International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 5658~5664
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp5658-5664

Speech encryption by multiple chaotic maps with fast fourier transform

Yahia Alemami[1], Mohamad Afendee Mohamed[2], Saleh Atiewi[3], Mustafa Mamat[4]
[1,2,4]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Malaysia
[3]Computer Science, Al Hussein Bin Talal University College of IT, Jordan

Article Info

Article history:

Received Mar 16, 2019
Revised Apr 28, 2020
Accepted May 28, 2020

Keywords:

Speech encryption
Chaotic map
Fourier transform
Logistic map
Sine map

ABSTRACT

There are various ways of social communication including writing (WhatsApp, Messenger, Facebook, Twitter, Skype, etc), calling (mobile phone) and voice recording (record your voice and then send it to the other party), but there are ways to eavesdropping the calls and voice messages, One way to solve this problem is via cryptographic approach. Chaos cryptography build on top of nonlinear dynamics chaotic system has gained some footstep in data security. It provides an alternative to conventional cryptography built on top of mathematical structures. This research focuses on the protection of speech recording by encrypting it with multiple encryption algorithms, including chaotic maps (Logistic Map and Sine Maps).

Corresponding Author:

Mohamad Afendee Mohamed,
Faculty of Informatics and Computing,
Universiti Sultan Zainal Abidin,
Besut Campus, 22200, Malaysia.
Email: mafendee@unisza.edu.my

1. INTRODUCTION

The information security can be regarded as the denial of unauthorized access and the protection of assets [1]. Various approaches originated from domains such as mathematics, computer sciences and engineering have been introduced. These mechanisms are responsible for securing the perimeter (firewall, intrusion prevention system, intrusion detection system) [2, 3], the computer system (biometrics, password) [4] and the information (steganography, cryptography) itself [5-7]. Cryptography via an encryption algorithm provides a cornerstone for secure communications [8]. Mostly the subjects of interest for encryption are text, image, video and speech. Mathematical based encryption algorithms can be classified into symmetric and asymmetric system [6, 8]. Encrypting of voice recording may prevent unauthorized user to access and steal the information and later use it as a threatening tool. There are many cryptographic algorithms available for protecting the voice recording, in this paper we will be using chaotic maps to encrypt the voice that was recorded by sender's voice receptor (speech recognition). However, there are some problems when recording the human voice. Some examples of these problems are the environmental factors like noise, delay and losses. Another would be ones of medical condition such as parkinson's disease (PD), one of the most common neurodegenerative disorders. This kind of disease affects a central nervous system which causes progressive loss of muscle control with the clear signs including shiver and difficulty in speech. Consequently, when a sender starts his speech by microphone or speaker and play speech recognition program (through windows) to transport his speech and put it into text, or using some application Android that is able to convert speech to text (e.g. speech texter Application), then send to the recipient, so for that of get protect and secret that data, it is necessary to encrypt it to prevent from disclosure. In this paper, we will be using some cryptography algorithms to encrypt the voice that was entered by sender's speech and decrypt

it by the recipient which are based on the Logistic Map, and resea Map. The main structure of mostly available speech encryption/ decryption system can be shown as in Figure 1.

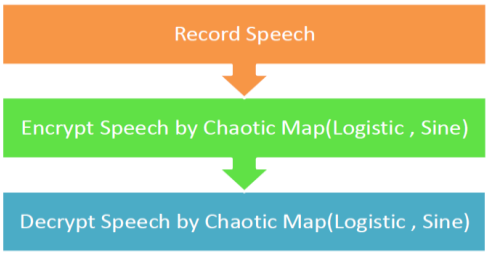

Figure 1. Encryption/decryption speech system

2. CHAOTIC MAPS

Electronic Chaotic-based cryptosystem is an encipherment system that is characterized by a nonlinear deterministic dynamical chaotic function [9-12]. The output values of chaotic method are extremely sensitive depending on values of input factors and premier conditions. In the following sections a summarized depiction for three types of chaotic maps, logistic map and Sine map are presented.

2.1. Logistic map

Logistic mapping is illustration of chaotic scheme that is a non-linear map given by [11]:

$$x_{n+1} = rx_n(1 - x_n)$$

Apply depending on the following conditions:

- x_n take value from [0,1].
- r is a control parameter, r € [0,4].
- initial value x_0=0.3.

