Implementation of VoIP Speech Encryption System Using Stream Cipher with Lorenz map Key Generator

Mahmood K. Ibrahem, Hussein Ali Kassim

Abstract— Voice over Internet Protocol (VoIP) is a fast growing service in communication technology. Due to the cost-effectiveness, many organizations have been deploying VoIP technology for their teleconferencing and video conferencing services. In recent decades, various types of unsecured applications have been developed, and different application protocols have been standardized but without providing any confidentiality to voice stream when traveling on the open or shared networks. However, most of VoIP applications were developed for transmitting voice data over an insecure network. The increasing demand for VoIP services results in increasing number of users who need a secure, a reliable, high quality of service, and efficient communication. In this paper, a VoIP system speech encryption has been designed and implemented which is optimized for best real-time service delivery and increases the confidentiality and authority. It has also focused on studying and the performance of VoIP system and encryption quality by using multiple data at the same time based on the chaotic Lorenz map. The results show that it is based on the chaotic maps for generating a one-time random key used to encrypt each voice data in the VoIP packet. Chaotic maps have been used successfully for encryption bulk data such as voice, image, and video, chaotic cryptography has good properties such as long periodicity, pseudo-randomness, and sensitivity to initial conditions and change in system parameters. The experimental work demonstrates that the proposed system provides confidentiality to voice data with voice over IP performance quality, minimum loss in transmitted packet, minimum average delay, and minimum jitter.

Index Terms— VoIP; Speech encryption; chaotic theory; Lorenz map; G.729; QoS; RTP

1 Introduction

Voice over Internet Protocol (VoIP) provides the voice streaming ability on successful implementation in the network. During last decade a growing technology makes it supports the merger of voice and video streaming and also provides the text transport ability over the network. Due to the implementation of it the cost effective solution, it can be developed for the intercommunication among users on a local area network or wide area network (www). The proposed idea has been implemented on the voice streaming area of the VoIP technology. In the audio streaming, the security vulnerabilities are possible on the VoIP server during communication between two parties [1].

In practice, many encryption algorithms are existing to improve the security services on VoIP. For Example, Secure Real-time Transport Protocol (SRTP) that attempts to provide the protection to voice through used traditional encryption algorithms and public-key algorithms such as RSA to provide authentication for traffic and management distributed a session key, and AES to provide confidentiality to the VoIP payload data packet, but still SRTP suffer from some weakness, the weakness due to SRTP depend on block cipher AES algorithm for encrypting the packet data contents" plaintext data" [2]. AES algorithm and any other block cipher cryptosystems require block size of input data should be multiple of 128 bits. If the size of the data is not fitting to multiple of 128 bits the algorithms will increase "padding" to make the size of data multiple of 128 bits, and then encrypts data (original plus padding data). In this situation, there are several threats in using SRTP protocol [3].

The attacker may use the encrypted padding part of message and apply the brute-force attack to conclude the encryption Key, and in general traditional block cipher cryptosystem such as AES, 3DES, and DES are not efficient scheme for multimedia data, speech and video, due to the large data size, high correlation and redundancy among data. Therefore, researchers have been begun to develop a novel technique aims to make the original speech corrupt and reduce the residual intelligibility of speech data, and the output of this technique, in general, is noisy data [4].

Chaotic Cryptography has been effectively used for encrypting large-scale data such as image, audio, and video data, because chaotic map have a good characteristic like generating a key with long periodicity, pseudo-randomness, and sensitivity to change in initial conditions and system parameters.

In this paper, Three-Dimensional Lorenz chaotic map has been used to generate a one-time key that successfully used to encrypt payload data of VoIP packet. Three-Dimensional map is a novel algorithmic operation for the key generation with a block size of 64 random bits is produced at each iteration. The binary floating-point 64-bit format is used from the IEEE 754-2008 standard for floating point arithmetic [5].

2 RELATED WORK

Several chaotic maps have been proposed for speech encryption schemes:

Zeeshan H., and Jan Sher K. [6]have submitted a new speech encryption algorithm based on scrambling speech signal in the frequency domain and permutation speech samples in Tangent Delay Ellipse Reflecting Cavity Chaotic Map System (TD-ERCS). The speech signal first captures from input audio source and captured speech signal is divided into small frames of equal length each frame consists of 64 samples then pass into Discrete Cosine Transform (DCT) for amplitude scrambling and coefficients scrambling in the frequency domain. After complete applying the DCT for amplitude scrambling used the chaotic map to generate a pseudo-random number is that will

- *Hussein Ali Kassim is currently pursuing master's degree program in College of Information Engineering - Al-Nahrain University in University, Baghdad, Iraq. E-mail: hussein.ali@coie-nahrain.edu.iq*
- *Mahmood Khalel Ibrahem, Scientific degree Assistant Professor in College of Information Engineering - Al-Nahrain University in University, Baghdad, Iraq. E-mail: mahmoodkhalel@coie-nahrain.edu.iq*

used for permuting speech samples. Then inverse Discrete Cosine Transform IDCT is applied on the permuted speech samples and transmission over a shared or insecure channel.

