A Combined Chaotic System for Speech Encryption

Salah Mokhnache
EBT Department
University Ferhat Abbas Setif 1
Setif, Algeria
mokhnachesalah@yahoo.fr

Mohamed El Hossine Daachi
ETA Laboratory, Electronics Department
Mohamed El Bachir El Ibrahimi University
Bordj Bou Arréridj, Algeria
mohamed.daachi@univ-bba.dz

Tewfik Bekkouche
ETA Laboratory, Electro-mechanics Department
Mohamed El Bachir El Ibrahimi University
Bordj Bou Arréridj, Algeria
bekkou66@hotmail.com

Nacira Diffellah
ETA Laboratory, Electronics Department
Mohamed El Bachir El Ibrahimi University
Bordj Bou Arréridj, Algeria
diffellahn@gmail.com

Received: 13 March 2022 | Revised: 26 March 2022 | Accepted: 29 March 2022

Abstract-This paper presents a speech encryption scheme by performing a combination of modified chaotic maps inspired by classic logistic and cubic maps. The main idea was to enhance the performance of classical chaotic maps by extending the range of the chaotic parameter. The resulted combining map was applied to a speech encryption scheme by using the confusion and diffusion architecture. The evaluation results showed a good performance regarding the chaotic behaviors such as initial value, control parameter, Lyapunov exponent, and bifurcation diagram. Simulations and computer evaluations with security analysis showed that the proposed chaotic system exhibits excellent performance in speech encryption against various attacks. The results obtained demonstrated the efficiency of the proposed scheme compared to an existing valuable method for static and differential cryptographic attacks.

Keywords- speech encryption; chaos; modified chaotic maps

I. Introduction

The development of technologies and means of communication puts in danger data transfers and confidential information in communication networks. As much information is transmitted over these networks in the form of verbal communications, the protection of voice communications pushes toward the search for new security techniques. Cryptographic techniques are used to improve security by converting speech into an unintelligible form to an unauthorized person [1-3]. Speech signal encryption has emerged as one of the most widely used techniques to ensure the security of verbal transmissions. Various standards and protocols involving cryptography have been proposed to deal with information security issues, such as speech encryption algorithms like the Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and the RSA algorithm [4-5].

Each standard encryption technique has its advantages and disadvantages, but the distribution of encryption keys remains unresolved by these cryptographic techniques. Chaotic cryptography appears as a good alternative to resolve this situation, as it offers great sensitivity and a large space of encryption keys. The appearance of chaotic cryptography [6], which defines a particular state of a nonlinear dynamic system whose behavior is never repeated, very sensitive to initial conditions, and unpredictable in the long term, gave new life to speech encryption systems [7-8] by applying chaotic maps of one, two, or three-dimensions [9,10]. Despite the success of chaotic map-based methods, they remain vulnerable to the narrow range of control parameters and the sensitivity of secret keys. Several algorithms combining chaotic maps have been proposed to expand the range of control parameters and reinforce the sensitivity of secret keys [11-12]. In this perspective, enhanced chaotic maps inspired by classic chaotic ones, such as Logistic and Cubic maps, were proposed in [13]. This approach introduced the composition of each sequence with the exponential function and then applied the arithmetic modulo to unity. The resulting new chaotic sequences were applied in a speech encryption scheme, jointly in the confusion and diffusion phases.

This study examines a speech encryption scheme by combining Logistic and Cubic maps. The performance of the chaotic sequences of Logistic and Cubic maps and their combination was examined, concerning the sensitivity of the initial value, bifurcation diagram, and Lyapunov exponent [14]. Moreover, the proposed method was simulated and experimental results were obtained concerning the estimation of different evaluation metrics. Furthermore, the behavior facing brute force attacks was also discussed by comparing the proposed with an existing valuable method.

