International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 3, June 2021, pp. 2203~2210
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i3.pp2203-2210

A new speech encryption algorithm based on dual shuffling Hénon chaotic map

Obaida M. Al-hazaimeh
Department of Computer Science and Information Technology, Al-Balqa' Applied University, Jordan

Article Info

Article history:

Received May 21, 2020
Revised Sep 23, 2020
Accepted Oct 4, 2020

Keywords:

Chaotic system
Cryptography
Hénon map
Speech signal

ABSTRACT

Over the past few decades, many algorithms have been proposed to improve the performance of speech encryption over un-secure channel (i.e., Internet). In this paper, the security level was enhanced using a dynamic dual chaotic based on Hénon chaotic map. In the proposed algorithm, the speech elements are shuffled in a random fashion. Moreover, when both Hénon state variables are free to be used for shuffling the index is toggled randomly between them according to toggle bit. After index shuffling each speech element is modified with XOR operation between the original speech element value and the key that is selected randomly from the updated key table. The same chaotic map is used to initiate the empty or full table and provide new table entries from the values that are already shuffled. The experimental results show that the proposed crypto-system is simple, fast with extra random toggling behavior. The high order of substitution make it sensitive to initial condition, common cryptanalysis attacks such as linear and differential attacks are infeasible.

Corresponding Author:

Obaida M. Al-hazaimeh
Department of Computer Science and Information Technology
Al-Balqa' Applied University
Irbid 21163, Jordan
Email: dr_obaida@bau.edu.jo

1. INTRODUCTION

Multimedia data is one of the most fundamental forms of human communications. Today, security and privacy are the two major requirements in the civilian and military applications to design and develop robustness crypto-systems for multimedia data (i.e., speech) [1, 2]. Cryptography is a technique that holds themultimedia data communications secure and incomprehensible to un-authorized access over the un-secure channel (i.e., internet) and provide many security related services (i.e., non-repudiation, authentication, and integrity) [3-5]. Generally, cryptography is classified into four categories as shown in Figure 1.

Most of the conventional cryptographic algorithms are built to protect the content test messages which are not suitable for multimedia data (i.e., speech) during communication because it involves some inherent features such as encryption and decryption process of speech is different from that test messages, and data redundancy [6]. In recent years, extensive studies have been observed in the research community to apply a various algorithms based on chaos cryptographyto design a robustness crypto-system for multimedia data due to it is desirable features such as non-linear, deterministic, aperiodicity, sensitivity to initial conditions, and un-regular behaviours (i.e., random-like performance) [6-14], but unfortunately there are fundamental drawbacks in these chaotic crypto-systems in terms of cryptanalysis attacks (i.e., low level of security, and small key space) [15, 16]. In general, chaotic crypto-systems can be classified into three categories based on their structure (i.e., analogue, or digital chaotic) each category represented by different

equations (i.e., differential, and partial differential) [11, 17-19]. Figure 2 illustrated the classification of chaotic systems with examples.