Experimental results related to speech intelligibility test, correlation, key sensitivity test and key space indicate that the suggested speech encryption algorithm performs powerfully, the encrypted speech is unintelligible and the recovered speech signal has good quality.**Ahmad et al** [7] present speech encryption system based on a high-dimensional chaotic map, it based on the combination process of two types of chaotic maps Chen and Lorenz. The generated sequences of the key have two stages first pre-processed and quantized and the second stage converted into a sequence of binary bits. After complete generating of random sequence of bits, the voice data also convert to stream bits and apply the XOR operation with the output key stream. **H. S. Kwork and Wallack K. S.** [8], Present system an online chatting system with an embedded real-time chaotic encryption/decryption method designed for the Internet. Such system not only provides a real-time communication platform but also ensures a secure channel for communication. By the use of cipher feedback and the skew tent map, the input text can be real-time encoded and the cipher text is sent via TCP/IP. With the properties of randomness of the map and its sensitivity to system parameters and the initial conditions, the encrypted transmitting messages are difficult to have eavesdropped. The implemented method is simple and can be easily embedded in any existing systems**. R. Gnanajeyaraman** [9], present a new voice encryption system based on chaotic theory. Implementation of system start with generating a look-up table using higher dimensions chaotic cat map, with eight dimension 8D, that used to mask the voice samples. The value of chaos-based cat map used for encryption, decryption system with high dimension chaotic map enhances the security level of the algorithm and the key space, and that makes the audio sample distributed uniformity. **Sheu** [10] , presented a Two- dimension chaotic theory speech Encryption using fractional Lorenz system for speech communication (henceforth called TCSE). Lorenz map used to generate a pseudorandom number generator (PRNG) will used for encrypting speech data. The TCSE can achieve high key sensitivity, large key space, and increase ability to resist chosen plaintext\cipher-text attack. **Ashtiyani et al** [11], presented speech encryption based on symmetric cryptography via the Cat Map. The speech signal was encrypted based on a combination of two operations of scrambling speech samples and then confusion. The Cat map was used for scrambling the speech samples, chaos cryptosystem also used in improvement of the simple form of the Advance Encryption Standard (AES), the improvement occur on the contain of original S-box, the cat map used to generate random 16 bits that substituted into the AES S-box, rather than based on fixed values. Su et al [9], suggest encryption scheme for G.729 standard speech based on two selective encryption methods. The research used chaos cryptosystems to minimize the computational complexity and provide full encryption to G.729 speech data. The algorithm started by portioning the G.729 speech data into two parts according to the sensitivity bits, the sensitivity part was encrypted by using a strong cipher used a companion the logistic and Cat maps, and the remaining part that has less sensitive bits was encrypted using a lightweight cipher based on one of the logistic or cat maps.

3 Chaotic Theory

A chaotic system is a non-linear behavior found in nature. The following are the most important properties of chaotic theory; a behavior of chaotic system pattern is a collection of many non-linear dynamics process sorted acts and under normal conditions each part doesn't play a leading role, chaotic system gives and reflects unpredictability and randomness values, and it is very sensitive to necessity in initial condition. Even two identical chaotic systems, they will quickly grow toward completely diverse states, if they are in two marginally different first states. The Butterfly effect shows that a small change in the initial conditions leads to drastic changes in the results. Unpredictability: Chaos theory shows unpredictability due to sensitivity to initial conditions. Feedback: Chaos theory shows feedback-response behavior. The next value is calculated using the last output as in the case of logistic equation. Chaotic maps classify into two categories, according to the time range that described by equation of system, continuous systems that have differential equations, or discrete systems that have difference equations. Logistic map and Henan map are example of the discrete systems. The Lorenz system and Rossler system are example of the continuous systems [12] [13].

3.1 Lorenz map

The Lorenz map is standout amongst the most prominent three dimensional chaotic attractors; it was analyzed and presented by Edward Lorenz in 1963. He demonstrated that a small change in the starting states or initial conditions of a climate model could give high differences in the subsequent or resulting weather. This implies that a slight contrast in the start state condition will affect the output of the whole system, which is called sensitive system depending on the initial stats. The non-linear dynamical system is sensitive to the initial value and is related the periodic behavior system [14].

Lorenz's non-linear dynamic system introduces a chaotic attractor, while the word chaotic is regularly used to explain the difficult manner of non-linear dynamical systems. Chaotic theory produces obviously arbitrary conduct yet in the meantime is totally deterministic, as shown in figure (1). The Lorenz attractor is characterized as follow [15]:

$$\frac{dx}{dt} = \sigma(y - x) \qquad (1)$$

$$\frac{dy}{dt} = x(\rho - z) - y \qquad (2)$$

$$\frac{dz}{dt} = xy - \beta z \qquad (3)$$

Where $(\sigma = 10, \rho = 28, \beta = 8/3)$ are the positive parameters of Lorenz system andx_0,y_0 , z_0 are the initial values Lorenz system between zero and one and t is time.

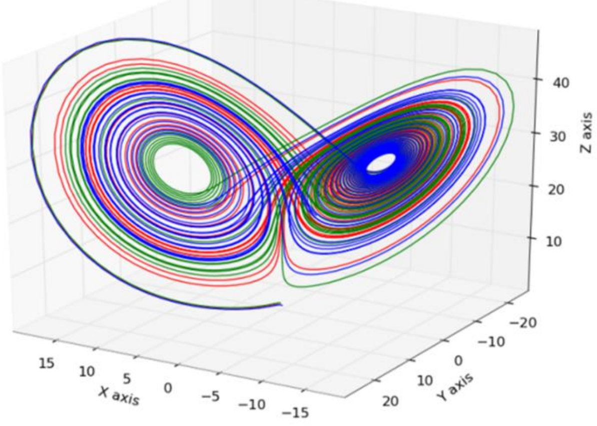


Figure 1: A plot of the trajectory of the Lorenz system

3.2 Generation a One Time key using chaotic Lorenz map

One-dimensional chaotic such as logistic map has some drawback that it has low control parameters; it has only one control parameter β but faster in generating pseudo-random numbers. The higher dimensional chaotic system such as Lorenz and Rossler can be used to increase the key space, complexity and enhances the randomness of pseudo sequence. The algorithm used for generating pseudo random numbers in this paper based on the chaotic Lorenz map given by equations (1, 2, and 3). The differential equations of Lorenz system are three dimensions, which cannot directly get values for this system equation because it has differential and must be solved using Runge Kutta (RK4) method with fourth order. Runge Kutta (RK4) can be summarized as [16]:

