Speech encryption using two dimensional chaotic maps

Conference Paper · December 2015

DOI: 10.1109/ICENCO.2015.7416354

CITATIONS
5

READS
370

4 authors, including:

Naglaa Fathi Soliman
Zagazig University
35 PUBLICATIONS **194** CITATIONS
SEE PROFILE

Fathi E. Abd El-Samie
Menoufia University
708 PUBLICATIONS **3,813** CITATIONS
SEE PROFILE

Speech Encryption Using Two Dimensional Chaotic Maps

° Alzharaa Mostafa *, Naglaa. F. Soliman *, Mohamoud Abdalluh* Fathi E. Abd El-samie°
*Faculty of Engineering, Zagazig University, Zagazig, Egypt. *
°Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt. °
Emails: zhraamostfa@yahoo.com, nagla_soliman@yahoo.com, mabdalla2010@gmail.com, fathi_syed@yahoo.com.

Abstract

Speech encryption is used to convert clear speech into unintelligible signal in order to avoid eavesdropping for this purpose, cryptographic techniques and chaotic maps can be applicable. In this paper, a speech cryptosystem based on substitution and permutation is presented. The speech signal has been processed using different discrete transforms. Then the system has been developed using different chaotic maps like 2D Logistic map, Henon map, and Baker. Different objective quality measures for speech have been used to measure the quality of encrypted and decrypted speech signals.

Keywords— Transform domain; Chaotic maps; 2 D Logistic map; Baker map; and Henon map.

1. Introduction

Speech is one of the most fundamental forms of human communications. Today, due to communications technology, we can send and received any speech files through the internet; conversation through internet must be protected as the numbers of internet eavesdropper's increase. To protect speech signal which is transmitted through any insecure channel, any of cryptograph techniques are needed to convert the intelligible speech to unintelligible form before transmission. There are two types of speech encryption techniques: digital and analog [1].

Digital speech cryptosystems like Advanced Encryption Standard (AES) and Data Encryption Standard (DES) produces digital speech encryption. Although digital encryption provides higher security than analog, it needs a complex implementation and a huge bandwidth for transmission through channel [2]. Most of speech communication system has used analog encryption techniques because it can be used in narrow band communication systems. Generally, there are four categories of cryptographic algorithms based permutation in speech communication: 1. time-domain scrambling as time element scrambling. 2. frequency-domain scrambling as frequency inverter and band splitter. 3. Amplitude scrambling in which speech signal added linearly by pseudorandom amplitudes).4. Two-dimensional scrambling which contains the time-domain scrambling with the frequency-domain scrambling [3, 4].5.Transform domain scrambling like discrete cosine transform, fast Fourier transform, wavelet transform, and so forth [4–5]. Nowadays, many new speech encryption algorithms including blind source separation-based [3, 6], and chaotic cryptosystem [7–10] have been developed. Chaotic maps encryption is widely used in speech and image encryption [11, 12]. The idea of taking advantage of chaotic systems to construct cryptosystems has been extensively investigated and attracts more and more attention because it behaves as random and it has sensitivity to initial conditions.

In this paper a comparison study of speech encryption in transform domain as DCT and DST with 2D chaotic maps based permutations like Baker, Henon, and 2D logistic encryption has been introduced. Different speech quality metrics have been used to measure encrypted signal quality and decrypted signal quality like Signal to Noise Ratio (SNR), Segmental Signal to Noise Ratio (SNR_{seg}), Log- Likelihood Ratio (LLR) and Spectral Distortion (SD).

The rest of this paper is arranged as follows: In section 2 a general chaotic system is discussed. In Section 3, the transforms is presented. The proposed cryptosystems is given in Section 4. Section 5 the experimental results for the proposed

cryptosystem is presented. Finally, the conclusion is presented in Section 6.

2. Chaotic System

A chaotic system is a nonlinear deterministic dynamical system. Its behavior like pseudorandom. The output values of chaotic systems depend on system parameters and initial conditions [11]. Different periods of oscillations at the output are produced by different parameter values of the chaotic system. Chaotic system is widely used because of its random behavior and sensitivity to initial conditions and parameter settings. It is very important for cryptography application to use chaotic function to satisfy the cryptographic properties such that confusion, diffusion and disorder. There is a small difference between starting state and parameter setting of chaotic systems which can lead to huge differences in the final state after a few iterations. Chaotic system is very attractive for pseudo-random number generators because it has sensitivity to initial conditions [12]. In mathematics, a function that possesses some kind of chaotic behavior is defined as a chaotic function or map. In the following sub sections, a brief description for three types of the chaotic maps (logistic map, Henon map and Baker map) that are used in this paper has been introduced.