The system has various features with various values of r, called the bifurcation parameter. When the value is closer to 4, the more chaotic the system response will be as shown in Figure 2.

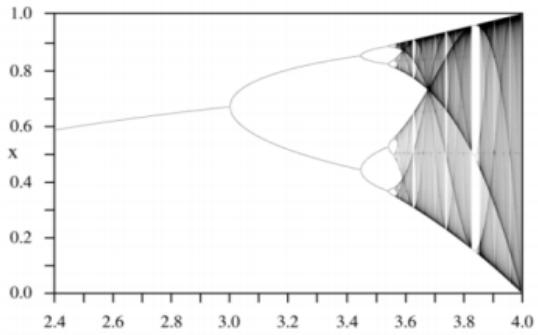

Figure 2. Bifurcation diagram for the logistic map [11]

2.2. Sine map

The Sine map is one of the discrete chaotic method having a following equation [13]:

$$Xn + 1 = A.\sin(\pi.Xn)$$

where $A \in [0,1]$, and Xn is in [0,1]. That the Sine map becomes chaotic when closer to 1, shown in Figure 3. The Sine map is simple as compared to some other chaotic methods with assurance of higher scale of security.

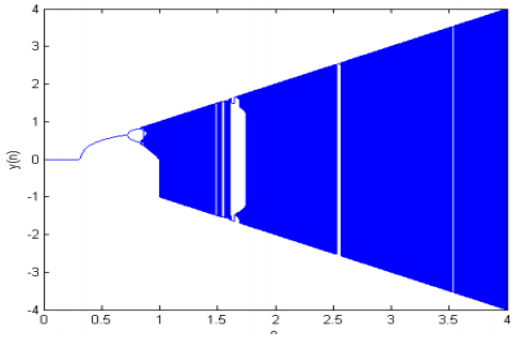

Figure 3. Bifurcation diagram of the Sine map [13]

3. LITERATURE REVIEW

This section describes some chaotic algorithms that were design for voice encryption. Studies in [14, 15] produced a new algorithm to perform encryption for audio files using a shuffling procedure, where a different shuffle bit is chosen and the substitution is changed. The statistical analysis showed based on the graph of PSNR that the algorithm is not subjected to statistical attacks unless when it was used to encode low-quality audio files. Different study [16] described the algorithm based on chaotic map and Blowfish algorithm. It is considerably a fast and efficient algorithm in the process of encryption and decryption and is presumably difficult to break. Another research [17] has proposed an algorithm for speech encipherment depend on three dimensional chaotic maps. The proposed algorithm includes three main units: creation of keys, samples substitution and samples permutation operation. Substitution is performed in two steps with cipher feedback, for the system. The Lorenz and Rossler chaotic system are presented for creation of key stream used for substitution and permutation process respectively. The proposed algorithm used to increase the confusion and diffusion of speech samples. From [18], a new algorithm for speech encryption was introduced by dividing the speech signal into overlapped blocks prior shuffling those blocks into the time domain. A second permutation is performed for the coefficients of the block which was obtained from the wavelet transforms by using chaotic key based on Hénon map, and partially encoding the shuffled online speech signal in a transform scope. The suggested algorithm is capable to produce strong speech encipherment in a real-time environment. Research in [19] suggested a new algorithm for speech encipherment that depends on two steps, it makes use of three chaotic maps (Henon, Logistical, and Ikeda) in addition to noise and then it elects bio-chaotic stream cipher which has encoded the speech signal to store it into the databases to increase security using a biometric key and a bio-chaotic function. The proposed algorithm was shown to be powerful, fast and more secure [19]. Different research [20] proposed an algorithm to speech encipherment using hybrid of DES-RSA and Genetic Algorithm. The classification of audio files was compared using artificial neural network (NN), and also support vector machine (SVM) algorithm. The outcomes were evaluated using MSE and PSNR factors to check the validation of the suggested algorithm. The suggested algorithm for speech cryptography provides a security at different levels.