Let the differential equation of Lorenz system $\frac{dx}{dt} = f(x, y, z)$with initial condition values$\frac{dx}{dt} = x_0, \frac{dy}{dt} = y_0, \frac{dz}{dt} = z_0$, then the approximate solution of $\frac{dx}{dt}$ using Runge Kutta is given by

$$x_{n+1} = x_n + \frac{h}{6} * [k_1 + 2k_2 + 2k_3 + k_4], \qquad t_{n+1} = t_n + h \quad (4)$$

Where x_{n+1} is the Runge Kutta approximation of $\frac{dx}{dt}$, h is the interval size, t is time, and

$$k_1 = f(x_n, y_n, z_n) \quad (5)$$

$$k_2 = f\left(x_n + \frac{h}{2}k_1, y_n + \frac{h}{2}k_1, z_n + \frac{h}{2}k_1\right) \quad (6)$$

$$k_3 = f\left(x_n + \frac{h}{2}k_2, y_n + \frac{h}{2}k_2, z_n + \frac{h}{2}k_2\right) \quad (7)$$

$$k_3 = f\left(x_n + \frac{h}{2}k_2, y_n + \frac{h}{2}k_2, z_n + \frac{h}{2}k_2\right) \quad (8)$$

$$k_4 = f(x_n + hk_3, y_n + hk_3, z_n + hk_3) \quad (9)$$

And calculating y_{n+1} and z_{n+1} by using the same equations of RK4 that used in calculating of x_{n+1} but replacing equation dx/dt with the dy/dt or dz/dt. Runge Kutta has error per step (h^5) and total accumulated error (h^4) and h equal to 0.5. The method that used for generating pseudo-random one time pad based on the output of Lorenz system. In each iteration, to generate pseudo random number apply a xor operations to the output of $(x_{n+1}, y_{n+1} z_{n+1})$ equations and convert to binary 8 Bytes (64 bits).This method allows producing 64 bits random sequences of bits that increasing the throughput of key generation, figure 2 shows the proposed scheme to generate one time key that based on Lorenz system.

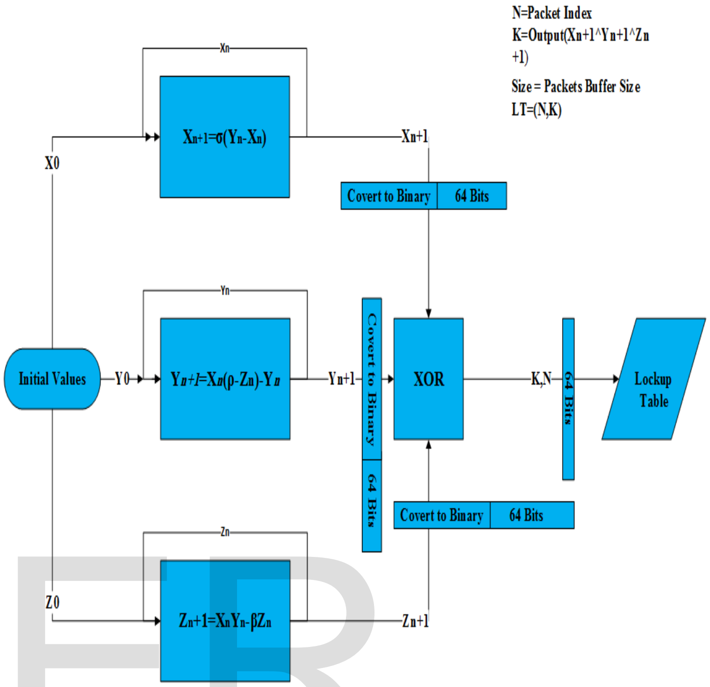


Figure 2: OTP Key Generation using Lorenz map

4 PROPOSED INTEGRATED VOIP PROTOCOL

The proposed protocol provided secure environment to start speech communication between two individual users. It uses public key scheme for user authentication to server, secure key exchange, and symmetric stream cipher encryption scheme for speech data that encoded and compressed by ITU G.729 standard. The protocol comprises of four stages; User Connection Stage, User Authentication Stage, Distributed chaotic initial parameters Stage and Communication Stage. Stages are described as follows:

Stage I: User Connection Stage: User send information to server includes (User ID and network information) Server accept request and validate the information with server Database, then send public key (KUs) to user .Stage I consist of steps of (1_3) of protocol.

Stage II: User Authentication Stage: In this stage, User try to establish secure communication with server based on Real Time Control Transport Protocol (RTCP) for network management and packet format and used the public key encryption algorithms (RSA) to encrypt encryption data packet. After user have received server public key, generate private, share public key, and send public key to server encrypted with server public key. Server receives public key and update online user list to all others user, after this stage user will be ready to start secure communication with any online user.

