FPGA Design of Encryption Speech system using Synchronized Fixed-Point Chaotic Maps Based Stream Ciphers

Zahraa M. Alroubaie, Muneer A. Hashem, Fadhil S. Hasan

Abstract: In this work, speech encryption using synchronized fixed-point chaotic map-based stream ciphers (SFPCM-SC) is suggested. Five chaotic maps named quadratic, henon, logistic, lozi and duffing are synchronized by using master-slave synchronization technique and then used to generate the pseudo random bit generator (PRBG) using fixed-point converter. The PRBG is then Xor-ed with digitized speech signal where the encrypted signal is created. In the other side, the same map is synchronized with the master one and used to recover the original speech signal. First this work is simulated by using MATLAB and then built the design using Xilinx system generator (XSG). Finally, the hardware co-simulation is applied for the proposed system by using FPGA SP605 XC6SLX45T device. The results show that the error between master and slave become zero after a small period and the original speech signal is recovered with real time environment in successful.

Keywords: speech encryption, fixed point representation, pseudo random bit generator (PRBG), chaotic maps, Chaos synchronization, system generator, FPGA Hardware co-simulation.

I. INTRODUCTION

In recent year, the speech encryption signal has been widely used in civilian communication and military systems, so that the protection for these signals is a very important requirement [1],[2]. It is generally possible to classify speech encryption techniques into two kinds; analog and digital schemes [3]. In narrow band signal, the analogue speech encryption is scrambled either in frequency, time [4], frequency and time [5], or in other domains [6], [7]. In digital speech encryption, the analog speech signal is transformed over analog to digital converter into digital stream bits and then summed up with "pseudo random bit generators" (PRBG) in mode 2. [8].

The advantage of analog methods is that it can be used by telephone analogies and band-limited radio systems while digital encryption techniques being more secure than analog [9]. We will concentrate in this article on the chaotic stream cipher digital encryption speech systems.

Nowadays, Unpredictable long-term assessment of chaotic systems has been appeared, initial parameters sensitivity and infinite period, that the usage make them suitable in pseudo random bit generator [10],[14] and permutation [15]. Therefore, different researchers are suggested the chaotic system in stream ciphers-based speech encryption system. In [1] Lorenz chaotic system and Henon map in hybrid discrete continuous chaotic system for real time wireless speech encryption are used. In [16] the chaotic system is synchronized using the same manner described in chaotic masking system. Furthermore, the proposed cipher speech system is implemented using FPGA Virtex-II development board. On [17] the PRBG is produced using a unified chaotic- map and used for digital voice encryption. In [2] After discrete cosine transformation (DCT), the digital voice signal is encrypted in two stages. The first level is the level of confusion where PRBG produced by Zaslavsky map is XORed with DCT output, while the second level diffuses the encrypted speech using Cat transform. In [18] The digital voice signal is encrypted using a stream cipher scheme where the PRBG is produced by converting the stream of chaotic map bit to a digital converter (ADC). In [19] A Henon map-based stream cipher scheme is suggested to confuse the digital voice signal and then diffuse the encryption signal using the Arnold cat map to improve safety. In [20] PRBG is produced using the Chen and Loren chaotic system that is diffused using the Linear-Feedback-Shift-Register (LFSR), the key generation is then used to encrypt speech in the stream cipher scheme and the PRBG is applied using the system generator. In [21] Lorenz map is used to generate PRBG where the three signals of the system are converted into binary streams and then they XORed together. The proposed PRBG is used to encrypt the speech signal using stream cipher. In [22] The digital voice signal is chipped with three types of chaos, logistic map, nonlinear chaotic algorithm and tangent-delay ellipse, reflecting-cavity map. In [23] Using stream cipher scheme, modified tent map and bit permutation are used to encrypt the voice signal and the scheme is implemented on the Virtex-5 FPGA kit, In this paper, the (PRBG) is generated by fixed-point chaotic maps. The PRBG is used to cipher the digital speech signal using stream ciphers. The synchronization between the PRBGs in the transmitter and the receiver is also presented using chaotic synchronization technique. Different types of chaotic systems including Lozi, Henon, Duffing, Quadratic and Logistic maps are used to test the randomness of PRBG and the security level of speech signal. Also, the proposed stream cipher systems are implemented using Xilinx system generator (XSG) and the hardware co-simulation over FPGA SP605 XC6SLX45T device is provided.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Zahraa M. Alroubaie*, Electronics and Communication Engineering, Mustansiriyah University College, Baghdad, Iraq. Email: alroubaiezahraa@gmail.com

Muneer A. Hashem, Electronics and Communication Engineering, Mustansiriyah University College, Baghdad, Iraq. Email: muneraboud@yahoo.com

Fadhil S. Hasan, Electronics and Communication Engineering, Mustansiriyah University College, Baghdad, Iraq Email: fadel_sahib@uomustansiriyah.edu.iq

II. CHAOTIC MAPS SYNCHRONIZATION

The word synchronization in origin is a Greek root mean “to share the common time”, in 1990’s [24] the researchers have been discovered that chaotic system can be synchronized. To achieve the synchronization for the key that generated from chaotic maps, each map must have the master system generated at transmitter side and slave system derive by the master system. Figure (1) shows the general structure of synchronization in chaotic maps. The master system is the chaotic system in the transmitter side where the general equations of master chaotic maps are written as:

$$x_{i+1} = f(x_i, y_i\ ) \qquad y_{i+1} = g(x_i, y_i) \tag{1}$$

At the receiver the x signal derives the slave system to obtain the synchronization between two systems according to the following equations:

$$w_{i+1} = f(x_i, z_i\ ) \qquad z_{i+1} = g(w_i, z_i) \tag{2}$$

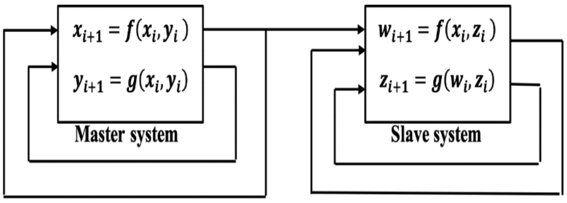

Fig. 1. “Master-Slave” mapping synchronization

The master and the slave system of each chaotic maps are summarized below.

