Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Speech Encryption Method Based On 3D Lorenz Map And Baker Map

Elsayed M. Elshamy[1] , Aziza I. Hussein[3] , Hesham F. A. Hamed[2,5] , M. A. Abdelghany[2,4]

[1]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt.

[2]Department of Computer & Systems Engineering, Faculty of Engineering, Minia University, Minia, Egypt.

[3]Electrical & computer Engineering Department Effat University
Jeddah, KSA

[4]Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Wadi Addwasir 11991, Saudi Arabia.

[5]Department of Telecommunications Eng., Egyptian Russian University, Cairo, Egypt.

Abstract - Today, Security and Privacy in Speech Communication systems is a growing concern given the rapid development of digital networks and networking technology. The chaotic schemes are common encryption techniques to provide the highest permutation. In this study, a dual-security cryptosystem for voice is introduced based on a hybrid Lorenz map 3D and Baker Map cryptosystem. The proposed technique and other chaotic techniques were tested using computer Matlab software to assess the correlation between the original and encrypted signal and to test the robustness of the quality metrics. The simulations of the proposed system showed good validation in the histogram metric, and improvement in correlation coefficient by a percentage of 13.7% and processing time by a percentage of 90% when compared with other chaotic schemes. Therefore, this paper proposes that the dual-security cryptosystem technique could be utilized to increase the immunity of voice security system.

Keywords— Baker map, cryptosystem, encryption, Lorenz map, voice security

I. Introduction

In recent years, security has become an extremely important aspect due to advances in communication technologies and, hence, the growing need for speech-based applications. Secure communication is aimed at overcoming unnecessary disclosures and unauthorized changes, while speech is transmitted through networks.

Redundancy, is a very important factor in a secure language system, where an associate individual can easily decode loads of information. An ancient approach was used to assure communications confidentiality via scrambling methods that encompassed basic permutations and affined in time or frequency domain transformations. As the computational power has rapidly increased over the past decade, such scrambling algorithms are prone to attacks. Many real-world cryptography applications have now switched to secret compression algorithms, reducing signal dimensions before secret writing and eliminating redundancy.

The first stage in coding is the conversion of the input voice signal in digital secret writing. The digitized signal is then compressed so that only the right bitrate stream can be generated. The following bitstream can be encrypted and then distributed through unreliable networks. In comparison, digital secret writing alone may be violated by the brute force of victimization excluding certain sophisticated mathematical techniques.

A range of voice encryption methods using various strategies, including mixing, chaotic, hashing, etc., have been recently suggested. In [1] 2017, proposed to use A5/3RC6 over the GSM network for effective end-to-end encryption. Aissa implemented speech encryption with stream cipher in 2015 [2]. Liu proposed a multi-scroll chaotic framework and one-time keys audio encryption system based on confusion as well as diffusion in 2016 [3]. Have also constructed a cosine number transform-based audio encryption in 2016 [4]. Introduced an algorithm of audio shuffle encryption in 2014 [5]. R. D., implemented compound chaotic mapping application of algorithms in voice encryption in 2014 [6]. Introduced compressive sensing and Arnold transformation strategy for audio encryption [7] in 2015. A novel approach in encrypting audio messages was proposed by Ghasemzadeh et al. in 2017, based on a mixture of chaos function [8]. An audio encryption approach, based on discrete wavelet transformation has been suggested in [9]. In [10] the writers also suggested an algorithm for audio encryption by modifying the elliptical curve and Arnold transformation. In [11], speech encryption is suggested based on a chaotic scheme with a large size key. The suggested voice cryptosystem displayed lower values of correlation coefficient and processing time than these strategies.

This paper is structured as follows: Section 2 provides the background of our work, an explanation of two techniques used (Baker Map and Lorenz map). Details about the proposed hybrid cryptosystem "Lorenz map and Baker map" are given in Section 3. The experimental findings are listed in Section 4, for the optimized code or the un-optimized code for the speech secret writing algorithm measuring unit. Finally, section 5 outlines the conclusion of the measurement unit.

II. Encryption Techniques

A. Lorenz Map

The Lorenz map is one of the most common chaotic attractors in three dimensions; In 1963 Edward Lorenz evaluated and reported it. He showed that a slight shift in the initial states or initial climate model conditions may result in high weather variations. It means that the performance of the whole system which is considered a sensitive system based on the initial stats will be affected by a small comparison of the starter stats. The non-linear dynamic method is adaptive to the original value and is associated with the periodic system of behavior [12].