Stage III: Distribution of chaotic initial parameters Stage: User A request start voice communication with destination user B (B must be online). Server generate chaotic parameters and implements message encryption by user A public key.

Stage IV: Communication Stage: User B build lockup table depend on the chaotic key generated as separate process to store one time key generated by chaotic Lorenz map and each packet will be encrypted with one time key of chaotic Lorenz map and a reception used the packet index to select the correct key from the lockup table that packet encrypt for successive packet decryption.

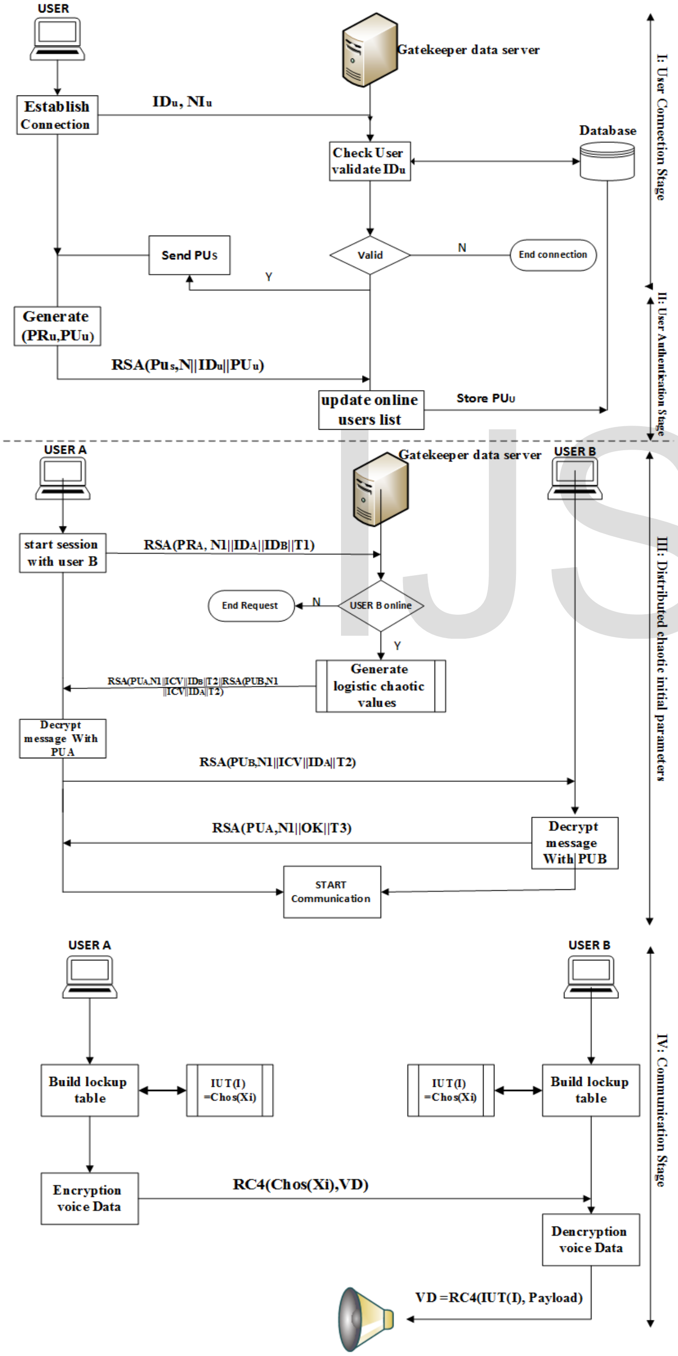


Figure 3: The Proposed VoIP System

Seq.	From/To	Activity
		Stage I: User Connection Stage
1	U ➡ S	Send User Information (IDu, NIu).
2	S	Check User validate using sever database, if not terminate connection (M1).
3	S ➡ U	Send PUS to User
		Stage II: User Authentication Stage
4	U	Generate Private, Public Keys of RSA algorithms.(PRu,PUu)
5	U ➡ S	Send RSA(PUs,N||IDu||PUu) to server
6	S ➡ all users	Server update online user list and store PUu in DBs
		Stage III: Distributed chaotic initial parameters
7	Ua ➡ S	User a request start session with user B. RSA(PRa, N1||IDa||IDb||T1)
8	S	Generate logistic chaotic values (ICV)
9	S ➡ Ua	Send RSA(PUa,N1||ICV||IDb||T2||RSA(PUb,N1||ICV||IDa||T2)
10	Ua	Decrypt message using PRA
11	Ua➡Ub	User a send RSA(PUb,N1||ICV||IDa||T2) message part to user b
12	Ub➡Ua	Send RSA(PUa,N1||OK||T3) and Start Session
		Stage IV: Communication Stage
13	a,b	Build lockup table ,IUT(I) ⬅ Chos(Xi)
15	a	Encoding and Encryption voice Data,RTP payload =RC4(Chos(Xi),VD)
16	a ➡ b	Send RTP packet over UDP protocol
17	b	Received Packet and decrypt RTP payload,VD =RC4(IUT(I), Payload).