II. The Proposed Enhanced Chaotic System

The combination of chaotic maps into a non-linear combination of two different chaotic maps can be represented as a single chaotic one by the expression:

$$x_{n+1} = A_{FG} = \big(F(a, x_n) + G(b, x_n)\big)\, mod\ 1 \quad (1)$$

Corresponding author: Salah Mokhnache

where $F(a, x_n)$ and $G(b, x_n)$ are two 1-D chaotic maps with parameters a and b, and n is the iteration number [15]. The proposed combination of chaotic systems is based on Logistic and Cubic maps, defined as follows:

A. Logistic Map

The Logistic map is one of the famed chaotic functions that have been studied for cryptography applications. The logistic function is expressed as :

$$x_{n+1} = r.x_n.(1 - x_n) \quad (2)$$

where x_n takes values in the [0, 1] interval and the parameter r is a positive constant taking values up to 4. Its value determines and explores the behavior of the logistic map. From r = 3.57, the iterations become chaotic.

B. Cubic Map

The Cubic map is another shape of the most commonly used chaotic maps to generate chaotic sequences. It is one of the most used maps in cryptographic applications. This map is formally defined by:

$$x_{n+1} = r.x_n.(1 - {x_n}^2) \quad (3)$$

where r is its parameter and x_n is a system variable whose value is (0, 1) $\forall\, i \geq 0$. This method shows chaotic dynamics for 2.3< r <2.6.

C. Combined Chaotic Map

The proposed chaotic system is a combination of Logistic and Cubic maps by introducing the composition of each sequence with the exponential function and then applying the arithmetic modulo to unity. The subtraction between logistic and cubic maps gives a new chaotic system, expressed as:

$$x_{n+1} = r.e^{2x_n}.(e^{x_n} - 1)\, mod\, 1 \quad (4)$$

D. Lyapunov Exponent

The study of the stability of a dynamic system uses the plot of the Lyapunov exponent, which allows locating the stable and the chaotic zones to quantify the stability or the instability of its movements. When the Lyapunov exponent has a positive value, it describes a chaotic zone and the system will be unstable. The performance of the dynamic system is related to the quantized values of the exponent. When the quantized value is large, the chaotic performance will be better. As shown in Figure 1(d), the Lyapunov exponents of the logistic map are negative when r < 3.57. For the Cubic map, the Lyapunov exponent values are less than zero when r < 2.3. This means that the systems governed by these two maps do not exhibit any chaotic behavior below these values. Figure 2 shows the plot of the Lyapunov exponent of the proposed chaotic map. Unlike the Logistic and the Cubic sequences, the combined presents a positive value of the Lyapunov exponent over the entire interval of the control parameter. This shows the improvement of the proposed system's performance by the expanse of the range of the chaotic parameters.