The non-linear dynamical method of Lorenz introduces a chaotic attractor, while the term chaotic is also used to describe the complicated way non-linear dynamic systems are employed. The chaotic theory clearly induces random behavior, but is fully deterministic in the meantime.

The Lorenz attractor is characterized as follow [13]:

$dx/dt=(y-x)$ (1)

$dy/dt=(\rho-z)-y$ (2)

$dz/dt=xy-\beta z$ (3)

Lorenz system's positive parameters are β=8/3, ρ=28, & σ=10, whereas Lorenz system's initial values x0, y0, z0 between one and zero and t is time.

B. Baker Map

The chaotic scheme is one of the common encryption schemes in this case and provides the highest permutation. Chaotic structures use specific maps to rearrange components in data blocks. It is important to note that chaotic structures are highly sensitive to initial parameters such as the device that runs in another orbit, which is hard to measure and evaluate if a different parameter is used. There is good randomness, non-predictability as well as low correlation value in-sequence performance of the system were reported [14].

Two kinds of chaotic Baker map approaches are available: discretized map and generalized map. The Baker map is an efficient means of randomizing elements in a square matrix as illustrated in Equation 4. Suppose B(n1,…,nk), signify the discretized map, where [n1, … ,nk] is the vector, expresses Skey i.e., the secret key. Specify N as element number of single row, the secret key is selected to divide N into ni each integer, and n1 + … + nk = N.

Suppose Ni = n1 + … + ni-1. The data variable at the indices (q, z) is shifted to the indices [14]:

$$B_{(n_1,\ldots,n_k)}(q,z)=\left(\frac{N}{n_i}(q-N_i)+z\ \mathrm{mod}\left(\frac{N}{n_i}\right),\frac{n_i}{N}\left(z-z\ \mathrm{mod}\left(\frac{N}{n_i}\right)\right)+N_i\right) \qquad (4)$$

where "Ni ≤ q < Ni + ni, 0 ≤ z < N, and N1=0"

III. Proposed Hybrid Cryptosystem

In the proposed hybrid encryption technique, the first stage is the method for Lorenz map encryption, and the second one is the method for Baker map encryption. Both stages have been developed for secured speech communication, as shown in figure 1. The original voice passes to the encryption process, based on Lorenz 3D map algorithm technique, then the result is encrypted with the Baker map algorithm technique. The decryption process is then applied vice versa to the encryption technique.

Both "Lorenz map & Baker map" encryption techniques help to enhance the safety and consumer protection of the voice mail system over the communication channels. The behavior of chaotic map in encryption process totally changes depending on the variation in key values used in Lorenz and Baker maps.

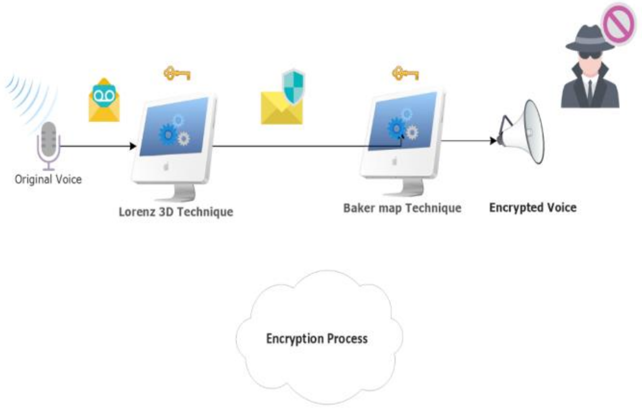


Fig. 1 Proposed encryption system

IV. Encryption Quality Mesurments and Analysis

In this study, many criteria are selected for voice cryptosystems quality assessments. These assessments are divided into two classes: encryption and decryption quality metrics. Encryption quality metrics is tested on encrypted voice signals for assuring the cryptanalysis attack immunity of the voice cryptosystem and to quantify the distortion degree throughout the encrypted signal. Decryption quality metrics are assessed for decrypted voice signals for ensuring the tolerance of the cryptosystems to noise, distortion as well as quantifying decrypted signal distortion. In general, the goals of quality metrics are showed in Figure 2.

