization for Chaotic Gyros Systems With Terminal Sliding Mode Control," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 6, pp. 1131–1140, Jun. 2019, doi: 10.1109/TSMC.2017.2736521.