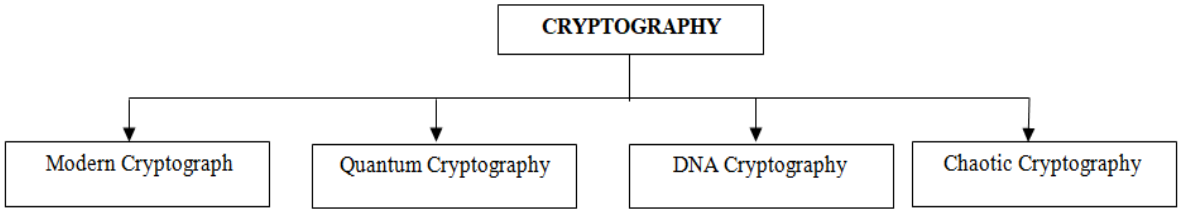

Figure 1. Classification of cryptology

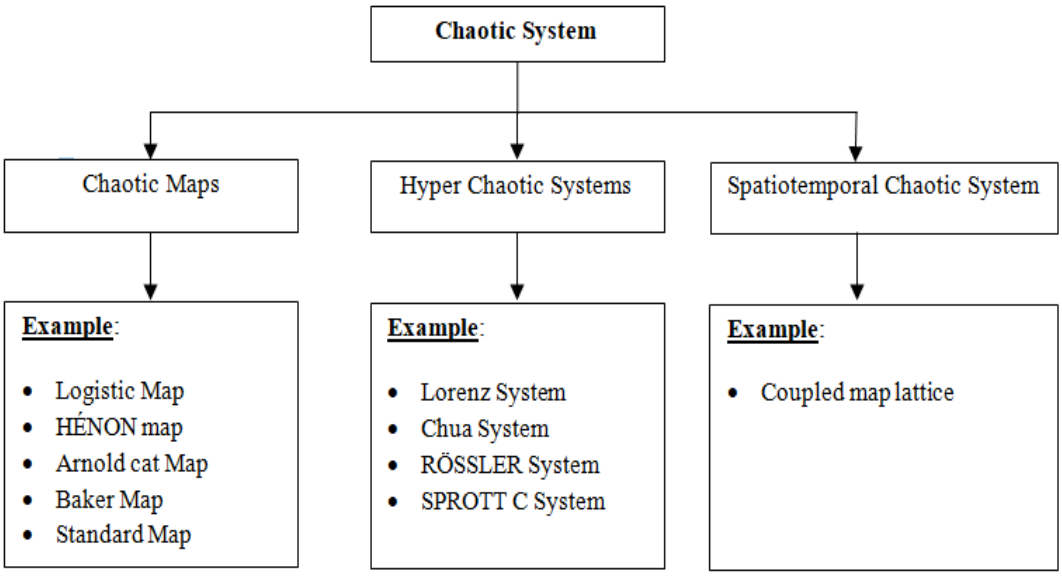

Figure 2. Categories of chaotic system

In this paper we have used chaos based cryptography (i.e., chaotic cryptography) to propose a new dynamic speech crypto-system using Hénon chaotic map to overcome the aforementioned drawbacks. The rest of this paper including the introduction is organized into seven sections as follows: Section 2 provides an overview of Hénon map. The next section i.e. section 3, describes the proposed algorithm. Section 4 presents and discusses the experimental results. Section 5 elaborates the security and performance analyses of the proposed speech crypto-system. A comparison with existing work (i.e., state-of-art) is given in section 6. The last section, i.e. section 7, concludes the paper.

2. HÉNON MAP

In the late 1946's the "Hénon map" was developed as a simplified for Lorenz map and named after its developer, M. Henon [18-20]. This chaotic map is a dynamical system (i.e., discrete-time) is presented by:

$$\begin{cases} x_{n+1} = 1 + y_n - ax^2 n \\ y_{n+1} = bx_n \end{cases} \quad (1)$$

where, the control parameters for Hénon map are a and b. This map is chaotic when a = 1.4 and b = 0.3 (i.e., classical values). In (1) exhibits a strange attractor for other control parameters values (i.e., a, and b). The chaotic attractor and the largest lyapunov exponent (i.e., maximum) of σ values for Hénon map are plotted in Figures 3 and 4.

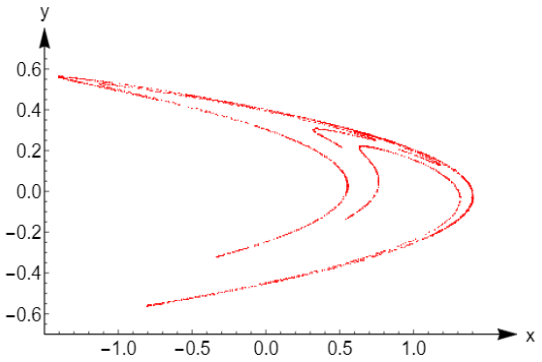

Figure 3. Chaotic attractor

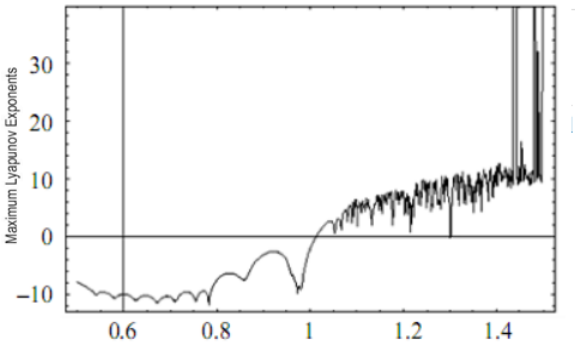

Figure 4. The plot of largest lyapunov exponents

3. PROPOSED ALGORITHM

In the proposed crypt-system, Hénon map as an example, in (1) is selected to be used from the chaotic maps in the encryption process. In Figure 5 (in Appendix) the block diagram of the proposed encryption process is presented. The proposed speech crypt-system involves a series of sequential steps are presented in Algortihm 1.