2.1 Logistic Map

Logistic map is one of the simplest chaotic functions that have been recently found for cryptography systems. The function of logistic map is defined as [9]:

$$x_m + 1 = h\, x_m(1 - x_m) \quad (1)$$

Where x_m takes value in the interval (0, 1), the parameter h is a positive constant and takes values up to 4. Its value determines the behavior of the logistic map. From h=3.57 the iterations become totally chaotic and begin to lend themselves to the purpose of encryption [9].When the value of h is chosen to be great, chaotic system becomes highly deterministic.

The above system is very simple and weak therefore a modified 2Dlogistic system is developed. The two-dimensional logistic map has been used for its complicated behaviors. It has more complex [13] than one-dimensional Logistic map. Mathematically, this 2D logistic map can be discretely expressed as follows:

$$x_{i+1} = h\,(3y_i + 1)\, x_i\,(1 - x_i) \quad (2)$$

$$y_{i+1} = h(3x_{i+1} + 1)\, y_i\,(1 - x_i) \quad (3)$$

where h is the system parameter and (x_i, y_i) is the pair-wise point at the i_{th} iteration.

2.2 Henon map

Henon chaotic map has been first discovered in 1978, which can be described as follows [14]:

$$x_{i+1} = 1 - a\,(x_i)^2 + b\,(y_i)^2 \quad (4)$$

$$y_{i+1} = x_i \quad (5)$$

where a,b is the system parameter and (x_i, y_i) is the pair-wise point at the i_{th} iteration. The system has two control parameters (a, b) and the system will show chaotic behavior when a=0.3 and b=1.4.

2.3 Baker encryption

Baker map in its discretized form is an efficient tool to randomize the elements in a square matrix $H \times H$ [15-16]. It can be described by $E\ (x_1, x_2, \ldots\ldots, x_k)$, where the sequence of integers $[x_1, \ldots, x_k]$, represents the secret key. The secret key is chosen such that each integer x_i divides H, and $x_1 + \ldots + x_k = H$. The data item at the indices (r,s) with $H_i \le r < H_i + n_i$ and $0 \le s \le H$ is moved to the indices according to formula in(6) :

$$E_{(x_1,\ldots,x_k)}(r,s) = \left[\frac{H}{x_i}(r - H_i) + s \bmod \left(\frac{H}{x_i}\right), \frac{n_i}{H}(s - s \bmod \left(\frac{H}{x_i}\right)) + H_i\right] \quad (6)$$

The chaotic permutation is performed as follows:

1) An $H \times H$ square matrix is divided into H *rectangles* of width x_i and number of elements H.
2) Each H × x_i vertical rectangle is divided into x_i boxes and every box contains H points.
3) The elements in each box are rearranged to a row in the permuted one. Rectangles are taken from left to right beginning with upper rectangles then lower ones.
4) Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

An example of the permutation of an (8 × 8) matrix is shown in Fig. 1. The secret key is [2, 4, 2] where H=8, x_1=2,x_2=4,x_3=2.

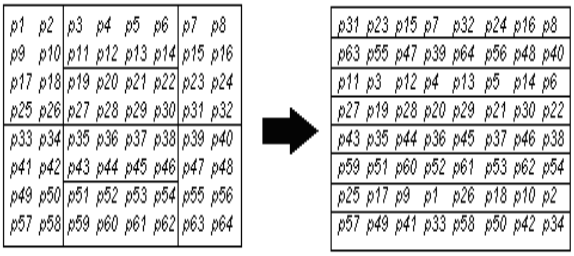

Fig. 1 Baker map.

3. Discrete Transformation

The transform is a technique for converting a signal from time domain into transform domain to yield transform components (coefficients), The encryption is achieved by permuting these coefficients. Then the encrypted transform coefficients are converted back to the time domain and transmitted [5]. Time domain permutation of speech signal will produce distortion of the speech signal envelope which decreases the speech intelligibility. However, some parts of speech signal remain intact, which may allow eavesdropper to spy the scrambled speech. So, it is very important to remove the rest of non-permutated portion of speech by substitution with DCT or DST. In this paper; the DST or the DCT can be used to remove the residual intelligibility caused by time domain permutation.