A. *Fixed-point Lozi Map*

The master equations of Lozi map can be expressed as [25]:

$$x_{i+1} = 1 + y_i - a * |x_i| \qquad y_{i+1} = b * x_i \tag{3}$$

and, the slave equations are:

$$w_{i+1} = 1 + z_i - a * |x_i| \qquad z_{i+1} = b * w_i \tag{4}$$

Master and slave error must be zero and can be given by:

$$e1_i = x_{i+1} - w_{i+1} \qquad e2_i = y_{i+1} - z_{i+1} \tag{5}$$

Figure 2 shows the master and slave systems error function for Lozi map. Where (i = n).

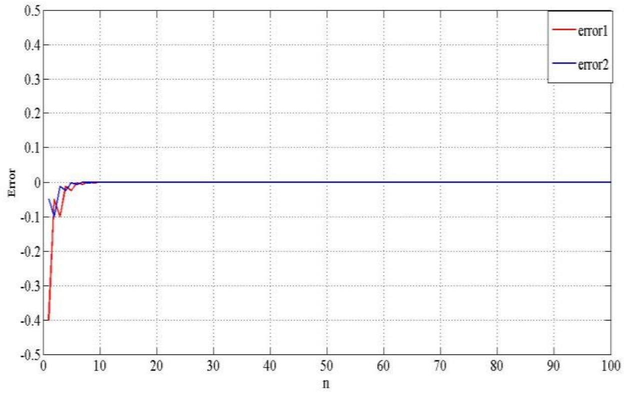

Fig. 2. Error function of master and slave systems for Lozi map.

B. *Fixed-point Henon Map*

The Master equations of Henon map can be expressed as:

$$x_{i+1} = 1 - a * x_i + y_i \qquad y_{i+1} = b * x_i \tag{6}$$

And the slave equations are:

$$w_{i+1} = 1 - a * x_i + z_i \qquad z_{i+1} = b * w_i \tag{7}$$

Figure 3 shows the master and slave systems error function for Henon map, Where (i = n).

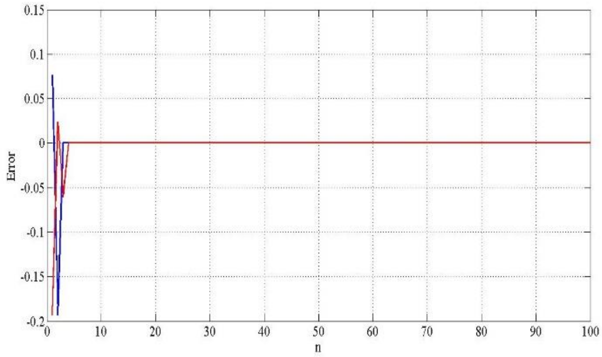

Fig. 3. The mater and slave systems error function for Henon map.

C. *Fixed-point Duffing Map*

The Master equations of duffing map are defined as:

$$x_{i+1} = y_i \qquad y_{i+1} = -b * x_i + a * y_i - y_i^3 \tag{8}$$

Also, the salve equation can be defined as:

$$w_{i+1} = z_i \qquad z_{i+1} = -b * w_i + a * y_i - y_i^3 \tag{9}$$

Figure 4 shows the master and the slave system error for duffing map, Where (i = n).

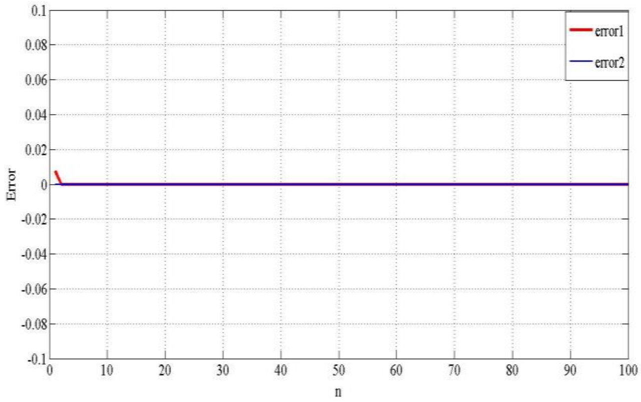

Fig. 4. The “master and slave” system error for duffing map

D. *Fixed-point Quadratic Map*

The master equation of quadratic map is defined as:

$$x_{i+1} = a - x_i^2 + (c * x_i - y_i) \tag{10}$$

and the salve equation can be defined as:

$$y_{i+1} = a * y_i^2 + (c * y_i - x_i) \tag{11}$$

where control parameter c=0.5. Figure (5) shows the error between master and slave system for Quadratic map, Where (i = n).

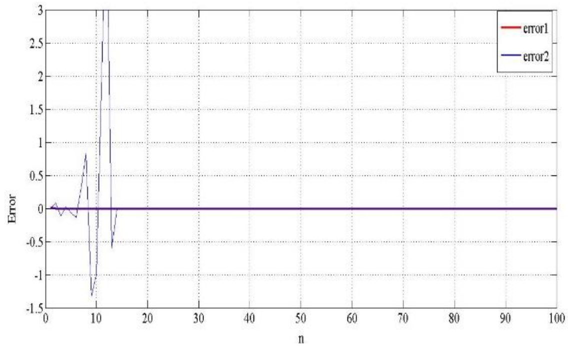

Fig. 5. The error function of Quadratic map.

