Securing Modern Voice Communication Systems using Multilevel Chaotic Approach

Mahmoud F. Abd Elzaher
Department of Electronics
and Electrical communications
Ain Shams University
Cairo, Egypt

Mohamed Shalaby
Department of Computer
Science,
Arab Academy for Science
Technology
Cairo, Egypt

Salwa H. El Ramly
Department of Electronics
and Electrical communications
Ain Shams University
Cairo, Egypt

ABSTRACT

In this paper, we present a new voice encryption for voice communication system. It is based on permutation and substitution of voice samples using transform domains and secret keys in time. To increase the security we design the system such that it is multilevel in the sense that two chaotic maps are used. This provides the encrypted signal with a high degree of confidence. The Arnold cat map is applied to a permutation of the samples, The Henon map is employed in key generation to generate mask keys to be used in the substitution process. The results show that the encryption system provides the speech signal with a high degree of confidence, key sensitivity and high quality recovered signal. Total key space for the proposed encryption system is larger than (2^{425}), which is large enough to protect the encrypted signal against attack.

Keywords

Voice encryption, Henon map, Arnold cat map, Permutation, Substitution.

1. INTRODUCTION

We ask Nowadays multimedia applications such as speech and sound are crucial, and their service is the foundation of the telephone industry, video conference and broadcast news. Thus, securing such systems is very important to overcome intrusion and eavesdropper attacks. The need for encryption and security has increased because modern voice communication systems demand huge amount of information to be exchanged across local networks and the Internet every day. The conventional cryptographic techniques may be efficient for the text data however, they are unsuitable to the bulk data capacity. Therefore, speech security requires efficient techniques like chaos-based techniques to deal with bulk data. Chaos-based techniques provide fast and highly secure encryption methods.

There are many categories of voice encryption techniques which use chaotic system in [1] authors presented an encryption of voice signals in transform domain by chaos. This algorithm, divides the segments of voice into two blocks each with fixed size. The elements of these blocks are permuted by using baker map. Then Discrete Cosine Transform (DCT) is used to substitute these permuted elements. A new technique of encryption based on Arnold cat and logistic map [2] was applied such that it uses two permutation keys, k_1 and k_2. The 1-D vector sample is transformed to the 2-D matrix, then Arnold map is applied. The permutation key k_1 is used for samples permutation and k_2 is used for the Permutation of the coefficients produced from discrete wavelet transform (DWT) or DCT. After that samples are masked with mask key through XOR operation. Finally the 1-D vector is converted to the 2-D matrix and the process is repeated for M times. In [3] authors proposed an algorithm that breaks the correlation by using Modified Overlapped Block Shuffling and encrypting with a Hybrid Chaotic System. First, the original speech signal is converted from a 1-D vector to 2-D matrix. Then, it is divided into overlapped squared blocks followed by a subsequent permutation. And, all permutated block are shuffled using Henon and Arnold transformation. Finally a Hybrid Chaotic is generating a key matrix to encrypt the scrambled blocks.

The main goal of this paper is proposing a voice encryption system that provides users with a high degree of confidence and key sensitivity, and preserving a good quality of the reconstructed speech signal by chaotic maps.

In section 2, discuss Chaos based cryptography systems. In Section 3 present the proposed speech approach and review transforms. In section 4 show the results of applying our proposed approach. Finally, conclude our work in section 5.

2. CHAOTIC SYSTEM

Chaos based cryptography is most important security techniques in modern cryptography area. Chaos theory has been developed by physicists and mathematicians. Chaos theory has eligible features such as deterministically, nonlinearity, irregularity, and Sensitivity to initial conditions. Therefore, and based on chaos theory features, security research community adopts chaos theory in modern cryptography. A function that possesses kind of chaotic behavior is defined as a chaotic function or map. In the following subsections discuss two types of chaotic maps, namely, Arnold cat map and Henon map that are used in this paper.