Algorithm 1: Encryption

1. Initialization. In this step, an empty cipher vector C and a flag vector F which has same length l of the one dimensional plain speech frame B_j, where $j=132$, represents the size of a 20-ms speech frame in $B = \{B_1, B_2, \dots, B_j\}$each element is an 8-bit representation of the bit 0 (BIT-0: FF81) or the bit 1 (BIT-1: 007F) of the coder parameters which is codified on 8 bits. Finally, an empty key table is created with 0 initial pointer and toggle bit is also initiated to zero.
2. The input conditions are initiated as follow ($X_{n+1} = 1 + Y_n - \alpha Xn^2$, $Y_{n+1} = \beta X_n$, with $\beta = 0.3$ and $\alpha = 1.4$), and the Hénon map is iterated 100 times to eliminate the transient effect.
3. In this step, the Hénon map is iterated once, and the result is converted into speech frame index l_j is done based on ($l_{j1}= x_{n+1}*10^{14}$ mod l, $l_{j2}=y_{n+1}*10^{14}$ mod l).
4. Test the flag bit against both $l_{j1}$and l_{j2}, if both flag bit of the 8-bit index are true (1) (i.e., exists in step 3), so, go back to the previous step (i.e., step 3). If one of them is true, the other one will be used as index for shuffling. If both flags are false, in this case the toggle bit is used to select between the two indices and the toggle bit is inverted. Otherwise, the index with false flag either l_{j1}orl_{j2} will be utilized as new location for shuffling process.
5. Here, the key table is checked, if it is empty or all its contents are used (Key_P=0 or Key_P=table size), then, a single iteration of Hénon map is performed to add a new entry to key table based on XOR operation as follow: ($l_{j1} = x_{n+1}*10^{14}$ mod 132, $l_{j2}=y_{n+1}*10^{14}$ mod 132, Key_T (Key_p+1) = $l_{j1} \oplus l_{j2}$).
6. As a next step, the current 8-bit speech element B_j is encrypted using key bit value and XOR operation, then the result is stored in the cipher vector $C(l_{jb})$ according to the shuffled location. After that, the pointer of the key table is updated and the flag bit of the encrypted element is set to 1 based on ((C_i (l_{jb}) = Key_T (Key_P)$\oplus B_j$, Key_P=Key_P+1, $F(l_{jb}) = 1$).
7. Repeat step 3 to complete encryption for all speech elements.

On the other hand, the ciphered speech elements need to receive the proposed crypto-system parameters including the generated keys (i.e., secret) and follow Algorithm 1 (i.e., encryption steps) in reverse order for decryption process.

4. EXPERIMENTAL RESULTS

In this paper, some subjective tests were conducted including several speech samples (i.e., TIMIT database) with different sampling rate (i.e., 5000 samples/sec, and 8000 samples/sec) [21]. The obtained results are presented in this sectionto demonstrate the efficiency (i.e., security level) of the proposed speech encryption algorithm. The histograms of the input speech, ciphered speech, spectrogram (i.e., original speech, ciphered, and decrypted), and the decrypted speech are presented in Figure 6. Our simulation is conducted on LENOVO E320 with a 1.8 GHz core (TM) i5-8250U CPU, 1-TB hard disk, and 4-GB RAM with MATLAB (R2013a)software.