E. *Fixed-point Logistic Map*

The master equation of Logistic map can be shown as:

$$x_{i+1} = \mu * x_i(1 - x_i) + \Delta\mu * x_i(1 - x_i) \qquad (12)$$

Also, salve equation can be defined as:

$$y_{i+1} = \mu * x_i(1 - x_i) + a_{11}(\mu + \Delta\mu) * x_i(1 - x_i) + (h_{11} - \mu + 2\mu a_{11} x_i)(x_i - a_{11} x_i) - \mu a_{11} x_i(1 - a_{11} x_i) \qquad (13)$$

By using the control parameter $a_{11} = 1$, $h_{11} = 0.65$, $\mu = 3.8$ and $\Delta\mu = 0.1$. The error result can be shown in Figure 6, Where (i = n).

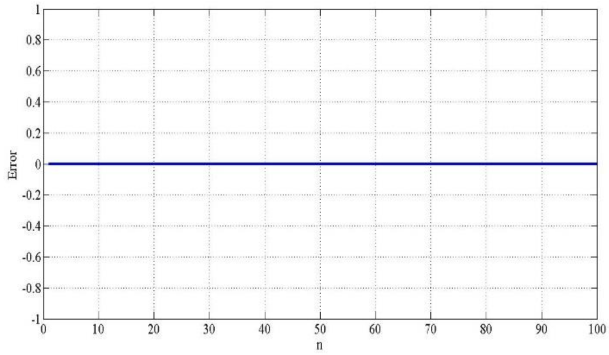

Fig. 6. error function for FPLoM-PRBG

III. SPEECH-ENCRYPTIONUSING SYNCHRONIZED FIXED-POINT CHAOTIC MAPS BASED STREAM CIPHER (SFPCM-SC)

Figure 7 Displays the overall speech encryption block diagram using (SFPCM-SC). Five types of PRBGs are generated named FPQM-PRBG, FPHM-PRBG, FPDM-PRBG, FPLM-PRBG and FPLoM-PRBG for fixed-point Quadratic, Henon, Duffy, Lozi and Logistic map respectively. The analogue speech signal is sampled with sampling frequency f_s=8 kHz and resolution bits, *n*=16. The sampled speech signal (*S*) is passing through pre-processing function to get fixed-point sequence with 32-word length for each sample. The sample with 32 bits then XOR-ed with the key stream bits (K_i) to generate encryption bits (C_i). At the receiver side, the encryption bits are XOR-ed with the synchronized key stream bits generated in the deciphered side to recover the original i-*th* bit ($\widetilde{S_\iota}$). Conversion process is the inverse function of pre-processing function at transmitter side to recover the source speech signal

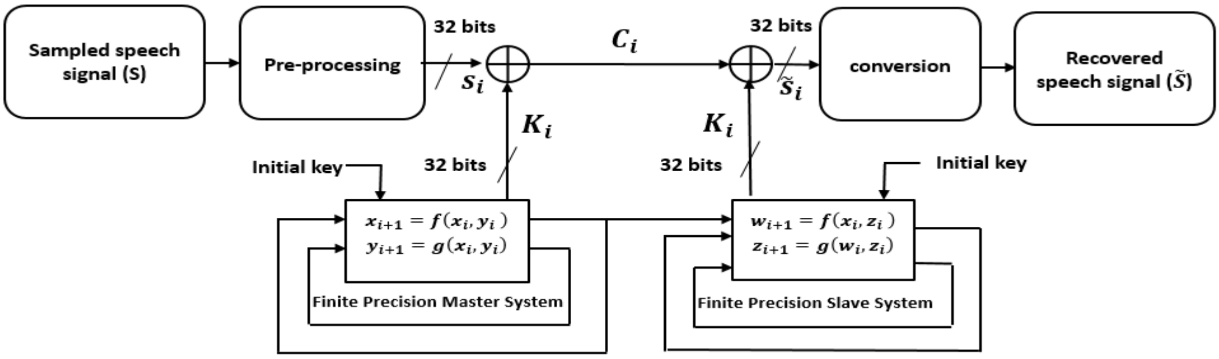

Fig. 7. Block diagram of speech encryption system using FPSCM-SC.

IV. MEASUREMENT OF RESIDUAL UNINTELLIGIBILITY FOR SPEECH SIGNAL

The “Log-likelihood Ratio Measure (LLR), frequency-weighted-segmental signal- to-noise ratio (fwSNRseg) and SNR-loss ($\mathrm{SNR_{LOSS}}$)” are The most significant measures used to evaluate voice encryption unintelligibility [20], [26], [27].

These test methods are applied for stream ciphers for each PRBGs and the outcomes are presented in Table 1.

Table- I: The remaining measures of unintelligibility for man's voice.