4. Proposed cryptosystem

The encryption process of the proposed cryptosystem can be summarized in steps as follows:

1. Framing input speech segments and converting it to 2D shape.
2. Initialization
   a. For Logistic and Henon Reading Initial condition and generating 2D Logistic sequence or Henon sequence.
   b. For Baker map
      Generate key for Baker permutation.

3. Transformation

The speech signal has been transformed using DCT or DST to perform their coefficients.

4. Permutation
   a. For Logistic and Henon
      Apply permutation to DCT or DST coefficients with ascending order of generating sequence.
   b. For Baker
      Apply permutation to DCT or DST coefficients according to generating key.

5. Applying inverse DCT or DST and reshaping into 1D.
6. Synthesis segments of reconstructed speech signal and decryption process is the reverse of encryption process as shown in Fig. 2.

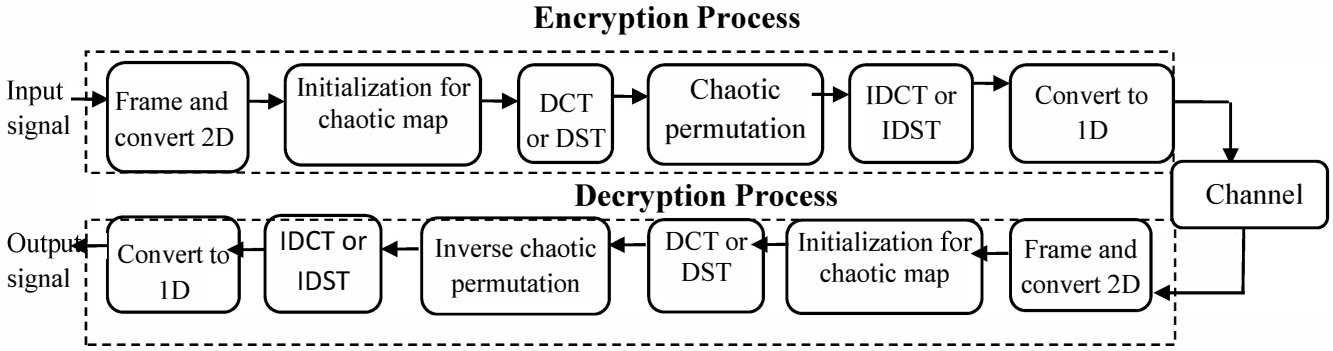

Fig. 2 Cryptosystem Block diagram

5. Simulation Results

The following sub sections are dedicated to present and discuss the results of the conducted tests by proposed cryptosystem to evaluate its performance. The objective measures used in this work are Signal to Noise ratio (SNR), Segmental Signal-to-Noise Ratio (SNRseg), Log-Likelihood Ratio (LLR) and Spectral Distortion (SD) [8, 12, 17]. For evaluation purposes, 'These days chicken legs are areal dish" speech signal with sampling frequency of 16 kHz has been selected as test material.

5.1 Quality of encrypted signal

The residual intelligibility is the accuracy with which we can hear what is being said. To measure the residual intelligibility of the encrypted signal four quality measures are used: SNR, LLR, SD and SNR_{seg} measure. As the value of the LLR, SD is increased and the values of SNR, SNRseg are decreased, the great quality of the encrypted signal. Table 1 explains the result for proposed system (for simplicity, DCT and DST will be used to refer to proposed cryptosystems used Discrete cosine transform and that used Discrete sine transform respectively). From Table 1 the LLR, SD measures for encrypted signals is high while SNRseg and SNR measures are very low (negative value) which means that no residual intelligibility. Fig.3 shows original speech signal and its spectrogram and encrypted signal in DST domain and in DCT domain for logistic encryption and their spectrograms. It is obvious that encrypted signal like Wight noise from encrypted spectrogram.