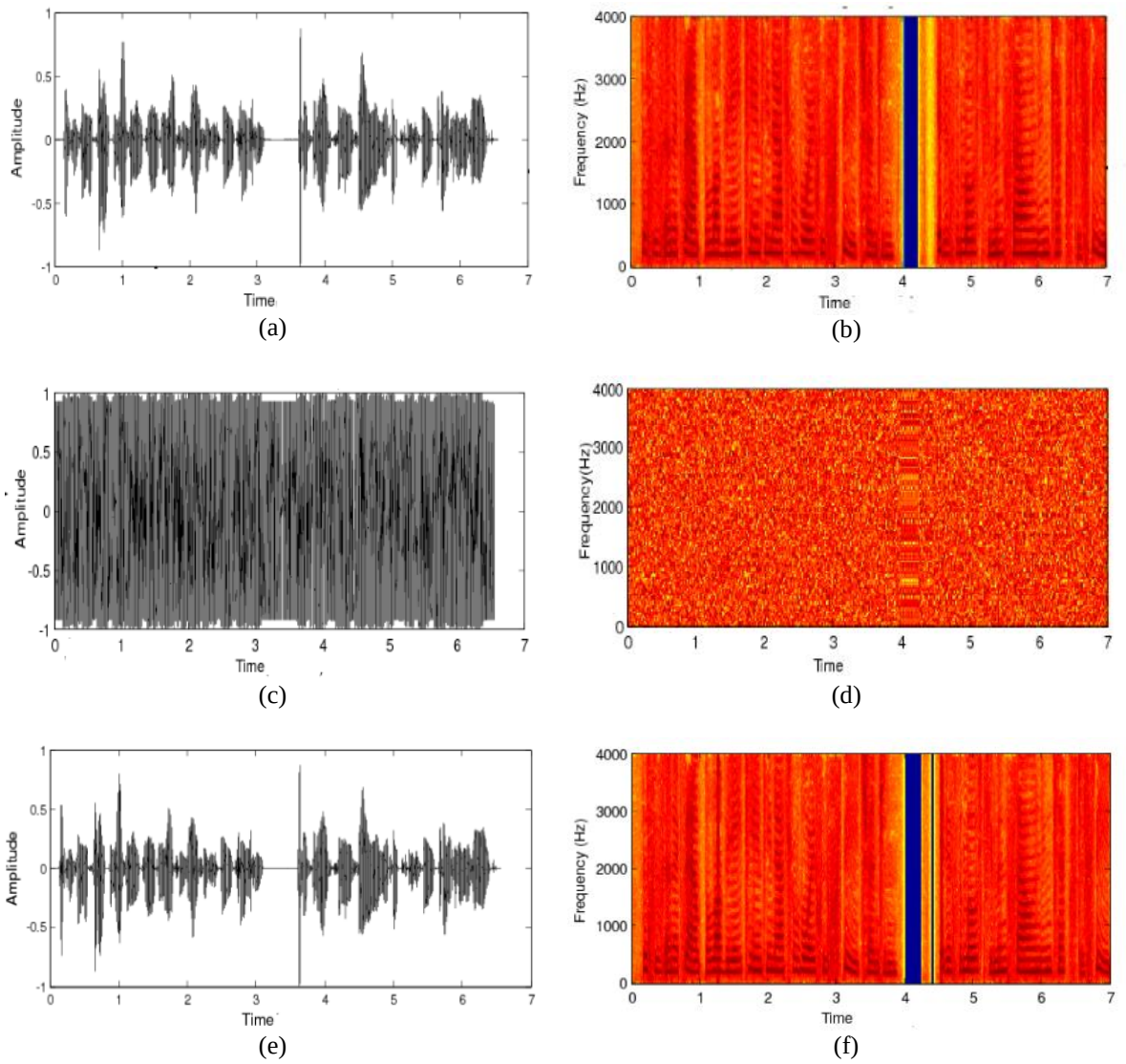

Figure 6. Histogram and Spectrogram analysis; (a) original speech, (b) spectrogram for original speech, (c) ciphered speech, (d) spectrogram for ciphered speech, (e) decrypted speech, (f) spectrogram for decrypted speech

5. SECURITY ANALYSIS

In general, the security analyses must be satisfied when a new chaotic crypto-system is proposed. A perfect chaotic crypto-system should be robust against all kinds ofcryptanalysis attacks (i.e., brute-force, statistical, etc) [22, 23]. Therefore, we have performed some security analyses to demonstrate the effectiveness of the proposed algorithm (i.e., security level). In this paper, as an example, in (2) is used to calculate the correlation coefficients.

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \;, r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (2)$$

The security tests values for different tests (i.e., correlation, ENT, DIEHARD, and NIST) are calculated and listed in Table 1. Additionally, the excellent quality of the encrypted speech must be sensitive in extreme way with respect to the secret keys [24, 25] to ensure the security procedure against brute-force attacks. In the proposed algorithm, any small variation (i.e., bit flip) on the sensitivity factors (i.e., index location, keys, and other encryption parameters) that would generate a decryption speech signals which is completely different from the original signals as shown in Figure 7.