2.1 Arnold Cat Map

Arnold cat map [4] proposed by Vladimir Arnold in 1960 is a double dimension chaotic system, therefore it is represented by two different equations (1, 2).

$$X_{n+1} = X_n + AY_n (Mod\ N) \qquad (1)$$

$$Y_{n+1} = BX_n + ABY_n (Mod\ N) \qquad (2)$$

Where X_n, Y_n are the position of samples in the $N \times N$ matrix, and $n = 1,2,3, \dots, N-1$ and X_{n+1}, Y_{n+1} are the transformed position after cat map,A , B are two control parameters and are positive integers. The encryption process is done via the iteration of cat map, after performing M iterations, there are T positive integers such that $(X_{n+1}, Y_{n+1}) =$

(X_n, Y_n). The period,T depends on parameters A ,B and the size of the samples matrix ($N \times N$ matrix).

2.2 Henon Map

The Henon map [3] is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. The Henon map takes a point (X_i,Y_i) in the plane and maps it to a new point. A Henon Chaotic system which is described by equations (3, 4).

$$X_{i+1} = 1 + aX_i{}^2 + Y_i \qquad (3)$$

$$Y_{i+1} = bX_i \qquad (4)$$

It presents a simple 2-D chaotic map with quadratic nonlinearity, depends on parameters a , b, initial value X_0 and initial value X_1. The parameter $a \in$ [1.07, 1.4]. Figure 1 shows a bifurcation of X versus parameter a, and Figure 2 shows iteration property when a = 1.4.

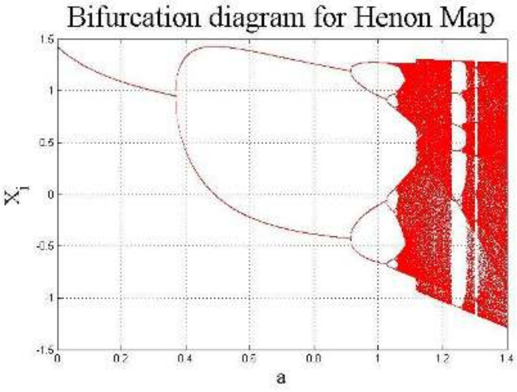


Figure 1: Bifurcation diagram for a ∈ [0, 1.4]

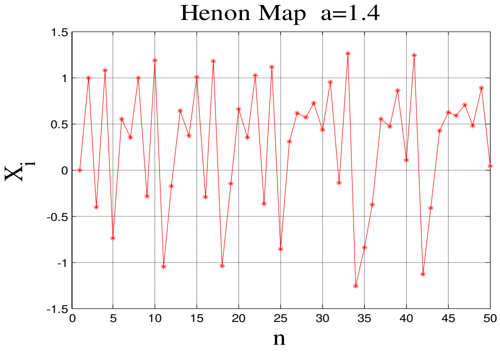


Figure 2: Iteration property when a = 1.4

3. THE PROPOSED CRYPTOSYSTEM

The proposed cryptosystem is used for permuting and masking the wave speech signal in the time domain.

3.1 The encryption performed in a number of iterations which are summarized as follows:

- Convert input speech wave signal from 1D to 2D.
- Permute the blocks, using Arnold cat map.
- Convert blocks into 1-D format.
- Generation of mask key using Henon map (First Proposed approach) or modified Henon map (Second Proposed approach). Explain these approaches in the next section.
- Application of XOR operation between mask key and speech samples.

3.2 The decryption steps for the cryptosystem can be summarized as follow:

- Generation of mask key using Henon map (First proposed approach) or modified Henon map (Second proposed approach).
- Application of XOR operation between mask key and speech samples.
- Reshape encrypted speech signal into 2D format.
- Permute the blocks, using Arnold cat map.
- Convert blocks into 1-D format.

3.3 Modified Henon Chaotic

Modify Henon Chaotic system [5] to increase the parameter a space which is described by equations (5, 6)

$$X_{i+1} = (aX_i + Y_i)\ mod\ 1 \qquad (5)$$

$$Y_{i+1} = \frac{b}{1-Y} \qquad i = 0,1,2 \qquad (6)$$

Extending the chaotic range of parameter a to be from 0 to more than 10^6 will increase the available chaotic values of parameter a. The proposed Henon chaotic map gives a very wide range of variable a for using in encryption. Figure 3 shows a bifurcation of X versus parameter a and Figure 4 shows the x-component of Henon map points, X_i versus the number of iterations n.