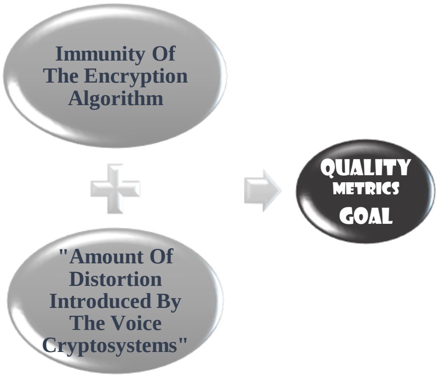

Immunity Of The Encryption Algorithm
"Amount Of Distortion Introduced By The Voice Cryptosystems"
QUALITY METRICS GOAL

Fig. 2 Quality metrics goal

A. Encryption Quality Metrics

For the encrypted algorithms design, voice cryptosystems quality metrics are essential. They can also be used to determine whether the voice cryptosystems are distorting, to determine the parameters and optimize the Voice Cryptosystems structures. The voice cryptosystem performance is better when distortion is higher.

The measures of Voice quality are used to calculate how often the original signal is crypted. They also evaluate the immunity to cryptanalysis attacks from the encryption algorithm.

1) S**tatistical Analysis:** A statistical analysis could solve many types of ciphers. This study is used to demonstrate their uncertainty as well as diffusion properties, that highly resist statistic attacks, on various voice cryptosystems. This is revealed by testing the histogram in encrypted voice signal, the association between encrypted, as well as clear signal samples and tests for SD (spectral distortion).

2) **Correlation:** The CC (correlation coefficient) between same samples in encrypted and clear signals is a valuable parameter for determining the encryption standard of the voice cryptosystem [15].

3) **Spectral Distortion:** The time taken to decrypt as well as a signal is called as processing time. The less time you take to process the more quickly you can encrypt. We have tested the procedure given and calculated the decryption time, since both decryption and encryption process take nearly the similar time.

4) **Processing Time:** Decryption quality metrics is more significance to voice cryptosystems' design as well as maintenance. It is advantageous to indicate the distortion applied for determining the parameter settings by every voice cryptosystem and to optimize the encryption algorithm. These measurements assess the protection from distortion and attack by the voice cryptosystem. They are executed to check the quality on a decrypted signal.

B. Decryption Quality Metrics

Decryption quality metrics is more significance to voice cryptosystems' design as well as maintenance. It is advantageous to indicate the distortion applied for determining the parameter settings by every voice cryptosystem and to optimize the encryption algorithm. These measurements assess the protection from distortion and attack by the voice cryptosystem. They are executed to check the quality on a decrypted signal.

The decrypted voice signals' quality is measured by two techniques: subjective as well as objective [18,19]. The quality relies on the visual judgments of a collection of listeners in subjective metrics. Objective metrics assess consistency and are cheaper to use with computer simulations as well as physical criteria. It saves time and performs more reliably. Objective speech metrics in functional applications are also ideal. Present objective voice quality metrics base their approximations on the utilization of both decrypted as well as original voice signals.

As shown in figure 2, a voice crypto device can be shown as a distortion board. In comparison with the original voice signal, this is useful to calculate the decrypted Voice Signal quality to show its effect.

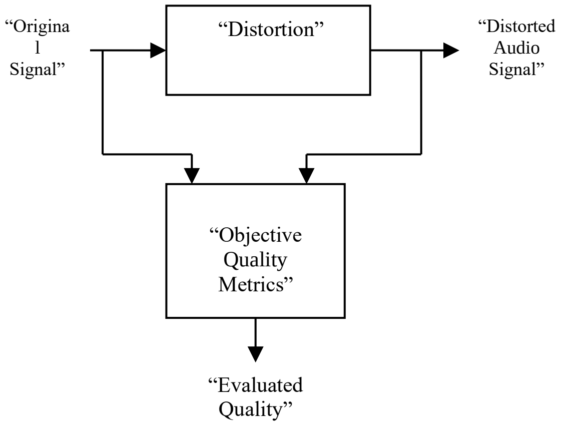


Fig. 3 Objective voice quality metrics based on both the clear and decrypted voice signals

1) **Log Likelihood Ratio:** The voice signal LLR metrics rely on the premise that all-pole linear predictive coding model of shape is present for each segment [20, 21]. The output audio signal quality is high when the LLR closer is zero.

2) **Spectral Distortion:** The SD is a metric form applied to the frequency spectrum of the initial as well as processed voice signals in the frequency domain. SD is expected to be as small as possible between the decrypted signal and initial signal.

C. Quality Metrics Results with Related Work Results Comparative and Discussions.

Crypt-analysis is generally classified as two types of offensive attack. The first sort is described as a passive attack, which aims to uncover the system data but does not damage the system resources. The offensive is hard to reveal since it does not require any data update. The second form is an active attack which attempts to manipulate information while transmitting, modifying device resources, or influencing the network by altering the data stream to mask an object, replaying previous communications, changing information while transmitting, or ultimately violent by a DOS (“Denial-of-Service”). The opposite properties of passive attacks are demonstrated by active attacks.

