Journal of Engineering and Applied Sciences 14 (17): 6392-6399, 2019
ISSN: 1816-949X

Speech Encryption Based on Zaslavsky Map

Sura F. Yousif
Department of Chemical Engineering, Collage of Engineering, University of Diyala, Diyala, Iraq
sura.fahmy@yahoo.com

Abstract: In information transmission such as speech information, higher security and confidentiality are especially required. Therefore, data encryption is pre-requisite for secure communication system to protect such information from unauthorized access. In this research, a new speech cryptographic technique based on combination of permutation and substitution of speech samples using chaotic Zaslavsky map is presented. The original speech signal is first, transformed from one dimensional to two dimensional blocks. Then Zaslavsky map is utilized to produce permutation and mask keys to be used in permutation and substitution processes. Third, each block is permuted to shuffle the positions of speech signal samples followed by substitution process to change the values of permuted samples. And finally, encrypted blocks are transformed back into one dimension to produce ciphered speech signal ready for transmission. The results demonstrate that the presented speech cryptosystem provides a high level of security, confidentiality and high intelligibility reconstructed speech signal.

Key words: Speech, encryption, decryption, cryptography, security, chaos, Zaslavsky map, permutation, substitution, analysis, quality metrics.

INTRODUCTION

In our daily life, speech communication has an important functionin all activities such as education, phone banking, e-Learning, commerce, military, politics etc. A huge amount of sensitive audio data is exchanged over shared and open networks in such applications. Thus, there is a dire need for cryptographic algorithms to provide a higher level of security because of the fast evolution of data communications and digital audio. Speech information as compared with digital data or text messages is different because it has stronger correlation among samples and higher redundancy (Elshamy *et al*., 2015). Speech encryption can be categorized to two types: analog (scramble) and digital. Analog speech encryption involves scrambling or permutation of the speech signal in time, frequency domain or in both. While digital speech encryption involves encryption of the speech signal by using modern digital cryptosystem like Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Analog speech encryption has several advantages such as high quality of the recovered speech, limited bandwidth and simplicity but they are relatively less secure as compared with digital speech encryption. On the other hand, digital speech encryption offer higher level of security but they require a large bandwidth for transfer and complex implementation (Al Saad and Hato, 2014; Hasan, 2016). For text data, traditional cryptographic schemes may be efficient but they are unsuitable to provide security for speech data because of high redundancy and bulk data capacity. So, security of the speech needs efficient algorithms such as chaos-based algorithms for dealing with redundant voice data. These algorithms provide fast and better secure encryption techniques (Elzaher *et al*., 2016).

A number of chaos-based encryption schemes have been presented in the last years. As examples, the researchers by Elshamy *et al*. (2015), used Arnold cat map or Baker map combined with Double Random Phase Encoding (DRPE) to encrypt the audio signal. The results of different encryption/decryption quality metrics indicate that the presented scheme increases the level of voice confidently and security. By Wahab and Mahdi (2015), a new approach based MOBS (Modified Overlapped Block Shuffling) and hybrid chaotic system is described. The speech signal is divided into overlapped squared blocks after converting it from 1 and 2 dimensions followed by permutation and shuffling processes using Henon and Arnold cat map in order to produce ciphered speech ready for transfer. By Hasan (2016), Fixed Point Chaos based Stream Cipher (FPC-SC) is utilized to encrypt the speech signal. The results on the proposed scheme show that it has good statistical and encryption measures. By Elzaher *et al*. (2016), a new voice encryption is introduced. Arnold cat map is applied to permute the samples of the original signal followed by the substitution process using Henon map. The proposed system has large key space and high quality decrypted speech signal. By Farsana and Gopakumar (2016), Zaslavsky map and Cat map transform are employed for speech encryption.

Original signal is encrypted using Zaslavsky map after compressing it by Discrete Cosine Transform (DCT) technique. Then, the output signal is processed by Arnold cat map to confuse the data samples. The analysis shows that the presented study is computationally efficient and simple. By Wahab and Mahdi (2016), the speech signal is shuffled in time domain after dividing it into overlapped blocks. Then the coefficients of each block which are generated from wavelet transform are permutated using Henon map. Many tests prove the validity of the introduced method. By Sheela *et al.* (2017), a combination of DNA coding rules, Hybrid Chaotic Shift Transform (HCST) and chaotic maps are applied to encrypt the audio signal. Standard and Henon maps are used to execute HCST while DNA coding technique is utilized to improve the cryptosystem security. Various encryption and decryption quality measurements are used to assess the algorithm performance. By Sathiyamurthi and Ramakrishnan (2017), the segments of input speech signals are divided to four layers, then each layer is shuffled via four different chaotic maps like Bernoulli's, quadratic, tent and logistic maps. Chen map is used at the end to complete the shuffling process. By Ibrahem and Kassim (2018), chaotic system and stream cipher technique are employed for developing Voice Over Internet Protocol (VOIP). A random key which utilized to encrypt the voice information in this method is generated using chaotic systems. The experiments indicate that this scheme can provide minimum delay and minimum lost in the transferred packet. By Praisy *et al.* (2018), the original audio signal is partitioned to four blocks, then each block is confused using various chaotic systems. The outcomes of different experiments prove the security of the presented strategy.

