Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 9, No. 2, March 2021, pp.510-523

Enhancement of speech scrambles using DNA technique and chaotic maps over transformation domain

Hussein A. Ismael[1], Alharith A. Abdullah[2], Zaid A. Abod[3]
[1, 2] College of Information Technology, University of Babylon, Babil, Iraq
[3] College of Food Science, Al-Qasim Green University, Babil, Iraq

ABSTRACT

This work presents and describes a new method for speech scrambles in light of chaotic maps and DNA coding. Both a wavelet transform (DWT) and Discrete cosine transform (DCT) are used to change the speech signal into another format for processing. The chaotic maps are represented by Logistic-Chebyshev map (LCH) and Random Logistic map (RLM) which are employed for generating sequences of keys that are used in the proposed system, hence the use of DNA encoding technology as an emerging technology for enhancing the security of speech. The proposed system is illustrated explicitly and tested with various security speech signals metrics, such as the coefficient, signal to noise ratio and peak signal to noise ratio. All tests of the proposed system concluded that the speech signal is reliably secure and undetectable, and hence the proposed system provides a sufficient security level.

Keywords: Speech scrambles, DNA encoding, Random Logistic Map (RLM), Logistic-Chebyshev (LCH), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT)

Corresponding Author:
Zaid A. Abod
College of Food Science
Al-Qasim Green University
Babil, Iraq.
E-mail: zaid@uoqasim.edu.iq , zaid.auw@gmail.com

1. Introduction

Security of speech communication represents a big challenge for the telecommunication, as these face the risk of different attacks. The essential tool to obtain such a security is through encryption. The encryption of speech communication needs more computation, as compared to others types of files such as pictures and texts. Therefore, the researchers proposed new ideas to produce more security with lower computation and higher speed [1]. Traditional encryption schemes do not suit speech data encryption, as they demand a longer computational time, higher power consumption, larger data size and actual timing constraint. Thus, the introduction of a novel speech encryption system of high security and speed became a major concern of research in speech communication. In [2], the authors introduced a method that made use of Logistic map to diffuse the samples, and a one dimensional circle map to confuse the samples. In [3] voice scramblers were proposed according to proposed chaotic maps. It tends to modify double chaotic maps (Chen and Lorenz) through its use as pseudorandom number generator (PR1NG). In [4], the authors presented secure improvements of voice scrambling through several chaotic maps, including three Chaotic Maps (Lorenz, Chen, Henon). The authors in

[5] introduced speech encryption based on the chaotic mapper and randomization for permutation in modern mobile applications that are used in communication systems. The researchers in [6] used the chaotic functions properties, which are improving the secureness of cryptography through a number of iterations of chaotic maps, as based on substitution and diffusion operations. In [7] the researchers proposed security system that consists of two security levels, the first being chaotic scrambling, whereas the other is chaotic masking. These two security level strengthen the encryption and thereby make key space larger than being equal to the summation of both chaotic dimensions. In [8] the researchers also proposed a security system including combinations of chaotic map based on Arnold and Lucas. This combination makes the scrambling quality stronger and hence the system better. The authors in [9] introduced a cryptosystem in light of substitution-permutation encryption structure, making use of DNA encoding at the substitution stage, in which the key generation is determined by a key-chaining algorithm for generating key block for every plain block, by means of a logistic chaotic map. Recently in [10], the author proposed security system including combination of four different techniques for audio encryption in the same scheme, namely self-adaptive scrambling, multi chaotic maps, dynamic DNA encoding and cipher feedback encrypting, and these techniques gives the system high security.

Our paper proposes an improved speech-scrambling scheme including discrete wavelet transform (DWT), discrete cosine transform (DCT), multi chaotic maps like Logistic-Chebyshev maps and random logistic maps, and dynamic DNA encoding. We used discrete wavelet (DWT) and discrete cosine transform (DCT) for transforming speech. The chaotic sequences generated by the pseudo-random numbers are based on IEEE754 single precision 64-b and were applied to the scrambling and diffusion processes. The dynamic changes of encoding, decoding, and substitution rules with DNA computing lead to the improvement of the algorithm's capability of resisting different types of attacks.

The outline of the paper can be sketched in the following way: Section 2 presents the relevant preliminary works. Section 3 presents the proposed scheme. As for Section 4, the simulation results and performance analysis are provided; Section 5 compares the proposed scheme. The concluding remarks are stated in Section 6.