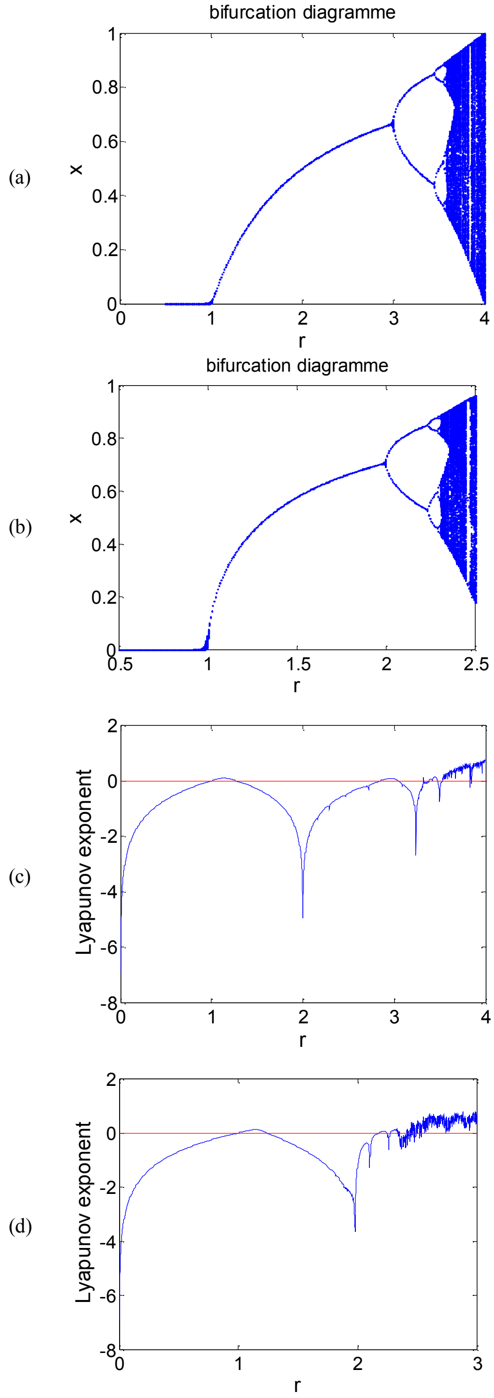

Fig. 1. Bifurcation diagrams for (a) Logistic and (b) Cubic maps – Lyapunov exponents for (c) Logistic and (d) Cubic (d) maps.

E. Bifurcation

Changes in the parameters of linear dynamical systems cause quantitative changes but do not modify the behavior of the system. In nonlinear dynamic systems, a small variation of certain parameters, called control parameters, can under well-defined conditions cause a complete change in the system's behavior at equilibrium. These are transitions of dynamic systems into chaotic states, also called bifurcations. The bifurcation diagram is one of the tools to locate the zones of the chaotic behavior of a dynamic system, and according to Figures 1(a), (b), which present the bifurcation diagrams of the Logistic and the Cubic maps, it is noted that the chaotic ranges of both maps are limited. Figure 1(a) shows that the chaotic range of the Logistic sequence is limited in the [3.57, 4.0] interval and that the control parameter *r* under this range cannot have chaotic behaviors. The Cubic sequence has a limited chaotic range between [2.3, 2.6]. The bifurcation diagram of the proposed combination in Figure 2(b) shows a very wide chaotic range with an invariant uniform distribution over the entire definition interval of the control parameter.

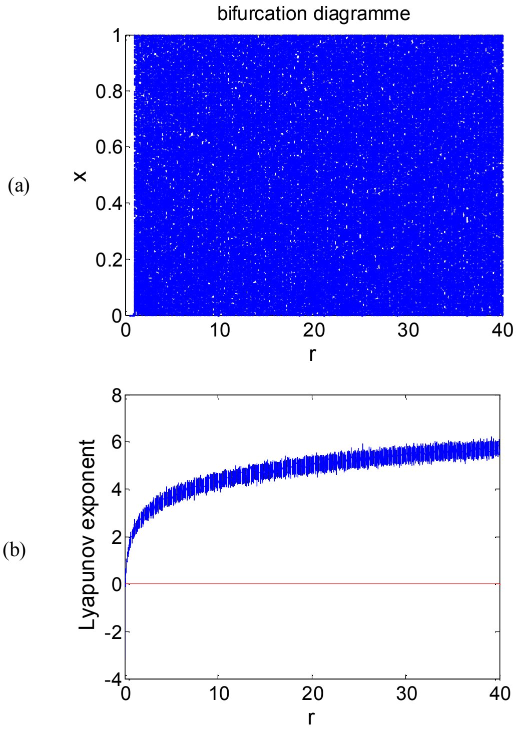

Fig. 2. (a) Bifurcation diagram and (b) Lyapunov exponent of the proposed chaotic map.

F. Sensitivity of Initial Conditions

Chaotic systems are extremely sensitive to disturbances. This fact was illustrated by the butterfly effect, popularized by Edward Lorenz [16]. A chaotic dynamical system is unpredictable and sensitive to initial conditions. Thus, two trajectories of initially neighboring phases deviate more quickly from each other, regardless of their initial proximity. The impact of the sensitivity to the initial conditions can be highlighted by a simulation by assigning two very close initial conditions to the proposed combined system. At first, the two systems evolve similarly, but soon their behavior becomes different, as shown in Figure 3 for two close initial conditions x_{01}= 0.58 and x_{01} = 0.58 + 10^{-16}.