Also, active threats have become quite challenging to avoid due to the vast range of potentials, software, physical, and network errors. The aim is more to face active threats and recover from delay or distortion that emerges from them.

In this paper, we have constructed a novel encryption scheme in Matlab with simplistic results. The hybrid cryptosystem "Lorenz map & Baker map" has been assessed by multiple systems. All these systems are required in decryption quality elements, such likelihood ratio or spectral distortion, contrary to encryption ones, like the spectral distortion or correlation coefficient. Both are essential if the immunity in these VoIP efficiency systems is to be improved.

The findings of this paper are compared with those of previous studies, in Table 1. These metrics reveal that the accuracy of the “Lorenz map & Baker map” scheme is second to none – unique? The lowest correlation coefficient value between the initial and encrypted voice signal and also the lowest time of processing for the encryption method was attributable to this spectral distortion between clear voice and encrypted signals. The method also obtained the lowest spectral distortion between processed and initial speech signals, the lowest log probability ratio between processed and simple voicing signals and the lowest processing time of the decryption method. These components together demonstrate that the encrypted and decrypted signal of the suggested method is of an outstanding standard.

TABLE I. **Experiments results**

Cryptosystem		**Correlation**	**Spectral Distortion**	**Likelihood Ratio**	**processing time in Sec**
Proposed Baker and Lorenz map	Enc. signal	0.0007	3.3113e-005	-	0.3011
	Dec. signal	-	21.9011	3.8659e-003	
Baker and DRPE [22]	Enc. signal	0.0049	21.9829	-	0 . 3343
	Dec. signal	-	5.8263e-003	9.1354e-007	
Arnold and DRPE [22]	Enc. signal	0.0051	20.36547	-	1 . 4343
	Dec. signal	-	6.0072e-003	1.1644e-006	

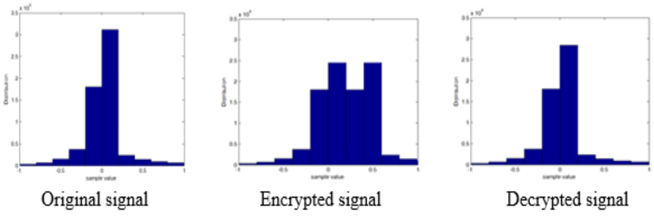
The value of the correlation coefficient is relative to zero, indicating that a greater data protection is provided by our proposed method than the existing methods. The suggested Lorenz map and Baker map is compared with other approaches, as shown in Table 2, as well as the value of parameter of the suggested and several other approaches.

Method	**Authors**	**Correlation**
Proposed Baker and	Elsayed et al.	0.0000
A5/3RC6	keshav et al.	0.0000
Stream Cipher	Aissa et al. [2]	0.0002
Confusion and	Liu et al. [3]	0.0044
Cosine number	Lima et al. [4]	0.0020
Shuffle encryption	Tamimi et al.	0.0263
Compound chaotic	Li et al. [6]	0.0282
Compressive	Augustine et al.	0.0014
Mixture chaos	Gasemzadeh et	0.0092
Chaotic shift key	Sathiyamurthi	0.0223
Software package	Eldin et al. [10]	0.0280
DNA computing	Hamidreza et	-

TABLE II. **Correlation coefficient results**

The correlation factor of the suggested Lorenz map and Baker map is smaller, compared to those obtained by other approaches, indicating that our suggested cryptosystem method is superior to the existing ones.

The histograms of the encrypted voice signals using the proposed cryptosystem as shown in (Fig. 4) reveal that the proposed encryption gives more uniform histograms, which means best encryption results.



Original signal Encrypted signal Decrypted signal

Fig. 4 Histograms of the original, encrypted & decrypted voice signals

V. CONCLUSION

In this paper, a Hybrid Voice Cryptosystem based on hybrid Lorenz map 3D and Baker Map cryptosystem is proposed to ensure the security of the transmission system. Encryption and decryption are two processes that have been popular when it comes to data security and protection. The architecture attains good diffusion and permutation mechanisms within a suitable time. The results of the research show that speech encryption provides a far better security system with its decryption qualities. The simulations of the proposed system show good validation in the histogram metric, an improvement in correlation coefficient by a percentage of 13.7% and processing time by a percentage of 90%. The reliability of the hybrid security cryptosystem is guaranteed through multi-modal analyses in this manner. These findings, together, ensure that the hybrid voice cryptosystem is efficient and effective.