NOTATION	
IDu	User Identification Number
NIu	Network Information of User (IP Address, Port No.)
PUs	Server Public key
RSA	Public-key Cryptosystems
PRu	User Private Key
PUu	User Public Key
N	Nonce Number
DBs	Gatekeeper Database Server
N1	Nonce Number for Distributed chaotic parameters
T1,T2,T3	Timestamp
ICV	logistic Chaotic Values
LUT	Lockup Table for synchronization between User A and User B
RTP	Real-time Transport protocol
I	RTP Packet Index

Chos(Xi)	Chaotic Key generation with Xi value
RC4	Stream encryption Scheme
VD	Voice Data
Payload	RTP Packet Payload
S	server
U	user

5 VOIP PERFORMANCE AND ENCRYPTION QUALITY

5.1 VoIP Performance metrics

The quality of the VoIP performance is represented in three important parameters packet loss, delay, and jitter [17].

A Packet loss: loss in the transmitted packet defines the percentage of the packet that transmitted via sender and never reaches the correct destination, or the destination has dropped these packets deliberately due to an error in the packet header (e.g. TTL=0), or a transmitted packets discarded by intermediate links. The VoIP system should be implemented with packet loss less than 1.5%.The packet loss through reasonably reliable estimates to define the grade of performance, Good between 0% and 0.5%, Acceptable between 0.5%- and 1.5%, Poor greater than 1.5%.

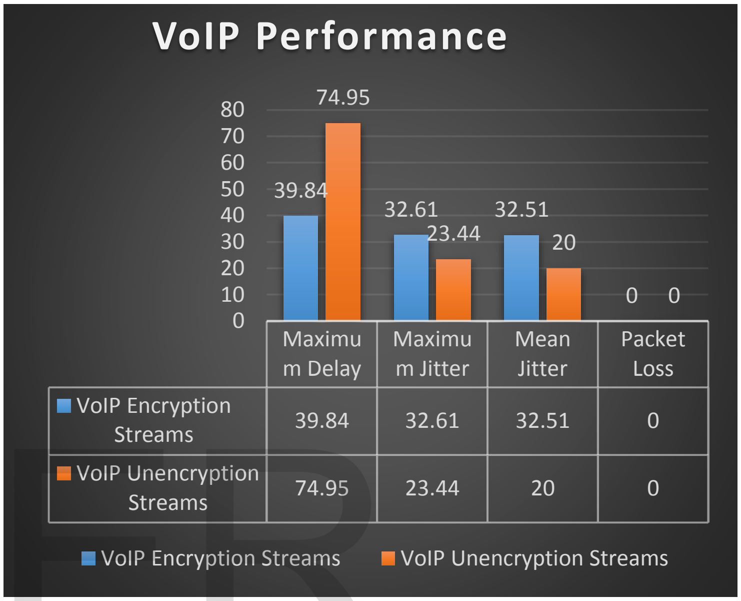
B Delay: is defined as the time that VoIP packet takes to successful transmitting from the sender to destination. Delay defined as three categories: Good between 0ms and 150ms, Acceptable between 150ms and 300ms, and poor greater than 300ms

C Jitter: is defined as the variation in the time delay from one end to another. If the time delay of transmitting packet has widely variation in a VoIP call, it causes greatly degraded in voice call quality. In VOIP network, at each endpoints having jitter buffers to store received packets, it is designed to deliver traffic to end user at the constant rate. When sender have been generated packets with different rates, this variation that called jitter result from delay in time for construction RTP packets, voice data compression, and data encryption. VoIP network that has higher jitter values, it causes loss in packet and degradation in voice quality. The grade of Jitter classify into three categories: Good between 0ms and 20ms, Acceptable between 20ms and 50ms, and poor greater than 50ms.

D RESULTS: The main goal here analysis the performance of VoIP and show the effect of proposed encryption algorithm on the VoIP quality, two types of VoIP streams were analyzed, stream without encryption (Plain-text stream), and encrypted packets stream based on stream cipher and Lorenz map to generate one-time pad. As mentioned earlier, four parameters were calculated using Wireshark program to analyze more than 50,000 RTP packets per duration for each stream. These four parameters were maximum delay, maximum and mean jitter, and packet loss. These results have been shown in figure 4.Results shows the proposed encryption system has small effects on the performance and table 1 shows performance results of VoIP systems (the proposed system, and system without Encryption).

TABLE 1: VoIP Performance Comparison the Proposed encryption System and System without Encryption

VoIP Systems	Packet loss	Maximum Delay	Mean Jitter	Maximum Jitter
The proposed system	Good	Good	Accepta-ble	Acceptable
System without Encryption	Good	Good	Good	Acceptable



	Maximum Delay	Maximum Jitter	Mean Jitter	Packet Loss
VoIP Encryption Streams	39.84	32.61	32.51	0
VoIP Unencryption Streams	74.95	23.44	20	0

Figure 4: VoIP Performance.

5.2 ENCRYPTION QUALITY

In this section, demonstrates the quality of proposed encryption scheme that based on the stream cipher RC4 algorithms to encryption voice data and chaotic Lorenz map to generate sequence of random keys. The results have been implemented using Visual C# 2012 on a laptop Windows 7, Intel® Core™ i3 with speed 2.3 GHz, and Ram 8GB. For encryption experimentations, we used 5-wave sound files with different size. Figure 7 shows a waveform and spectrogram of an original, encryption and decryption speech signal. From the Figure 7, the encrypted speech has been distributed uniformly and unintelligible. It is different from the waveform of original speech. In addition, the waveform of the decryption speech is identical to the original speech waveform [18].