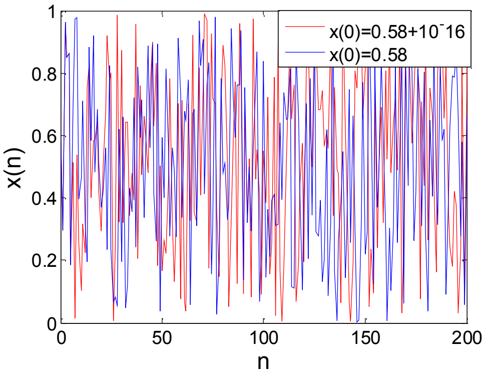

Fig. 3. Evolution of the proposed combined map for two very close initial conditions x_{01} = 0.58 (blue) and x_{01} = 0.58+10^{-16} (red).

III. THE PROPOSED VOICE ENCRYPTION SCHEME

This section presents the proposed encryption scheme and the details of its algorithm based on the combined model of the two chaotic maps and following its temporal evolution which reveals a purely chaotic behavior.

A. Encryption Process

The encryption process is illustrated in Figure 4 and consists of the following steps:

- Step 1: Reading or recording the original speech signal.
- Step2: Generation of a chaotic vector using the combined chaotic system based on Logistic and Cubic maps with an initial condition x_{01} and a control parameter r_{01}.
- Step 3: Arrange the chaotic vector in descending order to form a permutation vector.
- Step 4: Scramble the speech signal using the permutation vector for random changing the positions of the segments of the speech signal according to the generated chaotic vector.
- Step 5: For the diffusion phase, another chaotic vector is generated based on the same combination of Logistic and Cubic maps, with other parameters, initial condition x_{02} and control parameter r_{02}, to increase the sensitivity of the secret key and multiply the elements of this vector by 255.
- Step 6: Execute the XOR operation bit by bit between the generated chaotic and the permuted vector.
- Step 7: Obtain and extract the output encrypted speech.

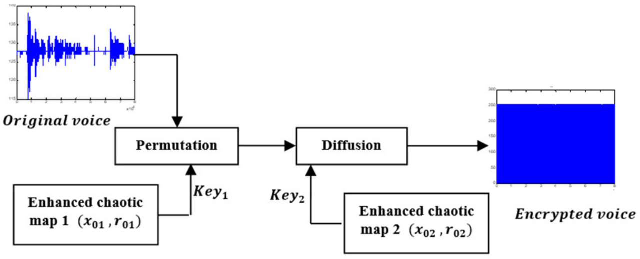
Original voice
Permutation
Diffusion
Encrypted voice
Key_1
Key_2
Enhanced chaotic map 1 (x_{01}, r_{01})
Enhanced chaotic map 2 (x_{02}, r_{02})

Fig. 4. Block diagram of the proposed encrypted voice scheme.

B. Decryption Process

After the acquisition or loading of the encrypted signal, the operation takes the same path as the encryption process, but in a reverse way.

IV. Simulation Results

MATLAB R2014 was used to perform the simulations. Various tests were performed to demonstrate the performance and security of the proposed system, such as waveform, spectrogram analysis, SNR, and correlation tests. Speech signals having an 8kHz sampling frequency with 8 bits per sample were used as test files. The improved chaotic map parameters were: x_{01} = 0.41 , x_{02} = 0.51, r_{01}= 40.31, and r_{02}= 50.31.

A. Waveform and Spectrogram

A visual examination of descriptive acoustic analysis of speech can be performed in two ways: the waveform in the time domain and the energy distribution in the time-frequency plane. The prototype of the energy representation is the spectrogram. As shown in Figures 5 and 6, the waveform and spectrogram of the encrypted signal were uniformly distributed and very different from those of the original signals. The intelligibility was destroyed, and the original signal became completely unintelligible.

