Lorenz and Rossler Chaotic System for Speech Signal Encryption

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

Dalya Shihab
Department of Computer Science,
University of Al-Mustansiriyah
Baghdad, Iraqi

ABSTRACT

In this paper an algorithm for speech encryption based on three dimension chaotic maps is proposed. The proposed algorithm consists of three main units: generation of keys, samples substitution and samples permutation process. In order to maximize the benefits of the substitution process, it is performed in two stages with cipher feedback, for the system. Moreover bit-level permutation for sample is introduced as substitution mechanism in the permutation stage. The Lorenz and Rossler chaotic system are employed as generation of keystream used for substitution and permutation process respectively. From the experimental results, it is concluded that the proposed algorithm has the advantages of very low residual intelligibility, key sensitivity and high quality recovered signal, and moreover the proposed algorithm can resist known- plaintext attacks and supports large key space make brute-force attacks infeasible.

Keywords

Speech encryption, Residual intelligibility, Lorenz system, Rossler system, Permutation, Substitution, Residual intelligibility.

1. INTRODUCTION

Speech is the primary mode of communication which uses words and accoutrements of languages. It is a way of sharing facts, thought and emotions, transfer of human intelligence, and information from person to person via sound.

Every single minute, billions and tons of sensitive speech data are travelled and transmitted over open and shared networks. In order to keep privacy or security, it is very important to protect these data over digital communications with fast and secure cryptosystems before transmission or distribution.Speech encryption system seeks to perform a completely reversible operation on a portion of speech, such that it is totally unintelligible format. In such a way, protected speech signal can be safely transmitted over public channels and networks, without worrying about being intercepted and captured.

Speech encryption techniques are generally, categorized into two types; analog and digital. The basic difference between these two types is the form in which the encrypted speech is transmitted. For an analog scrambler, the output is an analog signal while the output from a digital encryption, is a sequence of binary digits [1]. Analog speech encryption involves permutation of the speech segments in time, frequency or time–frequency domain. The main attraction of analog speech encryption is that it can be used with the existing analog telephone and narrow-band radio communication systems, while the disadvantage of the analog speech encryption techniques do not change the redundancy of speech greatly, which lead to the intelligibility of the encrypted signal [2]. And thus, analog encryption has low level of security. In Digital speech encryption, the signal is encrypted by modern digital cryptosystems such as the Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES) [3]. Therefore, Digital encryption is more secure than analog, but it needs a complex implementation.

Due to some intrinsic features of speech data, such as bulk data capacity and high redundancy, the conventional cryptographic algorithms may not be good candidates, especially for fast communication applications. To meet a great demand for real time applications, design of new algorithms that require less computational power while preserving a sufficient level of security is always a big challenge for researchers. Chaos has been introduced to cryptography with their many fundamental properties such as mixing properties ergodicity, pseudo-randomness, sensitivity to initial condition, and control parameters, which are close to confusion and diffusion in cryptography [4, 5]. These properties make chaotic systems a potential choice for constructing cryptosystems.

Unlike the conventional cryptographic algorithms which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Therefore, it can provide a fast and secure means for data protection, complexity, reasonable computational which is crucial for multimedia data transmission over fast communication channels [6, 7].This paper seeks to find out how to best benefit from chaotic maps characteristics in speech encryption. The ability to obtain complex global behavior from three dimension chaotic maps , low residual intelligibility, key sensitivity, large key space and breaking the correlation between speech samples effectively its main goal of the proposal.The remainder of the paper is organized as follows. In section 2 and 3 Lorenz and Rossler chaotic map are discussed as an example of three dimensions chaotic systems respectively. Section 4 explains in details the proposed speech encryption algorithm with the block diagram. Section 5 presents the test results for the proposed cryptosystem. Finally, the concluding remarks are given in Section 6.

2. CHAOTIC SYSTEM

Lorenz Chaotic Map is a system of three ordinary differential equations described by [8]:

$$\frac{dx}{dt} = \sigma(y-x)$$

$$\frac{dy}{dt} = x(\rho - z) - y \qquad (1)$$

$$\frac{dz}{dt} = xy - \beta z$$

Where t is time, x, y and z are initial conditions, and σ, ρ, β are the system parameters. When σ=10, ρ=8/3, β=28, the system exhibits chaotic behavior. Compared with one dimension chaotic map such as logistic map, tent map, and sine map, the Lorenz system has more complicated dynamical property, and number of state variables. Consequently, cryptosystem based on Lorenz system has stronger unpredictability and larger key space, so it can be candidate to provide excellent random sequence, which is suitable for information encryption [9].

3. ROSSLER CHAOTIC MAP

Rossler is continuous chaotic system. The three ordinary differential equations of Rossler can generate a chaotic behavior under certain conditions, which is defined in the following equations [10]:

$$\frac{dx}{dt} = -(y+z)$$

$$\frac{dy}{dt} = x + ay \qquad (2)$$

$$\frac{dz}{dt} = b + z(x-c)$$

Where the original classical Rossler system has parameters a=b=0.2 and c=5.7.

The Lorenz and Rossler differential equations are solved using RungeKutta-4 method with step size of 0.01 in this paper.

