International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 9 – No.3, June 2015 – www.ijais.org

Cellular Automata and Chaotic Maps for Speech Signal Encryption

Eman Hato
Department of Computer Science, University of Al-Mustansiriyah
Baghdad, Iraqi

ABSTRACT
Speech is widely used in our daily life with cell phones and over the Internet, especially for long distance calls. Higher security for transmitting these data is required. Therefore an encryption scheme for the speech signal encryption based on combination of permutation and substitution are proposed in this paper.

The permutation process is performed based on permutation key that generated from Game of Life matrix which is a simple cellular automaton, remarkable for its complex behavior. . The substitution performed with mask key that generated from one dimensional cubic and sine chaotic maps. The initial conditions and control parameters for chaotic maps are used as password for the sender and receiver.

In order to check the performance of the proposed encryption algorithm , experimental implementation has been done. The results indicate that the encryption system provides encryption speech signal of low residual intelligibility while preserves the good quality of the recovered speech signal. The system has a large key sensitivity because a small change in the secret key causes a large change in the encrypted signal.

Keywords
Keywords: Speech encryption, Cellular automata, Game of life, Chaotic maps, Residual intelligibility.

1. INTRODUCTION
Speech encryption seeks to perform a completely reversible operation on speech to be totally unintelligible to any unauthorized listener. The effectiveness of the speech encryption system is determined by the amount of residual intelligibility (which is defined as the fraction of the original speech that can be understood from the encrypted signal without decrypted it which helps in easier recovery of the original information), the quality of recovered speech, key space, encoding delay and complexity of the system [1].

The dealing with human auditory system should keep the signal with little distortion, because the human auditory system is sensitive to degradation in speech signal. The challenge is to decrease the amount of residual intelligibility as much as possible in encrypted speech signals and preserving good quality of recovered speech signal with low complexity.

Due to the bulk data capacity and high redundancy of speech data, conventional cryptosystems such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are rarely used in existing voice communication systems. They computationally not suitable in providing ample security in real time applications; in addition, they are very sensitive to the presence of noise.

Therefore, the design of efficient speech security methods demands new challenges which can provide high security to the speech data [2]. To achieve this, the chaos-based techniques and cellular automat are considered efficient for dealing with bulky, redundant speech data, in addition to their random-like behavior, sensitivity to initial conditions, and their high confusion property.

This paper seeks to find out how to best benefit from cellular automaton and chaotic maps characteristics in speech encryption. The ability to obtain complex global behavior from simple local rules, simplicity, key sensitivity, large key space and breaking the correlation between speech samples effectively its main goal of the proposal.

The reset of this paper is organized as follows: In the next section cellular automaton is reviewed . In Section 3 the game of life as an example of a cellular automaton is discussed. Section 4 presents chaotic system. The proposed speech algorithm is presented in Section 5. Section 6 presents the test results for the proposed algorithm. Finally, the concluding remarks are given in Section 7.

2. CELLULAR AUTOMAT
A cellular automaton (CA) is widely used in applications such as random number generation, pattern recognition, routing algorithms, and games. Cellular Automata is a collection of cells and each cell change in states by following a local rule that depends on the environment of the cell. The environment of a cell is usually taken to be a small number of neighboring cells. Every cell changes its state based on the states of neighboring cells [3]. Neighbors of a cell are cells that touch that cell, horizontal, vertical, or diagonal from that cell.

In two dimensions CA, two common neighborhoods methods are used: Von Neumann and Moore neighborhoods. The Von Neumann neighborhood of a two dimensions CA is a diamond shaped neighborhood surrounding the cell where every cell has four neighbors, Whereas The Moore neighborhood of a two dimensions CA is a square shaped neighborhood surrounding the cell [4].

3. CONWAY'S GAME OF LIFE
The Game of Life an example of a cellular automaton is played on an infinite two-dimensional rectangular grid of cells. The GL consists of an [M*N] matrix of cells, where each cell may take only two states: alive or dead, represented by one and zero, respectively. Each cell has eight neighbors, according to the Moore neighborhood. At every time step,

also called a generation, each cell computes its new state by determining the states of the cells in its neighborhood and applying the transition rules to compute its new state.

