Engineering and Technology Journal
Journal homepage: engtechjournal.org

Encryption VoIP based on Generated Biometric Key for RC4 Algorithm

Raya W. Abd Aljabar [a*], **Nidaa F. Hassan** [b]

[a] University of Technology, Baghdad, Iraq, cs.19.66@grad.uotechnology.edu.iq

[b] University of Technology, Baghdad, Iraq, 110020@uotechnology.edu.iq

*Corresponding author.

Submitted: 30/06/2020 Accepted: 09/11/2020 Published: 25/03/2021

KEYWORDS

VoIP, Cryptography, Stream Cipher, Biometric cryptosystem, Linear Discriminant Analysis (LDA), RC4.

ABSTRACT

Voice over Internet Protocol (VoIP) calls are susceptible to interfere at many points by many attackers, thus encryption considered an important part in keeping VoIP.

In this paper, Encryption VoIP based on Generated Biometric Key for RC4 Algorithm is proposed to encrypt the voice data before transmitting it over the network. The system uses a stream algorithm based on RC4 encryption with the new method of biometrics based Key generation technique. This system has generated complex keys in offline phase which is formed depend on features extracted using Linear Discernment Analysis (LDA) from face images.

The experimental work shows that the proposed system offers secrecy to speech data with voice cipher is unintelligible and the recovered voice has perfect quality with MSR equal to zero and PSNR equal to infinity.

How to cite this article: A. M. Jawad, S. B., Ali, and M. K. Naseer, “Encryption VoIP based on Generated Biometric Key for RC4 Algorithm,” Engineering and Technology Journal, Vol. 39, Part B, No. 01, pp. 209-221, 2021.

DOI: https://doi.org/10.30684/etj.v39i1B.1755

1. Introduction

Recently, the development in communications technology has been made persons in more need to communicate. Voice over Internet Protocol (VoIP) connects persons to put their voice call without any geographical limitation [1].

I. Voice over Internet Protocol

In the communication world, the technology of VoIP is considered as one of the most interesting technologies, since it is allowing a person in making phone calls via the internet, thus reducing the costs of communication when matched with traditional Public Switched Telephone Network (PSTN).

Many cryptographic systems are standing to increase the safety facilities on VoIP. A lot of research organizations attempted on tackling such issues for having VoIP communication which is considered to be safe. The digital information will be packetized and after that transmitted over the network, such data packets will be encrypted as well as decrypted via cryptosystems as can be seen in Figure 1.

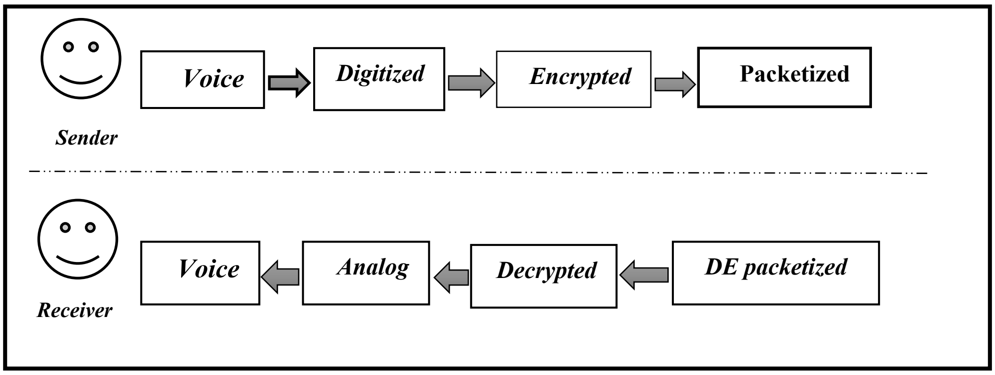

Figure 1: VoIP Technology [2]

II. Biometric System

The biometrical system can be defined as a standard approach for the identification and verifications of humans, according to the physical or personal identifications of the characteristics. The biometrics comprise approaches for the uniquely recognition of the human beings according to one or several inherent behavioral or physical features. In the area of the computer sciences, particularly, the biometrics are utilized as an identity access management form and access control. It is utilized as well for the identification of the individuals in the groups which are being surveyed. The biometrical features may be classified to 2 basic categories, which are: Physiological, which are associated with the body shape. Such as, the fingerprints, DNA, face recognition, Palm print, iris recognition and hand geometry. The behavioral are associated to a person's behavior. Such as the voice and typing rhythm. Some of the researchers coined the term behavior metrics for that category of the biometrics [3].