So, based on the literature, a new idea for speech encryption based on chaotic systems in time domain is proposed in this research. The two basic elements in any cryptographic schemes are permutation and substitution. These processes are achieved in this study by using Zaslavsky map. The presented speech cryptosystem provides a high security features and low correlation between the original and encrypted speech signals. The rest of this research is regulated as follows.

MATERIALS AND METHODS

Chaotic system: In modern cryptography area, the most important security algorithms are chaos based cryptography. Chaos theory is used mainly to develop physical and mathematical models of dynamical nonlinear system. This theory has desirable properties such as sensitivity to initial conditions and system parameters, deterministically, irregularity, ergodicity and mixing property. Thus, in modern cryptography, chaos theory is adopted by security research community based on these properties. Mathematically, chaotic function or map is a function that possesses kind of chaotic behavior. Pseudo-random sequences with good randomness can be produced by using chaotic systems which make them suitable for cryptographic properties like disorder, confusion and diffusion (Elzaher *et al.*, 2016; Ashtiyani *et al.*, 2012). In the following section, a brief discussionis introduced for chaotic map namely Zaslavsky map which is used in this research.

Zaslavsky map: In 1978, George M. Zaslavsky was the first who introduced Zaslavsky map. Zaslavsky map is a discrete-time dynamical nonlinear system. This map can be defined in the following mathematical Eq. 1 and 2:

$$x_{n+1} = \mathrm{mod}\left(x_n + \nu\left(1+\mu y_n\right) + \epsilon\,\nu\mu\cos\left(2\pi x_n\right), 1\right) \quad (1)$$

$$y_{n+1} = e^{-r}\left(yn + \cos\left(2\pi x_n\right)\right), \quad \mu = \frac{1-e^{-r}}{r} \quad (2)$$

Where:

x_0 and y_0 = The initial conditions
ν, ϵ, r = The control parameters of the system

By Farsana and Gopakumar (2016) and Alshibani and Ibrahim (2015). This map exhibits chaotic behavior when the values of the parameters are:

$$\nu = \frac{400}{3}, \epsilon = 0.3 \text{ and } r = 3$$

The proposed cryptosystem: The proposed scheme is discussed in this study. It consists of two operations: permutation and masking of the speech signal using Zaslavsky map in time domain. Then, the encrypted speech signal will be sent to the receiver through a channel. The encrypted speech signal will be decrypted in the receiver side in order to recover the original speech signal, according to chaotic map. The structure of the proposed model is shown in Fig. 1.

Encryption process The encryption process can be summarized in the following steps:

- Step 1: transform the audio speech signal from 1 and 2D blocks
- Step 2: generate a permutation key (key1) using Zaslavsky map
- Step 3: permute the samples in each block with key 1

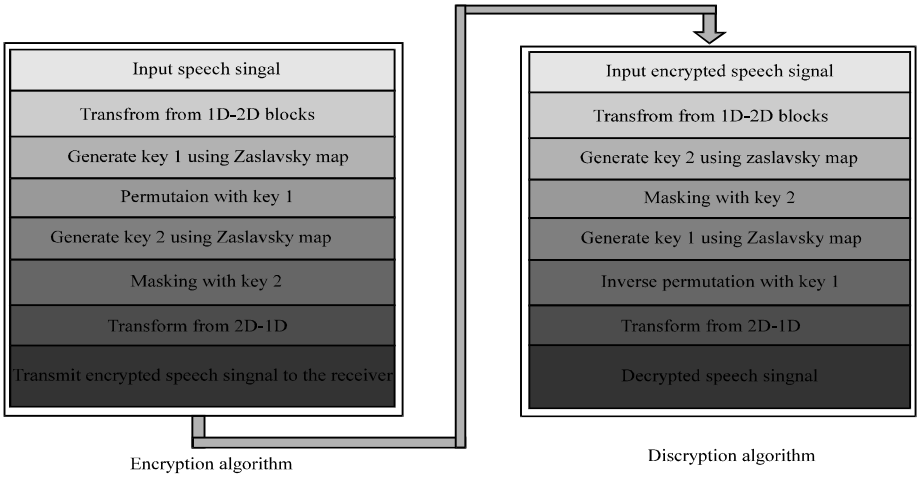

Fig. 1: Block diagram of proposed cryptosystem

- Step 4: generate a mask key (Key2) using Zaslavsky map
- Step 5: mask each block's samples with Key2 by applying of XOR operationbetween the mask key and the speech samples in each block
- Step 6: transform the encrypted speech signal from 2D to 1D
- Step 7: transmit the encrypted speech signal