Every cell uses the same update rules, and all the cells are updated simultaneously. A cell's next state is determined as follows [5]:

Birth: A cell dead at time t becomes alive at time t +1 if exactly three of its neighbors are alive at time t.

Death by overcrowding: A cell alive at time t dies at time t+1 if four or more of its neighbors are alive at time t.

Death by exposure: A cell alive at time t dies at time t+1 if one or none of its neighbors are alive at time t.

Survival: A cell alive at time t will remain alive at time t+1 if two or three of its neighbors are alive at time t.

The initial pattern is the first generation. The second generation evolves from applying the rules simultaneously to every cell on the game board, i.e. births and deaths happen simultaneously. Afterwards, the rules are iteratively applied to create future generations.

4. CHAOTIC SYSTEM

Chaotic system plays an active role in modern cryptography. The properties of chaotic system like sensitivity to a change in initial conditions and parameters, random-like behavior and unstable periodic orbits with long periods, are directly connected with cryptographic characteristics of confusion and diffusion, that makes chaotic system very important for application in cryptography [6].

In mathematics, a function that possesses some kind of chaotic behavior is defined as a chaotic function or map. The output of map is used as the input in the next calculation and that called iteration [7]. The iteration is similar to encryption rounds of a cryptographic algorithm that leads to the desired diffusion and confusion properties of the algorithm.

Brief descriptions for two types of the one dimensional chaotic maps that are used in this project are introduced in the following section:

4.1 Cubic Map

Cubic map is one of the most commonly used maps in generating chaotic sequences in various applications [8]. This map is formally defined by the following equation:

$$\boldsymbol{X_{n+1} = p.X_n\left(1 - X_n^2\right)} \quad (1)$$

The X_n is initial condition and p is control parameter. The Cubic map generates chaotic sequences in (0, 1) with p = 2.59.

4.2 Sine Map

Sine map is also one of the well-known and commonly employed maps in generating chaotic sequences as follows [9]:

$$\boldsymbol{X_{n+1} = r.sin(\pi X_n)} \quad (2)$$

Where the initial condition X_n takes value in the interval (0, 1) and the parameter **r** takes values 0.99.

5. PROPOSED SPEECH ENCRYPTION ALGORITHM

The general structure of the proposed Encryption algorithm is illustrated in figure (1). The input to this algorithm is the speech signal (waveform (.wav) file), where this file is segmented into blocks of length 256 samples per block. The proposed algorithm is encrypted speech signal at two levels. The permutation and substitution processes are performed at each level. At last the encrypted signal of two levels becomes the final output or encrypted signal for transmission.

The permutation process is performed in this project based on permutation key that generated from Game of Life matrix. The substitution performed with mask key that generated from one-dimensional cubic and sine chaotic maps. The initial conditions and control parameters for chaotic maps are used as password for the sender and receiver.

5.1 Permutation Level

The first level of proposed algorithm is permutation the samples in each block by permutation key. The final result is a new position to sample so the samples of the block appear to be randomly rearranged. The generation of permutation key based on Game of Life matrix and chaotic map which is used to generate the first generation of Game of life matrix. Either the sine or the cubic can be used to generation the first generation.

The first step in generation of permutation key is to generate a sequence of real number by chaotic map (sine or cubic). Then create two-dimensional array (cellular board) of size 16*16 (because the block size is 256) and storing the sequence of real number in it. Converting each value in cellular board array to zero or one is based on rule which is that if the value of cell in array is larger than (0.5), the corresponding cell is dead (0) else alive (1).The cellular board array is represented a seed of the Game of Life matrix.

The second step is to create two-dimensional array (perkey) of size 16*16 and set it to zero and set zero to counter which is represented the values in permutation key. When producing the first generation of the (cellular board) by applying the rules of Game of Life, for all position (i,j) such that cellular board(i,j) and perkey(i,j) equal to zero take the counter value and put it in the perkey(i,j) and increment counter value by one. The producing of Game of Life generation (cellular board) continues until all values of permutation key are completed (counter value equal to 256).

The last step is to convert two-dimensional array (perkey) to one dimensional array (key), by take column by column for more randomization. key array represented the permutation key.

The figure (2) displays simulation example for Generation of permutation key, and the procedure of the generation permutation key is provided in pseudo code (1).