4. A PROPOSED SPEECH ENCRYPTION ALGORITHM

The proposed chaotic based speech encryption algorithm is presented in this section, which is designed to make use from chaotic cryptography by employing three dimension chaotic maps in key generation used in encryption/decryption algorithms. A complete architecture of the proposed encryption algorithm consists of three components (stages): keys generation schema, samples substitutions scheme and samples permutation schema, as shown in Figure 1. For applying proposed encryption algorithm, the speech signal is first framing (size of block is M where M=N*N) and reshaping into tow dimension format after applying three stages the output is resized to one dimension vector again to obtain encrypted speech signal. The following sub-sections describe these stages:

4.1 Key Generation Scheme

In most cryptosystems, the cryptographic key plays a significant part. No matter how strong and how well designed the encryption algorithm might be, if the key is poorly chosen or the key space is too small, the cryptosystem will be easily broken. So the problem of key generation is therefore an important issue in the design of a encryption system.

4.1.1 Masking Key

The mask key controls the substitution process, in which the sample's values are changed to other values without changing their positions in the input signal. The Lorenz system is employed to generate the mask key. The Lorenz chaotic system is iterated continuously for M Times. For each iteration three values x, y and z can obtained. These real values are preprocessed first and converted to short sing integer number. The integer value for x, y and z is saved in maskx, masky and maskz respectively. These three matrixes are combined and mixed using XOR operations to produce mask key array which is reshaped to tow dimension format. The procedure of the generation mask key is provided in pseudo code (1).

Pseudo code (1) Mask Key Generation

```
Input: initial condition (x,y,z) , parameter (σ, ρ, β) in the acceptable intervals.
Output: Mask key.
Begin
 Set maskx[M] ⟵ zero
 Set masky[M] ⟵ zero
 Set maskz[M] ⟵ zero
 for (int i = 0, i < M , i++)
  {
    Lorenz -Rungekutta ($x_i$, $y_i$, $z_i$) // generate the Lorenz values
                                 // (eq1) using rungkutta method.
    maskx[i]⟵ConvertToInt16((Abs ($x_i$-Floor(Abs ($x_i$)))*$10^9$)
    masky[i]⟵ConvertToInt16((Abs ($y_i$-Floor(Abs ($y_i$)))*$10^9$)
    maskz[i]⟵ConvertToInt16((Abs ($z_i$-Floor(Abs ($z_i$)))*$10^9$)
  }
for (int i = 0 , i < M , i+=2)
 {
  mask[i]⟵ maskx [i] XOR masky [i+1] XOR maskz[i]
  mask[i+1]⟵maskx [i+1] XOR masky [i] XOR maskz[i+1]
 }
 Convert mask to 2 D (two dimeansion).
 Return mask.
End.
```

Where Abs (x) returns the absolute value of x. Floor(x) rounds the elements of x to the nearest integers less than or equal to x. The function ConvertToInt16 (x) is converted decimal number x to short sing integer number (16-bit representation value), because in the proposed cryptosystem the samples in speech signal declared as type short integer which has a bit length of 16 bits.

4.1.2 Permutation Key

The main requirement of any permutation key is to minimize correlation between neighboring samples as much as possible. Three permutation keys are generated with length N; each one is generated from one of the differential equations of Rossler system using the chosen initial conditions and control parameter. This process can be summarized in Pseudo code (2) as follows:

Pseudo code (2) Permutation Key Generation

```
Input: initial condition (x,y,z) , parameter (a, b, c) in the acceptable intervals.
Output: Permutation keyes (key1,key2,key3).
Begin
 Set Key1 [M] ⟵zero
 Set Key2 [M]⟵ zero
 Set Key3 [M] ⟵ zero
Set J1, J2, J3 ← zero
While (J1≠ N  OR  J2 ≠ N  OR  J3≠N)
 {
   Rossler - Rungekutta(x, y, z) // generate the Rossler values
                              // (eq2) using rungkutta  method.
    xnew← ((Abs (x - Floor (Abs (x)))* $10^{9}$))) mod N) +1
                              // to ensure newx  ∈ [1,N].
   ynew← ((Abs (y - Floor (Abs (y)))* $10^{9}$))) mod N) +1
                              // to ensure newy  ∈ [1,N].
    znew← ((Abs (z - Floor (Abs (z)))* $10^{9}$))) mod N) +1
                              // to ensure newz  ∈ [1,N].
  if  (notfind (key1, newx)   AND    newx ≠ j1 )
          {
              key1[j1] ← newx
              j1++;
          }
  if  (notfind (key2, newy)  AND    newy ≠j2 )
          {
              key2[j2]← newy
              j2++
          }
  if  (notfind (key3, newz)  AND    newz ≠ j3 )
          {
              key3[j3] ← newz
              j3++
          }
 }
Return key1, key2, key3.
End.
```