Decryption process: The decryption process can be summarized in the following steps:

- Step 1: transform the encrypted speech signal from 1D to 2D blocks
- Step 2: generate a mask key (Key2) using Zaslavsky map
- Step 3: apply of XOR operation between the mask key and the encrypted speech samples in each block.
- Step 4: generate a permutation key (Key1) using Zaslavsky map
- Step 5: apply inverse permutation on the samples in each block with Key1
- Step 6: transform the decrypted speech signal from 2 and1D to get the original one

Permutation step: For speech secrecy, security and to reduce the intelligibility of audio signal, the strong correlation among adjacent samples in the speech data must be disturbed. To achieve this aim, permutation process is used. In this step, the samples in each block in the speech signal are rearranged without changing their values and mapped to newpositions in the same block. Permutation process is performed using Zaslavsky map in the proposed cryptosystem in time domain. Real values which represent the chaotic sequence are generated from the iterated Zaslavsky map after setting the initial and the parameters map values. The resulting position row which came from sorting the chaotic sequence in ascending order is used as a permutation key. Due to the random behavior of Zaslavsky map and its sensitivity to initial conditions, permutation process is considered good (Wahab and Mahdi, 2016; Mosa *et al*., 2011).

Masking step: Generally, during speech communication, sufficient security cannot be provided by a cryptosystem against eavesdroppers with permutation only. For this reason, masking or substitution process is accomplished. In this step, the amplitudes of samples in each block in the speech signal will be changed. The value of each sample is substituted by XOR with the value of mask key (Elzaher *et al*., 2016; Wahab and Mahdi, 2015). Masking process is performed using Zaslavsky map in the proposed cryptosystem in time domain. To generate the mask key, specify x_0, y_0, υ, ϵ, r according to Eq. 1 and 2 to get the chaotic sequence x_i and y_i. These values must be normalized into integers as follows:

$$\begin{aligned} x_1 &= \text{mod}\left(\text{floor}\left(x_i * 10^{14}\right), 256\right) \\ y_1 &= \text{mod}\left(\text{floor}\left(y_i * 10^{14}\right), 256\right) \end{aligned} \tag{3}$$

Then, we reshape x_1 or y_1 to the same size of speech signal (row, column) to get the mask key as shown:

$$\begin{aligned} x_2 &= (i, j) = \text{reshape}\left(x_1, \text{ row, column}\right) \\ y_2 &= (i, j)\ \text{reshape}\left(y_1, \text{ row, column}\right) \end{aligned} \tag{4}$$

Finally, masking process is done to obtain the encrypted speech signal as given:

$$c(i, j) = p(i, j) \oplus x_2(i, j) \text{ or } c(i, j) = p(i, j) \oplus y_2(i, j) \quad (5)$$

Combination of permutation the positions of speech signal samples and change their values is performed in the proposed speech cryptosystem to shuffle the relationship between the original and the cipher-speech signals.

RESULTS AND DISCUSSION

Several experiments are carried out to evaluate the performance of the proposed speech cryptosystem in this study. The speech signals that have been used as test materials are extracted from TIMIT database. In this simulation results, the specification of the hardware used is represented by a personal computer HP, processor Intel (R) Core (TM) i3-3110, CPU 2.40 GHz and RAM of 3.90 GB. The software used for simulation is MATLAB (R2013a). The sampling frequency for each speech signal is 16 kHz for duration of 1.4150, 2.8550, 3.3150, 4.7350 and 5.3950 sec, respectively. The waveform of the original, encrypted and decrypted speech signals by the proposed cryptosystem are shown in Fig. 2. Obviously, it is evident form Fig. 2a and b that the original intonations have been removed from the encrypted speech signal and it likes white noise without any talk spurts. This implies that at the communication channel, no residual intelligibility can be helpful for the attackers. By applying the steps of the decryption process starting from the encrypted speech signal, the decrypted or the reconstructed speech signal is obtained. By comparing Fig. 2a-c, it can be seen that the original and the decrypted speech signals are identical.