2. Preliminary works

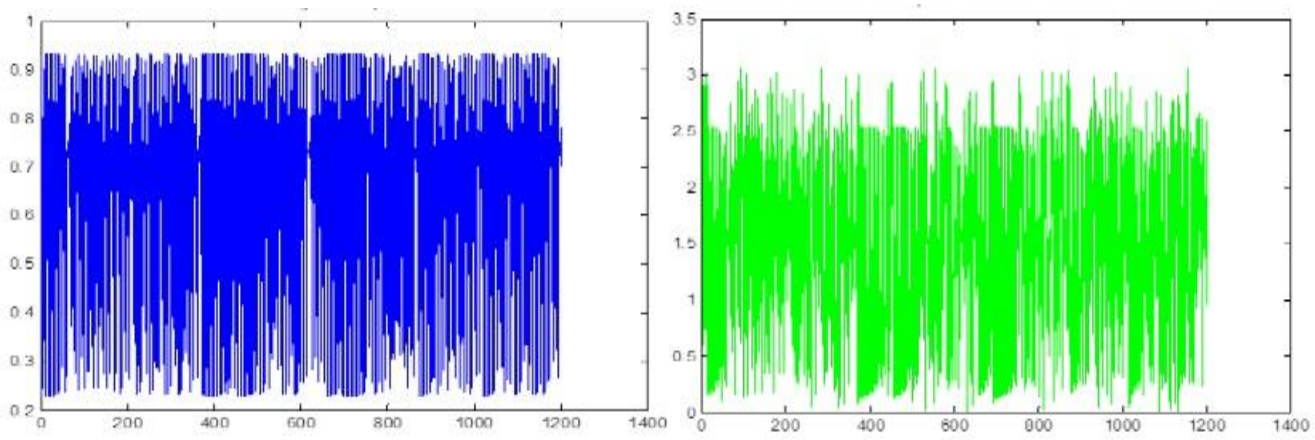
2.1 Chaotic map

The theory of Chaos describes a phenomenon which has inevitability latency rules that determine irregular appearances. It can be considered one of the hardest nonlinear problems. The origin of chaos has started in mathematics and physics and expanded into engineering. Mathematics has described that theory as 'random', which means that it results from the simple systems that are inevitability affected by the system's initial-conditions. Currently there is a significant interest in studying and applying chaotic systems, and the importance of this theory can be found in multidisciplinary areas of study such as cryptography, physics, engineering, neurophysiology, and many other fields. Chaos has a set of important properties including the sensitive, irregular, long-term prediction, deterministic, and the property of nonlinearity. Studies in the last century focused on the use of Chaos in cryptography so as to get features from which to achieve the system' security design, based on the phenomenon of chaos [11] [12]. The following subsection briefly introduces the Random Logistic Map and Logistic-Chebyshev Chaotic Map that are used for the proposed system.

2.1.1 Random logistic map (RLM)

This chaotic map is considered a modification of the Logistic map (LM) that is described in [13]. LM has a randomly property only when ($3.57 > r > 4$), as shown in Figure 1 for x. By applying the modification to LM ($\mathrm{val}_{\mathrm{Logistic}}$: x) as in (1) another expanded value ($\mathrm{X}_{\mathrm{Logistic}}$).

$$\begin{aligned} &\mathrm{Rrv}_{\mathrm{RLM}}(\mathrm{m}) = \mathrm{X}_{\mathrm{Logistic}}(\mathrm{m}) \bmod \mathrm{mean}_{\mathrm{Logistic}} \\ &\quad \text{or} \\ &\mathrm{Rrv}_{\mathrm{RLM}}(\mathrm{m}) = (\mathrm{e} + (\mathrm{f} - \mathrm{e})\mathrm{val}_{\mathrm{Logistic}}(\mathrm{m})) \bmod \mathrm{mean}_{\mathrm{Logistic}} \end{aligned} \tag{1}$$



(a) (b)

Figure 1. (a) Logistic map (b) RLM

"Fig. 1-b," shows the manipulation of (1) to LM ($val_{Logistic}$: x) by applying the (x0=0.23, r=3.738, e= -10, f=10, m=1020), and then apply (mod) to $mean_{Logistic}$ to obtain random real values Rrv_{RLM} [13]

2.1.2 Logistic-Chebyshev (LCH)

A mathematical description of this concept could be presented in the following way (2) [14]:

$$y_{i+1} = \left[\lambda y_i(1 - y_i) + \frac{(4-\lambda)\cos\left(b.arccos(y_i)\right)}{4}\right] mod\ 1 \quad (2)$$

Where $\lambda \in [0,4]$ is considered the control parameter, $y_0 \in [0,1]$ the initial condition, and b refers to the degree of Chebyshev map. It is used within proposed system for generating sequence secret keys.

2.2 DNA Encoding

The substitution method applied in the present work is the chaotic DNA transformation [15]. Two types of rules for DNA substitution are determined: binary encoding and complementary rules.

2.2.1 DNA encoding and decoding rules

The DNA sequence is made up of four bases: adenine (A), thymine (T), cytosine (C), and guanine (G). In binary, 0 and 1 are complementary. Similarly, 00 is complementary to 11, 01 is complementary to 10. Using these four bases A, C, G, and T in representing the binary numbers 00-11, there will be a total of 24 DNA coding schemes. Based on the Watson-Crick rule, only eight of them are eligible [16]. Table 1 illustrate the coding rules.

During the speech signal encrypting procedure, the binary sequence length of each sample is 32, corresponding to a DNA sequence of 16 in length. In case the sample value equals 0.1234, so the binary sequence id that belongs to it will be '0011110111111100 1011100100100111'. Whenever coded in light of DNA coding rule 3, then the DNA sequence is 'TAAGAAATCACGTCGA'. Using rule 1 for decoding it, the binary sequence is '11000001000000111000100111100100'; whereas decoding through rule 7 leads to another binary sequence, namely '01101000101010011110110001110010'.

2.2.2 DNA XOR Operations

In DNA XOR operations, there are combinations that are different from the existing binary format of 0s and 1s, as these are characterized by their reflexivity and uniqueness. The encrypting and decrypting processes for speech signals and storage in DNA sequences are of high security, due to the use of genes sequences as key values for the DNA XOR operation. The differentiates binary and DNA XOR operations were noted in Table 1, and showed different combinations of A, T, G and C letters are shown in comparison with 0/1 combinations. Eight different combinations are possible; hence this gives the current operation its uniqueness and reflexivity.

Table 1. Xor Operation with DNA

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

3. Proposed system

In this paper, the original speech is first read, after which the discrete wavelet transform (DWT) is applied to convert the speech to transform domain, and divide it into frames of 500 samples. Each frame is permuted by using Logistic-Chebyshev map. Then, a discrete cosine transform (DCT) is used on the resulted frame for the preprocessing of a speech signal, so as to get a sparse representation within the frequency domain. After that, each frame is converted to binary. On the other hand, a binary sequence of pseudo-random numbers is generated based on IEEE754 Single precision 64-bit converter, by using XOR operator between two chaotic maps Logistic-Chebyshev and Random Logistic). The XOR operator is applied between resulting key and binary frame, after which the resulted frame are coded into the DNA sequence as based on Table 2, using random key to select a rule. A sequence is generated using Logistic-Chebyshev map, which is coded into DNA based on same rule that was selected from Table 2. The XOR operation is applied between the DNA of the resulted frame and the DNA of the resulted key. Finally, the DNA sequence that results from the past stage will undergo conversion into binary bits and then into double, which represents the scrambled frame. It is them sent with the initial values and parameters of keys to the other side securely, using Diffie–Hellman (DH) method.