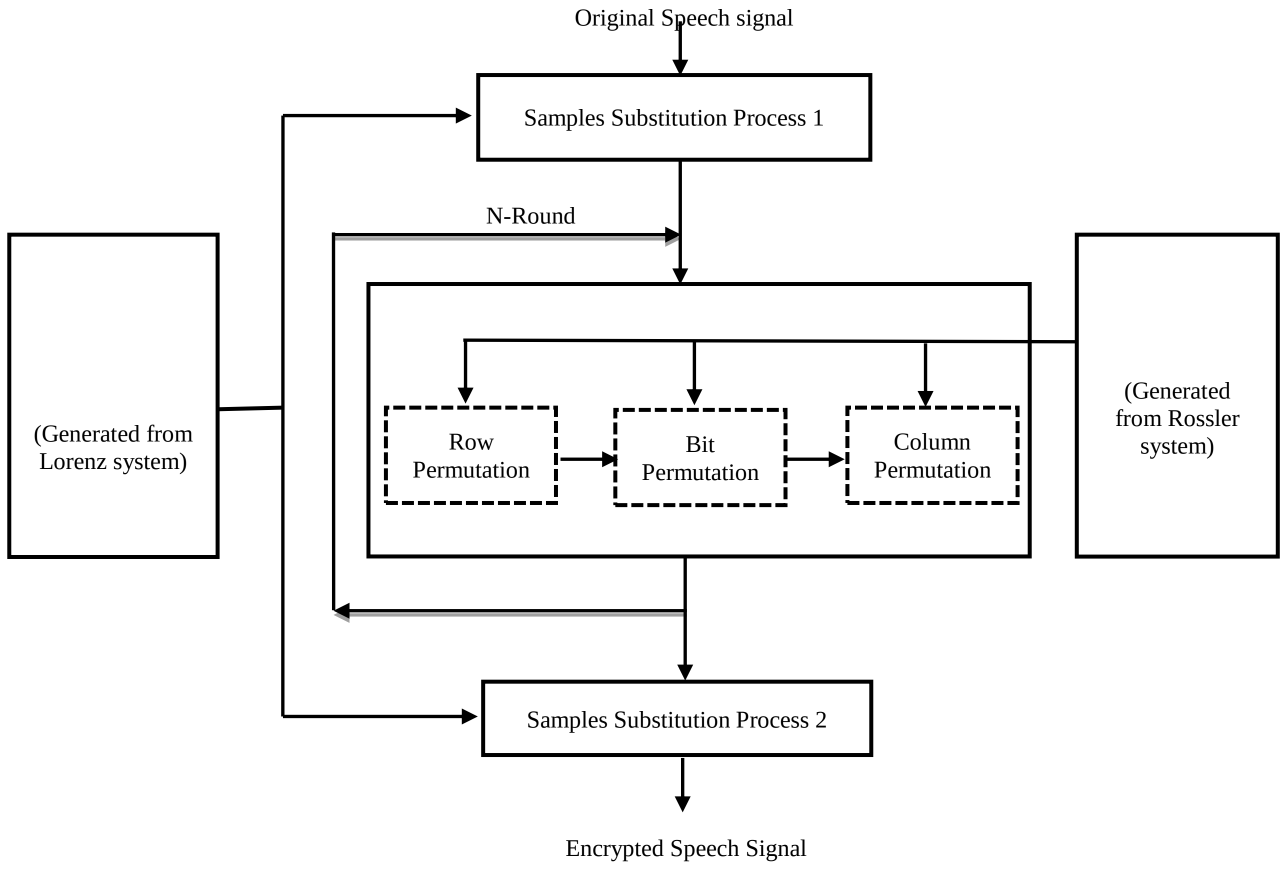

Original Speech signal
Samples Substitution Process 1
N-Round
(Generated from Lorenz system)
Row Permutation
Bit Permutation
Column Permutation
(Generated from Rossler system)
Samples Substitution Process 2
Encrypted Speech Signal

Fig (1) Structure of proposed system

Key matrix is an integer sequence containing N non-repeat integers and 1 ≤ key[i] ≤ N. It is excellent to be used for permutation samples in speech signal.

4.2 Samples Substitution Scheme

It is necessary to tack the substitution process it is role in the proposed encryption algorithm, because the permutation process only changes the original sample's position, however the discrete time's values have not been changed. The purpose of the substitution step is to change the power spectrum of the speech to overcome cryptanalysis attacks and removal of speech silence patterns. To make this encryption algorithm more secure and difficult to analyze, substitution is performed in two phases: The first phase the input block XOR with mask key by followding operation:

```
For (int i = 0, i < N, i++)
  For (int j = 0, j < N, j++)
  {
    if (i = 0)
       output[i, j] ← (input[i, j] XOR mask[i, j])
   else
   output[i,j]← (input[i,j] XOR mask[i,j] XOR output [i-1,j])
 }
```

Where mask is the mask key and output (i-1,j) is the feedback input row from the past encryption output.After permutation stage each permutation block is then substituted for another time (second phase) with another secret masking key, in the same procedure .To make the used of secret mask key unpredictable, one of permutation keys is selected randomly. The selected key used to permutated the row or column of masking key to produce the secret masking key that is used in second masking operation.The first objective of this step is to increase the key sensitivity and key space by using two different keys. The second objective is to prevent a cryptanalyst from discovering the secret key with known-plaintext attacks.

4.3 Samples Permutation Scheme

Permutation of speech samples will result in distortion of the speech time envelope, which reduces the intelligibility of the speech. The row – column permutation is an effective method to change all data locations within a two dimension data matrix (input block). Applying this method only one time can completely change all samples locations, achieving excellent diffusion property.There are three phases in this stage. The positions of row of the input block are permuted using the first permutation key to produce block1. Then the block 1 are transposed to produce block 2. Bit permutation is done for each sample in block 2 after convert it to binary form by using second permutation key. The columns of the block 2 are again permuted with third permutation key.