4. PROPOSED SYSTEM

In Figure 4 shows the operation's steps that depict the suggested speech encipherment, where it is performed by MATLAB version 7.0 programming. The suggested encipherment system can be summarized into as followings:

- Input speech signal.
- First processing step
  - Using fast fourier transform function
- Second processing step:
  - Creation of logistic function
  - Start of Confusion
- Third processing step:
  - Creation of diffusion key by Sine map
- Fourth processing step:
  - Application of XOR operation between second step and third step

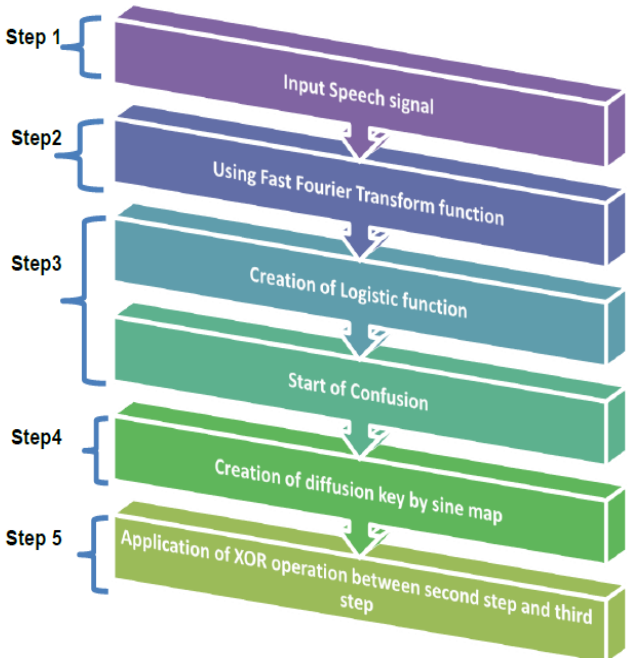

Figure 4. Structure of proposed system

4.1. Fast fourier transform (FFT)

May be the most significant numerical algorithm in science, engineering, and applied mathematics is FFT [11], it is likewise a model or case of how algorithms can be made efficient and how a hypothesis can be created to characterize optimality. The development of fast algorithms for the most part comprises of utilizing exceptional properties of the algorithms important to expel excess or unnecessary tasks of an immediate execution, it can likewise be applied directly to convolution to divide it into numerous short convolutions that can be executed quicker than an immediate usage.

4.2. Creation of logistic function and start of confusion

The encryption method can be expressed by the following code:

```
x=initial value;
r= control parameter to logistic map;
for z=1:y-1 % y is length of record speech that stored in Database
       x(z+1)=r*x(z)*(1-x(z));%Logistic map theory
end
%Start of Confusion -swap
timg=timg(:);
for h=1:size(timg,1)
       temp=timg(h);
       timg(h)=timg(in(h));
       timg(in(h))=temp;
end
%End of confusion
```

4.3. Creation of diffusion key by sine map

The encryption this method can be expressed by the following code:

```
K=initial value;
r= control parameter to Sine map;
for z=1:y-1 %y is length of record speech that stored in  Database
        k(z+1) =r* sin(pi*k(z));% Sine map theory;
end
temp1=de2bi(k);
temp1=circshift(temp1,1);
temp1=bi2de(temp1)';
key=bitxor(k,temp1);
%Ending creation of diffusion key by Sine map
```

4.4. Application of XOR operation

The encryption of this method can be expressed by the following code:

```
result_encryption=bitxor(uint8(first output),uint8(second output));
% first output (second step)
% second output (Third step)
```

5. SIMULATION RESULT

The following section presents and discusses the outputs of the proceeded tests to evaluate the performance of the proposed systems. Figure 5 shows original signal, and after applying FFT function by MATLAB programming, this signal is transformed to that of shown in Figure 6, where each number in the result of FFT is a complex number. FFT represents one of the applications to reveal and remove cyclic components in data before applying regression techniques to suit forecasting models to the data [21]. Thereafter an absolute function is performed on previous result and is shown in Figure 7. Figure 8 shows the result after we start encrypting the speech by creation of logistic function. After that, we performed final encryption by confusion with logistic map (where r=4) and diffusion key with Sine map (where r=3.628) to produce Figure 9. Figure 10 show the decryption process to obtain original speech signal.