Table 1. Security analysis

TESTS				
Correlation Test	Speech samples	Original speech	Encrypted speech	DECISION
[22, 26]	Speech_1	0.99016	0.000763	Statistical attacks - Secure
	Speech _2	0.98126	0.000829	
ENT Test	Test	Obtained value	Theoretical value	DECISION
[27, 28]	Entropy	7.989896	Close to 8	Cryptanalysis attacks -Secure
	Serial correlation	0.0000981	Close to 0	
	Chi-square coefficient	127.5007	Close to 127.5	
DIEHARD Tests	Success range	*p*-value	RESULT	DECISION
[29, 30]	0.01 - 0.99	Within the range	Passed all tests	Cryptanalysis attacks -Secure
NIST Tests	Success range	*p*-value	RESULT	DECISION
[24, 31]	0.01 - 0.99	Within the range	Passed all tests	Cryptanalysis attacks -Secure

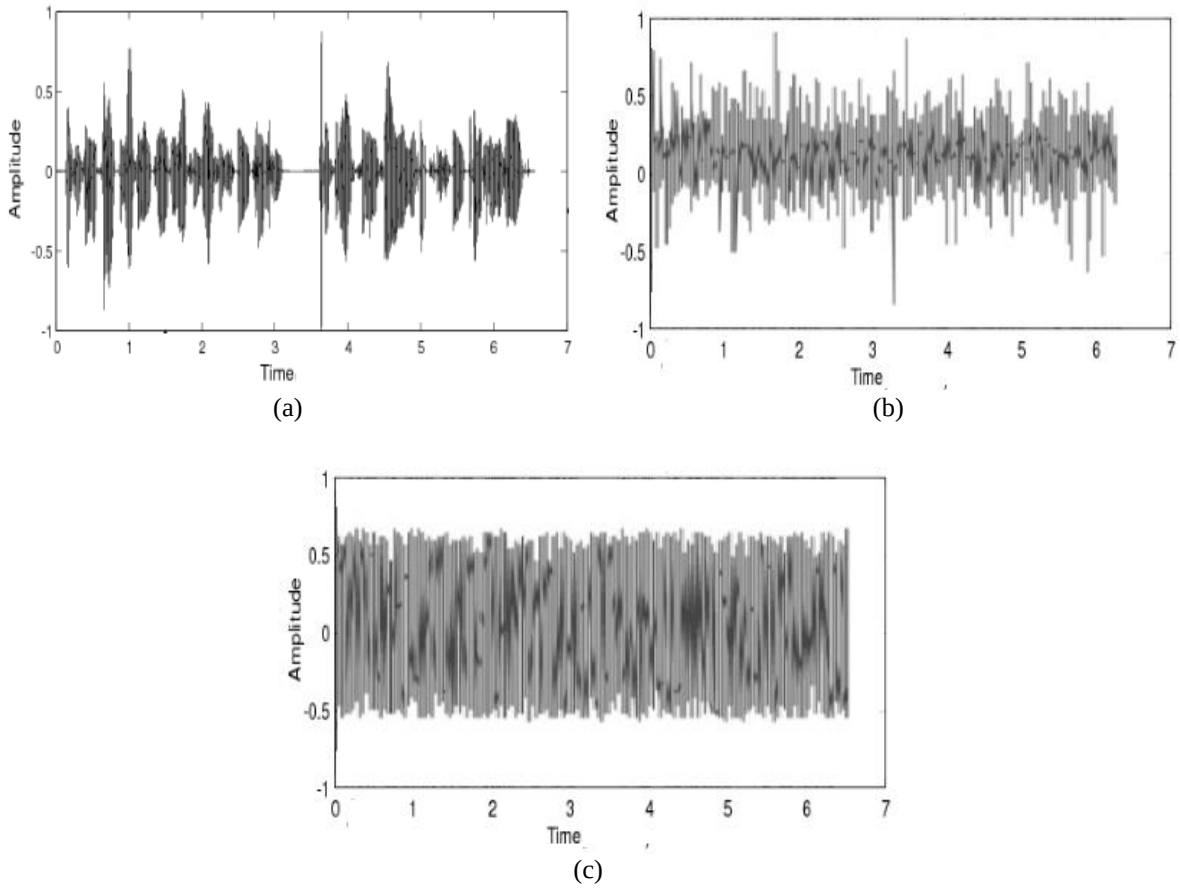

Figure 7. Sensitivity analysis, (a) original speech, (b) decryption with incorrect index, (c) decryption with incorrect key

6. COMPARISON WITH EXISTING WORKS

In this section, a comparison is made between the average time needed in our proposed speech encryption algorithm with some of existing algorithms (i.e., advanced encryption standard) in both of encryption and decryption processes (i.e., delay budget). To be more accurate, the proposed algorithm and AES have been implemented and tested and evaluated in the same environment same platform and same conditions (i.e., parameters). The results of that test are presented in Table 2. The line charts showing the relationship between the proposed algorithm delay time and AES delay time in both cases (i.e., encryption, and decryption) are shown in Figures 8 and 9 respectively.