Table 2. Mechanism designed for DNA

Rule	A	T	C	G
Rule-1	00	11	10	01
Rule-2	00	11	01	10
Rule-3	11	00	10	01
Rule-4	11	00	01	10
Rule-5	10	01	00	11
Rule-6	01	10	00	11
Rule-7	10	01	11	00
Rule-8	01	10	11	00

The algorithms of sender and receiver side proceedings for the proposed speech scramble are shown in Figure 2 and summarized in the following algorithms:

Algorithm of sender side

Input: Speech Signal

Output: Scrambled frames, initial values and parameters of keys

Begin

Step1: Read the speech signal and apply DWT on it.

Step2: Divide the speech into frames.

Step3: For each frame in speech do:

1. Generate sequence $key1_i$ using logistic-chebyshev map.
2. Permute $frame_i$ by using sequence $key1_i$.
3. Apply DCT on $frame_i$
4. Convert $frame_i$ to binary.
5. Generate sequence $key2_i$ and sequence $Key3_i$ using logistic-chebyshev map and random logistic map and convert them to binary using IEEE754.

6. $keyR_i = key2_i$ XOR $Key3_i$
7. Apply the XOR operation between the frame and $keyR_i$.
8. Coding the sequence of binary that produced from previous step to DNA based on random key that generates values between 1 and 8 to select number of rules.
9. Generate sequence $keyD_i$ using logistic-chebyshev map and coding it to DNA based on rule that used in the previous step.
10. Apply the XOR operation between the DNA of the $frame_i$ and the DNA of the $keyD_i$.
11. Change the three initial values of $key2_i$, $Key3_i$ and $keyD_i$ depending on the previous sequence of pseudo-random numbers.
12. Convert the result to binary bits and then converts to double.
13. Send the initial values and parameters of keys to receiver by Diffie-Hellman (DH).
14. Send the scrambled $frame_i$ to receiver side.

End for.

End.

The receiver side procedures are similar to the sender side procedure, but the steps are applied by the recipient on the scramble speech signal in inverse order to acquire the speech signal, which is analogous to the original one.

Algorithm of Receiver side

Input: Scrambled frames, initial values and parameters of keys

Output: Speech Signal

Begin

Step 1: For each Received scrambled frame do:

1. Convert the $frame_i$ to binary.
2. Coding the sequence of binary that produced from step (1) to DNA based on random key that generates values between 1 and 8 to select number of rule.
3. Generate sequence keyDi using logistic-chebyshev map and coding it to DNA based on rule that used in the previous step.
4. Apply the XOR operation between the DNA of the framei and the DNA of the keyDi.
5. Generate sequence key2i and sequence Key3i using logistic-chebyshev map and random logistic map and convert them to binary using IEEE754.
6. keyRi = key2i XOR Key3i
7. Apply the XOR operation between the framei and keyRi .
8. Convert the result from previous step to double.
9. Apply IDCT on framei
10. Generate sequence key1i using Logistic-chebyshev map.
11. Re-permute framei by using sequence key1i.
12. Change the three initial values of key2i, Key3i and keyDi depending on the previous sequence of pseudo-random numbers.

End for.

Step 2: Apply DWT on scrambled speech signal to recover the original speech signal

End

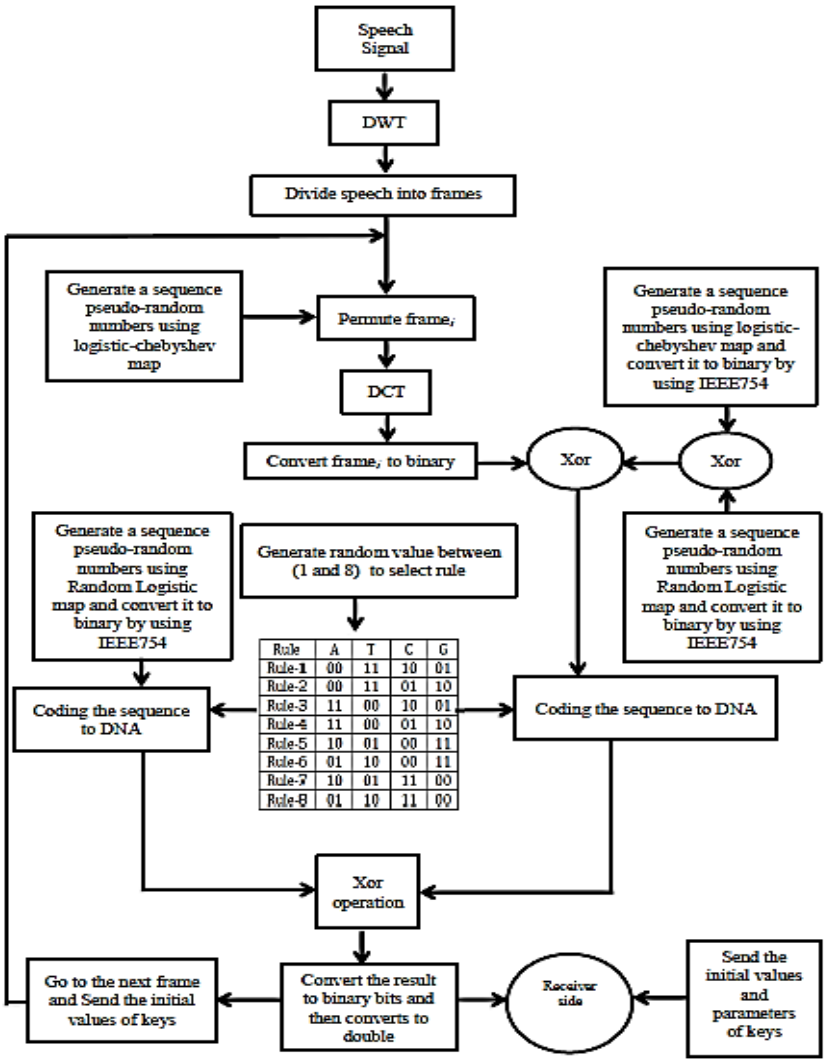
4. Experimental results and performance analysis

Several security metrics are used in this section for the verification of the scramble speech signal quality based on DNA techniques and Chaotic maps, as well as to determine the proposed system immunity. The following tests show the importance and efficiency of using the DNA technique based on chaotic maps (Random-Chebyshev and Random Logistic) on the speech scrambling, particularly in terms of security.