Statistical analysis: To evaluate the performance of the proposed cryptosystem in this research, the common objective metrics used are the following: Signal-to-Noise Ratio (SNR), segmental Signal-to-Noise Ratio (SNRseg), frequency-weighed Signal-to-Noise Ratio (fwSNRseg), correlation coefficient (rxy) and Log-Likelihood Ratio (LLR). The brief description of these metrics is summarized in the following.

Signal-to-Noise-Ratio (SNR): To measure the level of distortion in speech signal, SNR is one of the most widely used objective measurements. This common measure can be calculated as follows:

$$SNR = 10 * \log 10 \frac{\sum_{i=1}^{L} x_i^2}{\sum_{i=1}^{L} [x_i - y_i]^2} dB \quad (6)$$

where, x_i and y_i are the original and the encrypted speech samples in the block, respectively (Farsana and Gopakumar, 2016; Sheela *et al*., 2017).

Segmental Signal-to-Noise-Ratio (SNRseg): If SNR is measured over in short frames and then averaged, segmental SNR is obtained. It is an improved version measure of SNR. It can be given as:

$$SNR_{seg} = \frac{10}{M} \sum_{m=0}^{M-1} \log 10 \frac{\sum_{n=Lm}^{Lm.L-1} x_i^2}{\sum_{n=Lm}^{Lm+L-1} [x_i - y_i]^2} dB \quad (7)$$

Where:

M = The number of framesin the speech signal
L = The frame length or number of samples in the signal

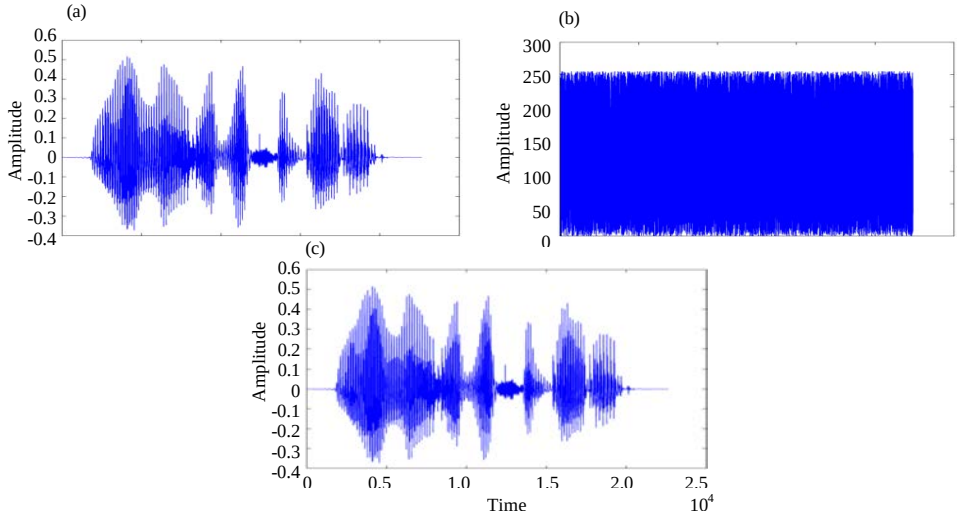

Fig. 2: a) Original speech signal; b) Encrypted speech signal and c) Decrypted speech signal

SNRseg is a good estimator for the quality of speech signal (Al-Saad and Hashim, 2013).

Frequency-weighed Signal-to-Noise Ratio (fwSNRseg): Frequency-weighed SNR (fwSNRseg) is another variation to the SNR. Essentially, it is a weighted SNRseg in the frequency band that is proportional to the critical band. It can be calculated as:

$$fwSNR_{seg} = \frac{10}{M}\sum_{m=0}^{M-1}\frac{\sum_{j=0}^{K-1} W(j,m)\log 10\frac{X(j,m)^2}{\left[X(j,m)-\hat{X}(j,m)\right]^2}}{\sum_{j=0}^{K-1} W(j,m)}dB \quad (8)$$

Where:

K = The number ofsub bands in the speech signal

W (j, m) = The weight on the jth sub band in the mth frame

X (j, m) and $\hat{X}(j,m)$ = The magnitude of spectrum of the original and the distorted speech signals, respectively (Taal *et al*., 2011)

Correlation coefficient: To assess the quality of encryption of any cryptosystem, the correlation coefficient is a useful measure between similar frames in the original and encrypted speech signals. This measure is defined as follows (Sathiyamurthi and Ramakrishnan, 2017; Mosa *et al*., 2011):

$$r_{xy} = \frac{cov(x,y)}{\sigma_x\sigma_y} = \frac{\sum_{i=1}^{L}(x_i-E(x))(y_i-E(y))}{\sqrt{\sum_{i=1}^{L}(x_i-E(x))^2}\sqrt{\sum_{i=1}^{L}(y_i-E(y))^2}} \quad (9)$$