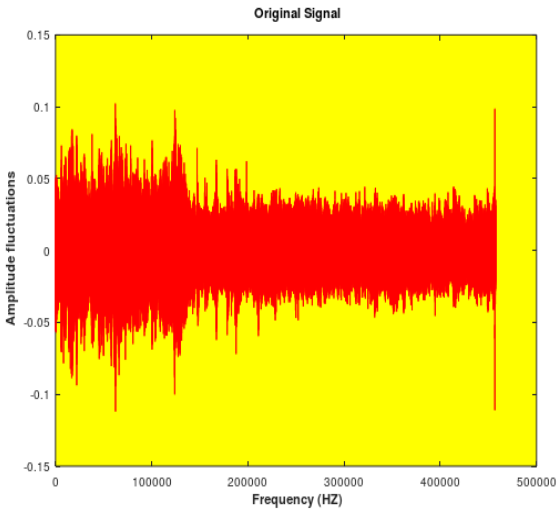

Figure 5. Original speech signal

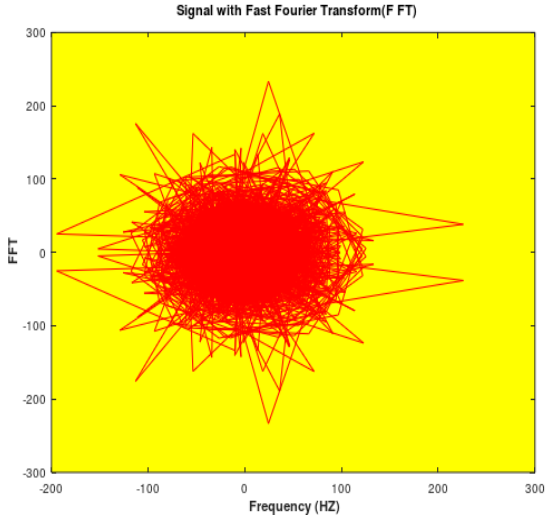

Figure 6. Signal by using FFT

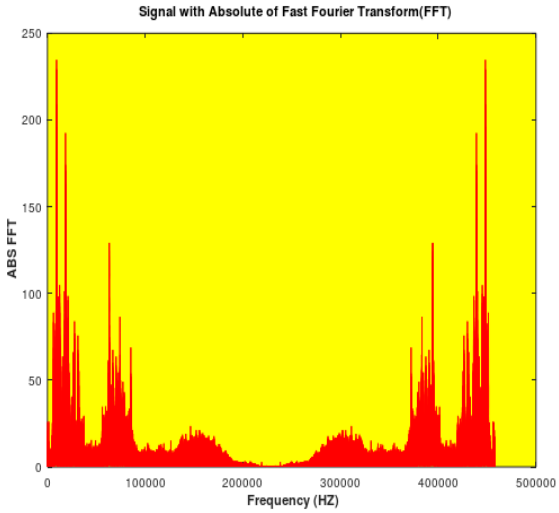

Figure 7. Result by using ABS (FFT)