REFERENCES

[1] Enhanced, “Efficient End-to-End Voice Encryption Using A5/3RC6 over GSM Network”, Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-1, 2017.

[2] Aissa Belmeguenai, Khaled Mansouri, Mohamed Lashab, “Speech Encryption Using Stream Cipher”, British Journal of Applied Science & Technology 107-125, 2015, Article no.BJAST.2015.190.

[3] Liu, H., Kadir, A., & Li, Y., “Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one time keys”, Optik, 127(19), 7431–7438, 2016.

[4] Lima, J. B.,&Da Silva Neto, E. F., “Audio encryption based on the cosine number transform”, Multimedia Tools and Applications, 75(14), 8403–8418, 2016.

[5] Tamimi, A. A., & Abdalla, A. M., “An audio shuffleencryption algorithm”, In The world congress on engineering and computer science, 2014.

[6] Li, R. D. Y., “Application of compound chaotic mapping”, in voice encryption algorithm. International Journal of Computer Science and Network Security (IJCSNS), 14(8), 44, 2014.

[7] Augustine, N., George, S. N., Pattathil, D. P., “An audio encryption technique through compressive sensing and Arnold transform”, International Journal of Trust Management in Computing and Communications, 3(1),74–92, 2015.

[8] Ghasemzadeh, A.,&Esmaeili, E., “Anovel method in audio message encryption based on a mixture of chaos function”, International Journal of Speech Technology, 20(4), 829–837, 2017.

[9] Chloe Albin, Dhruv Narayan, Ritika Varu, V Thanikaiselvan, “DWT based Audio Encryption scheme”, ICECA Conference – IEEE Xplore, pp. 29-31, 2018.

[10] Ramesh Shelke, Milind Nemade, “Audio Encryption Algorithm Using Modified Elliptical Curve Cryptography and Arnold Transform for Audio Watermarking”, I2CT - IEEE Xplore, pp. 1-4, 2018.

[11] Maher K. Mahmood Al-Azawi, Ali M. Gaze, “Combined speech compression and encryption using chaotic compressive sensing with large key size”, IET Signal Processing, Vol. 12, pp. 214 – 218, 2018.

[12] D. S. Eman Hato, "Lorenz and Rossler Chaotic System for Speech Signal Encryption," nternational Journal of Computer Applications, vol. 128, no. 11, pp. 25 25-33, October 2015.

[13] E. Ghys, The Lorenz Attractor, a Paradigm for Chaos,Poincare Seminar 2010,2013 Springer Basel AG, 2010.

[14] Y. Honglei, W. Guang-shou, W. Ting, L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei, M. Yuankao, "An image encryption algorithm based on two dimensional Baker map", Proc. ICICTA, 2009.

[15] Bartosz Kunka and Bozena Koste, “An New Method of Audio-Visual Correlation Analysis”, Proceedings of the International Multiconference on Computer Science and Information Technology, vol. 4, 2009.

[16] A. Prodeus and N. Bogdanova, “Objective quality evaluation of speech band-limited signals”,

Electronics and Communications, vol. 19, no. 6,2014.

[17] K.S. Zamsha, B.V. Lozynskiy, J.A. Mytiay, E.S. Stepanovskaya and A.M. Prodeus, “Objective and subjective assessment of bandlimited signaling speech quality”, Electronics and Communications, vol. 21, no. 1, 2016.

[18] W. Yang, M. Benbouchta, R. Yantorno, "Performance of the modified bark spectral distortion as an objective speech quality measure", International Conference on Acoustics, Speech and Signal Processing, Vol. 1, pp. 541 – 544, 1998.

[19] J.C. Hardin, C. D. Creusere, "Objective analysis of temporally varying audio quality metrics", 42nd Asilomar Conference on Signals, Systems and Computers, pp. 1245-1249, 2008.

[20] W. K. Sang, G. K. Young and M. K. Simon, "Generalized selection combining based on the log-likelihood ratio", IEEE International Conference on Communications ICC 2003, Vol. 4, pp. 2789-2794, 2003.

[21] J. K. Kwon, S. Park, D. K. Sung, "Collision mitigation by log-likelihood ratio (LLR) conversion in orthogonal code-hopping multiplexing", IEEE Transactions on Vehicular Technology, Vol. 55, Issues 2, pp. 709-717, March 2006.

[22] Elsayed M. Elhamy, Osama S. Farag Allah. Efficient audio cryptosystem based on chaotic maps and double random phase encoding, Springer, 2015.