B. Signal to Noise Ratio (SNR)

The signal-to-noise ratio (SNR) metric is an efficient estimator to measure the intelligibility of a speech signal [17-19], and it is defined as the average of the SNR values of short segments of the output signal as:

$$SNR = 10log_{10}\frac{\sum_{i=1}^{N_s} x^2(i)}{\sum_{i=1}^{N_s}(x(i)-y(i))^2} \quad (5)$$

where $x(i)$ is the original speech, $y(i)$ is the decrypted speech signal, and N_s is the number of samples. As SNR decreases, the higher is the quality of the encrypted signal.

C. Correlation Analysis

The correlation coefficient is an effective metric to measure encryption quality. The correlation coefficients for original signals are close to 1, which shows that the samples are strongly correlated, while for encrypted signals the correlation coefficients are close to 0, as there is no correlation between the original and the encrypted signal. This confirms the quality of the encryption process since there is no similarity between the original and the encrypted signals. The correlation coefficient is given by [19]:

$$r_{xy} = \frac{cov(x,y)}{\left(\sqrt{var(x)}\sqrt{var(y)}\right)} \quad (6)$$

$$cov(x,y) = \frac{1}{N_s}\sum_{i=1}^{N_s}\big(x(i)-E(x)\big)\big(y(i)-E(y)\big) \quad (7)$$

$$E(x) = \frac{1}{N_s} \quad (8)$$

$$var(x) = \frac{1}{N_s}\sum_{i=0}^{N_s}\big(x(i)-E(x)\big)^2 \quad (9)$$

where N_s is the number of speech samples involved in the calculations, $cov(x,y)$ is the covariance, $E(x)$ is the expected value of x, and $var(x)$ is the variance. The correlation and the SNR analysis results are illustrated in Table I. The values of the correlation coefficient r_{xy} between the original and the encrypted signals were very low, and the same remark is noted for the values of the SNR metric, indicating that the encrypted signal is highly noisy. During the decryption phase, the correlation coefficients between the original and corresponding decrypted speech reveal values equal to unity, which confirms the strong resemblance between the signals. However, the measurements of the SNR coefficients are high positive, which indicates a very good quality of the recovered speech signals.

TABLE I. QUALITY OF ENCRYPTED AND DECRYPTED VOICE SIGNALS

Speech files	SNR (in dB)	r_{xy}
	Encrypted/Decrypted	Encrypted/Decrypted
Signal 1.wav	-10.4925/39.2841	0.0032/1
Signal 2.wav	-11.3701/45.1425	0.0012/1
Signal 3.wav	-11.8293/39.8948	-0.0002537/1
Signal 4.wav	-16.3239/40.6553	-0.0002593/1
Signal 5.wav	-14..3535/43.1726	-0.0052/1

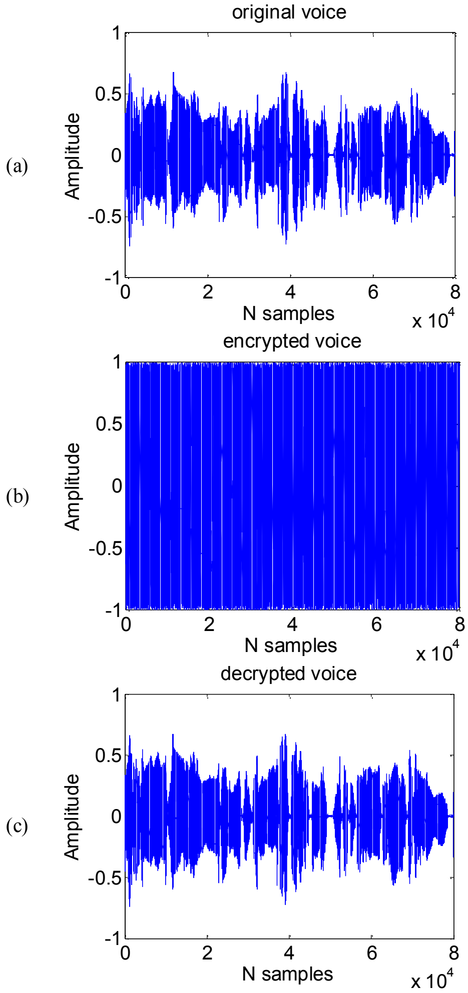

Fig. 5. Waveform plot of: (a) original voice, (b) encrypted voice, and (c) decrypted voice.