A Mean Square Error (MSE): MSE is a frequently calculate the difference between two samples speech and it indicates the measurement of the error with estimate to the center of the mean of the value of speech samples, MSE is describe in equation (6). At most, it has already been used to estimate the error that has occurred due to the encryption and decryption process in the recovered speech data [19].

$$MSE = \frac{1}{N}\sum_{i=0}^{N-1}(\hat{O}i - O\ i)^2 \qquad (10)$$

Where O represent the samples of audio file, Ô represent the samples of encrypted or decrypted audio samples, and N represent the length of audio samples. When MSE equal to zero or near to zero it indicates that decryption process have a perfect recovery operation to return the original audio samples, otherwise, when MSE of is greater value that indicate the distortion between two sequence of samples is hugely. Table 2 shows MSE measures of the tested encryption and decryption speech data.

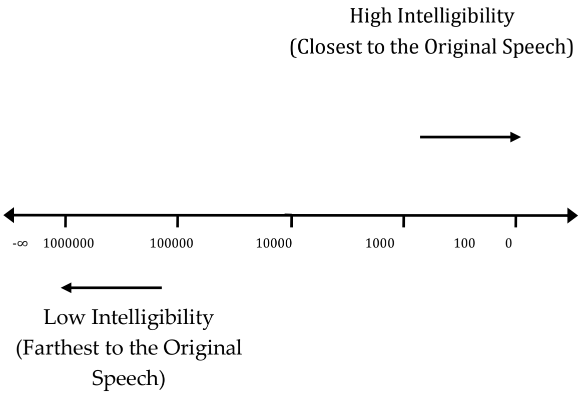


Figure 5: The mean square error measure.

B Signal-to-Noise-Ratio: It is one of the widely used as objective measurement to measure the distortions level of speech signal cryptography. It is the most possible simple measure distortion in the time domain and it (abbreviated SNR or S/N) ratio. Its aim is to measure the distortion of the waveform-encrypted file that reproduce the original waveform file. It is calculated as follows:

$$SNR = 10 * \log_{10} \frac{\sum_{i1}^{l} x_i^2}{\sum_{i=1}^{l}(x_i - y_i)^2}(dB) \qquad (11)$$

Wherex_i, and y_i are the original and encrypted speech signal indexed by i, l is the total number of the samples for the wave signal, often expressed in decibels (dB). Table 2 shows SNR measures of the tested encryption and decryption speech data.

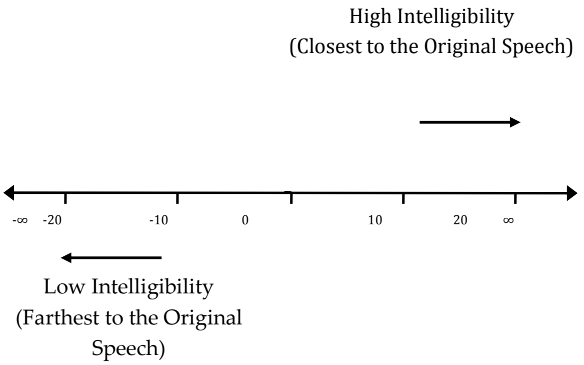
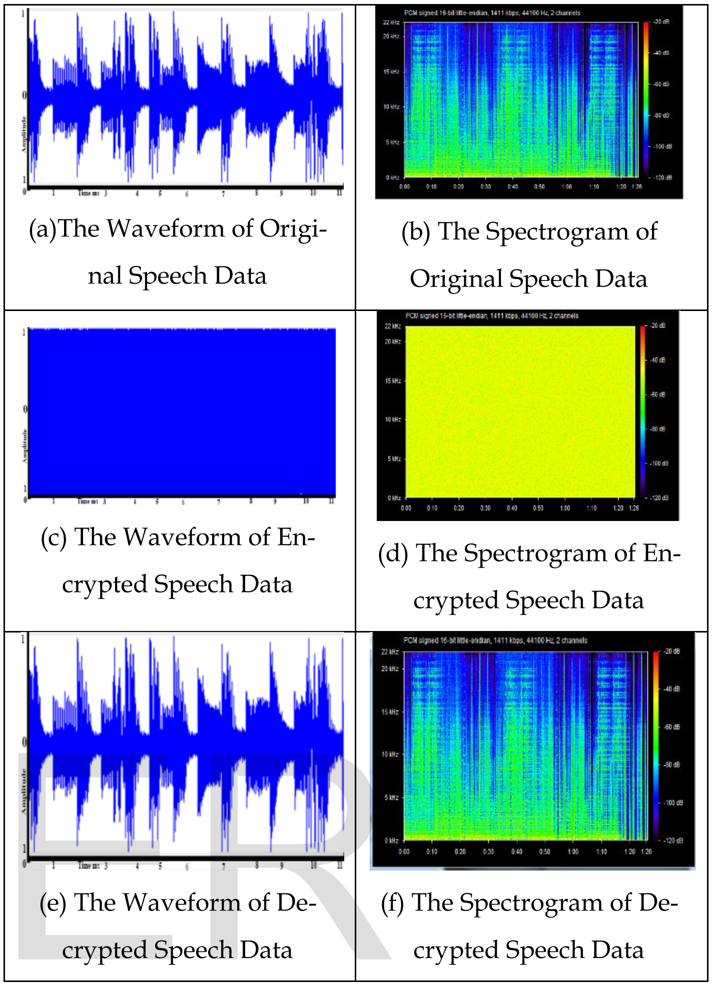


Figure 6: The signal to noise ratio measure.