Type Of PRBG	*LLR*	*SNR*	*Fwsnrseg*
FPQM-PRBG	2.7997	0.983	-20.0638
FPHM-PRBG	1.0693	0.9762	-14.386
FPLM-PRBG	2.8872	0.9829	-19.9028
FPDM-PRBG	2.71	0.9846	-20.0764
FPLOM-PRBG	2.5763	0.9787	-20.0476

V. RANDOMNESS MEASURE

The difficulty of proving the unpredictability of any sequence by using the theoretical way and to enhance the security at the same time, the sequence that generated from chaotic method must pass the statistical test. These experiments play a very significant part in the contemporary design of the stream cipher. NIST test consist of 15 tests that are widely use in the cipher design. All the tests have a threshold value which is concerned as the standard value of success and the passing value (Pvalue) should be greater than 0.01(P_{value} > 0.01) to pass the test. If the generated sequence passing a several tests from the whole test, then it can be classified as a random sequence. In this work a several tests named "**Frequency, Frequency with Block Test, Serial, Discrete Fourier Transform Test (DFT) and Cumulative Sum Tests"** are used [28]**.**

These tests methods are applied for stream ciphers for each PRBGs and the outcomes are shown in Table below.

Table- II: The randomness measures for PRBGS.

PRBG *Measurement Methode*	*FPQM-PRBG*	*FPHM-PRBG*	*FPLM-PRBG*	*FPDM-PRBG*	*FPloM-PRBG*
Frequency-test	0.9718	0.9944	0.5813	0.9015	0.9226
Block Frequency-test	0.9989	0.8999	1	0.9789	0.989
Serial-test	1	0.0395	1	1	1
Discrete-Fourier (DFT)	0.125	0.3634	0.0195	0.0155	0.5743
Cumulative Sum test	1	1	1	1	1

VI. XSG IMPLEMENTATION OF SPEECH ENCRYPTION BASED ON SFPCM-SC

The generation keys between transmitter and receiver side are synchronized using chaotic synchronization system for each fixed-point chaotic map. Figure (8) to (12) show the XSG implementation of speech encryption based on synchronized FPLM, FPLoM, FPHM, FPDM and FPQM stream cipher respectively.

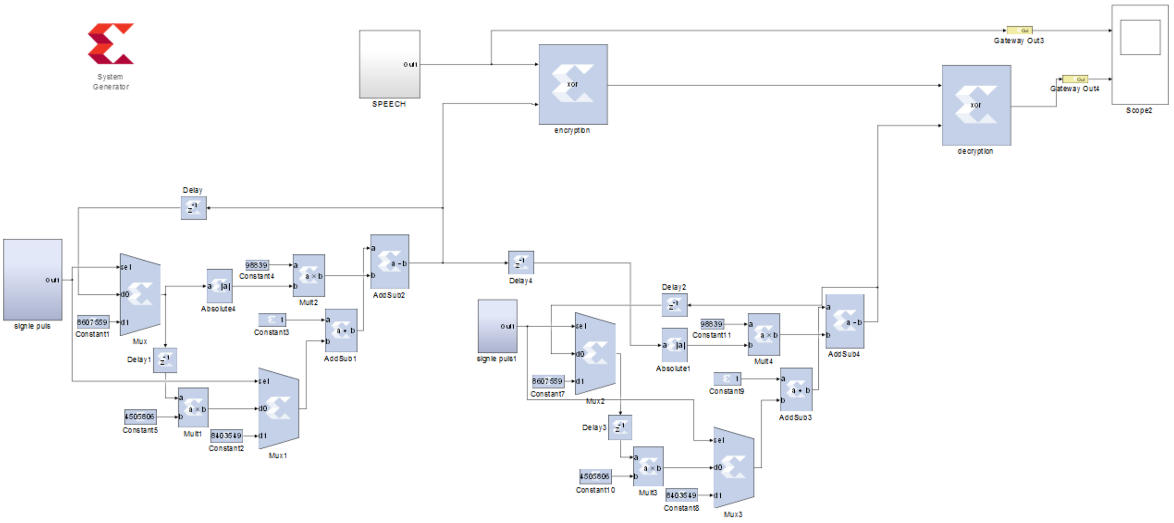

Fig. 8. System generator of synchronized-FPLM block diagram for speech encryption system.

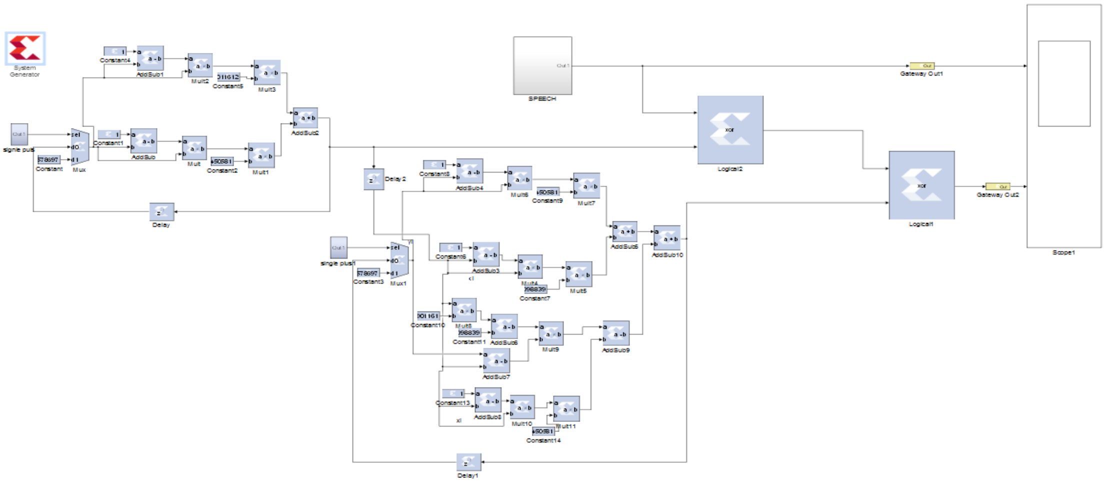

Fig. 9. System generator of synchronized-FPLoM block diagram for speech encryption system.