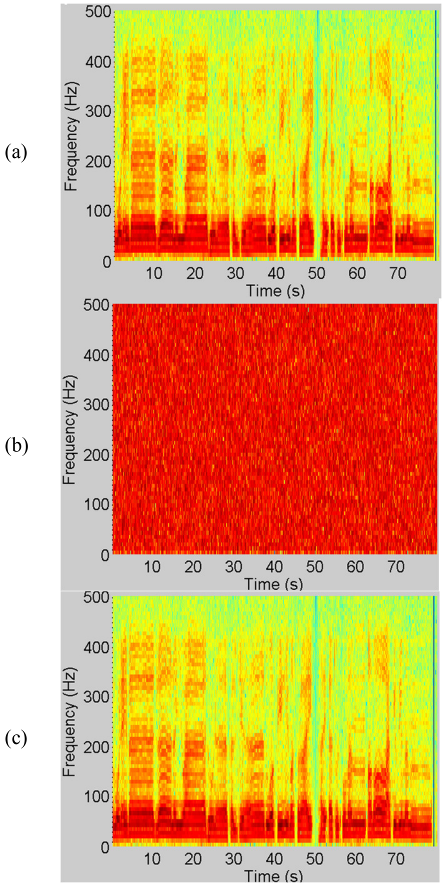

Fig. 6. Spectrogram plot of (a) original voice, (b) encrypted voice, and (c) decrypted voice.

D. Key Space Analysis

In general, the accepted keyspace of an encryption algorithm must be larger than 2^{100} to thwart brute-force attacks. The proposed system has two keys with initial conditions and control parameters (x_{01}, x_{02}, r_{01}, and r_{02}). The proposed system has 10^{16} precision for both initial conditions and 10^{14} for both control parameters. So the total keyspace is $10^{16\times2}\times10^{14\times2} \cong 2^{180}$. This confirms that the proposed approach is highly efficient against brute-force attacks.

E. Key Sensitivity Analysis

A reliable speech signal encryption approach must be sensitive to the slightest change in the secret key, i.e. changing a single value in the secret key must produce a completely different encrypted signal. Keys for encryption (x_{01}, r_{01}) and decryption (x_{02}, r_{02}) were examined to demonstrate the sensitivity of the proposed approach. The results shown in Figure 7 indicate that if the sender's keys are identical to the receiver's, the decrypted signal is identical to the original, but if a minor change in the parameters occurs, the decrypted image in each case is still completely unknown, although the change made in the parameters is very small.