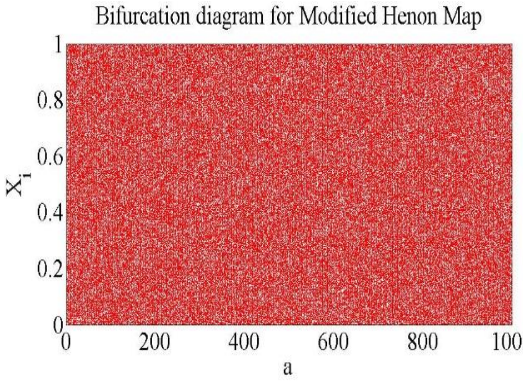


Figure 3: Bifurcation diagram for $a \in [0,\ 10^6]$

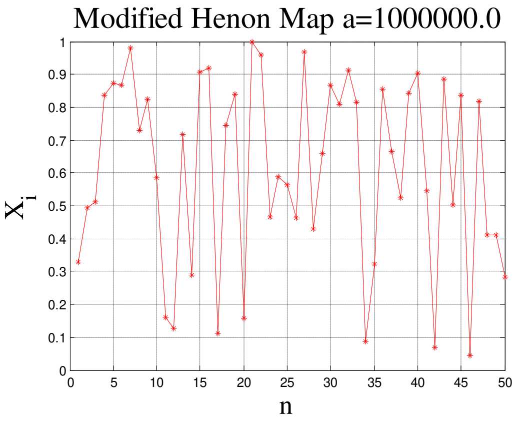


Figure 4: Iteration property when a = 1000000.0

3.4 Application of Arnold Cat Map

For applying Arnold cat map[6], the block of samples in time domain must be converted from 1-D vector to 2-D matrix, and then permuted by multiplying the position of each sample by Arnold cat map matrix. This process is repeated for M iterations where the final result is a new position of the sample so that samples of the block appear to be randomly rearranged. The output is resized to 1-D vector again.

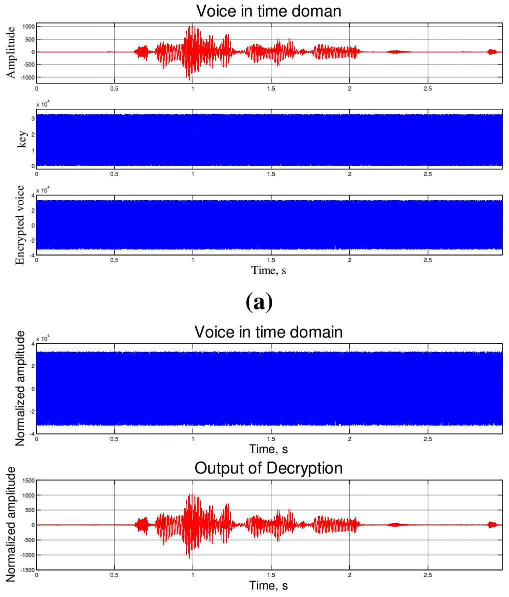
3.5 Generation of mask key

The permutation process changes the original sample's position, however the sample's value has not been changed. Substitution process is changing the amplitudes of samples in each block. Each sample value is changed by XOR operation with mask key value. The mask is generated from Henon map and proposed modified Henon map. The secret key elements are generated using equation (7) [3].