III. Biometric Cryptosystem

These systems are merging biometrics with cryptography to take the benefits of the two. With regard to these systems, as the cryptography is specified for being of high importance in securing data, non-repudiation is provided via biometrics, also reducing the need for remembering keys or carrying tokens, and so on. In the field of biometric cryptosystems, the cryptographic key will be created from a biometric template including a face image so that the key might not be discovered without effective biometric key [2] [4].

IV. Biometric of Face

The face is one of the most acceptable biometrics because it is arguably a person's most unique physical characteristics. There is various feature extraction methods from face biometrics, they may be categorized either as photometric or geometric methods, the latter have been based upon the development of the model according to the geometric distances between the fiducially points, whereas photometric methods have been based upon the extracted statistical values [3].

2. Related Works

In the following section, some approach of VoIP encryption to make the safe transmission of VoIP are presented:

A study conducted by M. Singh and N. Sharma [5] Suggested providing VoIP with security framework, in this model authentication has been initially applied for the authentication of true users and then the cryptographic approaches have been utilized for the secure transmission of information stream via network. The part of the authentication will be implemented with the use of the biometrics due to the fact that there is not possibility of stealing anybody's physical traits.S. Bhuvaneshwari and P. Arul. [2] Submitted secure VoIP Network by fusion of irises, this suggested system is composed of 1) Iris feature extraction 2) Cryptographic key- generation 3) Iris fusion 4) PNRG fusion with the fused iris key. That is providing a good approach for transmitting the packets safely between networks. In the case when an iris is stolen, an intruder won't have the ability for accessing the data due to the fact that the iris related to receiver and sender have been fused, also pseudo-random numbers were fused with a biometric key. Thus, there will be an ability for producing billions of matchless keys, which will make the VoIP technology difficult for attackers to guess the key. A study conducted by E. Hato et al. [6] Presented an audio encryption system, depends on three chaotic maps. The suggested system is consisted of three key entities: keys generation, samples substitution and permutation procedure. To increase the advantages of the substitution procedure, it is implemented in two steps with cipher feedback for the scheme. Additionally the permutation of bit-level for sample is presented as substitution procedure in the permutation phase. The Lorenz and Rossler chaotic system are utilized as a keystream generation for substitution and permutation procedure consequently. From the experimental results, it was determined that the suggested system has the benefits of so low remaining intelligibility, key sensitivity and good quality returned signal. A study conducted by E. Albahrani. [7] Suggested a system based on a mixture between chaotic maps and block encryption. The suggested system encodes and decodes a chunk of bytes. Each chunk is enters into three steps: Permutation step, Xor adding step, Substitution step. In Permutation step the voice chunk is permuted by chaotic Tent map. Then the output chunk is Xored with the key chunk and lastly the generated chunk is switched by novel substitution technique depend on multiplication inverse. The key is produced by novel key generation system depend on Chebyshev polynomial. The result from key space analysis, statistical analysis, MSE (mean square error) analyses, PSNR (Peak signal to noise ratio) analyses and entropy analyses revealed that the system is not susceptible to attacks. A study conducted by S. Yousif. [8] Proposed a novel cryptosystem for voice signals encoded and decoded that based on three diverse methods is offered in this paper. The primary voice signal is separated into three equivalent blocks. Then, DNA coding technology along with Genetic procedure and RSA procedure are used to encode the coefficients of voice samples of the first, second and third blocks consecutively once applying DCT into every block. The consequences of experiments show that the presented system attains good consequences for both encryption and decryption and it has the ability to resist numerous cryptographic attacks efficiently. A study conducted by H. Kakaei et al. [9] presented a new technique for speech cryptography depended on an advanced encrypting system, a DNA encoding technique, and a permutation method. The suggested system utilizes mixture of these three diverse methods to use in construction of the technique to rise the difficulty of the system containing an advanced encrypting, encryption and a permutation method of DNA. In order to estimate the dependability of the suggested system. The results prove applicability of the proposed system in safe and fast encoded of voice data

3. Problem Statement

There are a number of risks associated with VoIP network. Different threats and vulnerabilities are classified in attack categories. For the sake of keeping security or privacy, it is a high importance protecting those voice data over the digital communications with secure and fast crypto-systems prior to the transmissions or distributions.