Table 1 quality metrics for encrypted signal in DST and DCT for logistic, Henon and baker encryption

	2D Logistic		Baker		Henon	
	DCT	DST	DCT	DST	DCT	DST
SNR(dB)	-3.0013	-2.9921	-2.6200	-2.6679	-3.0250	-3.0223
LLR	0.6309	0.6425	0.7972	0.7377	0.6727	0.7253
SD	13.7541	13.7656	13.0816	13.1611	13.8544	13.8071
SNR_{seg} (dB)	-3.0197	-3.0104	-2.6676	-2.7075	-3.0423	-3.0380

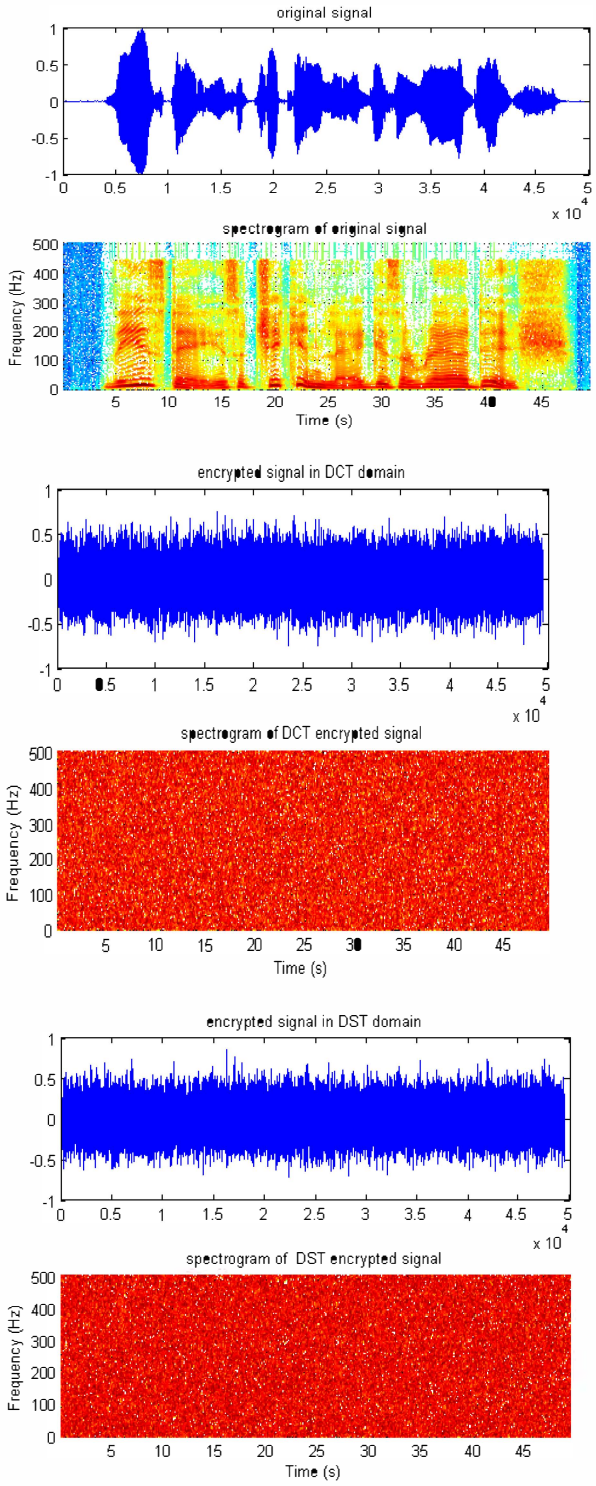

Fig.3 Waveform and spectrograms for original and Logistic encrypted signal in DCT and DST domain.

5.2 Quality of decrypted signal

Table 2 illustrates a comparison between the three chaotic maps techniques for the decrypted

signal with four quality measures; SNR, LLR, SD and SNR_{seg} measures. As the values of the LLR and SD are decreased, and the values of SNR and SNRseg are increased, the great quality of the decrypted signal.it is observed that SNRseg and SNR measures in Tables 2 are very high (positive values) for all the decrypted signals while the LLR and SD measures have small values that indicates high precision data and very good quality of the recovered speech signals. It is clear the recovered waveform is nearly equal to original signal shown in Fig. 4.

Table 2 quality metrics for Decrypted signal in DST and DCT for logistic, Henon and baker encryption.