It is clear from Table 2 the average time needed (i.e., delay time) to encrypt and decrypt the speech packet using the proposed algorithm is much smaller than that in AES algorithm. The ratio is about 1:2 which make the proposed algorithm is considered to be big for this type of application such as Internet speech applications.

Table 2. Time requirement

METHOD	ENCRYPTION		DECRYPTION	
	Trial No.	Delay	Trial No.	Delay
AES	1	1.083813452	1	1.105283425
	2	1.047655243	2	1.098274552
	3	1.088726224	3	1.100422763
	4	1.038455265	4	1.099819762
	5	1.090726228	5	1.108687613
	Average (ms)	1.069875282	Average (ms)	1.102497623
PROPOSED	Trial No.	Delay	Trial No.	Delay
	1	0.43038297	1	0.58374982
	2	0.41227197	2	0.60214912
	3	0.41497785	3	0.54877941
	4	0.39352131	4	0.60125153
	5	0.64924367	5	0.54177679
	Average (ms)	0.460079554	Average (ms)	0.575541334

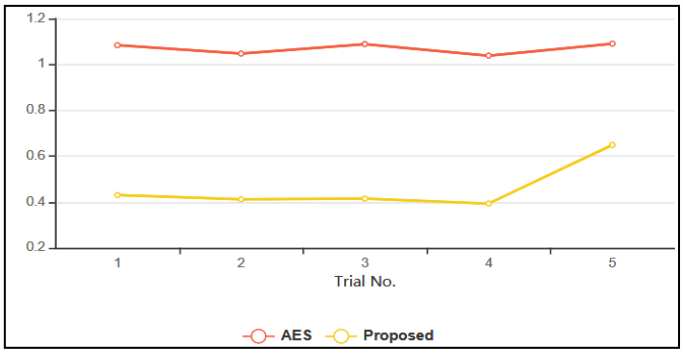

Figure 8. Average time for encryption process

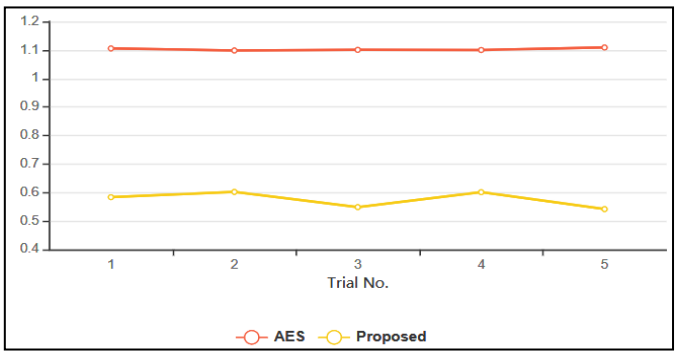

Figure 9. Average time for decryption process

7. CONCLUSION

In this paper we have achieved our objectives of proposing a new dynamic dual chaotic based on Hénon chaotic map to enhance the multimedia data services (i.e., security level, reduces delay time). Our methodology was divided into three processes: initialization for flag, Hénon map, key table, key pointer, and toggle bit and encryption and decryption process. In the encryption process, the speech elements are shuffled in a random fashion. Moreover, when both Hénon state variables are free to be used for shuffling the index is toggled randomly between them according to toggle bit. After index shuffling each speech element is modified with XOR operation between the original speech elements value and the key that is selected in a random fashion from the updated key table. The same chaotic map is used to initiate the empty or full table and provide new table entries from the values that are already shuffled. The experimental results show that the cryptanalysis attacks such as linear and differential attacks are infeasible in the proposed crypto-system. In addition, the delay budget (i.e., delay time) of the proposed crypto-system is made compare to AES (i.e., existing algorithms) and the results endorse that the proposed crypto-system has the lowest average delay time, the ratio is about 1:2.