4.1. Residual Intelligibility

In this measure, (.wav) files have been used, which represent different men or women of different wavelengths,

sample rate (8KHz per second), number of bits (16 bit per sample), and size of frame (500 sample). One channel and several measurements are used to evaluate the proposed approach in research, including (SSNR), (CC), (SNR), (RMS) (PSNR) and (CF) measures. Table 3 shows the residual intelligibility of speech scrambling. "Fig. 3," shows the waveform of original, scrambling, and recover speech signals without noise.



Rule	A	T	C	G
Rule-1	00	11	10	01
Rule-2	00	11	01	10
Rule-3	11	00	10	01
Rule-4	11	00	01	10
Rule-5	10	01	00	11
Rule-6	01	10	00	11
Rule-7	10	01	11	00
Rule-8	01	10	11	00

Figure 2. Proposed system architecture at the sender side

Table 3. Residual Intelligibility of Speech Scrambling by the proposed system

Wav file	File length in second	SSNR	PSNR	SNR	CC	RMS	CF
Wav	4	-23.4258	-0.069325	-16.7252	-0.001399	0.9973	0.0235
Wav	8	-29.7136	-0.045691	-17.804	0.0015539	0.9972	0.0238
Wav	3	-42.2714	0.015151	-28.6611	0.00004475	0.9976	0.0208
Wav	6	-36.8306	0.017346	-29.62	-0.0000560	0.9975	0.0218
Wav	3	-32.3321	0.0040712	-24.0263	0.0002071	0.9976	0.0208
Wav	3	-33.1799	0.0062724	-24.3182	0.0022995	0.9976	0.0208
Wav	10	-37.4965	0.019364	-29.6893	0.0038132	0.9974	0.0227
Wav	7	-29.8972	-0.066579	-17.0524	-0.0030249	0.9975	0.0216
Wav	9	-29.4401	-0.02315	-20.0771	-0.003350	0.9975	0.0219
Wav	5	-30.6171	-0.077356	-16.4981	-0.0036764	0.9973	0.0232

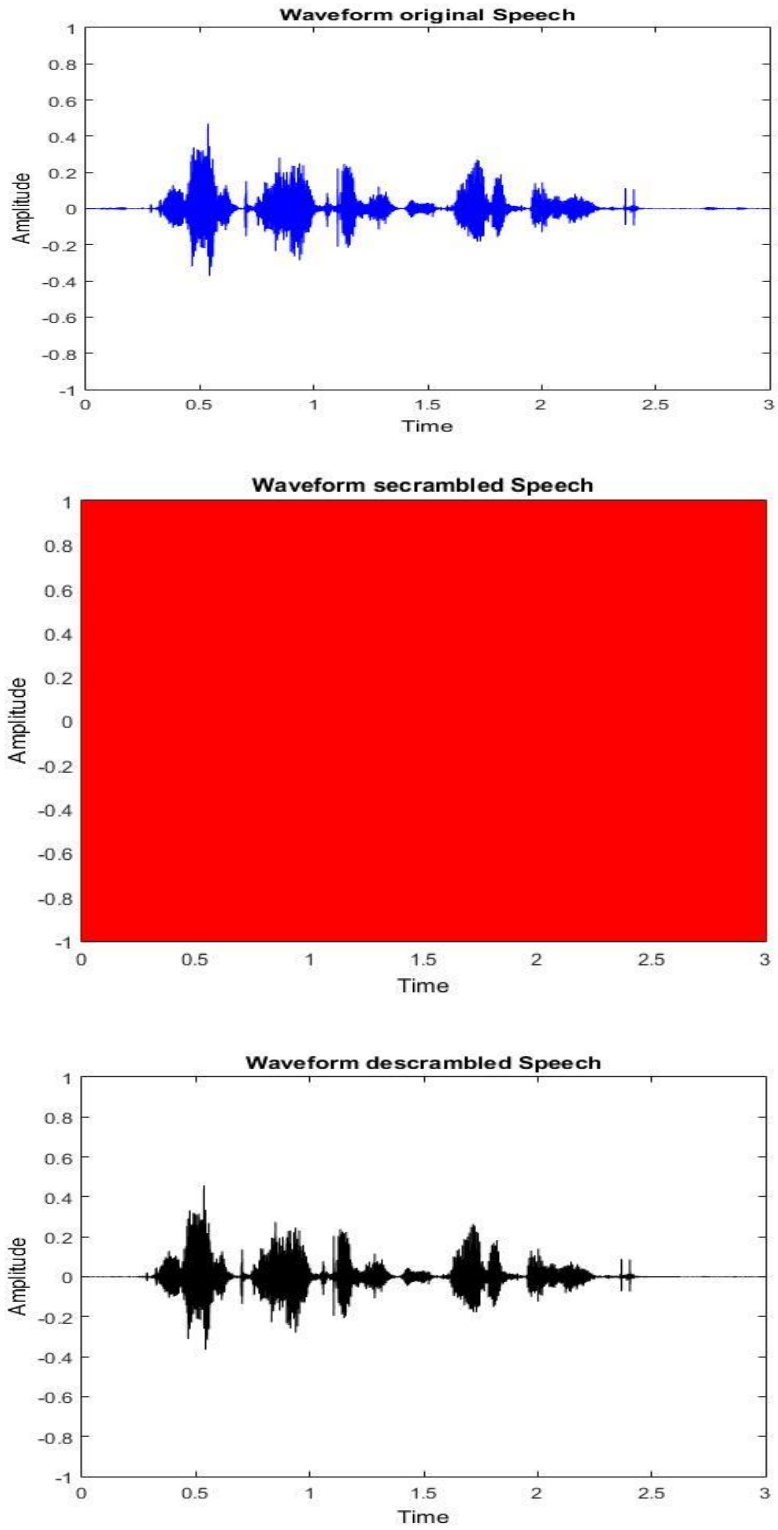


Figure 3. Waveform of original, scrambled, and recover speech signals without noise

4.2. Key sensitivity

The existence of a tiny alteration within the secret key that represents the initial value and the parameters of chaotic map, means that the scrambled speech cannot be descrambled. This research has used a chaotic map (Logistic-Chebyshev and Random Logistic) for generating the DNA sequence, which implies that the DNA sequence is very sensitive as the chaotic map is sensitive to initial condition. The proposed approach must therefore be very sensitive to key to ensure the security of the approach. Table 4 shows an impact chaotic maps

(logistic-Chebyshev and Random Logistic) as a key with very small changes through the add of 10^{-12} to initial values or k parameter on recovered speech, using several measurements mentioned above.