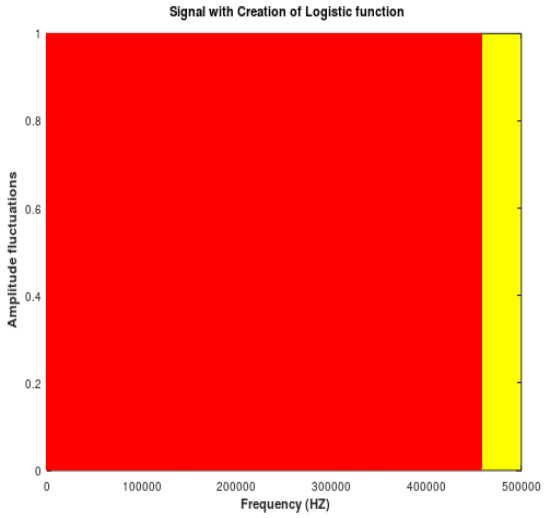

Figure 8. Result of logistic map, for r=4

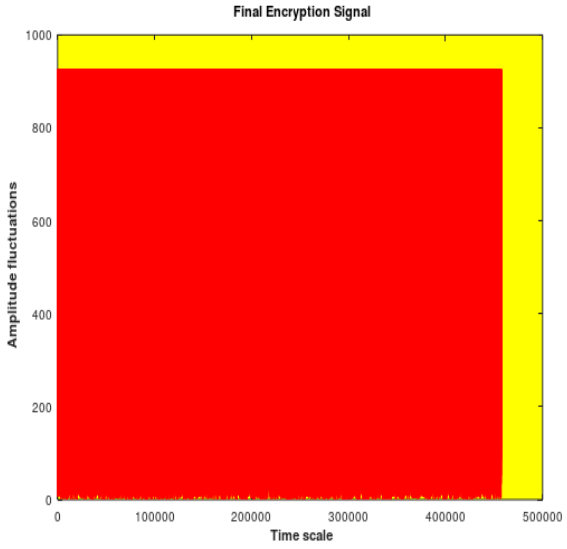

Figure 9. Final speech encryption by confusion and diffusion

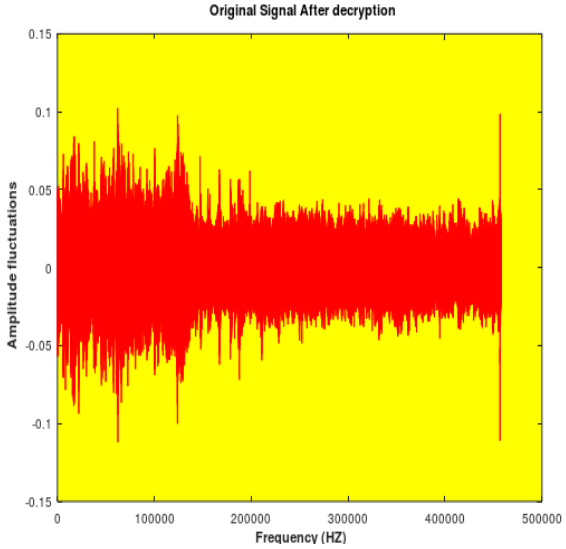

Figure 10. Original signal after decryption

6. PEARSON CORRELATION COEFFICIENT

It is a significant measurement used to assess the quality of encipherment calculation of cryptosystem, by comparative like samples in original sound signal and the encoded sound signal. The Pearson correlation coefficient is a linear correlation coefficient, which is utilized to mirror the linear correlation of two typical ceaseless variables, the Pearson correlation coefficient is defined as follows [22]:

$$r = \frac{(N\sum xiyi - \sum xi \sum yi)}{\sqrt{Nxi^2 - (\sum xi)^2}\sqrt{Nyi^2 - (\sum yi)^2}}$$

where r [-1,1], the greater the value is, the higher X, Y linear correlation rate will be. At the point when r=1, X and Y are totally positive correlation.

At the point when r=-1, X and Y are totally negative correlation. At the point when r=0, the linear correlation among's X and Y isn't explicit. A correlation coefficient drawing nearer to 1 demonstrates a powerful correlation while the coefficient near 0 implies so low correlation. Lowest value is the best for more quality of encipherment algorithm. Table 1 displays the correlation coefficient between original and encoded speech signal and it illustrates the proposed system has better quality for encipherment algorithm.

Table 1. Quality of encrypted signal

Test number	correlation coefficient
Test 1	0.0051651
Test 2	-0.0076928
Test 3	-0.0037363
Test 4	-0.0043465
Test 5	0.0047094

7. CONCLUSION

Speech is a means of communication between humans, so it is necessary to save voice messages and protect it from any attack (unauthorized persons) [23-25]. In this research, speech text messages were encrypted by combining with two of chaotic approaches (Logistic, Sine). The first approach is using Logistic map in confusion process and the second approach Sine map in Creation of diffusion key process. The two approaches encrypt the original signal, which makes the cryptanalysis a hard task and increases the security of the sound signal. They are very sensitive to the first condition and control parameters that mean the encrypted signal cannot be decrypted easily.

ACKNOWLEDGEMENTS

This project is funded by the Center for Research Excellence, Incubation Management Center, Universiti Sultan Zainal Abidin.