Pseudo code (1) Permutation Key

Input: initial condition x, control parameter r.

Output: Permutation key.

Begin

Set perkey[] to zero

Set counter to zero

```
For ( i = 0, i < 16, i++)
      For (j = 0,  j < 16,  j++)
           {
              x = r * Math.Sin(Math.PI * x)
             if (x <= 0.5)
                  cellularboard [i, j] = 1
             else
                 cellularboard [i, j] = 0
           }
While (counter < 256)
{
     Update   cellularboard //applying Game of Life rule
     For ( i = 0, i < 16, i++)
          For (j = 0,  j < 16,  j++)
               if (cellularboard [i, j] == 0 && key[i, j] == 0)
                  {
                     per  key[i, j] =counter
                     counter++
                  }
}
       For ( i = 0, i < 16, i++)
          For (j = 0,  j < 16,  j++)
             {
              key[a] = perkey[j, i]
              a++
              }
End
```

5.2 Masking Level

To make this encryption algorithm more secure, the permuted samples are again fed to substitution process. Each sample value is changed by XOR operation with mask key value. The advantage of the masking process is removal of speech silence patterns.

The generation of mask is based on two chaotic maps (sine and cubic map), starting from random independent initial conditions (X_n and $Y_n \in (1,0)$ and Xn ≠ Yn, r and p are control parameters):

$$X_{n+1} = r.\sin(\pi X_n) \quad (3)$$

$$Y_{n+1} = p.Y_n(1 - Y_n^2) \quad (4)$$

The output values of these maps are real value in interval (0, 1). The bit sequence (0 or 1) is generated by comparing the outputs of both the sine and cubic maps in the following way:

$$Bit = \begin{cases} 0 \ if \ X_{n+1} < Y_{n+1} \\ 1 \ if \ X_{n+1} \geq Y_{n+1} \end{cases} \quad (5)$$

The sequence of Bit represented the final output for tow maps. To increasing randomization anther pare of sine and cubic maps with deferent initial conditions are taken to generation anther sequence of Bit, these sequence mixed with the first one. Each 16 Bits are converted to integer number and save in array that has the same length of block (in this project 256). This array represented the mask key.

The set of initial conditions and control parameters serves as the seed for the masking key. Figure (3) show the block diagram that describe the proposed of mask key generation.

All process in speech decryption algorithm will be performed in a reversed manner at the receiver side to obtain the decryption speech signal. The receiver must use the same procedure to generated keys (permutation and mask key) with the same initial conditions and control parameters that used in the transmitter side in order to generate the same keys.

6. PERFORMANCE TEST

The objective measures used in this work to assess the performance of the proposed algorithm are the following: Signal-to-Noise Ratio (SNR) and Correlation (r_{xy}) [10]. Four speech signals with sampling frequency of 8 kHz and 16 bits per sample have been selected as test files material.

6.1 Quality of Encrypted and Decrypted Signal

The residual intelligibility should be minimized as much as possible for encrypted signal. The residual intelligibility is the accuracy with which we can hear what is being said.