Permutation process needs to be performed alternatively for T (T>1) rounds according to the security requirement. Obviously, the more rounds are processed, the more secure the encryption is, but at the expense of computations and time delays.All process in speech encryption will be performed in a reversed manner at the receiver side to obtain the recovered signal. The keys are generated in the same procedure with the same initial conditions and control parameters to generate the same keys that used in transmitter side.

5. PERFORMANCE EVALUATION

Encryption speech system effectiveness 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), the quality of recovered speech, key space, and key sensitivity. Thus for low intelligibility and high key space and sensitivity the encryption effectiveness has higher level of security. Some security analysis has been performed on the proposed speech encryption scheme using ten speech signals with sampling frequency of 8 kHz and 16 bits per sample as test files material.

5.1 Waveform and Spectrogram Plotting

The waveform plotting is viewed signal in time domain while a spectrogram is a method for viewing signal, which plots the frequency of a signal against time against amplitude. The spectrogram plotting is used because it is a powerful tool that allows seeing the difference in the frequency and time domains.Figure (2) and (3) show the waveform and spectrogram plotting for original, encrypted and the decrypted signal respectively that resulted from applying proposed system.

As shown in figure (2.b) and figure (3.b) The waveform and spectrogram of the encrypted signal is uniformly distributed and is significantly different from that of the original signal that mean the residual intelligibility have been obviously destroyed, while in figure (2.c) and figure (3.c) the proposed algorithm preserving the high quality of recovered signal.

5.2 Quality of Encryption and Decryption Signal

The objective measures used in this paper to assess the performance of the considered schema are the following:

5.2.1 *Signal-to-Noise Ratio (SNR)*

Signal-to-Noise Ratio (SNR) is one of the oldest and widely used objective measures. It is mathematically simple to calculate, but requires both distorted and undistorted (clean) speech samples. SNR can be calculated as follows [11]:

$$\mathrm{SNR} = 10\log_{10} \frac{\sum_{n=1}^{N} x^2\ (n)}{\sum_{n=1}^{N} [x(n)-y(n)]^2}\,(\mathrm{dB}) \qquad (3)$$

Where x (n) is the clean speech, y (n) is the distorted speech and N is the number of samples. When the value of the SNR is decreased, the higher is the quality of the encrypted signal, and when the value of SNR is increased, the higher is the quality of the decrypted signal.

5.2.2 *Log-Likelihood Ratio (LLR)*

The Log-Likelihood Ratio (LLR) measure is a distance measure that can be directly calculated from the LPC vector of the original and distorted speech. LLR measure can be calculated as follows [12]:

$$d_{LLR}(a_d, a_c) = log\left|\frac{a_c R_d a_c^T}{a_d R_d a_d^T}\right| \qquad (4)$$

Where ac is the LPC coefficient vector for the original speech, ad is the LPC coefficient vector for the distorted speech, aT is the transpose of a, and Rc is the auto-correlation matrix for the distorted speech. As the value of the LLR is increased, the higher is the quality of the encrypted signal. While the closer the LLR to zero, the higher is the quality of the decrypted signal.

5.2.3 *Correlation Analysis*

A useful measure to assess the encryption quality of any cryptosystem is the correlation coefficient between original signal and the distorted signal (encrypted or decrypted signal). It can be calculated as follows [12]:

$$r_{xy} = \frac{c_v(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (5)$$

Where cv (x, y) is the covariance between the original signal x and the distorted signal y. D(x) and D(y) are the variances of the signals x and y. In numerical computations, the following discrete formulas can be used [10]:

$$E = \frac{1}{N_s}\sum_{i=1}^{N_s} x_{(i)} \qquad (6)$$

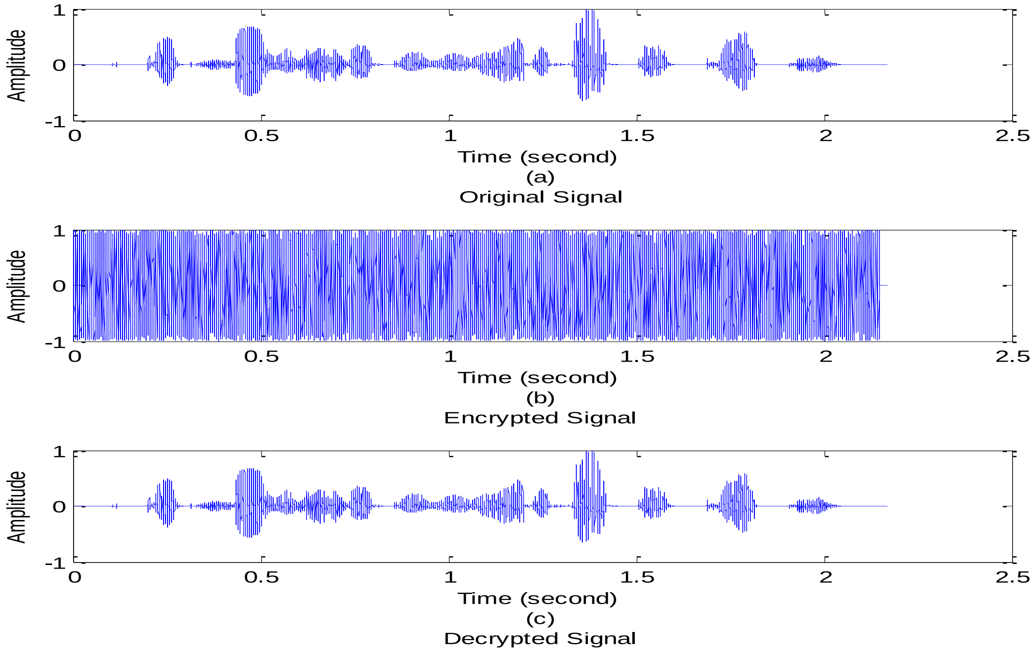


Fig (2): Waveform plotting for speech signal

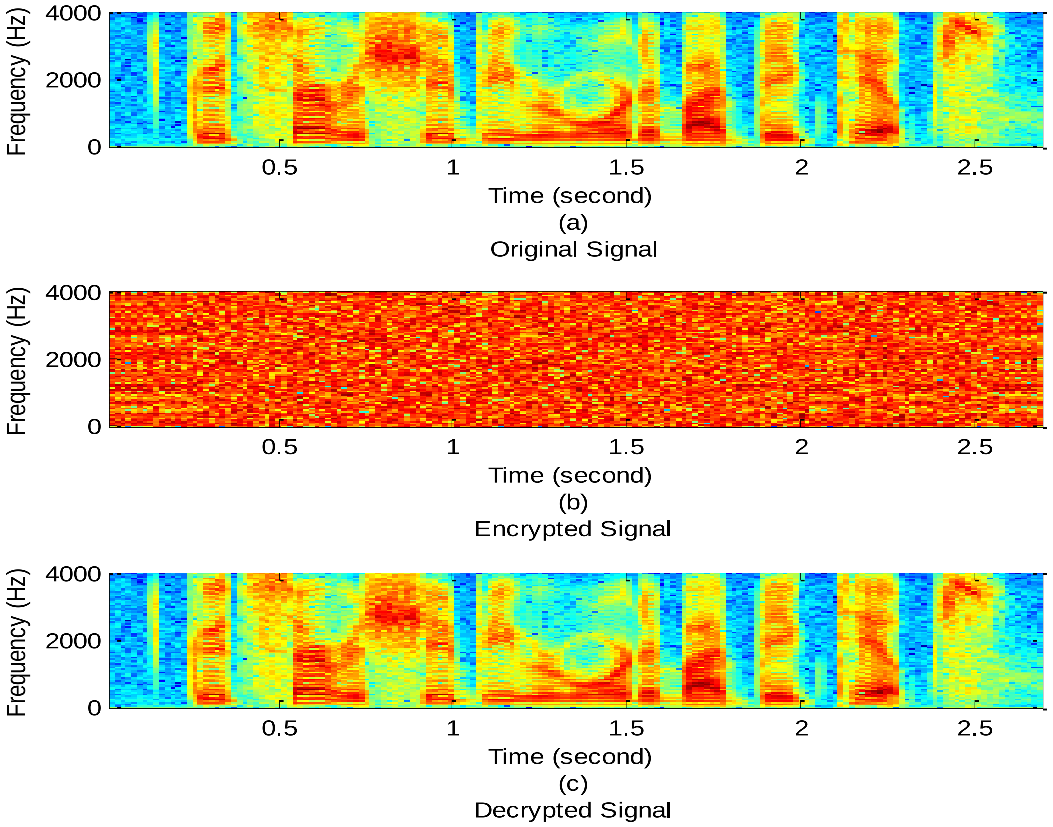


Fig (3): Spectrogram plotting for speech signal

$$D(x) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i) - E(x))^2 \quad (7)$$

$$D(y) = \frac{1}{N_s}\sum_{i=1}^{N_s}(y(i) - E(y))^2 \quad (8)$$

$$c_v(x, y) = \frac{1}{N_s}\sum_{i=1}^{N_s}\big(x(i) - E(x)\big)\big(y(i) - E(y)\big) \quad (9)$$

Where Ns is the number of speech samples involved in the calculations.Possible correlations range from +1 to –1. A zero correlation indicates that there is no relationship between the variables. A correlation of –1 indicates a perfect negative correlation, indicating that as one variable increases, the other decreases. A correlation of +1 indicates a perfect positive correlation, indicating that both variables move in the same direction together.The closer the correlation coefficient to zero indicates a good encryption signal quality. While the high value of the correlation coefficient (closed to +1) indicates a high quality of the recovered speech signals.

Tables (1) and (2) illustrate the result for the result of residual intelligibility for encrypted signal and the quality for decrypted signal respectively.