	2DLogistic		Baker		Henon	
	DCT	DST	DCT	DST	DCT	DST
SNR	306.6085	302.210	306.6093	302.1817	306.5684	302.1390
LLR	$9.78E^{-16}$	$9.32E^{-16}$	$1.40E^{-15}$	$8.93E^{-16}$	$1.02E^{-15}$	$9.10E^{-16}$
SD	$1.07E^{-14}$	$1.70E^{-14}$	$1.16E^{-15}$	$2.03E^{-14}$	$1.02E^{-14}$	$1.68E^{-14}$
SNR_{seg}	306.518	302.1559	306.5699	302.1450	306.5173	302.0967

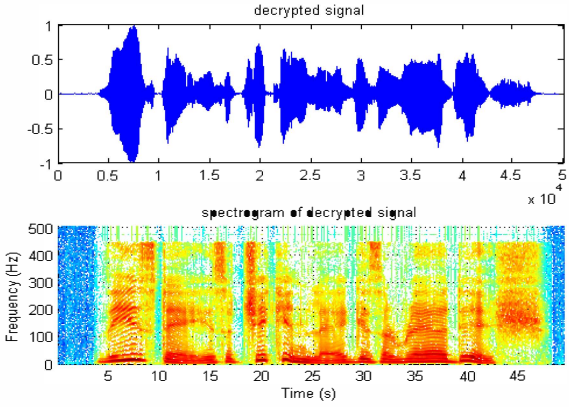

Fig.4 Waveform and spectrogram for recovered signal

5.3 Effect of noise on decrypted signal

The experiments have been implemented on the decryption in the presence of noise at different SNR values. The experiments results have been shown in Figs. (5,and 6). It has been carried out by adding AWGN with SNRs ranges from 0 up to 40 dB for Logistic, Baker and Henon encryption methods in DCT and DST domains. It is clear that the objective quality metrics values are better at high SNR values. Therefore, the speech cryptosystem can tolerate noise with high SNR values above 30dB.

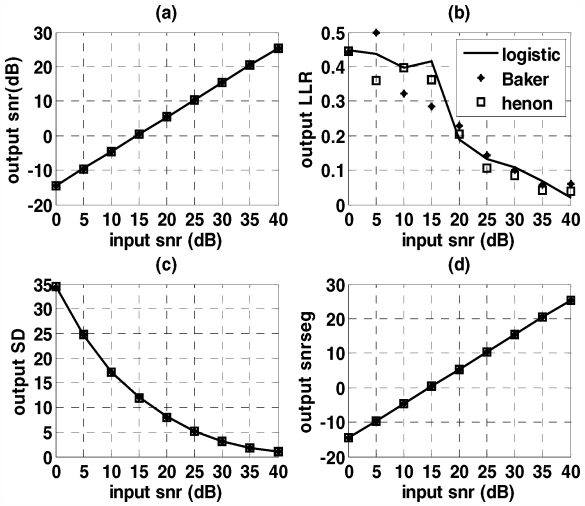

Fig. 5 Quality metrics for the decrypted signal with different SNR due to noise for DCT logistic, Baker and Henon encryption (a) SNR. (b) LLR (c) SD d) SNRseg

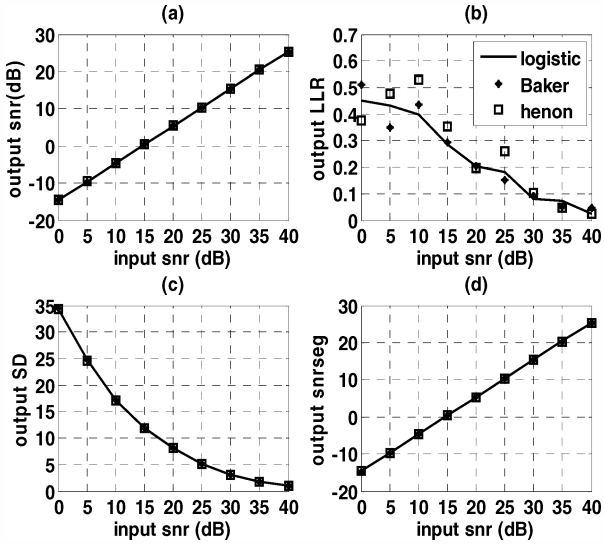

Fig.6 Quality metrics for the decrypted signal with different SNR due to noise for DST logistic, Baker and Henon encryption. (a) SNR. (b) LLR. (c) SD. d) SNRseg.