Where:

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \quad (10)$$

Log-Likelihood Ratio (LLR): Log-Likelihood Ratio (LLR) is an important metric to evaluate the cryptosystem quality. This distance measure can be calculated directly from the LPC vector of the original and cipher speech signals as shown below:

$$d_{LLR}(a_c, a_o) = \log\left(\frac{a_c R_o a_c^T}{a_o R_o a_o^T}\right) \quad (11)$$

Where:

a_o and a_c = The LPC vectors of the original and cipher speech signals, respectively

a^T = The transpose

R_o = The auto-correlation matrix of the original speech signal (Al-Saad and Hashim, 2013)

Key space and key sensitivity analysis: The most important criteria of the performance analysis of any cryptosystem are key space and key sensitivity analysis. Good cryptosystem should be very sensitive to the value of the key and the initial conditions also have a large key space (Mosa *et al*., 2011).

Key space analysis: The total number of different keys that are used for the encryption/decryption scheme is called the key space size. It should be large enough to resist brute-force attacks. 10^{-6} is used in the proposed cryptosystem as floating point precisionfor atleast (K = 5) secret keys (two initial conditions and three control parameters). Therefore, the key space of secret keyscomes out as $(10^{16})^K = (10^{16})^{15} = 10^{80} \approx 2^{266}$. This key space is extensively large enough to resist all kinds of attacks (Sheela *et al*., 2017; Alshibani and Ibrahim, 2015).

Key sensitivity analysis: Key sensitivity is the most important characteristic of chaos encryption. Key sensitivity means that if there is a small change between encryption and decryption keys, then the encrypted speech signal cannot be decrypted correctly. To test the key sensitivity of the proposed cryptosystem we will change only one parameter of keys by a tiny amount at a time, all other remaining parameters of keys are keeping unchanged. The decryption of the encrypted speech signal is performed with five different keys which are generated by changing only one parameter in the original secret keys (Alwahbani and Bashier, 2013). The secret keys for Zaslavsky map are $x_0 = 0.1$, $y_0 = 0.1$, $\nu = 133.3$, $\epsilon = 0.3$ and $r = 3$. Key sensitivity of this approach is tested by adding 10^{-16} to the correct key. For example, the incorrect parameters will be $x_0 = 0.10000000000000001$, $y_0 = 0.10000000000000001$, $\nu = 133.30000000000000001$, $\epsilon = 0.30000000000000001$ and $r = 3.0000000000000001$. Figure 3 shows the decrypted speech signals with three incorrect keys (x_0, y_0 and ν). From these figure, it can be noticed that the reconstructed speech signal is completely different from the original, it's like a random noise and unintelligible. The and LLR between the original and decrypted speech signals with incorrect keys are estimated and tabulated in Table 1. The lower value of correlation coefficient (closer to zero) and larger value of LLR indicates the large key sensitivity of the introduced cryptosystem. It is clearly from this table that the correlation among the decrypted signals with incorrect keys is very low while LLR is large which proves the key sensitivity.

Spectrogram analysis: The spectrogram of an audio signal is a powerful tool that divides it in time domain into multiple blocks, then Fast Fourier Transform (FFT) is plotted and displayed for each block in the same