Table 1.Quality of encrypted signal

Speech Files	File Length(sec)	Residual Intelligibility for Encrypted Signal		
		SNR	r_{xy}	LLR
File1.wav	4	-12.1727	0.003709	3.903171
File2.wav	7	-12.5180	-0.0070302	1.583985
File3.wav	3	-13.1761	0.0040266	2.492488
File4.wav	5	-12.8276	-0.0079925	3.903265
File5.wav	3	-14.2173	0.0041806	3.012454
File6.wav	7	-12.8664	-0.006945	2.421469
File7.wav	3	-11.2945	-0.004219	2.553185
File8.wav	7	-11.8330	0.00463585	1.466915
File9.wav	2	-16.9325	0.00143716	1.586511
File10.wav	2	-10.8529	-0.0007413	2.818174

Table 2.Quality of decrypted signal

Speech Files	File Length(sec)	Residual Intelligibility for Encrypted Signal		
		SNR	r_{xy}	LLR
File1.wav	4	46.51441	0.99998884	0.00291744
File2.wav	7	46.02466	0.99998751	0.00024889
File3.wav	3	62.94940	0.99999974	0.00027866
File4.wav	5	43.92237	0.99997973	0.00956166
File5.wav	3	43.92237	0.99997671	0.00417508
File6.wav	7	45.68213	0.99998648	0.00015018
File7.wav	3	43.52031	0.99997777	0.00200069
File8.wav	7	46.73266	0.99998939	0.00085952
File9.wav	2	96.94488	0.99999999	0.00018656
File10.wav	2	46.21872	0.99998805	0.00084561

From Table (1) the r_{xy} measure has low value that means low correlation between original and the encrypted signals. The LLR measure for all the encrypted signals is high while SNR measures are very low (negative value) which means that no residual intelligibility and encrypted signals are very noisy.

One can observe that SNR measures in Tables (2) is high (positive values) for all the decrypted signals while the LLR measure has a small value that indicates very good quality of the recovered speech signals.Correlation coefficients (r_{xy} measure) indicate high correlation between original and the decrypted signals for all the encrypted signals.

5.3 Key Analysis

A good encryption should resist all kinds of known attacks, it should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible.

5.3.1 Key Space Analysis

It is generally accepted that a key space of size larger than 2^{128} is computationally secure against brute-force attack.The initial values of Lorenz and Rossler chaotic system are used as secret keys, if the precision is 10^{-12}, all keys parameters can take 10^{12} possible values. Therefore, the key space comes out as $(10^{12})^6 \approx 2^{238}$, which is large enough to resist all kinds of brute-force attacks.These results suppose a known secret control parameters and the number of rounds in permutation stage by the attacker, but really they are unknown making the search infeasible.

5.3.2 Key Sensitivity Analysis

A good encryption algorithm should be sensitive to all the secret keys in order to have large variation in outputs even if there is only a tiny change in the keys.In order to evaluate the key sensitivity of the proposed algorithms, only one parameter of keys is changed at a time by a tiny amount of (0.0000000001) keeping all other parameters of keys unchanged and the decryption operations is applied to recover the speech signal.

The SNR, r_{xy} and LLR are estimated between each decrypted signal using different keys with slight changes (key1, key2, key3, key4) and the signal decrypted with the original key, and the results are listed in Table (3). The low SNR, r_{xy} value and large LLR value show the large key sensitivity of the proposed algorithms.It is clear from the Table (3) that very low correlation exists among the signals decrypted with tiny changed key and they are totally different from the decrypted signal with the original key.

Table 3.Test for key sensitivity

keys	SNR	r_{xy}	LLR
Key1	-16.8486	-0.0007739	1.5541921
Key2	-17.0923	-0.0003076	1.6733727
Key3	-16.8789	0.0082955	1.7815166
Key4	-17.3588	-0.0074569	1.6129031

The key sensitivity can be viewed by waveform and spectrogram plotting for decrypted signals with different keys as shown in figure (4) and (5). From Figure (4) and (5) one can find that the waveform and spectrogram of the encrypted signal with tiny change is fairly uniform, this is totally different from that of decrypted signal with the original key. From two tests prove that the proposed speech encryption algorithm is highly sensitive to the secret key and can flatten the waveform.

5.3.3 Known-Plaintext Attack

The known-plaintext attack is an attack model of cryptanalysis, where the attacker has samples of both the plaintext and its ciphertext and has liberty to make use of them to reveal the secret key (XOR both the values and obtain the key value that was XORed to the original plaintext). In modern cryptosystems that use standard block sizes, permutation and substitution processes may be analyzed to discover the key, while in the proposed cryptosystem; there is no standard block size. Therefore, the knowledge of the input signal without knowledge of the block size is useless as it is very difficult to guess the key. Moreover the feedback scheme makes it difficult to predict the key value XORed to the original input signal.

6. CONCLUSION

An efficient speech encryption algorithm based on three dimension chaotic maps is presented in the paper. It is based on permutation and substitution process that are controlled by multiple secret keys in several rounds to increase the confusion and diffusion of speech samples. Due to the sensitivity to initial values, system parameters, ergodicity and complex behavior in three dimension chaotic system, Lorenz and Rossler maps are candidate to design and generate the secret keys.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 measured for encrypted and decrypted signal quality showed that the proposed algorithm has a noisy encrypted signal and high quality of recovered speech signal.

Security analysis are given to demonstrate that the proposed encryption algorithm has large key space which makes a brute-force attack impracticable , highly sensitivity to the secret keys even if there is only a slight change, makes the cryptanalysis a difficult task and increases the security of the speech signal.

7. REFERENCES

[1] Sadkhan Sattar B. and Abbas Nidaa A., "Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach" ATTI DELLA “Fonazione Giorgio Ronchi” Anno Lxvi, No. 5 PP. 601-6014 (2011).