4. RC4 algorithm

RC4 can be defined as one of the Stream Cipher Encryption Algorithm developed via Ron River [10]. RC4 verifies its effectiveness in software, hardware and speed. It is particularly straightforward and fast compared to other encryption algorithms. Furthermore, RC4 no longer offers broad security, also it might be producing weak stream key due to the user-defined weak key, yet it is still utilized in many applications due to the fact that it is used easily in addition to its rapidity in decryption and encryption. This algorithm majorly includes 2 stages: Key Scheduling Algorithm (KSA) to produce, from the key, an initial permutation of the S array in addition to Pseudo-Random Generation

Algorithm (PRGA) for creating keystream. A secret key k (seed) is selected via the algorithm, also an array S which is referred to as S-box containing N (N=2n) elements (typically N=256, n=8). With regard to KSA, and S-box will be filled from (0 - N-l), and will be thrown in confusion via secret k, while in the PRGA, a pointer i exists. It will be calculating another pointer j (j=j+S[i]) that is considered to be secret similar to element S[i] which is also secret. There are 2 elements in the S-box that were swapped via pointers i as well as j. Then, another secret pointer will be estimated, while the secret pseudo-random word will be exported. For the purpose of separating the S-box states in various loops, the states SO, S1, S2 ... St-l, St, St+1 will be specified. Figure 2 shows the RC4 flowchart [11] [12].

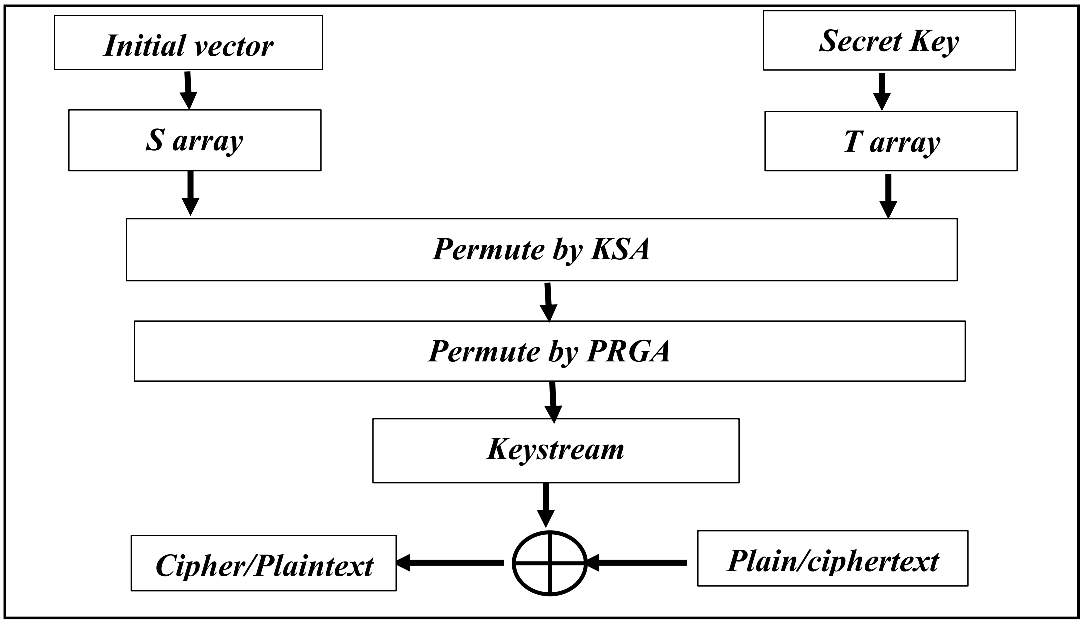

Figure 2: Encryption / Decryption by RC4 [13]

From the RC4 description, it is indicated that its security is based on the security related to internal states of S-box and the security of the secret key. Thus, a lot of attacks focused to resume the secret key regarding S-box internal states [14].