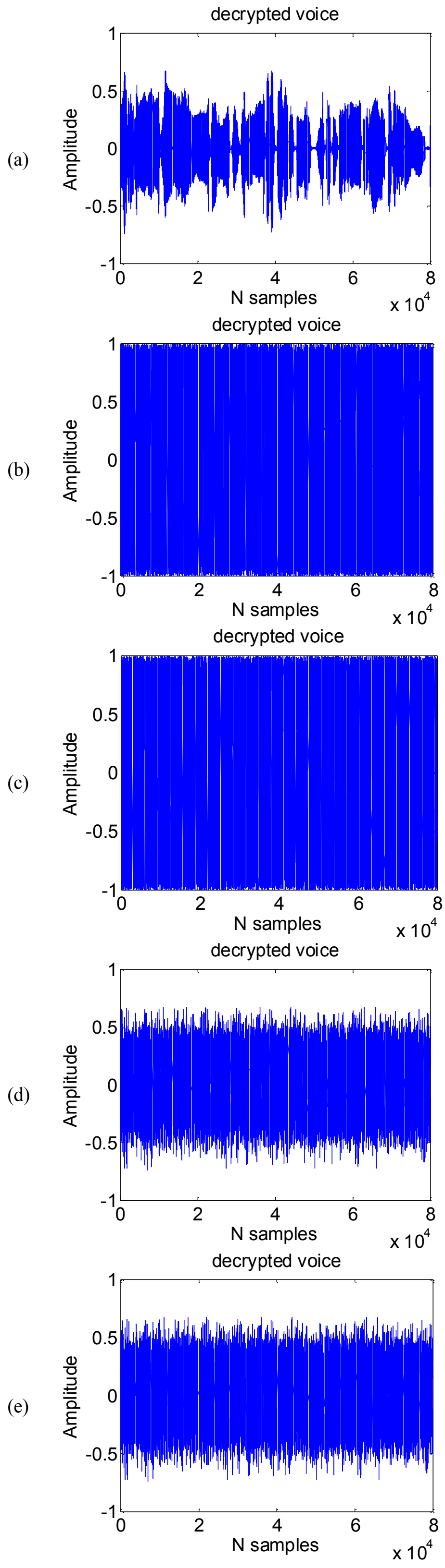

Fig. 7. Decrypted speech signal with a little change in parameters. (a) Identical parameters, (b) $x_{02} = x_{02} + 10^{-15}$. (c) $r_{02} = r_{02} + 10^{-14}$ (d) $x_{01} = x_{01} + 10^{-16}$, (e) $r_{01} = r_{01} + 10^{-14}$.

V. Comparative study

Table II presents the results of the proposed method, showing very acceptable values of correlation and the SNR coefficients, in the encryption and decryption phase compared to the method described in [19]. The correlation coefficients between the original and the decrypted signal are close to 1 for the proposed method, which shows that the samples are strongly correlated, while the correlation coefficients for the encrypted signals are close to zero. The SNR coefficients between the original and the encrypted signal for the proposed method are much reduced compared to [19], showing the improved quality of the encrypted signal. The SNR coefficients between the original and the decrypted signal show very satisfactory values, close to 45.1425dB, therefore better than those found in [19]. These results show the improved performance of the proposed compared to an existing valuable method, showing unintelligible encrypted signals and highly intelligible decrypted signals.

TABLE II. RESULTS OF COMPARISON WITH [19]

Speech files	Proposed method		[19]	
	SNR (in dB)	r_{xy}	SNR(in dB)	r_{xy}
	Encrypted/ Decrypted	Encrypted/ Decrypted	Decrypted	Encrypted/ Decrypted
Signal 1.wav	-10.4925/ 39.2841	0.0032/1	33.7464	0.0233/ 0.999
Signal 2.wav	-11.3701/ 45.1425	0.0012/1	32.5781	0.0384/ 0.999
Signal 3.wav	-11.8293/ 39.8948	-0.0002537/1	33.0569	0.0157/1
Signal 4.wav	-16.3239/ 40.6553	-0.0002593/1	34.7112	0.0119/1
Signal 5.wav	-14..3535/ 43.1726	-0.0052/ 1		

VI. Conclusion

This paper presented a new chaotic system that combines two classical maps, the Logistic and the Cubic, for speech signal encryption. The obtained combined sequence presents a positive value of the Lyapunov exponent over the entire definition interval of the control parameter, improving the performance of the proposed system by expanding the range of the chaotic parameters. The bifurcation diagram of the new combination shows a very wide chaotic range with an invariant uniform distribution without windowing over the entire definition interval of the control parameter. The parameters of the chaotic map were the secret key of the proposed encryption scheme, which is basically structured from the confusion and diffusion architecture. Objective and subjective analyses, such as visual examination of the waveform in the time domain and spectrograms, as well as statistical analysis, were performed to prove the security of the proposed encryption approach. Performance analysis confirmed that the proposed combined system is highly secure.