APPENDIX

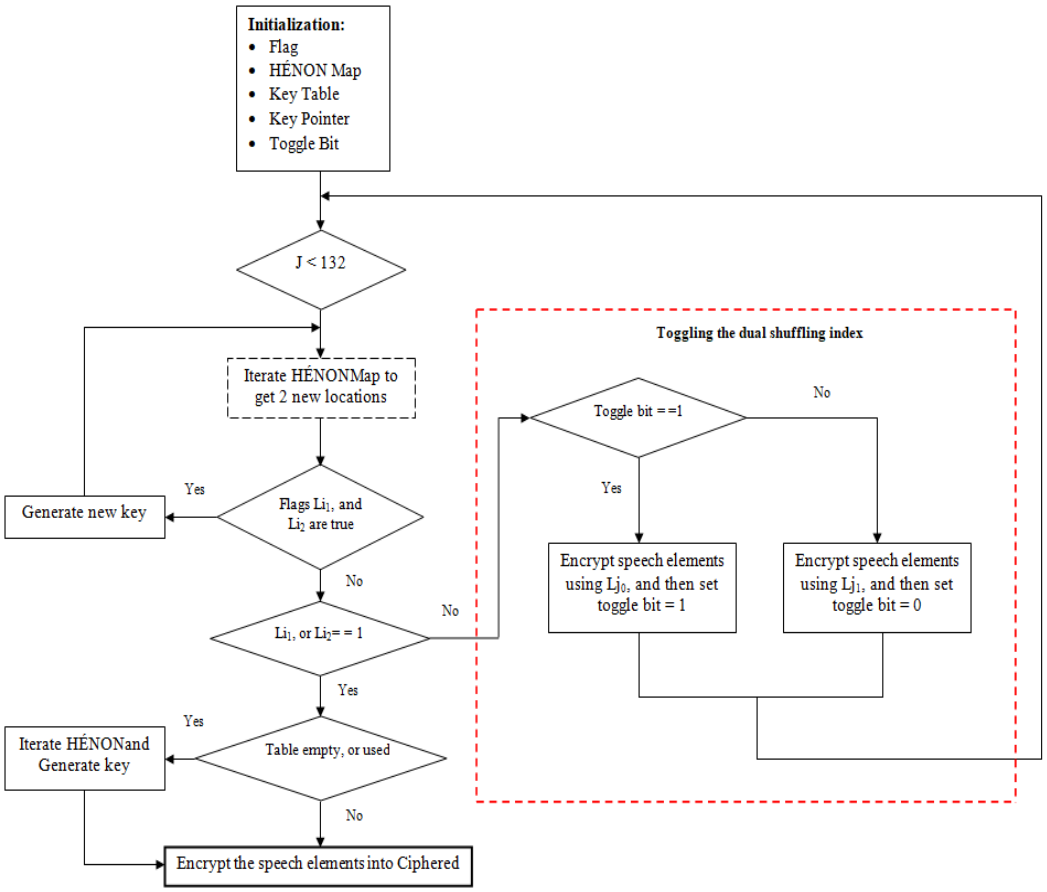

Figure 5. Block diagram

REFERENCES

[1] S. N. Al Saad and E. Hato, "A speech encryption based on chaotic maps," *International Journal of Computer Applications*, vol. 93, no. 4, pp. 19-28, 2014.

[2] K. A. Ma'moun Al-Smadi and R. A. Salama, "Dynamic Features Descriptor for Road User Recognition Using Hierarchal Graph Dynamic Gradient Pattern," *International Journal of Recent Technology and Engineering*, vol. 7, no. 6S2, pp. 414-418, 2019.

[3] O. M. Al-Hazaimeh, N. Alhindawi, and N. A. Otoum, "A novel video encryption algorithm-based on speaker voice as the public key," *IEEE Int. Conference on Control Science and Systems Engineering*, 2014, pp. 180-184, doi: 10.1109/CCSSE.2014.7224533.

[4] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, pp. 1-11, 2017.

[5] O. M. Al-hazaimeh, "A novel encryption scheme for digital image-based on one dimensional logistic map," *Computer and Information Science*, vol. 7, no. 4, p. 65, 2014.

[6] A. K. Mittal, A. Dwivedi, and S. Dwivedi, "Secure communication based on chaotic switching and rapid synchronization using parameter adaptation," *Int. J. Innov. Comput. Inf. Control*, vol. 11, no. 2, pp. 569-585, 2015.

[7] O. M. Al-hazaimeh, "A new dynamic speech encryption algorithm based on lorenz chaotic map over internet protocol," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 4824-4834, 2020, doi: 10.11591/ijece.v10i5.pp4824-4834.