Table 4. The Impact of chaotic maps as a Key with slight change on Recovered Speech.

Map	Change Parameter	SSNR	Percentage difference	PSNR	SNR	CC
RLM	x_0+10^{-12}	-42.2614	100	0.029706	-28.6499	0.01071768
RLM	e+10^{-12}	-42.2593	100	0.025523	-28.6504	-0.0009514
RLM	f+10^{-12}	-42.2546	100	0.026744	-28.6446	-0.0149957
RLM	r+10^{-12}	-42.2547	100	0.033629	-28.6469	0.01337644
RLM & LCH	x_0 +10^{-12}	-42.2611	100	0.026399	-28.6505	0.00206095
RLM & LCH	y_0 +10^{-12}	-42.2621	100	0.023097	-28.651	-0.0065372
LCH	λ+10^{-12}	-42.2556	100	0.029227	-28.6451	-0.00592718
LCH	b+10^{-12}	-42.2636	100	0.026188	-28.6516	0.00483572

Fig. 4, represents the waveform of the original and recover speech signal when become very small change in secret key.

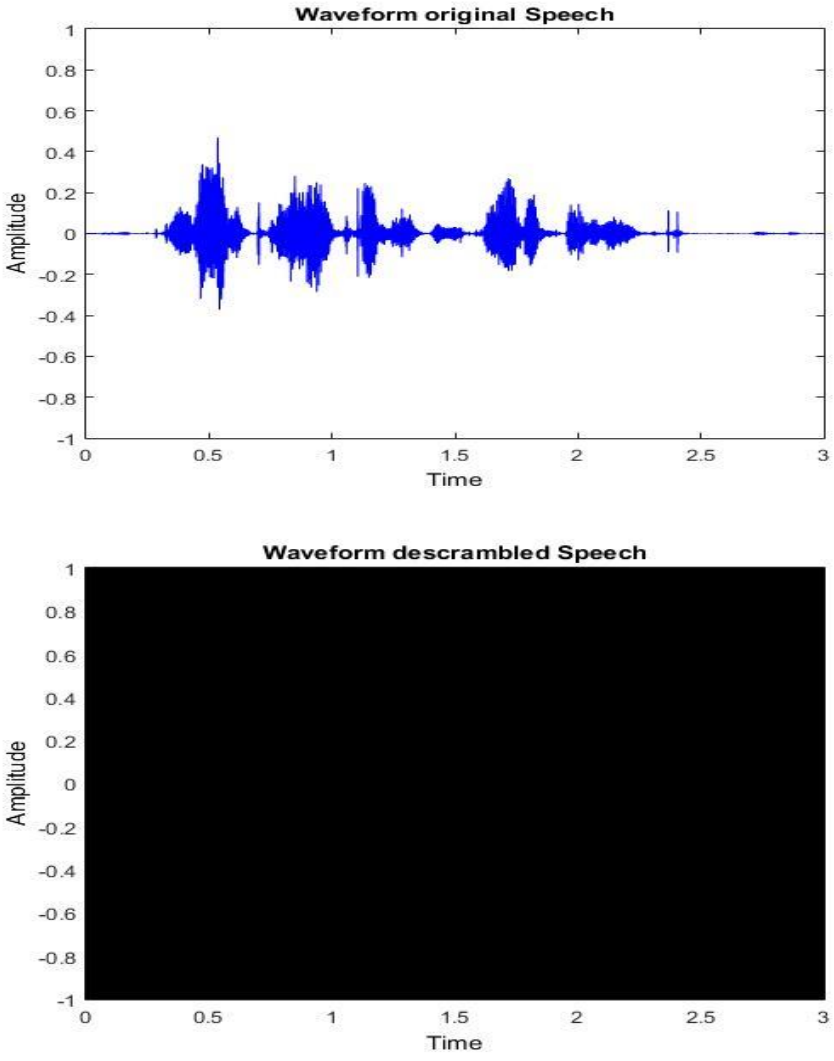


Figure 4. Waveform of the original and recover speech signals with change parameter value of random logistic map of (10^{-12})

5. Spectrogram analysis

Spectrograms can be defined as visual representations of audio file frequency spectrums as they vary over time, and the can be obtained through Fourier transform. They are represented in two dimension diagrams: time and frequency. Audio samples are divided into chunks, after which the Fourier transform is applied for computing frequency spectrum magnitudes for every chunk. Figure 5 shows the spectrogram of original, scrambled, and recover speech signals.

The results in the Figure 4 proves that the original speech signal and their scrambled versions are not similar.