5. Advanced Encryption Standard (AES)

AES, which has been known as well by the original name Rijndael, is one of the specifications for encrypting the electronic data which has been established in 2001by US National Institute of Standards and Technology (NIST). It was extensively analyzed and has been utilized now worldwide for protecting the classified information up to TOP SECRET level, which is the level of the maximum security and characterized as the information that would result in causing "exceptionally grave damages" to the national security in the case of being disclosed publicly. The AES supports 128 bit, 192 bit and 256 bit key sizes and serves as substitute for DES that has a 56 bit key size. Besides the increase in the security, coming with larger sizes of the keys, AES has a higher speed of data encryption compared to the 3DES, a DES enhancement which is utilized essentially for encrypting a document or a message 3 times [15]. AES includes 4 stages, making up a round that is iterated 10 times for a key which is 128-bits long, 12 times for a 192-bit key, and 14 times for a 256-bit key. It is a sufficient approach. It is usually unlikely to crack this algorithm [16].

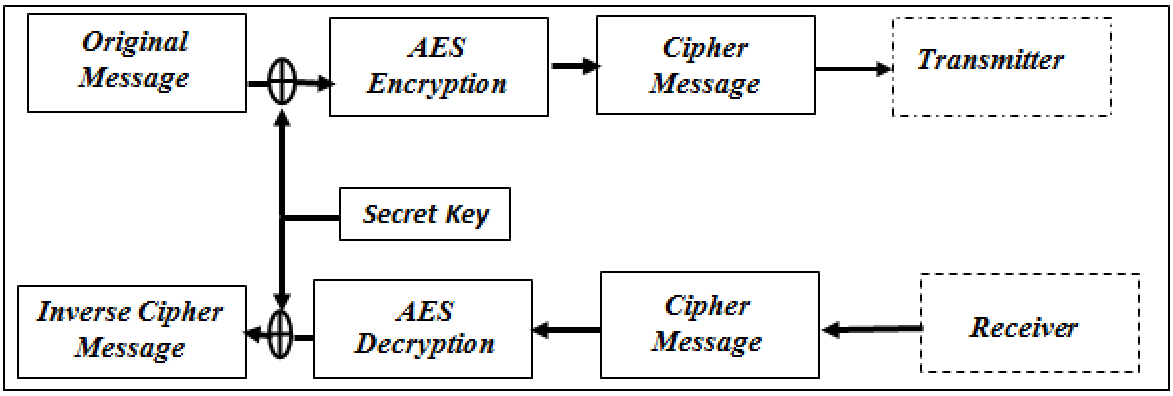

Figure 3: Encryption / Decryption by AES [16]

6. The Proposed system

With regard to the presented work, a new system is proposed to generate a specific key to obtain a more secure RC4 algorithm, the key generated using biometric merits in face image which has been selected as the template biometrics. The Proposal is composed of three phases, and they are:

I. Key-Generation Phase: (Offline Phase)

More than one stage is applied to generate the key in offline phase which is used for encryption/decryption process; Figure 4 illustrate the main block of this phase. These stages are sequentially described with its functionality as following:

1. Face Image Pre-processing Stage:

The pre-processing is a set of the operations which are utilized for the visual enhancement of the input image and reduction of the significant data to make it ready for the following stage. Initially face images input from the MUCT Face dataset [17], the dataset consists of 240 images of 20 individuals (12 images per person), these images are passing through pre-processing phases as illustrate in figure 4, which includes the following steps:

A. Grayscale Image Step: In this stage, color schemes are not needed for processing. Thus, there will be a need for conversion into gray-scale. The conversion allows decreasing the space utilized to record the data in the image; actually, for representing the various color's levels, 24-bits are needed by the color pixels, at the same time, in grayscale just 8-bits are required for each of the pixels as just 256 gray levels existing.

B. Contrast Enhancement Step: The contrast of grayscale images is enhanced with the use of the cumulative histogram equalization approach, the method will raise the global contrast of the image, particularly in the case when the image's data is specified via close contrast values. By using this adjustment, the intensities might be dispersed with more efficiency on the histogram. In addition, this allows offering high-contrast to low local contrast areas.

C. Face Detection Step: is the method of extracting foreground area from image's background, since the foreground includes the most characteristic features, this step would decrease the size of the image and simplify the extraction of features. The technique that is used in this paper for detecting the facial images ROI is the Viola-Jones method. The major 4 steps of the algorithm are in the following way:

1) Haar Features: The simple rectangular features, referred to as the Haar features, the digital image feature is utilized for detecting facial expressions, pedestrians, human faces, and objects. In addition, all the human faces have comparable features such as the nose's bridge, eyes, and mouth, the features are put to comparison with the use of Haar feature and majorly utilized to detect faces.
2) Integral Image: The concept of the integral image with regard to fast feature detection. Also, the rectangle features might be rapidly estimated with the use of an image's intermediary representation that is referred to as an integral image, while the integral

image is computing a pixel value in a rapid and efficient approach at each of the pixels (x, y).