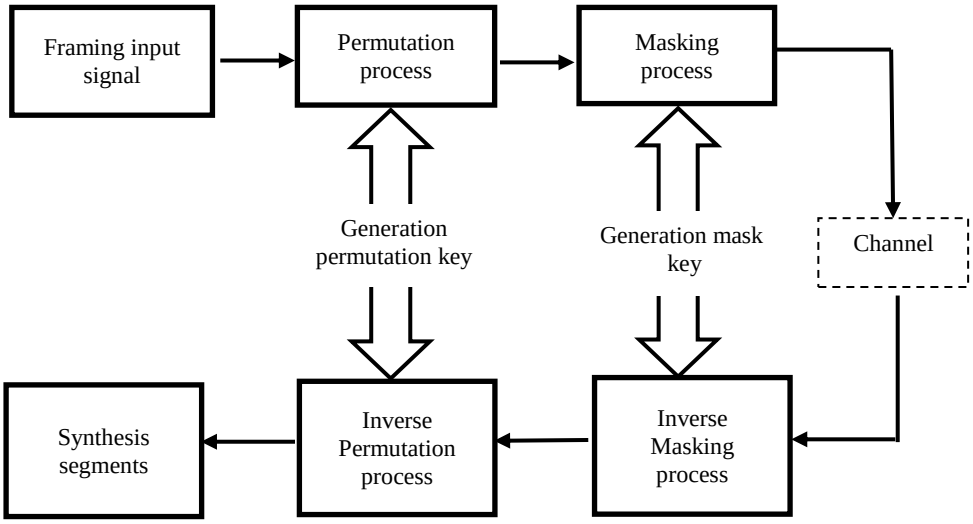

Fig (1): Structure of the proposed encryption algorithm

First

First Generation				
1	1	0	0	0
1	1	0	1	0
1	1	0	1	1
0	0	0	1	1
0	0	0	0	0

Pass

First Round in Key				
		0	1	2
		3		4
		5		
6	7	8		
9	10	11	12	13

Second

Pass

Second Generation				
1	1	1	0	0
0	0	0	1	1
1	1	0	0	0
0	0	1	1	1
0	0	0	0	0

Second Round in Key				
		0	1	2
14	15	3		4
		5	16	17
6	7	8		
9	10	11	12	13

After several passes the key will be:

Final Round in Key				
18	21	0	1	2
14	15	3	22	4
19	24	5	16	17
6	7	8	23	20
9	10	11	12	13

Final Permutation Key																							
18	14	19	6	9	21	15	24	7	10	0	3	5	8	11	1	22	16	23	12	2	4	17	20	13

Fig (2): Simulation example for Generation of permutation key

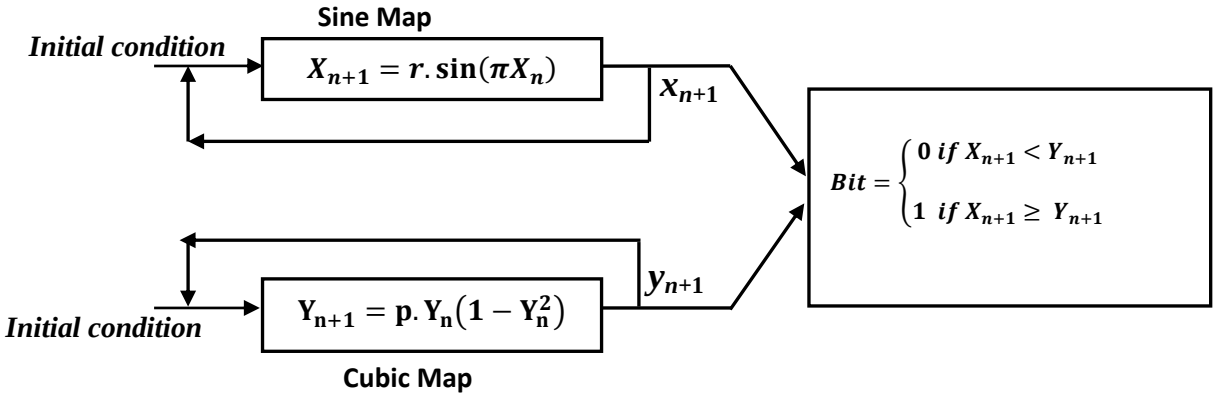

Fig (3): Generation of mask

To measure the residual intelligibility of the encrypted signal SNR and r_{xy} measures are used(calculated from the original and the distorted speech signal). As the value of the SNR and r_{xy} are decreased, the higher is the quality of the encrypted signal. While to measure the quality of decrypted signal, as the value of the SNR and r_{xy} are increased, the higher is the quality of the decrypted signal. Table (1) explains the result for encryption and decryption algorithm.

Table 1. Quality of encrypted and decrypted Signal

Test File	Encrypted Signal		Decrypted Signal	
	SNR	r_{xy}	SNR	r_{xy}
Sig1	-14.51423	-0.001268	103.33656	0.9999999
Sig2	-12.57547	0.008657	86.127819	0.9999999
Sig3	-12.98438	0.008274	109.66471	0.9999999
Sig4	-14.55949	-0.005108	100.37949	0.9999999

From table (1) the SNR measures for all the encrypted speech files are low (negative value) which means that the residual intelligibility is very low. While the r_{xy} measure has low value that indicates low correlation between original and the encrypted signals. Also one can observe that SNR measures are very high (positive values) for all the decrypted signals and correlation r_{xy} indicate a perfect positive correlation closed to one that means high correlation between original and the decrypted signals.