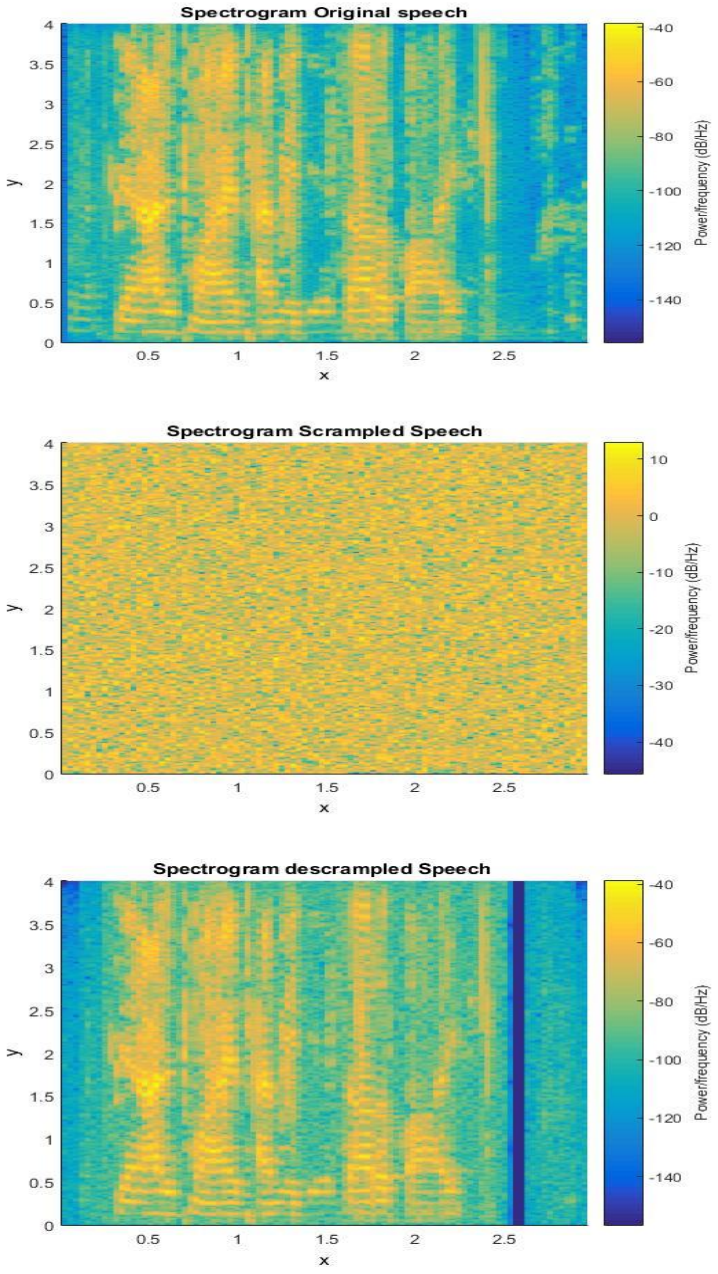


Figure 5. Spectrograms of original, scrambled, and recover speech signals

5. Histogram analysis

Histogram analysis can be used to accurately measure the quality of scrambled speech signals. A sufficient scrambled scheme needs to scramble the original speech signal to a random-like noise with sample value distributions that are almost nearly flat and could therefore face statistical attacks. Figure 6 illustrates the Histogram of the original, scrambled, and recover speech signals.

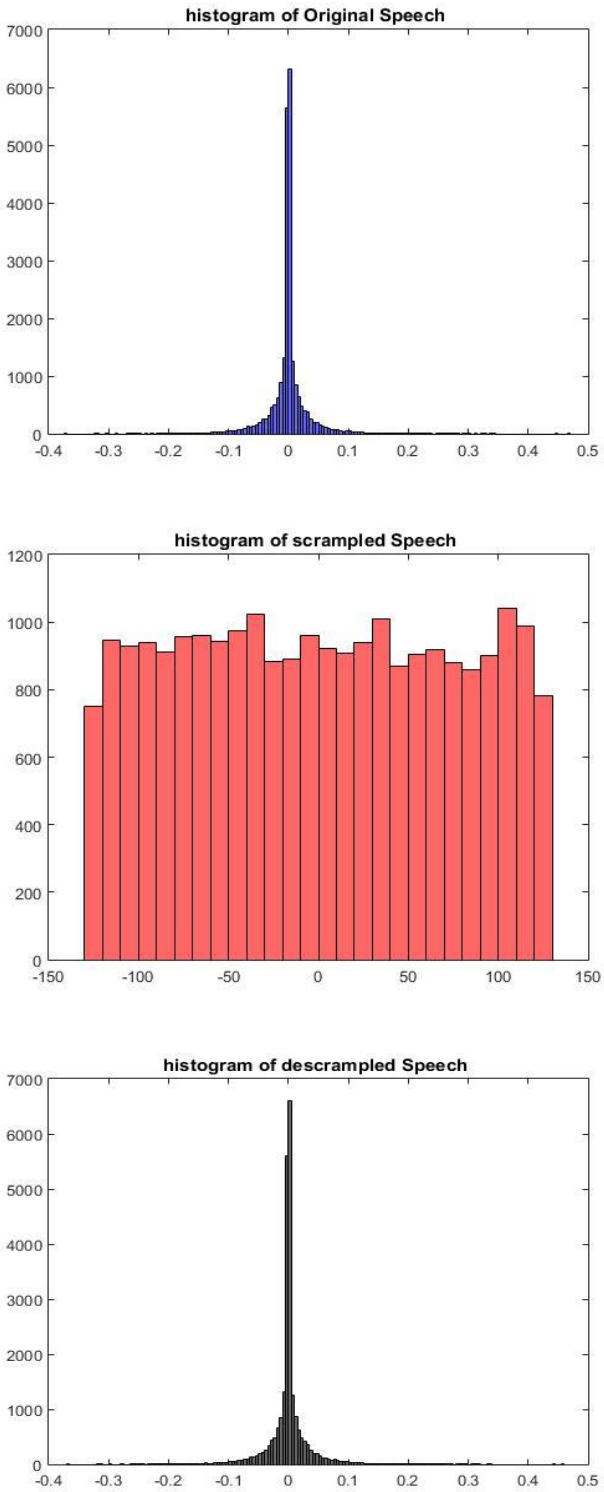


Figure 6**.** Histogram of original, scrambled, and recover speech signals

6. Correlation analysis

The correlation analysis can be defined as being one of the statistical metrics for measuring the strength of an encryption scheme against different statistical attacks [17]. In general, a measurement is made of mutual relationships shared by similar segments within the original and scrambled speech signals. A robust scrambled scheme must convert the speech signal to random-like noisy signal having a lower correlation coefficient. Figure 7 shows the correlation of the original, scrambled, and recover speech signals.