3) AdaBoost: this can be defined as one of the machine-learning algorithms selecting a small number of weak classifiers, each of them is allocated with a single Haar like feature, also combining them for creating a strong classifier.

4) Cascading Classifiers: The approach used to merge the classifiers that quickly castoff the background window, thus more computation might be achieved on the face-like regions. It might be maintaining the low false-positive rate and high detection rate.

D. Face Cropping Step: In such a phase, in the case when detecting the human face via the Viola-Jones algorithm, an image will be cropped face area.

E. Image Resize Step: In this phase, the images are created from the previous phase as well as resized and decrease to a small size of 70×70 pixels with the use of a bilinear interpolation approach. With regard to bilinear interpolation, the value related to the sub-pixel will be interpolated from the 4 nearest neighbors in a linear way. In addition, the horizontal fractional component (related to sub-pixel coordinate) will be utilized for computing 2 interpolated points that lie on the horizontal grid, after that the vertical fractional component will be applied for interpolating between 2 points.

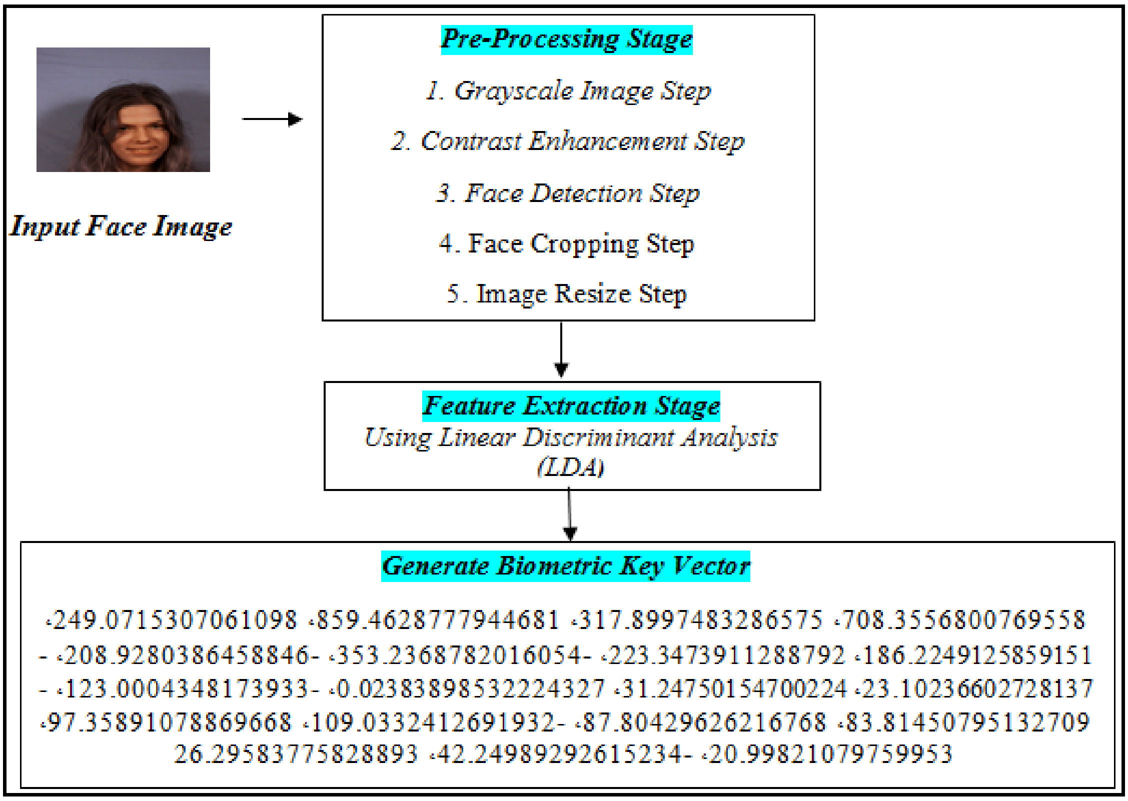

Figure 4: Block Diagram Illustrates Stages of Biometric Key Generation

2. Feature Extraction Stage:

Raw data, which is captured by sensors undergo processing for the extraction of the properties for every feature distinguishing the trait of every individual from the others. Initially, raw data require some steps of the pre-processing for the purpose of helping the increase in the feature extraction such as the gray-scale, histogram equalization or some morphological operations. Following the pre-processing of features, they have been represented in digital form, known as the template. In the suggested, model face has been utilized as the traits. Which is why, the feature extraction for this biometrical trait will be explained. In this paper, one method which is Linear Discriminations Analysis (LDA) is used, the following section explain the details of this method.