[8] F. Farsana, V. Devi, and K. Gopakumar, "An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams," *Applied Computing and Informatics*, 2019.

[9] F. Farsana and K. Gopakumar, "Speech encryption algorithm based on nonorthogonal quantum state with hyperchaotic keystreams," *Advan. in Math. Physics*, vol. 2020, 2020, doi: https://doi.org/10.1155/2020/8050934.

[10] R. S. Mohammed and S. B. Sadkhan, "Speech scrambler based on proposed random chaotic maps," *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 2016, pp. 1-6, doi: 10.1109/AIC-MITCSA.2016.7759928.

[11] S. B. Sadkhan, A. Al-Sherbaz, and R. S. Mohammed, "Chaos based cryptography for voice encryption in wireless communication," *2013 Int., Conf., on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE)*, 2013, pp. 191-197, doi: 10.1109/ICECCPCE.2013.6998760.
[12] L. J. Sheu, "A speech encryption using fractional chaotic systems," *Nonlinear dynamics*, vol. 65, no. 1-2, pp. 103-108, 2011.
[13] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2017, no. 1, pp. 1-11, 2017.
[14] K. Kordov, "A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture," *Electronics*, vol. 8, no. 5, p. 530, 2019, doi: 10.3390/electronics8050530.
[15] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, "Issues and challenges in securing VoIP," *computers & security*, vol. 28, pp. 743-753, 2009.
[16] M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Bouridane, "Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 2035-2047, 2013.
[17] E. Mosa, et al, "Chaotic encryption of speech signals," *Int. Journal of Speech Technology*, vol. 14, p. 285, 2011.
[18] S. Sheela, K. Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimedia Tools and Applications*, vol. 77, pp. 25223-25251, 2018.
[19] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *Journal of Information Security and Applications*, vol. 34, pp. 142-151, 2017.
[20] V. Patidar, G. Purohit, and K. K. Sud, "Dynamical Behavior of q-deformed Henon map," *International Journal of Bifurcation and Chaos*, vol. 21, pp. 1349-1356, 2011.
[21] L. F. L. John S. Garofolo, et al., "TIMIT acoustic-phonetic continuous speech corpus," *linguistic data consortium*, 1993.
[22] J. Soto, "Statistical testing of random number generators," *Proc. of the 22nd national information sys. security conf.*, 1999.
[23] A. Mostafa, N. F. Soliman, M. Abdalluh, and F. E. A. El-samie, "Speech encryption using two dimensional chaotic maps," *2015 11th International Computer Engineering Conference (ICENCO)*, 2015, pp. 235-240.
[24] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101-111, 2014, doi: 10.1016/j.cnsns.2013.06.017.
[25] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 326-337, 2010.
[26] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 3075-3085, 2013.
[27] J. Machicao, A. G. Marco, and O. M. Bruno, "Chaotic encryption method based on life-like cellular automata," *Expert Systems with Applications*, vol. 39, pp. 12626-12635, 2012.
[28] J. S. Teh, A. Samsudin, M. Al-Mazrooie, and A. Akhavan, "GPUs and chaos: a new true random number generator," *Nonlinear Dynamics*, vol. 82, pp. 1913-1922, 2015.
[29] C. E. Shannon, "Communication theory of secrecy systems," *Bell sys., tech. journal*, vol. 28, pp. 656-715, 1949.
[30] M. M. Alani, "Testing randomness in ciphertext of block-ciphers using DieHard tests," *Int. J. Comput. Sci. Netw. Secur*, vol. 10, no. 4, pp. 53-57, 2010.
[31] M. Blaszczyk and R. A. Guinee, "Experimental validation of a novel chaotic circuit for true random binary digit generation in cryptographic module application," *Ph. D. Research in Microelectronics and Electronics*, 2009, pp. 236-239, doi: 10.1109/RME.2009.5201338.

BIOGRAPHY OF AUTHOR

Obaida M. Al-Hazaimeh received his BSc in Computer Science from Applied Science University, Jordan in 2004 and MSc in Computer science from University Science Malaysia, Malaysia, in 2006. He received his PhD degree in Network Security (Cryptography) from Malaysia in 2010. He is an associate professor at department of computer science and information technology, Al-Balqa' Applied University, Jordan. His main research interests are cryptology, image processing, machine learning, and chaos theory. He has published more than 36 papers as author and Co-author in international refereed journals.