$$Key(i) = Floor(x(i) * 2^{15})mod(2^{15} - 1) \qquad (7)$$

4. EXPERIMENTAL RESULTS AND ANALYSIS

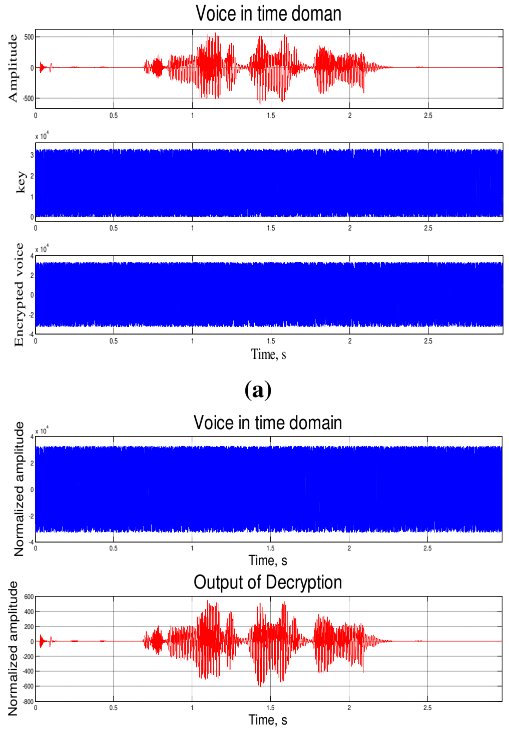
The proposed approach is first implemented using an Arnold cat map and Henon map. Second, it is implemented using an Arnold cat map and modified Henon map. Figure 5(a) shows the waveform of original signal, waveform of mask key and waveform of encrypted signal for the first proposed approach. Figure 5(b) shows the waveform of received signal and waveform of decrypted signal for the first proposed approach. Figure 6(a) shows the waveform of original signal, waveform of mask key and waveform of encrypted signal for the second proposed approach. Figure 6(b) shows the waveform of received signal and waveform of decrypted signal for the second proposed approach.



(a)

(b)

Figure 5: First proposed approach (encrypted signal - decrypted signal)



(a)

(b)

Figure 6: Second proposed approach (encrypted signal - decrypted signal)

In the following subsections analyzing the results of applying the first proposed approach (using Henon map) and the second proposed approach (using a modified Henon map) according to different perspectives.

4.1 Statistical Analyses

To statistically analyze our results, four different measures [7] are used, Signal-to-Noise-Ratio (SNR), Segmental signal-to-Noise-Ratio (SNRseg), Log-Likelihood Ratio (LLR), and Correlation Coefficient Analysis (CCA) and Processing time (PT). Table 1, 2 show the average of the samples which have been analyzed using first and second proposed approaches.

Table 1. Statistical Analyses

App	SNR	SNRseg	LLR	CCA	PT
First	-41.05 dB	-55.2 dB	1.92	-0.00118	1.314
Second	-48.55 dB	-52.74 dB	1.91	0.0004	1.257

Table 2. Recovered signals Statistical Analyses

App	SNR	SNRseg	LLR	CCA
First	240.16 dB	80.15 dB	0.00	1.00
Second	241.43 dB	78.1 dB	0.00	1.00

4.2 Spectrogram Analyses

The spectrogram is a powerful tool that divides the voice sample into multiple "blocks" (in time domain) then plotting the Fast Fourier Transform (FFT) of each block and displaying all of them in the same graph. Figure 6 shows the spectrogram of the original signal frequency versus time and the spectrogram of the encrypted signal frequency versus time (for the first proposed approach) and figure 7 shows the spectrogram of the original signal frequency versus time and the spectrogram of the encrypted signal frequency versus time (for the second proposed approach).

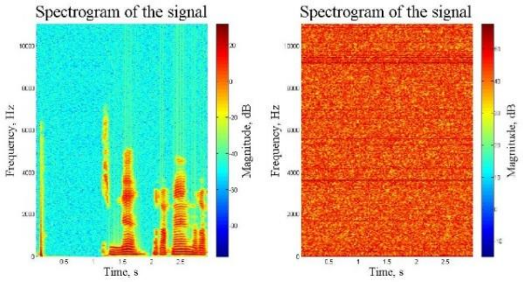


Figure 7: First proposed approach spectrogram (Original signal - encrypted signal)

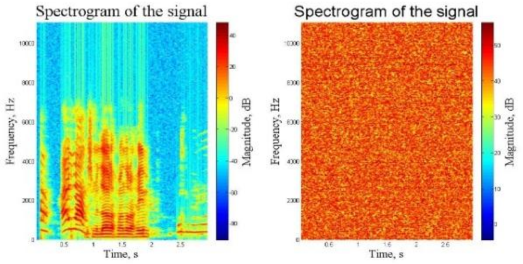


Figure 8: Second proposed approach spectrogram (Original signal - encrypted signal)

4.3 Histogram Analysis

Distributions of data values in a system comprised the histogram. Histogram analysis can be made by examining data distributions in many different fields. In encryption practices, if the distributions of numbers that represent encrypted data are close, this means encryption has been performing well. The closer the encrypted data distributions are, the higher their encryption level. Figure (8) shows the distribution versus sample value (for the first proposed approach) and figure (9) shows distribution versus sample value (for the second proposed approach).