[2] Ambika D. and Radha V., "Secure Speech communication – A Review” International Journal of Engineering Research and Applications (IJERA), Vol.2 Issue 5 PP. 1044-1049 (2012).

[3] Mosa E.; Messiha N.W.; Zahran O. and Abd El-Samie F.E. "Encryption of Speech Signal with Multiple Secret Keys in Time Transform Domains " Int. J Speech Technol., Vol. 13 PP. 231-242 (2010).

[4] 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).

[5] Prabu A.V.; Srinivasarao S.;Tholada Apparao, Jaganmohan Rao M. and Babu Rao K., "Audio Encryption in Handsets" International Journal of Computer Applications (0975 - 8887), Vol. 40 No. 6 PP. 40-45 (2012).

Amit Pande and Joseph Zambreno, "A Chaotic Encryption Scheme for Real-Time Embedded Systems: Design and Implementation" Springer Science-Business Media, LLC (2011).

[6] 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).

[7] Osama S. Faragallah, "An Efficient Block Encryption Cipher Based on Chaotic Maps for Secure Multimedia Applications" Information Security Journal: A Global Perspective, Vol.20 PP.135–147 (2011).

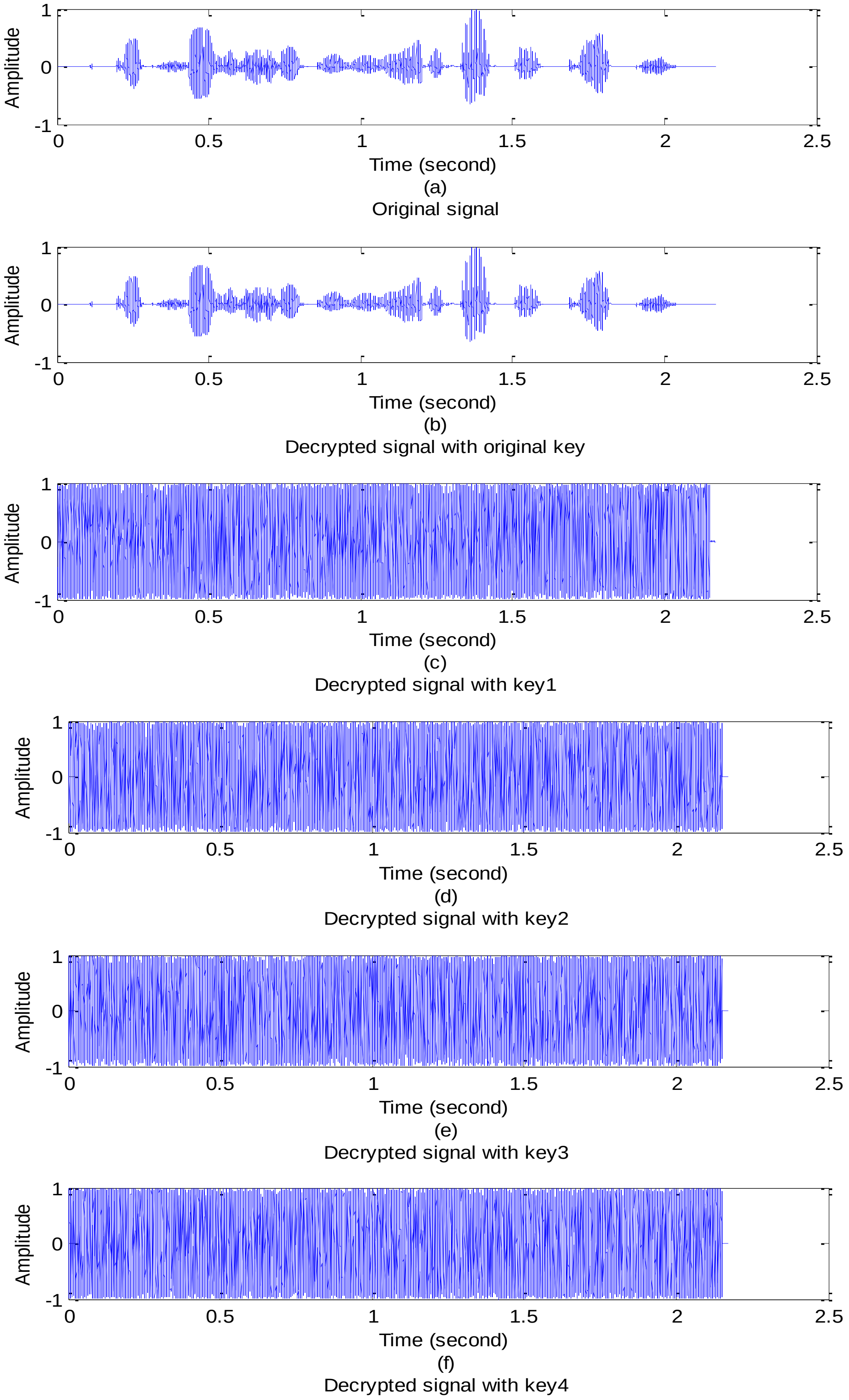
[8] Ashtiyani M.; Moradi Birgani P. and Karimi Madahi S. S., "Speech Signal Encryption Using Chaotic Symmetric Cryptography" J. Basic. Appl. Sci. Res., Vol. 2 No. 2 PP. 1678-1684 (2012).