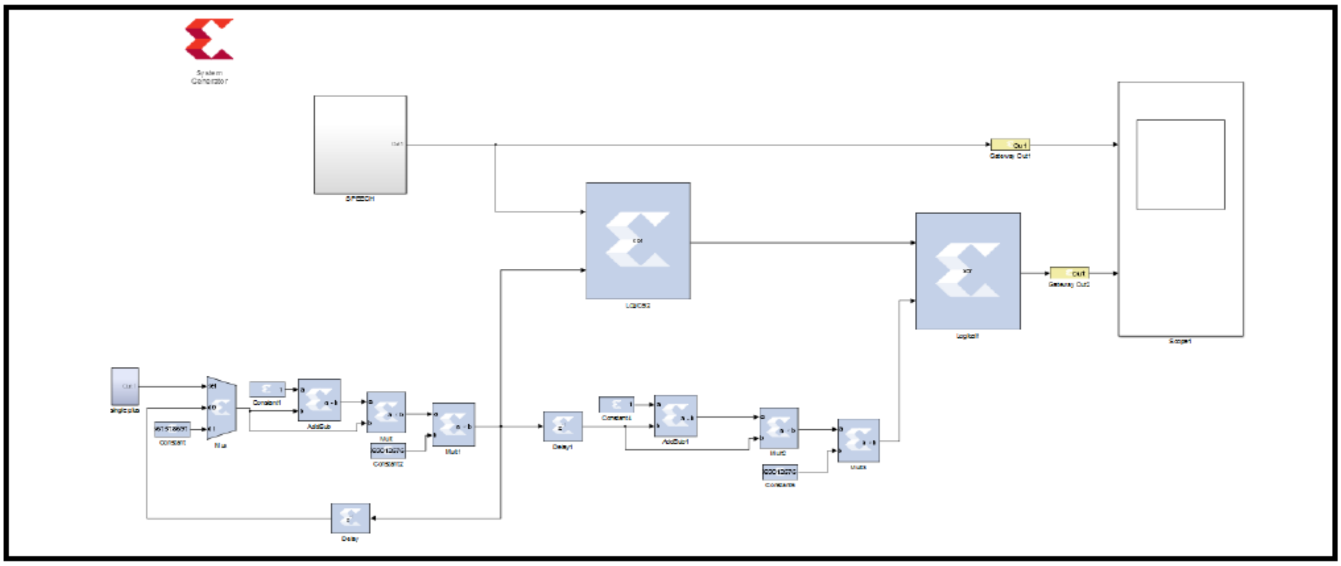

Fig. 10. System generator of synchronized-FPHM block diagram for speech encryption system.

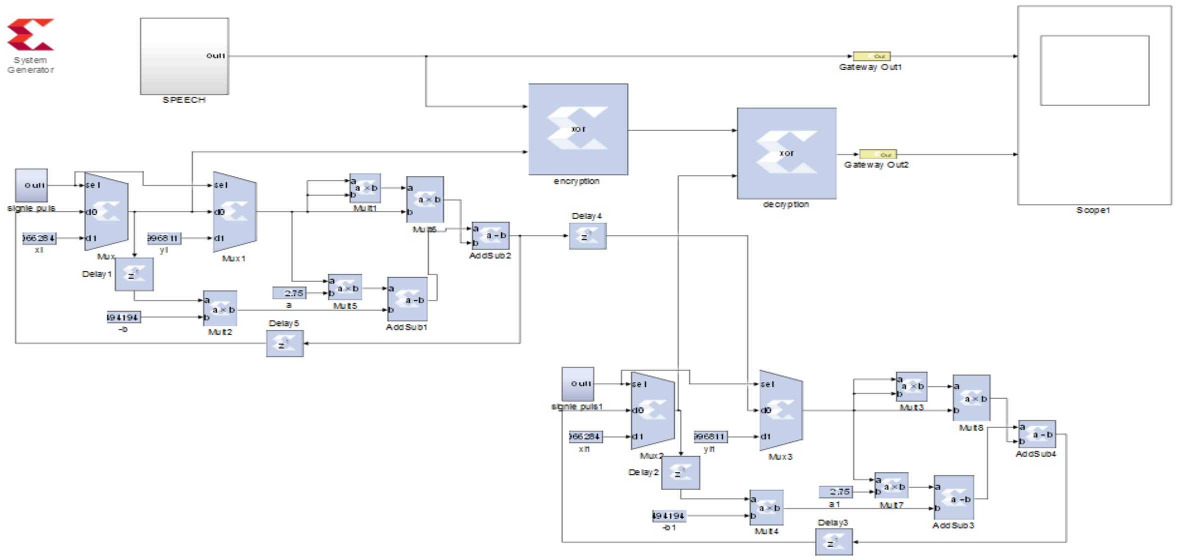

Fig. 11. System generator of synchronized-FPDM block diagram for speech encryption system