(a)The Waveform of Original Speech Data

(b) The Spectrogram of Original Speech Data

(c) The Waveform of Encrypted Speech Data

(d) The Spectrogram of Encrypted Speech Data

(e) The Waveform of Decrypted Speech Data

(f) The Spectrogram of Decrypted Speech Data

Figure 7: Waveform and spectrogram of original, encrypted, decrypted speech data.

TABLE 2: Encryption and Decryption Quality (MSE and SNR) Measurement

		Encryption		Decryption	
File Name	Data Size(bytes)	MSE	SNR	MSE	SNR
Amy.wav	1,751,020	172313540.6	1.385901466	0	Infinity
Brian.wav	1,737,196	171761426	1.481424	0	Infinity

Emma.wav	1,539,052	173759942	1.383223	0	Infinity
Eric.wav	1,645,036	171761628	1.468129	0	Infinity
Jennifer.wav	1,631,212	171853672	1.278779	0	Infinity

5.3 Time Analysis

The performance is determined by evaluating the running speed that can measured by, the average encryption/decryption times, and the encryption throughput. The encryption throughput (ET) defined as [20]:

$$\boldsymbol{ET} = (\boldsymbol{Speech\ data}\ (\boldsymbol{Byte}))/(\boldsymbol{Encryption\ time}(\boldsymbol{millisecond})\ )(\mathbf{8})$$

These equations permit to compare the running speed of different cryptosystems working on different platforms. Different encryption algorithms are analyzed using the same tools and the speech data in section 5.2, AES with 256-bit long key size as a case study of the block cipher, proposed encryption scheme based on stream cipher (RC4) and Lorenz map for key generation. Table 3 contains the time for encryption and decryption process of the proposed algorithms and AES. Table 4 contains the encryption throughput of the proposed algorithms and AES with 256-bit long key size.

Table 3: Comparison Encryption Time between Proposed Encryption method and AES

speech data	Size in Bytes	Time Analysis for Encryption and Decryption			
		Lorenz Map		AES (256)	
		Encryption	Decryption	Encryption	Decryption
Amy.wav	1,751,020	933	980	4376	4417
Brian.wav	1,737,196	759	844	4051	4041
Emma.wav	1,539,052	702	678	3519	3988
Eric.wav	1,645,036	998	777	3799	3731
Jennifer.wav	1,631,212	730	735	4965	3666
Average		824.4	802.8	4142	3968

Table 4: Comparison Encryption Throughput between Proposed Encryption method and AES

Speech data	**Size in Bytes**	**Encryption /Decryption Throughput of Proposed method and AES**			
		Lorenz Map		AES (256)	
		Encryption	Decryption	Encryption	Decryption
Amy.wav	1,751,020	1876	1786	400	396
Brian.wav	1,737,196	2288	2058	428	429
Emma.wav	1,539,052	2192	2269	437	385
Eric.wav	1,645,036	1648	2117	433	440

Jennifer.wav	1,631,212	2234	2219	328	444
Emma.wav	1,539,052	2047.6	2089.8	405.2	418.8
Average		2047.6	2089.8	405.2	418.8

By finding the average for the encrypting and decrypting time and throughput from tables 3 and 4. The proposed encryption is faster and higher throughput by five times than AES. Figure 8 and 9 demonstrate the chart for the time and throughput.