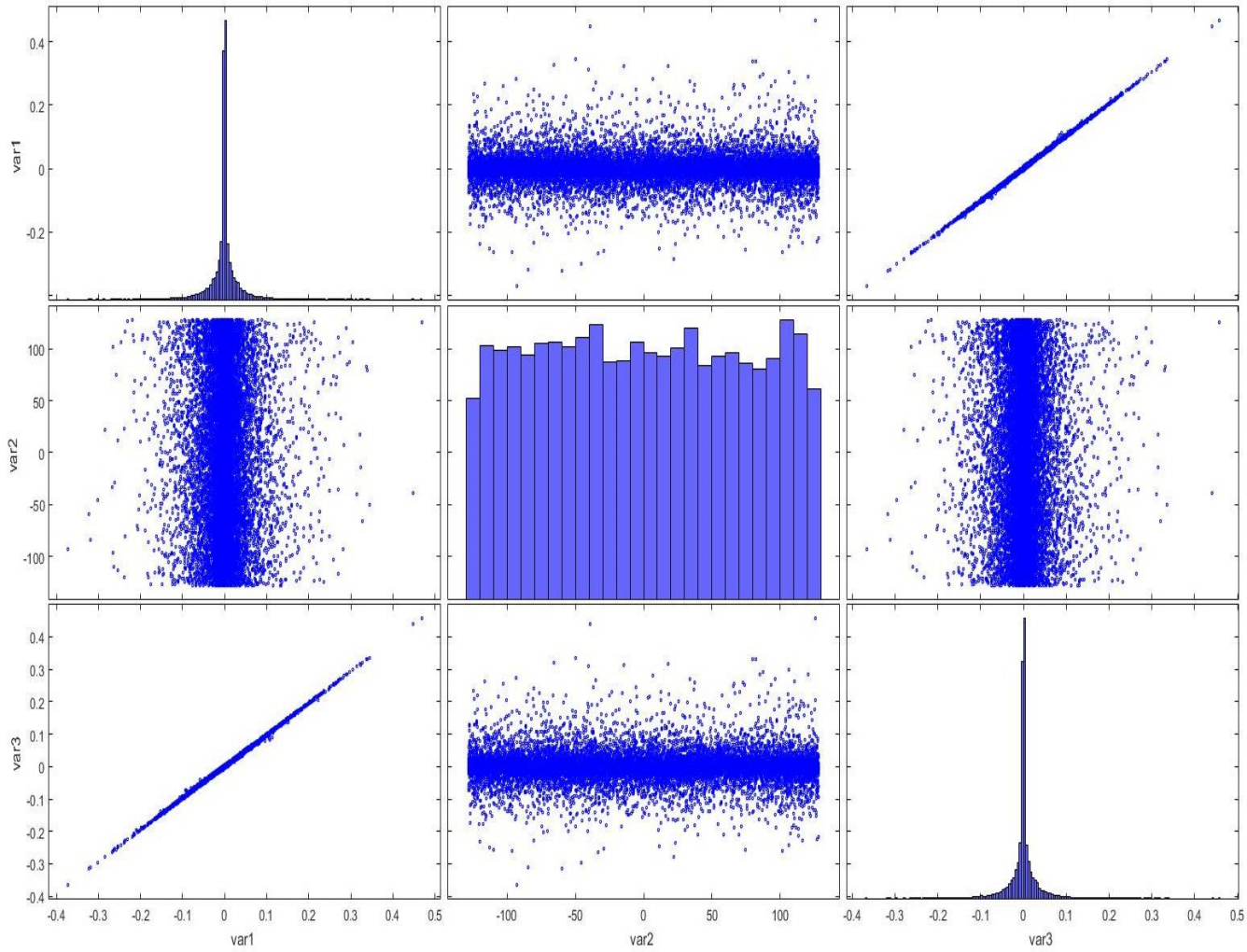


Figure 7. Correlation of original, scrambled, and recover speech signals

7. Computational time analysis

Table 5 points out the computational speeds of the proposed scheme for the ten tested wave files. It requires about 0.2344 to 0.2364 s for scrambling 1KB of data. An increase in total time results from the increase in the wave file length. As compared to the study conducted in [10], it has been proved that the proposed system is faster and could thus be used for speech data encryption.

Table 5. Computational time analysis

Wave file	Size	Total time in second	Time/KB
Wave-1	62.5 KB	14.656199	0.2344
Wave-2	125 KB	29.008634	0.2320
Wave-3	46.9 KB	11.077671	0.2361
Wave-4	93.7 kB	21.674991	0.2313
Wave-5	46.9 KB	11.206295	0.2389
Wave-6	46.9 KB	11.000351	0.2345
Wave-7	156 KB	36.080805	0.2312
Wave-8	109 KB	25.162039	0.2308
Wave-9	140 KB	32.505620	0.2321
Wave-10	78.1 KB	18.468276	0.2364

8. Comparative study

An evaluative comparison will be drawn between the capability of the proposed scheme and alternative ones in Table 6. The commonly considered security parameters like correlation coefficient (CC), signal to noise ratio (SNR), peak signal to noise ratio (PSNR), and transform domain option, will be used for the performance comparison. The results indicate that the proposed scheme has a lower value of CC among other schemes, namely 0.00004475, where a robust value of this measure is represented by low correlation coefficient. In addition, negativity of the SNR is accompanied by a scheme of greater power, and better negative SNR are obtained (-28.6611) comparing to the others schemes except for [10], where the difference is little. Moreover, for the lowest value of PSNR compared to other schemes, the difference as found to be very high (0.015151) which means that the security of encryption speech is better, compared to others schemes. Our proposed scheme also has the transform domain, which makes the system more advantageous.

Table 6. Comparison with other schemes

Scheme	CC	SNR	PSNR	Transform domain
Ref.[6]	-0.000217	-	-	No
Ref.[9]	0.000207	-	-	No
Ref.[10]	0.000053	-38.02	4.25	No
Ref.[18]	0.00035	-	4.426	No
Ref.[19]	0.00023	-23.89	-	No
Ref.[20]	0.0092	-	-	No
Ref.[21]	-0.0011	-10.63	47.98	No
Ref.[22]	0.0119	34.71	62.31	No
Ref.[23]	0.0038	-16.04	4.39	No
Proposed method	0.00004475	-28.6611	0.015151	Yes

9. Conclusion

A novel speech scrambles system determined by chaotic maps and DNA encoding has been introduced through this work. The algorithm made use of chaotic maps such as Random-Chebyshev map and Random Logistic map to generate sequence pseudo random numbers as keys. Furthermore, DNA encoding technology is integrated for increasing the security of the cryptosystem. A comparison and evaluation of the performance of the cryptosystem is made in light of the existing algorithms. The extensive simulation results illustrate how this system could scrambled differing speech signals with a high security level and thereby resist attacks. The proposed system provided relatively more security than existing algorithms. In addition, it has been proven that this model produced a secure speech signals, as the lowest value of correlation coefficient obtained is 0.00004475 and the lowest value of PSNR is 0.015151. This indicates that the suggested system is highly secure and stronger than other similar, recently presented speech encrypting schemes proposed to function against different types of attacks.