It is obvious that cryptosystem is low complex for speech signal and has high quality recovered signal. It has been shown that proposed cryptosystem is proved to be robust to noisy environment.

7. Conclusion

In this paper, we have used different versions of 2D chaotic maps to encrypt speech signal. As 2D chaotic maps involve more controlling parameters and sensitive to initial conditions, these give encryption and decryption process high security. The experimental results show that 2D chaotic maps encryptions are effective, give a high level of security and produce a good quality of recovered speech signal. Where permutation process is not sufficient in encryption process in time domain to remove all intelligibility of speech, substitution with transform domains are used to remove rest of intelligibility and increase level of security. The proposed system is tested under different levels of Wight Gaussian noise and proves that it can tolerate noise with high SNR and gives a good decrypted speech signal. In future, these encryption methods can be applicable for the watermarking techniques in different versions

References

[1] H. Kohad, V. R .Ingle, and M. A. Gaikwad "An Overview of Speech Encryption techniques", International Journal of Engineering Research and Development ISSN, vol. 3, Issue 4 , pp. 29-32, 2012.

[2] D. Ambika and V. Radha, "Secure Speech communication – A Review", International Journal of Engineering Research and Applications (IJERA), Vol. 2 Issue 5 PP, 2012.

[3] B. Goldburg, S. Sridharan, and E. Dawson, "Design and cryptanalysis of transform-based analog speech scramblers", IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, pp. 735–744, 1993.

[4] A. Matsunaga, K. Koga, and M. Ohkawa, "Analog speech scrambling system using the FFT technique with high-level security", IEEE Journal on Selected Areas in Communications, vol. 7, no. 4, pp. 540–547, 1989.

[5] S. B. Sadkhan,N. H. Kaghed and L. M. AlSaidi "Design and Evaluation of Transform – Based Speech Scramblers using different Wavelet Transformations", Communication System, Networks and Digital Signal Processing, Fifth International Symposium Conference. (CSNDSP), University of Patras, Greece, 19-21, July 2006.

[6] H. Zhao, S. He, Z. Chen, and X. Zhang "Dual Key Speech Encryption Algorithm Based Underdetermined BSS", The Scientific World Journal , 2014.

[7] S. M. H. Alwahbani and E. B. M. Bashier, "Speech scrambling based on chaotic maps and one time pad", in Proceedings of the International Conference on Computing, Electrical and Electronics Engineering (ICCEEE '13), pp. 128–133, August 2013.

[8] E. Mosa, N. W. Messiha , Z. Zahran and F. E. Abd El-Samie, "Encryption of Speech Signal with Multiple Secret Keys in Time Transform Domains", Int. J Speech Technol., vol. 13, pp. 231-242, 2010.

[9] N. A. Saad. and H. Eman, "Speech Encryption based on Chaotic Maps", International Journal of Computer Applications (0975 – 8887), vol. 93, no 4, May 2014.

[10] G. Manjunath and G. V. Anand, "Speech encryption using circulant transformations", in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '02), vol. 1, pp. 553–556, 2002.

[11] A. V. Prabu, S. Srinivasarao, A. Tholada, M. Jaganmohan Rao and K. Babu Rao, "AudioEncryption in Handsets", International Journal of Computer Applications , vol. 40 No. 6, pp. 40-45, 2012.

[12] G. Haojiang, Z. Yisheng, L. Shuyun and L. Dequn, " A new chaotic algorithm for image encryption", Chaos, Solitons and Fractals, vol. 29, Issue 2, pp. 393–399,2006.

[13] W. Yue, Y. Gelan, J. Huixia and P .N. Joseph P. N, "Image Encryption using the Two-dimensional Logistic Chaotic Map", Journal of Electronic Imaging Volume 21, Issue 1, January 2012.

[14] M. Henon, **"**A two-dimensional mapping with a strange attractor**",** Commun. Math.Phys., vol. 50, pp. 69-77, 1976.

[15] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps", Int. Journal of Bifurcation and Chaos, vol. 8, Oct. 1998.

[16] F. Han, X. Yu, and S. Han, "Improved Baker Map for Image Encryption", in ISSCAA, pp. 1273–1276, 2006.

[17] H. Yi and C. L. Philipos "Evaluation of Objective Quality Measures for Speech Enhancement", IEEE Transaction on Audio, Speech, and Language Processing, vol. 16, NO. 1, JAN. 2008.