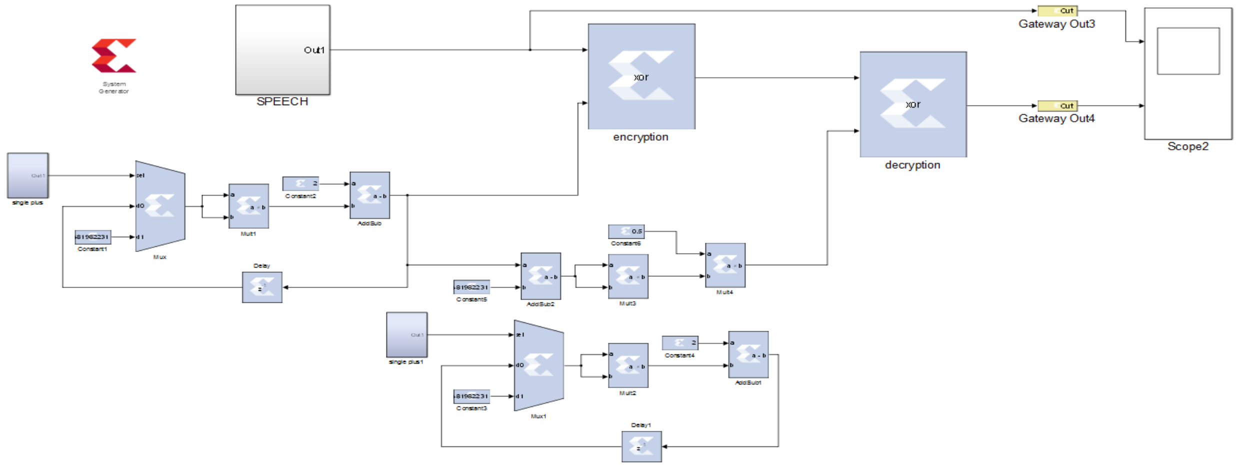

Fig. 12. System generator of synchronized-FPQM block diagram for speech encryption system.

Figure 13 shows the time waveform of the clear speech and the recovered speech signals that implemented with SFPCM can be in.

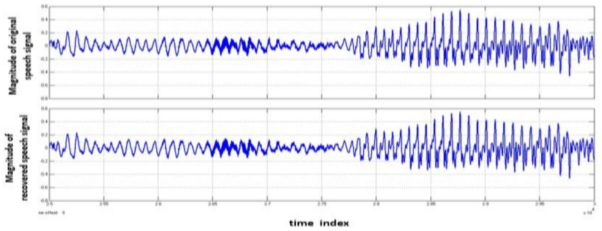

Fig. 13. Original and recovered speech signal.

VII. FPGA HARDWARE CO-SIMULATION OF SPEECH ENCRYPTION BASED ON SFPCM-SC

The VHDL codes for all synchronized FPCM-PRBGs are generated using system generator block in XSG tools. The resource utilization summary of the proposed systems are shown in Table 3. The throughput is calculated by multiplying the maximum frequency ($f_{\max}$) allowed for each system by number of bits for each sample (WL=32), (Throughput= $f_{\max} \times$ WL). The SFPCM system is hardware tested using hardware co-simulation with clock frequency 27 MHz. The system is performed on SP605 XC6SLX45T-3FGG484 evaluation board. Fig. 14 shows the real-time hardware co-simulation of SFPCM system. The serial data of the speech signal send to the FPGA through USB UART port after JTAG co-simulation link is performed. Then, the serial stream output from the FPGA device is taken and send back to the PC to test with the MATLAB results. In the same figure, the above two plots refer to encrypted speech signal and recovered speech signal with synchronized key for the MATLAB results , The results show that the real time of the proposed system is working well and matching the expected design.

Table III: Resource utilization summary for FPSCM-PRBG systems.

RESOURCE TYPE	FPQM-PRBG	FPDM-PRBG	FPHM-PRBG	FPLM-PRBG	FPLoM-PRBG
SLICE REGISTERS /%	33/1	98/1	66/1	130/1	101/1
Slice LUTs/%	120/1	219/1	120/1	290/1	419/1
OCCUPIED SLICE /%	49/1	111/1	78/1	109/1	156/2
DSP48AIS	12/20	32/55	16/27	16/27	48/82
MAX. PATH DELAY(NS)	17.682	34.250	33.228	20.743	43.25
MAX. FREQUENCY (MHZ)	56.55	29.19	30.09	48.209	23.120
THROUGHPUT (GBPS)	1.8096	0.9340	0.9629	1.5427	0.7398