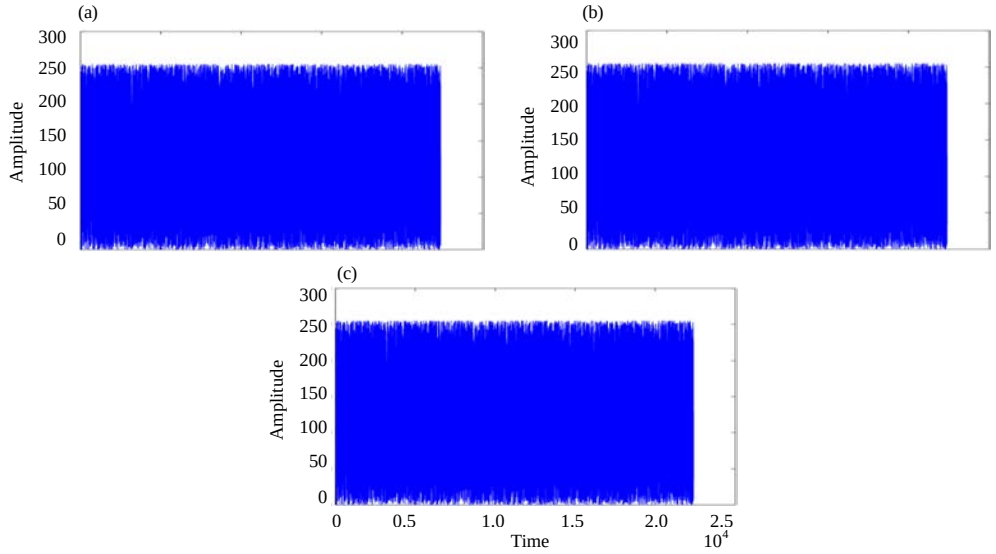

Fig. 3: Decryption with incorrect: a) Key1; b) Key2 and c) Key3

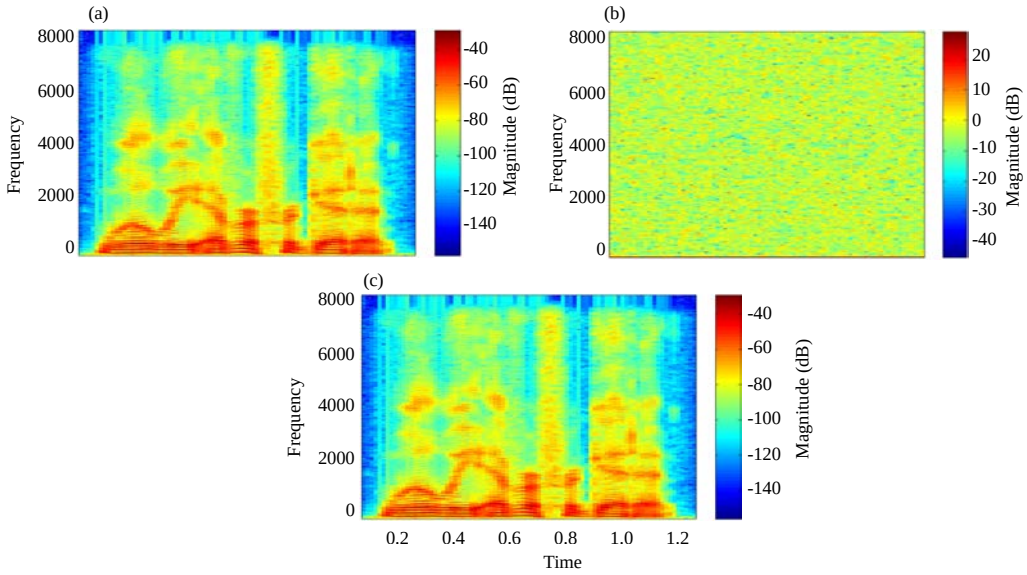

Fig. 4: a) Original signal spectrogram; b) Encrypted signal spectrogram and c) Decrypted signal spectrogram

Table 1: Correlation coefficient and LLR values for key sensitivity test

	Key1		Key2		Key3	
File name (Signal)	r_{xy}	LLR	r_{xy}	LLR	r_{xy}	LLR
1	8.8604×10^{-4}	2.1029	$1.56^{19}\times10^{-4}$	2.0381	8.8604×10^{-4}	2.0811
2	5.8847×10^{-4}	1.4070	2.6799×10^{-4}	1.3476	4.4468×10^{-4}	1.3587
3	6.6730×10^{-4}	2.2529	4.0386×10^{-4}	2.3004	-1.4352×10^{-4}	2.2366
4	1.2042×10^{-4}	1.6953	3.4115×10^{-4}	1.6265	1.0570×10^{-4}	1.7391
5	9.0881×10^{-4}	1.0930	4.4275×10^{-4}	1.1368	-8.7098×10^{-4}	1.1029

graph. In Fig. 4, the spectrograms of the original, encrypted and decrypted speech signals are presented (Elshamy *et al*., 2015; Elzaher *et al*., 2016). It can be easily noticed by comparing Fig. 4a and b that the spectrograms of the original and encrypted speech signals are completely different which implies higher encryption quality. On the other hand, by comparing Fig. 4a and c, it is evident that the spectrograms of the

Table 2: Quality measure results for encryption process

File name (Signal)	SNR (dB)	SNRseg (dB)	fwSNRseg (dB)	r_{xy}	LLR
1	-56.8661	-58.1464	-59.1289	-9.2444×10^{-4}	2.0759
2	-59.2183	-66.3833	-61.4436	-5.7565×10^{-4}	1.3681
3	-57.6822	-56.7948	-60.3781	-8.6871×10^{-4}	2.2863
4	-60.2793	-59.3577	-61.9012	6.5486×10^{-4}	1.7151
5	-61.9996	-65.3828	-63.7911	2.5005×10^{-4}	1.1228