The waveform plotting is viewed signal in time domain. The waveform plotting is used because it is a powerful tool that allows seeing the difference in the time domains. Figures (4) to (7) show the waveform of original and their encryption and decryption signal respectively.

In Figures (4) to (7) it is important to note that the first level in the proposed algorithm (permutation) show a considerable residual intelligibility wills remains. The information has not been obviously destroyed in the encrypted signal; therefore, the substitution process is an important part in the proposed encryption algorithm.

6.2 Key Space and Sensitivity Analysis

Key space analysis is one of the important criteria of the performance analysis of encryption system. A good encryption algorithm should have a large key space, and also should be sensitive to the key value.

Key space size is the total number of different keys that can be used in the encryption. In the proposed algorithm, all initial conditions and control parameters constitute the secret key of encryption algorithm.

Key sensitivity means that the encrypted signal cannot be decrypted correctly, if there is any change between encryption and decryption keys. Large key sensitivity is required by all secure cryptosystems.

For testing the key sensitivity of the proposed algorithms the encrypted signal is decrypted with different key are generated by changing only one parameter in the original secret key.

The effect of tiny change can be viewed by waveform plotting for decrypted signals with different keys (changing initial condition for sine (x) and cubic (y) maps) which are totally different from waveform plotting for the decrypted signal with the original key as shown in figure (8).

It is clear from figure (8) that the waveform for signal decrypted with tiny changed key are totally different from the decrypted signal with the original key.