Recommendation

The speech scrambles system determined by chaotic maps and DNA encoding can be optimized by genetic algorithm [24]. Also, Internet of Thing (IoT) and cloud computing can be incorporated in this system as future work [25-27].

References

[1] A. A. Abdullah and Y. K. Abbas, "Quantum audio steganography system," *Journal of Engineering Science and Technology,* vol. 15, no. 3, pp. 1562-1588, 2020.

[2] S. M. H. Alwahbani and E. B. M. Bashier, "Speech Scrambling Based on Chaotic Maps and One Time Pad," in *INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)*, Sudan, 2013.

[3] R. S. Mohammed and S. B. Sadkhan, "Speech scrambler based on proposed random chaotic maps," in *International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, Baghdad, 2016.

[4] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," in *Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)IEEE*, Baghdad, 2017.

[5] D. G and J. Jayakumari, "Speech Scrambling Based on Chaotic Mapping and Random Permutation for Modern Mobile Communication Systems," *APTIKOM Journal on Computer Science and Information Technologies*, vol. 2, no. 1, pp. 20-25, 2017.

[6] S. J. Sheela, K. V. Suresh and D. Tandur, "A novel audio cryptosystem using chaotic maps and DNA encoding," *Journal of Computer Networks and Communications*, vol. 2017, pp. 1-12, 2017.

[7] A. K. Jawad, H. N. Abdullah and S. S. Hreshee, "Secure speech communication system based on scrambling and masking by chaotic maps," in *International Conference on Advances in Sustainable Engineering and Applications (ICASEA)*, Kut, 2018.

[8] N. A. Abbas and Z. H. Razaq, "Speech Scrambling Based on Arnold-Lucas Mapping," in *International Conference on Advanced Science and Engineering (ICOASE)IEEE*, Kurdistan Region, 2018.

[9] P. K. Naskar, S. Paul, D. Nandy and A. Chaudhuri, "DNA encoding and channel shuffling for secured encryption of audio data," *Multimedia Tools and Applications*, vol. 78, no. 17, p. 25019–25042, 2019.

[10] R. I. Abdelfatah, "Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations," *IEEE Access*, vol. 8, pp. 69894-69907, 2020.

[11] Z. A. Abod, H. A. Ismael and A. A. Abdullah, "Chaos-Based Speech Steganography and Quantum One Time Pad," *Journal of Engineering and Applied Science*, vol. 13, no. 3, pp. 739 - 745, 2017.

[12] Z. A. Abod, "A Hybrid Approach to Steganography System Based on Quantum Encryption and Chaos Algorithm," *Journal of Babylon University/Pure and Applied Sciences*, vol. 26, no. 2, pp. 280 - 294, 2018.

[13] S. R. Mohammed, An Enhancement of Some Chaotic Maps for Speech Encryption, Babylon: Babylon University, 2014.

[14] B. Abd-El-Atty, M. Amin, A. Abd-El-Latif, H. Ugail and I. Mehmood, "An Efficient Cryptosystem based on the Logistic-Chebyshev Map.," in *International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA)*, Maldives, 2019.

[15] S. Chakraborty, A. Seal, M. Roy and K. Mali, "A novel lossless image encryption method using DNA substitution and chaotic Logistic map," *International Journal of Security and Its Applications*, vol. 10, no. 2, pp. 205-216, 2016.

[16] X. Chai, Y. Chen and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in engineering*, vol. 88, pp. 197-213, 2017.

[17] D. Lambić, "Cryptanalyzing a novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 89, no. 3, pp. 2255-2257, 2017.

[18] H. Liu, A. Kadir and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and onetime keys," *Optik*, vol. 127, no. 19, pp. 7431-7438, 2016.

[19] F. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaalavsky map as pseudo random number generator," *Procedia Computer Science*, vol. 93, pp. 816-823, 2016.

[20] A. Ghasemzadeh and E. Esmaeili, "A novel method in audio message encryption based on a mixture of chaos function," *International Journal of Speech Technology*, vol. 20, no. 4, pp. 829-837, 2017.

[21] A. Belmeguenai, Z. Ahmida, S. Ouchtati and R. Djemii, "A novel approach based on stream cipher for selective speech encryption," *International Journal of Speech Technology*, vol. 20, no. 3, pp. 685-698, 2017.

[22] 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.

[23] K. Kordov, "A novel audio encryption algorithm with permutation substitution architecture," *Electronics*, vol. 8, no. 5, p. 530, 2019.

[24] Y. S. Mezaal, S. F. Kareem, “Affine Cipher Cryptanalysis Using Genetic Algorithms,” JP Journal of Algebra, Number Theory and Applications, vol. 39, no. 5, pp. 785-802, 2017.

[25] Y. S. Mezaal, L. N. Yousif, Z. J. Abdulkareem, H. A. Hussein, S. K. Khaleel, “Review about effects of IOT and Nano-technology techniques in the development of IONT in wireless systems,” International Journal of Engineering and Technology (UAE), vol. 7, no. 4, 2018.

[26] Y. S. Mezaal, H. H. Madhi, T. Abd, S. K. Khaleel, “Cloud computing investigation for cloud computer networks using cloudanalyst,” Journal of Theoretical and Applied Information Technology, vol. 96, no. 20, 2018.

[27] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, & S. F. Abdulkareem," Iraqi e-government and cloud computing development based on unified citizen identification", *Periodicals of Engineering and Natural Sciences*, vol.7, no.4, pp.1776-1793, 2019.