Table 3: Quality measure results for decryption process

File name (Signal)	SNR (dB)	SNRseg (dB)	fwSNRseg (dB)	r_{xy}	LLR
1	223.1428	225.2040	54.4610	1	1.9925×10^{-12}
2	221.0352	218.4514	56.2366	1	1.3115×10^{-13}
3	219.7899	216.4882	56.0761	1	3.3877×10^{-13}
4	217.9880	214.5635	59.1844	1	-1.6056×10^{-14}
5	222.2268	223.6059	54.9183	1	1.2170×10^{-13}

Table 4: Comparison with existing schemes

Scheme	SNR (dB)	SNRseg (dB)	fwSNRseg (dB)	Correlation coefficient	LLR
Elshamy *et al.* (2015)	-	-	-	0.0051	-
Al Saad and Hato (2014)	-	-17.70727	-16.9303	-0.009221	-
Hasan (2016)	-	-	-22.3019	-	-
Elzaher *et al.* (2016)	-41.05	-55.2	-	-0.00118	1.92
Wahab and Mahdi (2015)	-13.3816	-14.3917	-	-5.64×10^{-4}	-
Farsana and Gopakumar (2016)	-22.45	-	-	0.000569	-
Wahab and Mahdi (2016)	-25.7558	-28.107	-27.9231	-0.0011	0.5858
Sheela *et al.* (2017)	-	-	-	-0.00021724	-
Sathiyamurthi and Ramakrishnan (2017)	-	-	-	0.0233	-
Al-Saad and Hashim (2013)	-2.62555	-2.56744	-	-	-
Alwahbani and Bashier (2013)	-13.3015	-	-	-0.0014	-
Proposed method	-56.8661	-58.1464	-59.1289	-9.2444×10^{-4}	2.0759

original and decrypted speech signals arevery similar to each other. This implies higher decryption quality.

Quality of encrypted speech signal: To assess the residual intelligibility of the encrypted speech signal, five quality metrics are used: SNR, SNRseg, fwSNRseg, r_{xy} and LLR. The higher is the encrypted speech signal quality as the values of the SNR, SNRseg, fwSNRseg and r_{xy} are decreased and the value of LLR is increased (Al Saad and Hato, 2014; Wahab and Mahdi, 2016). The results for the proposed cryptosystem are explained in Table 2. From this table, it can be observed that the r_{xy} measure is very low (close to zero) which validates low correlation between the original and the encrypted speech signals. Moreover, the SNR, SNRseg and fwSNRseg measures for all encrypted files are very low (negative value) while the LLR measure is high which demonstrates that residual intelligibility is very low and the encrypted speech signals are completely noisy.

Quality of decrypted speech signal: The same five quality metrics are used to measure the quality of decrypted speech signal which are SNR, SNRseg, fwSNRseg, r_{xy} and LLR. The higher is the decrypted speech signal quality as the values of the SNR, SNRseg, fwSNRseg and r_{xy} are increased and the value of LLR is decreased (Elshamy *et al*., 2015; Al Saad and Hato, 2014). The results for the proposed cryptosystem are explained in Table 3. From this table, it can be observed that the r_{xy} measure is very high (one) which validates high correlation between the original and the decrypted speech signals. Moreover, the SNR, SNRseg and fwSNRseg measures for all decrypted files are very high (positive value) while the LLR measure is low which demonstrates that the reconstructed speech signals are of good quality and high precision.

Comparison with existing schemes: Comparison is made with other techniques in order to measure the novelty of the introduced scheme security and encryption in terms of quality metrics that has been mentioned before. The comparison is presented in Table 4. In this scheme, large negative value of SNR, SNRseg fwSNRseg obtained shows that the noise power is higher than signal power which makes it difficult todetect (Farsana and Gopakumar, 2016). Another measure is correlation coefficient. The value of correlation in this scheme is almost zero which indicates that the original and the encrypted speech signals are totally uncorrelated. Finally, LLR in this technique is higher compared to others which show higher encryption quality. It can be concluded that in most of the quality measures, the presented speech cryptosystem over rides other existing schemes.