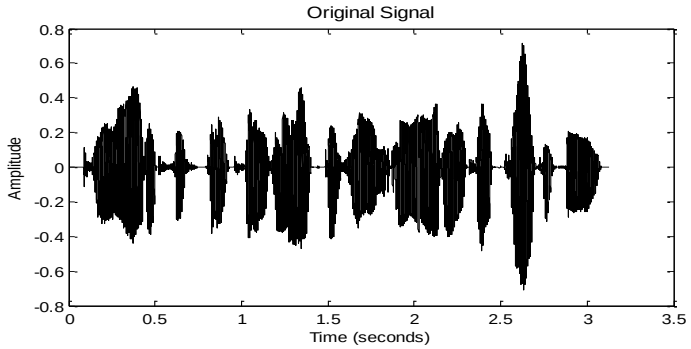

Fig (4): Waveform for original signal

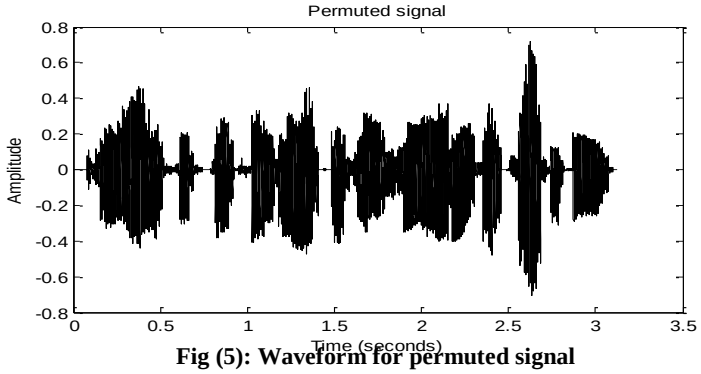

Fig (5): Waveform for permuted signal

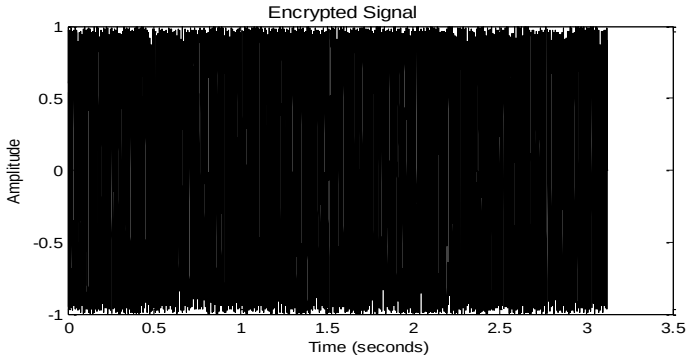

Fig (6): Waveform for encrypted signal

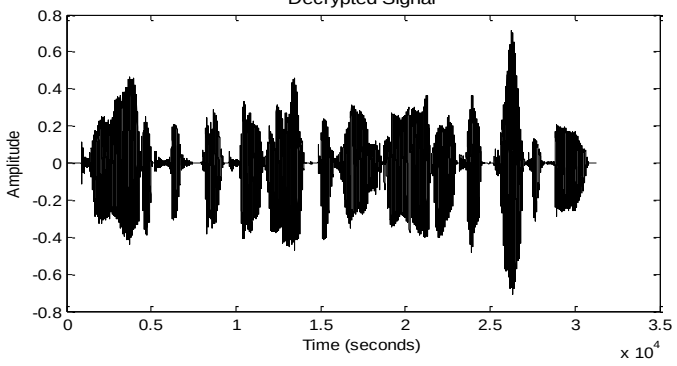

Fig (7): Waveform for decrypted signal

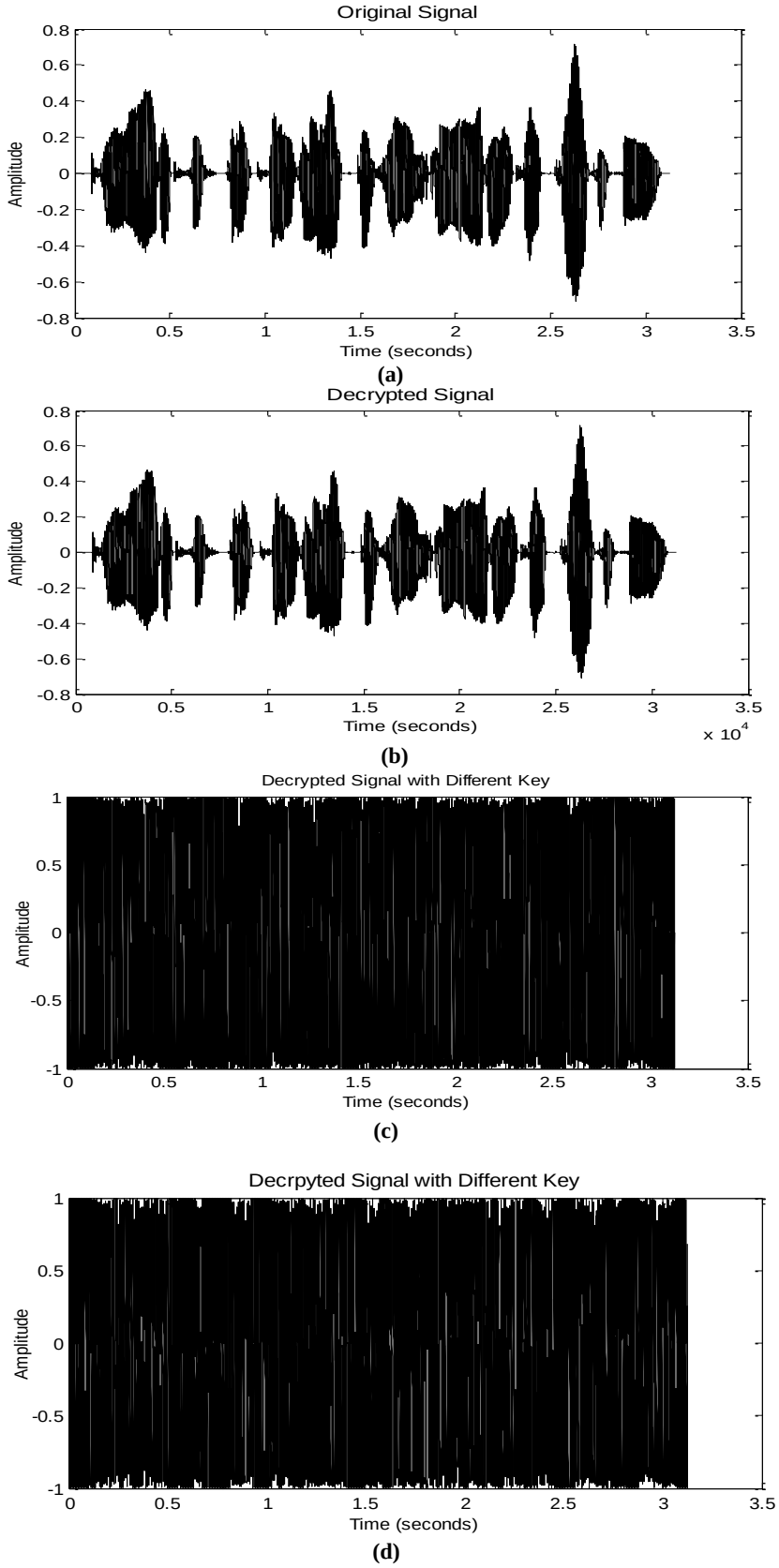

Fig (7): Waveform of: (a) Original signal (b) Decrypted signal with original key
(c) Decrypted signal with different key (changing y value from 0.55 to 0.54)
(d) Decrypted signal with different key (changing x value from 0.99995 to 0.99996)

7. CONCLUSIONS

The proposed algorithm in this paper encrypt speech signal using two parts; the first part works with permutation process and the second part works with substitution process with advantage of chaotic system and cellular automata (dynamic , nonlinear ,sensitivity to initial conditions, topological transitivity with iterative process) make the speech signal difficult to decrypt and more secure. The results show that the proposed algorithm returns a signal with very low residual intelligibility and high quality of recovered speech quality. The permutation process is not sufficient to remove speech silence patterns. Therefore, a masking step is very necessary in order to change the remaining non-permutated and silence portions of speech signals and that increases the security of the proposed algorithm. Also the proposed algorithm very sensitive to the initial condition .Key sensitivity indicates a high security and suitability of the proposed algorithms.

8. REFERENCES

[1] Srinivasan A. and Arul Selvan P., "A Review of Analog Audio Scrambling Methods for Residual Intelligibility", Innovative Systems Design and Engineering, Vol. 3, No. 7, PP. 22-39, 2012.