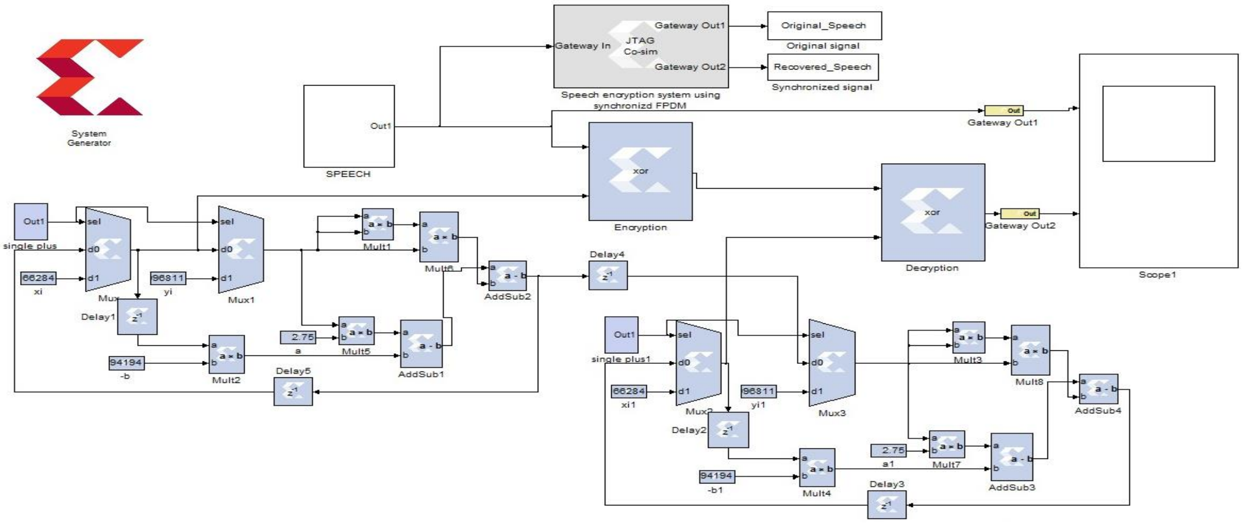

Fig. 14, Real time hardware co-simulation of the FPSCM-SC system

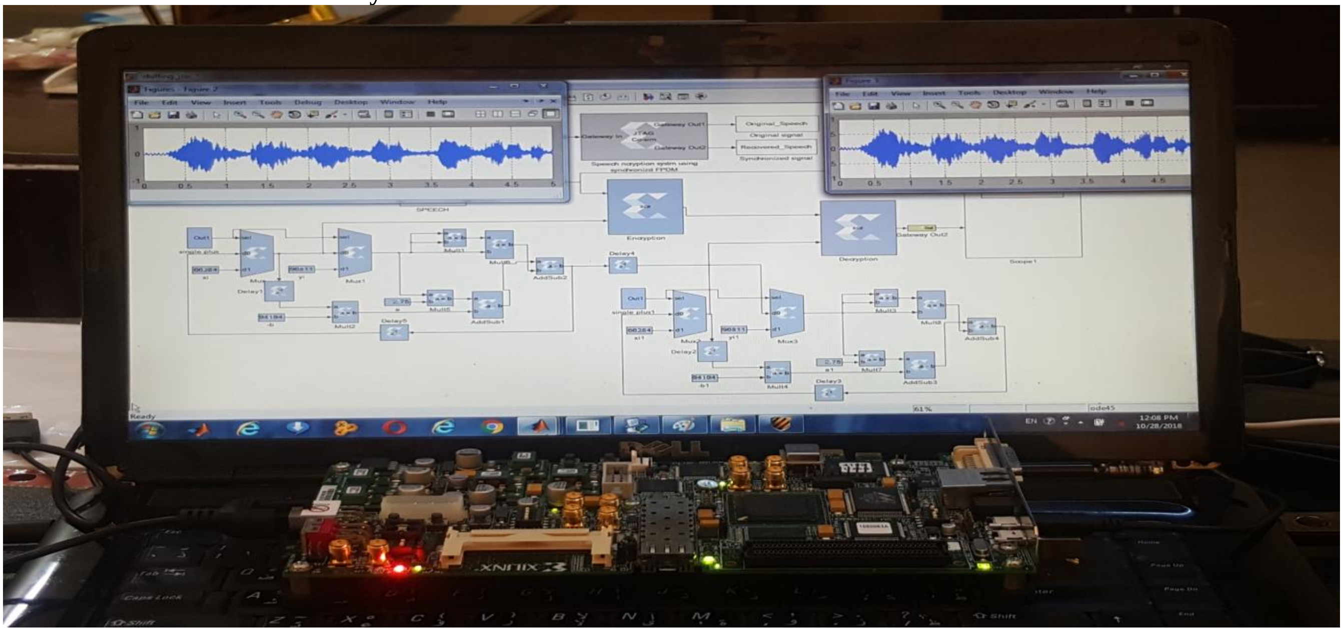

Fig. 15. continuous.

VIII. CONCLUSION

In this paper , five-different chaotic maps named “Quadratic, Logisitic, Lozi, Duffing and Henon map” are synchronized by using master-slave synchronization and used in speech encryption system. The measurment of the unintelligibilty speech signal and the master- slave error function are presented and the results show that the error is zero after a small period and the quality measures for speech are proved the randomness of the encrypted speech signal and robust against the attacker.

The FPGA hardware co-simulation reults proved that the proposed system staisfies the real time requirements and matched with the expected results.

ACKNOWLEDGMENT

This work is supported by Electrical Department/ Faculty of Engineering/ Mustansiriyah University.