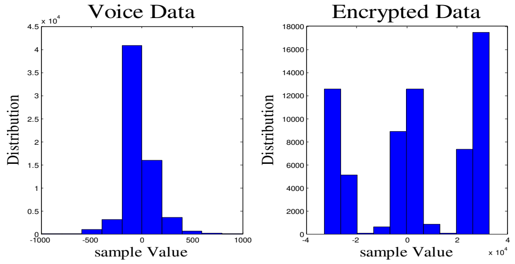


Figure 8: First proposed approach Histogram (Original signal - encrypted signal).

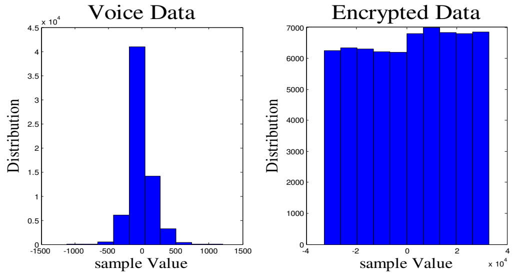


Figure. 9: Second proposed approach Histogram (Original signal - encrypted signal)

4.4 Key Space and Key Sensitivity

Key space and sensitivity analysis are the most important criteria of the performance analysis of the encryption system. A good encryption algorithm should have a large key space, and also should be sensitive to the initial condition and key value.

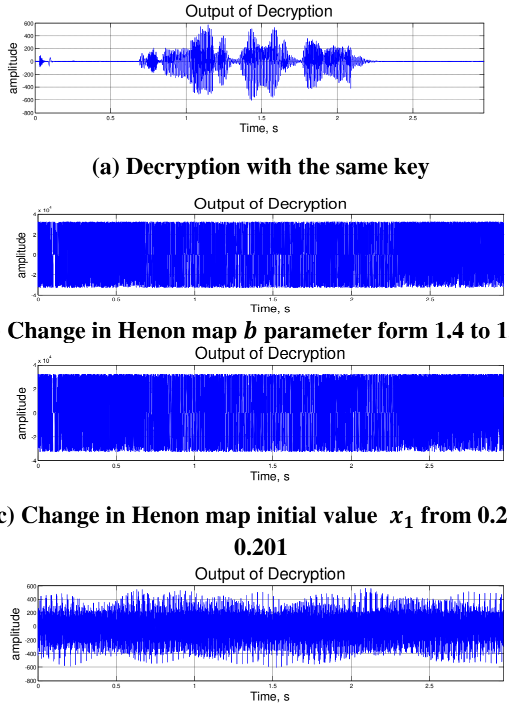
4.4.1.1 Key space

The size of the key space defines the total number of different keys that are used for the encryption / decryption algorithm. It should be large enough to resist the attack. In the proposed scheme, signed floating point precision of $10^{-16}$is used for at least (K =8) secret keys (4 Arnold cat map parameters and 4 Henon Map parameters) [8], the key space size of secret keys is $(10^{16})^{\ k}$ =10^{128}, which is large enough to resist the attack. Control parameters of the Henon map (a) to be from 0 to more than 10^{6} in the second proposed approach.

4.4.1.2 Key Sensitivity

The most important feature of chaos encryption is key Sensitivity. A small change in the key lead to different results during the decryption, encrypted data cannot be decrypted even if only one parameter has been changed. It is also necessary to know the order of the keys, otherwise the data cannot be decrypted with knowing all the keys because the decryption does not happen in the correct order. Figure (10-a) shows the decrypted wave form of the second proposed approach when used the same key, and figures (10-b, 10-c, 10-d) show the effect on decrypted waveform when make small change in parameter during the decryption process.

Figure (10-b) shows this effect, according to the change in Henon map b parameter form 1.4 to 1.401. Figure (10-c) shows this effect, according to the change in Henon map initial value x_1 from 0.2 to 0.201. Figure (10-d) shows this effect, according to the change in cat map iteration from 92 to 90.