[9] Bin Muhaya Fahad T., " Chaotic and AES Cryptosystem for Satellite Imagery" Telecommun Syst, Vol. 52 PP. 573–581 (2013).

[10] Sadkhan Sattar B. and Abbas Nidaa A., "Speech Scrambling Based on Wavelet Transform," in , "Advances in Wavelet Theory and Their Applications in Engineering" Physics and Technology, edited by: Dumitru Baleanu, InTech, (2012).

[11] Kondo, K., "Subjective Quality Measurement of Speech its Evaluation, Estimation and Application" Springer (2012).

8. APPENDIX



(a)
Original signal

(b)
Decrypted signal with original key

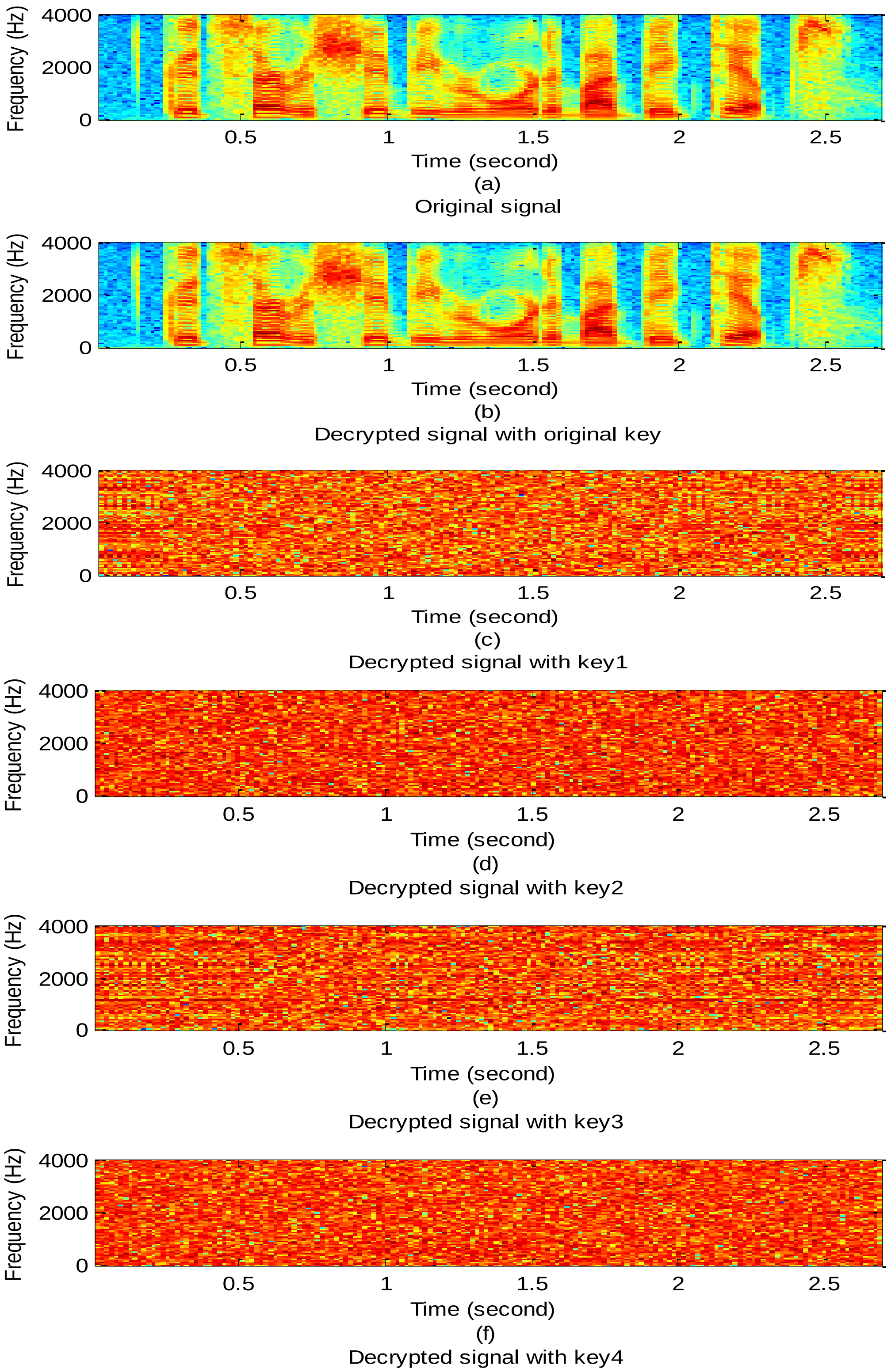
(c)
Decrypted signal with key1

(d)
Decrypted signal with key2

(e)
Decrypted signal with key3

(f)
Decrypted signal with key4

Fig (4): Waveform plotting for speech signal



(a)
Original signal

(b)
Decrypted signal with original key

(c)
Decrypted signal with key1

(d)
Decrypted signal with key2

(e)
Decrypted signal with key3

(f)
Decrypted signal with key4

Fig (5): Spectrogram plotting for speech signal