[2] Musheer Ahmad, Bashir Alam and Omar Farooq, "Chaos Based Mixed Keystream Generation for Voice Data Encryption", International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 1, PP. 39-48, 2012.

[3] Musheer Ahmad, Bashir Alam and Omar Farooq, "Chaos Based Mixed Keystream Generation for Voice Data Encryption", International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 1, PP. 39-48, 2012.

[4] Fasel Qadir , M. A. Peer, K. A. Khan, "Digital Image Scrambling Based on Two Dimensional Cellular Automata", I. J. Computer Network and information Security, Vol. 2, PP. 36-41, 2013.

[5] Alia Madain, Abdel Latif Abu Dalhoum, Hazem Hiary·Alfonso Ortega, Manuel AlfonsecaAlia Madain " Audio Scrambling Technique Based on Cellular Automata", Multimedia Tools and Applications, Vol. 71, Issue 3, PP. 1803-1822 , 2014.

[6] Ljupco Kocarev and Shiguo Lian (Eds.), "Chaos-Based Cryptography Theory, Algorithms and Applications, Studies in Computational Intelligence", Springer Vol. 354, 2011.

[7] Swati Rastogi and Sanjeev Thakur," Security Analysis of Multimedia Data Encryption Technique Using Piecewise Linear Chaotic Maps", International Journal on Recent and Innovation Trends in Computing and Communication Vol. 1, Issue 5, PP. 458 - 461, 2013.

[8] Hui Lu, Xiaoteng Wang, Zongming Fei, and Meikang Qiu, "The Effects of Using Chaotic Map on Improving the Performance of Multiobjective Evolutionary Algorithms" , Hindawi Publishing Corporation Mathematical Problems in Engineering , Article ID 924652,16 pages, 2014.

[9] N.K. Pareek , Vinod Patidar , K.K. Sud, "Cryptography using Multiple One-Dimensional Chaotic Maps", Communications in Nonlinear Science and Numerical Simulation, Vol.10, PP. 715–723, 2005.

[10] Mosa E. , Messiha N.W. , Zahran O. and Abd El-Samie F.E., " Chaotic Encryption of Speech Signals", Int. J Speech Technol., Vol. 14, PP. 285-296, 2011.