(a) Decryption with the same key

(b) Change in Henon map b parameter form 1.4 to 1.401

(c) Change in Henon map initial value x_1 from 0.2 to 0.201

(d) Change in Arnold cat map (M) iteration from 92 to 90

Figure 10: Second proposed approach (decrypted signals)

5. CONCLUSIONS

The two chaotic approaches for securing modern voice communication systems. The first approach is using Arnold cat map in permutation process and Henon map in substitution process and the second approach is using Arnold cat map in permutation process and modified Henon map in the substitution process. The two approaches encrypt the original signal with two-levels, which makes the cryptanalysis a difficult task and increases the security of the voice signal. They are very sensitive to the initial condition and control parameters that means the encrypted signal cannot be decrypted correctly, if there is a very small change between encryption and decryption keys. Experimental results show that the Second proposed approach is better because it extends parameter a in the Henon map to be from 0 to more than 10^6. Also, the histogram Analysis shows that the distributions of the encrypted signals of the second approach are closer than the first approach counterparts, and hence encryption using second approach is better than first approach.

6. REFERENCES

[1] E.Mosa, O.Zahran," Chaotic Encryption of Speech Signals in Transform Domains" Computer Engineering & Systems, 2009. ICCES 2009. International Conference, PP. 300 - 305 (Dec. 2009).

[2] Saad Najim Al Saad, Eman Hato , " A Speech Encryption on Chaotic Maps" International Journal of Computer Application (0975-8887) volume 93-No 4 ,PP. 19 – 28 (May 2014).

[3] Hala B.Abdul Wahab , Sundus I. Mahdi "Modify Speech Cryptosystem Based on Shuffling Overlapping Blocks Technique" International Journal of Emerging Trends & Technology in Computer Science Volume 4, No.2, PP. 70 - 75 (2015).

[4] Akif Akgül, Sezgin Kaçar, İhsan Pehlivan "An Audio Data Encryption with Single and Double Dimension Discrete-Time" Journal of Science and Technology Volume 5, Issue 3, PP. 14-23 (July 2015).

[5] Mona F. M. Mursi, H Eldin H. Ahmedand Ayman H. Abd El-aziem" Image Encryption Based on Development of Henon Chaotic Maps Using Fractional Fourier Transform" International Journal of Strategic Information Technology and Applications (IJSITA) Volume 5, Issue 3, PP. 62-77 (2014).

[6] Elsayed M. Elshamy, Sayed El -Rabaie, Osama S. Faragalla h, Osama Elshakankiry " Efficient audio cryptosystem based on chaotic maps and double random phase encoding" International Journal of Speech Technology, Volume 18,Issue 4, PP. 619-631 (December 2015).

[7] E.Mosa, O.Zahran"Chaotic encryption of speech signals" International Journal of Speech Technology Volume 14, Issue 4, pp 285-296 (December 2011).

[8] Sattar B. Sadkhan, Rana Saad Mohammed "A Proposed Voice Encryption Based on Random Lorenz Map with DCT Permutation"International Journal of Advancements in Computing Technology, Vol. 7 Issue 3, PP. 90-101 (May, 2015).

[9] Musheer Ahmad, Bashir Alam, Omar Farooq "Chaos Based Mixed Keystream Generation for Voice Data Encryption" International Journal on Cryptography and Information Security, Vol. 2, No. 1, pp. 36-45, (2012).

[10] M. Ashtiyani, P. Moradi Birgani , S. S. Karimi Madahi "Speech Signal Encryption Using Chaotic Symmetric Cryptography" Journal of Basic and Applied Scientific Research, vol. 2, No.2, pp. 1678-1684,(2012).

[11] osama faragallah , Elsayed Elshamy , Sayed El-Rabaie "Voice Encryption Based on Arnold Cat Cap and Double Random Phase Encoding" International Journal of Speech Technology. No. 14, pp. 14-24, (2013).

[12] Sattar B. Sadkhan, Rana Saad Mohammed" Proposed random unified chaotic map as PRBG for voice encryption in wireless communication" International Conference on Communication, Management and Information Technology (ICCMIT),Vol. 65, pp. 314-323(2015).