REFERENCE

1. M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Bouridanec, " Synchronized hybrid chaotic generators: application to real-time wireless speech encryption," Communications In Nonlinear Science and Numerical Simulation, 2013, vol.18, no. 8, pp. 2035-2047.
2. J. Farsana and K. Gopakumar, “ A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," Procedia Computer Science, vol.93, pp. 816-823, 2016.
3. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, “Chaotic encryption of speech signals," Int. J. Speech Technol, 2011, vol.14, pp. 285-296.
4. L. S. Lee, G. C. Chou, and C. S. Chang, "A new frequency domain speech scrambling system which does not require frame synchronization," IEEE Transactions on Communications, 1984, vol. 32, pp. 444-456.
5. R. M. Milton, "A time and frequency-domain speech scrambler," IEEE, Southern African Conference on Communications and Signal Processing (COMSIG) , 1989, pp. 125-130.
6. F. Ma, J. Cheng and Y. Wang, " Wavelet transform-based analogue speech scrambling scheme," Electronics Letters, 1996, vol. *32*, no. 8, pp. 719-721.
7. G. Manjunath and G. V. Anand, "Speech encryption using circulant transformations," IEEE, Int. Conf. Multimedia and Exp, 2002 pp. 553-556.
8. A. Belmeguenai, K. Mansouri and M. Lashab, “Speech encryption using stream cipher”, British Journal of applied Science and Technology, 2015, vol. 8, no.1, pp. 107-125.
9. E. Hato, and D. Shihab, "Lorenz and Rossler systems for speech encryption," International Journal of Computer Applications, 2015., vol. 128, no. 11, pp. 25-33
10. T. Addabbo, M. Alioto , A. Fort, S. Rocchi, V. Vignoli," The digital tent map: performance analysis and optimized design as a low-complexity source of pseudorandom bits," IEEE Transactions on Instrumentation and Measurement, 2006, vol. 55, no. 5 ,pp. 1451-1458.
11. V. Patidar, K. K. Sud and N. K. Pareek "A pseudo random bit generator based on chaotic logistic map and its statistical testing," Informatica ,2008, vol. 33, pp. 441-452.
12. A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," Chaos, Solitons and Fractals, 2009, vol. 40, pp. 2557-2568.
13. P. Dabal, R. Pelka, "A chaos-based pseudo-random bit generator implemented in FPGA device," 14th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems, 2011, pp. 1-4.
14. M. Riaz, J. Ahmed, R. A. Shah and A. Hussain, " Novel secure pseudorandom number generator based on duffing map," Wireless Pers. Commun. ,2018, vol. 99, pp. 85–93.
15. M. Farouk, O. Faragallah. O. Elshakankiry, A. Elmhalaway, "Comparison of audio speech cryptosystem using 2-D chaotic map algorithms," Mathematics and Computer Science, 2016, vol. 1, no. 4, pp. 66-81.
16. V. MilanoviC and M.E. Zaghloul, "Improved masking algorithm for chaotic communications systems," Electronics Letters, 1996, vol. 32 , no. 1, pp.11-12.
17. S. B. Sadkhan, R. S. Mohammedm "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication," Procedia Computer Science, 2015, vol. 65, pp. 314-323.
18. A. Mahdi and S. Hreshee, "Design and Implenentation of Voice Encryption System using XOR based on Henon Map," IEEE, Al-Sadeq International Conf. on Multidisciplinary in IT and Comm. Science and Application (AIC-MITCSA) , 2016, pp. 1-5.
19. M. F. Abd-Elzaher, M. Shalaby, S. H. El-Ramly, "Securing modern voice communication systems using multilevel chaotic approach," International Journal of Computer Applications, 2016, vol. 135, no. 9, pp. 17-21.
20. F. S. Hasan, "Speech encryption using fixed point chaos-based stream cipher (FPC-SC)," Eng. &Tech. Journal, 2016, vol. 34, no. 11, pp.2152-2166.
21. M. K. Ibrahem and H. Kassim, "Implementation of VOIP speech system using stream cipher with Lorenz map key generator," International Journal of Scientific and Eng. Research, 2017, vol. 8, no. 7, pp.533540.
22. A. Ghasemzadeh and E. Esmaeili, "A novel method in audio message encryption based on a mixture of chaos function," Int. J. speech Technol, 2017, vol. 20, no. 4, pp. 829-837.
23. M. F. Tolba, W. S. Sayed, A. G. Radwan, and S. K. Abd-El-Hafiz, "Chaos-based hardware speech encryption scheme using modified Tent map and bit permutation," IEEE, International Conf. on Modern Circuit and System Technologies (MOCAST) , 2018, pp.1-4.
24. S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, C.S. Zhou ,” The synchronization of chaotic systems” 2002 Published by Elsevier Science B.V. Physics Reports 366 (2002) 1–101.
25. L. Merah, A. Ali-Pacha, N. Hadj-Said, B. Mecheri, and M. Dellassi, "FPGA hardware co-simulation of new chaos-based stream cipher based on Lozi map," International Journal of Eng. And Technology, 2017, vol. 9, no. 5, pp.420-425.
26. Y. Hu and P. C. Loizou, "Evaluation of objective quality measures for speech enhancement," IEEE Transactions on Audio, Speech and Language Processing, January 2008, vol. 16, no. 1, pp.229-238.
27. J. Ma and P. C. Loizou, "SNR loss: a new objective measure for predicting the inteliigibility of noise suppressed speech," Speech Communication, 2011, vol. 53, pp. 340-354.
28. P. B. J. H. M. Wilson, “Information Security Handbook: A Guide for Managers.” National Institute of standards and Technology, 2006.

AUTHORS PROFILE

Zahraa M. Alroubaie was born in Baghdad, Iraq in 1992. She received her B.Sc. degree in Computer Communication Engineering from AL-Rafidain University College, Baghdad, Iraq in 2014, her M.Sc. degree in Electronics and Communication Engineering from the Mustansiriyah University College. Her recent research activities are FPGA Hardware Co-simulation of Speech Encryption using Finite Precision Chaotic Maps Based Stream Ciphers
Email: alroubaiezahraa@gmail.com

Muneer Aboud Hashem an assistant professor in electronic engineering. He received a B.Sc., M.Sc., and Ph.D. degree in electronic engineering in 1981, 1989, and 1996, respectively all from University of Technology in Iraq. Currently, Mr. Hashem is a senior lecturer in the electrical engineering department/ collage of engineering/ Al. Mustansiriyah university in Iraq. His field of interest concerns analysis of large electronic networks, design of analog integrated circuits, and modeling of semiconductor devices.
Email: muneraboud@yahoo.com

Fadhil S. Hasan was born in Baghdad, Iraq in 1978. He received his B.Sc. degree in Electrical Engineering in 2000 and his M.Sc. degree in Electronics and Communication Engineering in 2003, both from the Mustansiriyah University, Iraq. He received Ph.D. degree in 2013 in Electronics and Communication Engineering from the Basrah University, Iraq. In 2005, he joined the faculty of Engineering at the Mustansiriyah University in Baghdad. His recent research activities are Wireless Communication Systems, Multicarrier System, Wavelet based OFDM, MIMO System, Speech Signal Processing, Chaotic Modulation, FPGA and Xilinx System Generator based Communication System. Now he has been an Assist. Prof. at the Mustansiriyah University, Iraq.
Email: fadel_sahib@uomustansiriyah.edu.iq