CONCLUSION

The security of audio is involved with insuring the confidentially, accessibility, reliability and secrecy of data. Protecting audio systemsfrom the illegal access, alteration, disruption, extermination and use is the main target of speech security. This research presents an efficient algorithm for speech encryption based on chaotic system. In this algorithm, Zaslavsky map is utilized to provide two layers of security, permutation and substitution which increases the speech signal security and makes the cryptanalysis a difficult task. To assess the quality of the encrypted and decrypted speech signal, several statistical analyses are used. Simulation results for the encrypted speech signal demonstrate a low correlation coefficient (near to zero), very low SNR, SNRseg and fwSNRseg while LLR metric is high which means that the residual intelligibility is completely removes in this scheme. On the other hand, the results for the decrypted speech signal show a high correlation coefficient (one), very high SNR, SNRseg and fwSNRseg while LLR metric is very low which indicate that the recovered speech signal is of high quality. Moreover, the key space is reasonably large and the introduced cryptosystem is highly sensitive to the change in the initial and control parameters which indicates a suitability, high security and resistivity against brute-force attacks. Comparison with other existing techniques concludes the superiority of the presented encryption system. As an evaluation of the proposed approach, it can be concluded from the previous results that the presented scheme has shown good results in the sense of correlation coefficient, SNR, SNRseg, fwSNRseg and LLR in both encryption and decryption processes. It achieves good permutation, substitution and good immunity of the speech signal to different attacks which makes it suitable for applications in real time systems.

REFERENCES

Al Saad, S.N. and E. Hato, 2014. A speech encryption based on chaotic maps. Int. J. Comput. Applic., 93: 19-28.

Al-Saad, S.N. and E.H. Hashim, 2013. A speech scrambler algorithm based on chaotic system. Al-Mustansiriyah J. Sci., 24: 357-374.

Alshibani, D.R. and R.S. Ibrahim, 2015. Implementation of gray image encryption using multilevel of permutation and substitution. Intl. J. Appl. Inf. Syst., 10: 25-30.

Alwahbani, S.M. and E.B. Bashier, 2013. Speech scrambling based on chaotic maps and one time pad. Proceedings of the International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), August 26-28, 2013, IEEE, Khartoum, Sudan, ISBN:978-1-4673-6231-3, pp: 128-133.

Ashtiyani, M., P.M. Birgani and S.K. Madahi, 2012. Speech signal encryption using chaotic symmetric cryptography. J. Basic Appl. Sci. Res., 2: 1668-1674.

Elshamy, E.M., E.S.M. El-Rabaie, O.S. Faragallah, O.A. Elshakankiry and F.E.A. El-Samie *et al*., 2015. Efficient audio cryptosystem based on chaotic maps and double random phase encoding. Intl. J. Speech Technol., 18: 619-631.

Elzaher, M.A., M. Shalaby and S.H. El Ramly, 2016. Securing modern voice communication systems using multilevel chaotic approach. Intl. J. Comput. Appl., 135: 17-21.

Farsana, F.J. and K. Gopakumar, 2016. A novel approach for speech encryption: Zaslavsky map as pseudo random number generator. Procedia Comput. Sci., 93: 816-823.

Hasan, F.S., 2016. Speech encryption using Fixed Point Chaos based Stream Cipher (FPC-SC). Eng. Technol. J., 34: 2152-2166.

Ibrahem, M.K. and H.A. Kassim, 2018. VoIP speech encryption system using stream cipher with chaotic key generator. J. Fundam. Appl. Sci., 10: 204-210.

Mosa, E., N.W. Messiha, O. Zahran and F.E.A. El-Samie, 2011. Chaotic encryption of speech signals. Intl. J. Speech Technol., 14: 285-296.

Praisy, S.G., J. Jeevitha and R.G. Harinee, 2018. Secured speech communication based on chaotic mapping using cryptographic algorithm. SSRG Intl. J. Electron. Commun. Eng., 1: 113-120.

Sathiyamurthi, P. and S. Ramakrishnan, 2017. Speech encryption using chaotic shift keying for secured speech communication. EURASIP J. Audio, Speech Music Process., 2017: 1-11.

Sheela, S.J., K.V. Suresh and D. Tandur, 2017. A novel audio cryptosystem using chaotic maps and DNA encoding. J. Comput. Networks, Commun., 2017: 1-12.

Taal, C.H., R.C. Hendriks, R. Heusdens and J. Jensen, 2011. An evaluation of objective measures for intelligibility prediction of time-frequency weighted noisy speech. J. Acoust. Soc. Am., 130: 3013-3027.

Wahab, H.B.A. and S.I. Mahdi, 2015. Modify speech cryptosystem based on shuffling overlapping blocks technique. Intl. J. Emerging Trends Technol. Comput. Sci., 4: 70-75.

Wahab, H.B.A. and S.I. Mahdi, 2016. Speech encryption based on wavelet transformation and chaotic map. Eng. Technol. J., 34: 721-729.