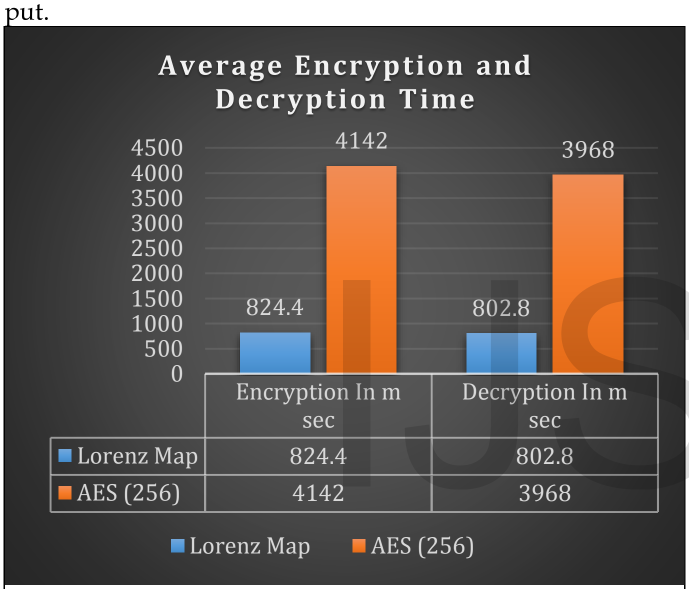


Figure 8: Average of encryption Time of Proposed Encryption method and AES

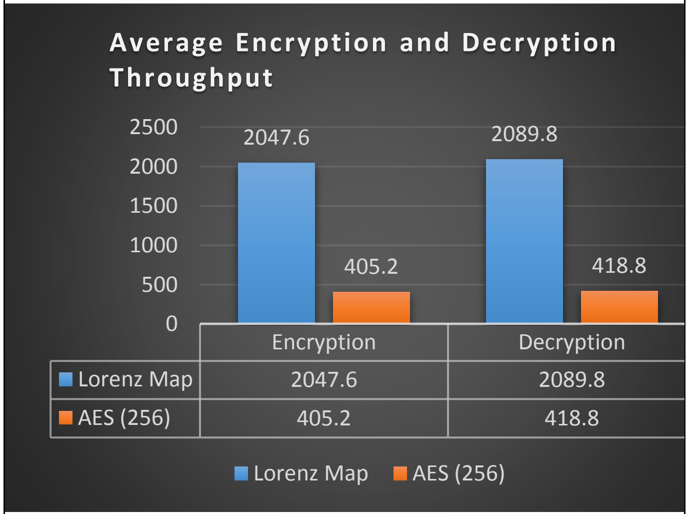


Figure 9: Average of encryption throughput of Proposed Encryption method and AES

6 Conclusion

In this paper, a novel VoIP speech encrypting system is proposed based on stream cipher RC4 algorithm with three-dimension Lorenz chaotic map for one time pad key generation. The VoIP system based chaotic encryption scheme and quality of encryption are implemented using C#.net and the VoIP performance analysis using Wireshark. The experimental results of proposed system demonstrate that the proposed method satisfies the speech encryption requirements. The encrypted voice is unintelligible, and the payload of VoIP packet has the same size without any padding .The recovered speech has perfect quality with MSR equal to zero and SNR equal to infinity. The VoIP system is implemented using Microsoft windows environment with Framework version 4, and In the future, we can implementing the system using a new Kotlin Programming Language for Android application.

REFERENCES

[1] J. Bereka, VoIP Client for Multi-core Server Enhancing Quality of Real Time Service Delivery, Stockholm, Sweden: Degree project in Electronic and Computer Systems KTH-The Royal Institute of Technology, 2012.

[2] A. E. R. E.-m. Mazen Tawfik Mohammed, "Confidentiality enhancement of Secure Real Time Transport Protocol," *Computer Engineering Conference (ICENCO)*, pp. 43-48, Dec. 2012.

[3] K.-P. Man, "Security Enhancement on VoIP using Chaotic Cryptography," *IECON 2006 - 32nd Annual Conference on IEEE*, pp. 3703-3708, 2006.

[4] M. a. u. a. I. Q. Abduljaleel, "Speech Encryption Using Chaotic Map and Blowfish Algorithms," *Journal of Basrah Researches ((Sciences))*, vol. 39, no. 2, pp. 68-76, 2013.

[5] M. François, "A Fast Chaos-Based Pseudo-Random Bit Generator Using Binary64," *Informatica 38*, pp. 115-224, 2014.

[6] J. S. a. J. A. Zeeshan H., "Secure Speech Communication Algorithm via DCT and TD-ERCS Chaotic Map," *International Conference on Electrical and Electronics Engineering*, vol. DOI: 10.1109/ICEEE2.2017.7935827, pp. 246-250, April 2017.

[7] B. A. ,. a. F. Musheer A., "CHAOS BASED MIXED KEYSTREAM GENERATION FOR VOICE DATA ENCRYPTION," *International Journal on Cryptography and Information Security*, vol. 2, no. 1, pp. 36-45, 2012.

[8] W. K. S. T. a. K. F. M. H. S. KWOK, "ONLINE SECURE CHATTING SYSTEM USING DISCRETE CHAOTIC MAP," *International Journal of Bifurcation and Chaos*, vol. 14, no. 1, January 2004.

[9] K. R. R.Gnanajeyaraman, "Audio encryption using higher dimensional chaotic map," *International Journal of Recent Trends in Engineering*, vol. 1, no. 2, pp. 103-107, May 2009.

[10] L. J. Sheu, "A speech encryption using fractional chaotic systems," *An International Journal of Nonlinear Dynamics*

and Chaos in Engineering Systems, 2011.

[11] P. M. a. S. S. M. M. Ashtiyani, "Speech Signal Encryption Using Chaotic Symmetric Cryptography," *Journal of Basic and Applied Scientific Research,* vol. 2, no. 2, pp. 1668-1674, 2012.

[12] Modified and Efficient Image Encryption Algorithm Based on Chaos Theory, DNA Complementary Rules and SHA-256, Holmgatan: Master's Thesis to Computer Engineering in Mid Sweden University, 2016.

[13] F. M. M. R. a. G. P. G. Alvarez, "Cryptanalysis of a chaotic encryption system," *Physics Letters,* vol. 276, no. 1, pp. 1-13, Oct. 2000.

[14] a. D. S. Eman Hato, "Lorenz and Rossler Chaotic System for Speech Signal Encryption," *International Journal of Computer Applications,* vol. 128, no. 11, pp. 25-33, October 2015.

[15] E. Ghys, The Lorenz Attractor, a Paradigm for Chaos, Poincare Seminar 2010,2013 Springer Basel AG, 2010.

[16] F. S. Hasan, "Speech Encryption using Fixed Point Chaos based Stream Cipher (FPC-SC)," *Engineering and Technology journals,* vol. 34, no. 11, pp. 2152-2166, 2016.

[17] M. M. Alani, "Measuring the Effect of AES Encryption on VoWLAN QoS," *International Conference on Software, Telecommunications ,* Sept. 2010.

[18] K. Kondo, Subjective Quality Measurement of Speech, Signals and Communication Technology, Springer-Verlag Berlin Heidelberg 2012, 2012.

[19] C. B. a. G. L. G. Kun He, "Privacy Protection for JPEG Content on Image-Sharing Platforms," *Information Hiding and Multimedia Security,* pp. 20-23, June, 2016.

[20] a. M. E. R. S. Pavithra, "PERFORMANCE EVALUATION OF SYMMETRIC ALGORITHMS," *Journal of Global Research in Computer Science,* vol. 3, no. 8, pp. 43-45, August 2012.