References

[1] S. NajimAlSaad and E. Hato, "A Speech Encryption based on Chaotic Maps," *International Journal of Computer Applications*, vol. 93, no. 4, pp. 19–28, May 2014, https://doi.org/10.5120/16203-5488.

[2] M. O. Al-Dwairi, A. Y. Hendi, and Z. A. AlQadi, "An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images," *Engineering, Technology & Applied Science Research*, vol. 9, no. 3, pp. 4165–4168, Jun. 2019, https://doi.org/10.48084/etasr.2525.

[3] R. J. Rasras, Z. A. AlQadi, and M. R. A. Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, Feb. 2019, https://doi.org/10.48084/etasr.2380.

[4] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," *Journal of Computing*, vol. 2, no. 3, pp. 152–157, Mar. 2010.

[5] P. Patil, P. Narayankar, Narayan D.G., and Meena S.M., "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, Jan. 2016, https://doi.org/10.1016/j.procs.2016.02.108.

[6] R. Matthews, "On the Derivation of a 'Chaotic' Encryption Algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989, https://doi.org/10.1080/0161-118991863745.

[7] Y. Hu and R. Tian, "Image Encryption and Decryption Based on Chaotic Algorithm," *Journal of Applied Mathematics and Physics*, vol. 8, no. 9, pp. 1814–1825, Sep. 2020, https://doi.org/10.4236/jamp.2020.89136.

[8] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation and Chaos*, vol. 08, no. 06, pp. 1259–1284, Jun. 1998, https://doi.org/10.1142/S021812749800098X.

[9] X. Wang and Q. Yu, "A block encryption algorithm based on dynamic sequences of multiple chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 2, pp. 574–581, Feb. 2009, https://doi.org/10.1016/j.cnsns.2007.10.011.

[10] B. Flaeh and M. Dhiaa, "Multi-Levels Image Encryption Technique based on Multiple Chaotic Maps and Dynamic Matrix," *International Journal of Computer Applications*, vol. 151, no. 3, pp. 1–5, Oct. 2016, https://doi.org/10.5120/ijca2016911693.

[11] E. Hato and D. Shihab, "Lorenz and Rossler Chaotic System for Speech Signal Encryption," *International Journal of Computer Applications*, vol. 128, no. 11, pp. 25–33, Oct. 2015, https://doi.org/10.5120/ijca2015906670.

[12] A. Elsharkawi, R. M. El-Sagheer, H. Akah, and H. Taha, "A Novel Image Stream Cipher Based On Dynamic Substitution," *Engineering, Technology & Applied Science Research*, vol. 6, no. 5, pp. 1195–1199, Oct. 2016, https://doi.org/10.48084/etasr.729.

[13] M. Boumaraf and F. Merazka, "Partial and full speech encryption schemes based on 1D chaotic maps for AMR-WB codec," in *2018 2nd International Conference on Natural Language and Speech Processing (ICNLSP)*, Algiers, Algeria, Apr. 2018, pp. 1–5, https://doi.org/10.1109/ICNLSP.2018.8374388.

[14] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, Sep. 2017, https://doi.org/10.1016/j.sigpro.2017.03.011.

[15] S. Gokavarapu and S. V. Kumari, "A Novel Encryption Using One Dimensional Chaotic Maps," in Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1, 2015, pp. 193–203, https://doi.org/10.1007/978-3-319-13728-5_22.

[16] E. N. Lorenz, "Deterministic Nonperiodic Flow," *Journal of the Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, Mar. 1963, https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

[17] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map," *Multimedia Tools and Applications*, vol. 79, no. 25, pp. 17817–17835, Jul. 2020, https://doi.org/10.1007/s11042-020-08729-5.

[18] I.-I. B. Ltd, "Speech Encryption Technique using S - box based on Multi Chaotic Maps," *TEM Journal*, vol. 10, no. 3, pp. 1429–1434, 2021, https://doi.org/10.18421/TEM103-54.

[19] 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, Sep. 2017, Art. no. 20, https://doi.org/10.1186/s13636-017-0118-0.