REFERENCES

[1] H. H. Carr, C. A. Snyder, "Data Communications & Network Security," *McGraw-Hill*, 2006.
[2] A. Shamim, et al., "Layered Defense in Depth Model for IT Organizations," *2nd International Conference on Innovations in Engineering and Technology (ICCET'2014)*, pp. 21-24.
[3] S. Juma, Z. Muda, M. A. Mohamed, W. Yassin, "Machine Learning Techniques for Intrusion Detection System: A Review," *Journal of Theoretical & Applied Information Technology*, vol. 72, no. 3, pp. 422-429, 2015.
[4] N. A. Mahadi, M. A. Mohamed, A. I. Mohamad, M. Makhtar, M. F. A. Kadir, M. Mamat, "A survey of machine learning techniques for behavioral-based biometric user authentication," *Recent Advances in Cryptography and Network Security, IntechOpen*, 2018.
[5] S. Pund-Dange, "Steganography: A Survey," In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. *Advances in Intelligent Systems and Computing*, 2018.
[6] O. G. Abood, S. K. Guirguis, "A Survey on Cryptography Algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495-516, 2018.
[7] M. A. Mohamed, "A Survey on Elliptic Curve Cryptography," *Applied Mathematical Sciences*, vol. 8, no. 154, pp. 7665-7691, 2014.
[8] R. Sivakumar, B. Balakumar, and V. A. Pandeeswaran, "A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security," *International Research Journal of Engineering and Technology*, vol. 5, no. 4, pp. 4133-4137, 2013.
[9] S. Vaidyanathan, et al., "A new chaotic jerk system with three nonlinearities and synchronization via adaptive backstepping control," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 1936-1943, 2018
[10] Aceng Sambas, et al., "A new hyperchaotic hyperjerk system with three nonlinear terms, its synchronization and circuit simulation," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 1585-1592, 2018.
[11] E. Hato, "Lorenz and Rossler Chaotic System for Speech Signal Encryption," *International Journal of Computer Applications*, vol. 128, no. 11, pp. 25-33, 2015.
[12] W. Sayed, A. G. Radwan, and H. A. H. Fahmy, "Design of a Generalized Bidirectional Tent Map Suitable for Encryption Applications," *11th International Computer Engineering Conference (ICENCO)*, pp. 207-211, 2015.
[13] Y. Liu, L. Chen, "A Survey of Chaos Theory," *Chaos in Attitude Dynamics of Spacecraft*, 2013.
[14] A. A. Tamimi, A. M. Abdalla, "An Audio Shuffle-Encryption Algorithm," *Proceedings of the World Congress on Engineering and Computer Science, WCECS 2014*, vol. 1, San Francisco, USA, 22-24 October, 2014.
[15] M. Farouk, O. Faragallah, O. Elshakankiry, A. Elmhalaway, "Comparison of Audio Speech Cryptosystem Using 2-D Chaotic Map Algorithms," *Mathematics and Computer Science*, vol. 1, no. 4, pp. 66–81, 2016.
[16] M A. Nasser, I. Q. Abduljaleel, "Speech Encryption Using Chaotic Map and Blowfish Algorithms," *Journal of Basrah Researches (Sciences)*, vol. 39, no. 2, pp. 68–76, 2013.
[17] S. Vishwakarma, S. Qureshi, "Secure Transmission of Video using (2, 2) Visual Cryptography Scheme and Share Encryption using Logistic Chaos Method," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 1, pp. 1502–1514, 2018.
[18] H. Oğraş, M. Türk, "A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator," *American Journal of Signal Processing*, vol. 6, no. 3, pp. 67–76, 2016.
[19] A. Belazi. A. A. A. El-latif, "A simple yet efficient S-box method based chaotic sine map," *Opt. - Int. J. Light Electron Opt.*, vol. 130, pp. 1438-1444, 2016.
[20] Y. Alemami, L. Almazaydeh, "Pathological Voice Signal Analysis Using Machine Learning Based Approaches," *Computer and Information Science*, vol. 11, no. 1, pp. 8–13, 2018.
[21] Y. Saleem, M. Amjad, M. H. Rahman, F. Hayat, T. Izhar, M. Saleem, "Speech Encryption Implementation of 'One Time Pad Algorithm' In Matlab," *Pakistan Journal of Science*, vol. 65, no. 1, pp. 114-118, 2013.
[22] P. Sun, N. AlJeri and A. Boukerche, "A Fast Vehicular Traffic Flow Prediction Scheme Based on Fourier and Wavelet Analysis," *IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, 2018.
[23] F. Mansouri et al., "A Fast EEG Forecasting Algorithm for Phase-Locked Transcranial Electrical Stimulation of the Human Brain," *Frontiers in neuroscience*, vol. 11, 2017.
[24] R. Lafta, et al. "A Fast Fourier Transform-Coupled Machine Learning-Based Ensemble Model for Disease Risk Prediction Using a Real-Life Dataset," *In: Kim J., Shim K., Cao L., Lee JG., Lin X., Moon YS. (eds) Advances in Knowledge Discovery and Data Mining. PAKDD 2017. Lecture Notes in Computer Science*, vol. 10234. 2017.
[25] P. Sathiyamurthi, S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *J. Audio Speech Music Proc.*, 2017.