- Linear Discriminant Analysis (LDA)

The LDA is the generalization which is associated with fisher's linear discriminant, a method which has been applied in the statistics, pattern recognition and machine learning for obtaining the linear combinations that are associated with features that separate or characterize a minimum of 2 event or object classes. The aim this method is projecting the original matrix of the data to a lower dimensional space. For the purpose of achieving that aim, 3 steps are required to be carried out.

The 1^{st} step is the calculation of separability between various classes (in other words, the distance between the different class means), referred to as between-class variance or between-class matrix through the use of following equations:

$$\mu j = \frac{1}{n_j} \sum_{x_i \in w_j} x_i \qquad (1)$$

Where μ: represents the every class's mean, nj represents the number of the samples in every one of the classes, xi each sample.

$$\mu = \frac{1}{N} \sum_{i=1}^{N} x_i = \sum_{i=1}^{c} \frac{n_i}{N} \mu i \qquad (2)$$

Where is the total or global mean of all classes, N: Total number of samples in database.

$$S_B = \sum_i^c n_{i(\mu_i - \mu)(\mu - \mu_i)^T} \qquad (3)$$

WhereS_B: is represents the between-class variance, c: is the total number of classes

The 2^{nd} step is the calculation o distance between the mean and the samples of every one of the classes, referred to as within-class variance for the achievement of such goal, by using those Equations.

$$S_W = \sum_{j=1}^{c} \sum_{t=1}^{n_j} (x_{ij} - \mu_j)(x_{ij} - \mu_j)^t \qquad (4)$$

WhereS_W: stands for within-class variance ، x_{ij}: stands for every sample in $j - th$ class.

The 3rd step is the construction of lower dimensional space, maximizing between-class variance and minimizing within-class variances as following:

$$W = S_W^{-1} S_B \qquad (5)$$

Where W: stands for transformation matrix.

$$Y = XV_k \qquad (6)$$

Where: Y stands for projection of original data, V stands for Eigen vectors of W, k: represents the lower dimensional space's dimension (V_k) .

The output is feature vectors include two hundred and forty vectors for all images of classes. It has two uses: at the encryption phase (in sender side), it is used as the secret key of the RC4 algorithm. The second use is at decryption phase (in receiver side), it is used as LDA feature of the legitimate receiver (identity database) who is authorized to decrypt the voice after comparing it with the decrypted key.

II. Encryption Phase:

Encryption can be defined as an approach used to transform the original voice into some other format (cipher voice). As illustrated in Figure 5.A at Sender Side:

1) Reading input digital voice .The input file that used in this phase is off-line voice signal obtained from a recorded wave file. Voice data consist of great number of bits which contain both negative and positive bit values, these data serve as input to the proposed system.
2) Use the 256 bits of key previously generated by using LDA from face images as in figure 4 as a secret key of RC4 algorithm which is illustrated in Figure 2, this step increases the complexity of the keystream generation by RC4.
3) The output from the RC4 algorithm is added XOR to the 256 bits block of voice data.
4) In this paper, a random key is generated, even though it's highly impractical breaking the keys based biometric, attackers have a good possibility to steal by the cryptographic attacks . An effectual solution with adding security is the encryption of cryptographic key vector with the use of the AES. Which is why, in the present study, the AES steps have been utilized for the encryption of key vector by consider it as block columns before transmitting it with the encrypted voice data packet over internet protocol .

III. Decryption Phase:

Decryption is applied to transform the encrypted data packets into the original voice. As illustrated in Figure 5.B: at Receiver Side:

1) At the receiver, the encrypted key will decrypt using AES and matches the result with the identity database, which have LDA feature of the legitimate receiver to ensure the identity of the receiver (verification mode).
2) If the decrypted key is known then using it to decrypt the encrypted voice data packets using the RC4 algorithm.
3) Else if this key does not match it will be rejected.

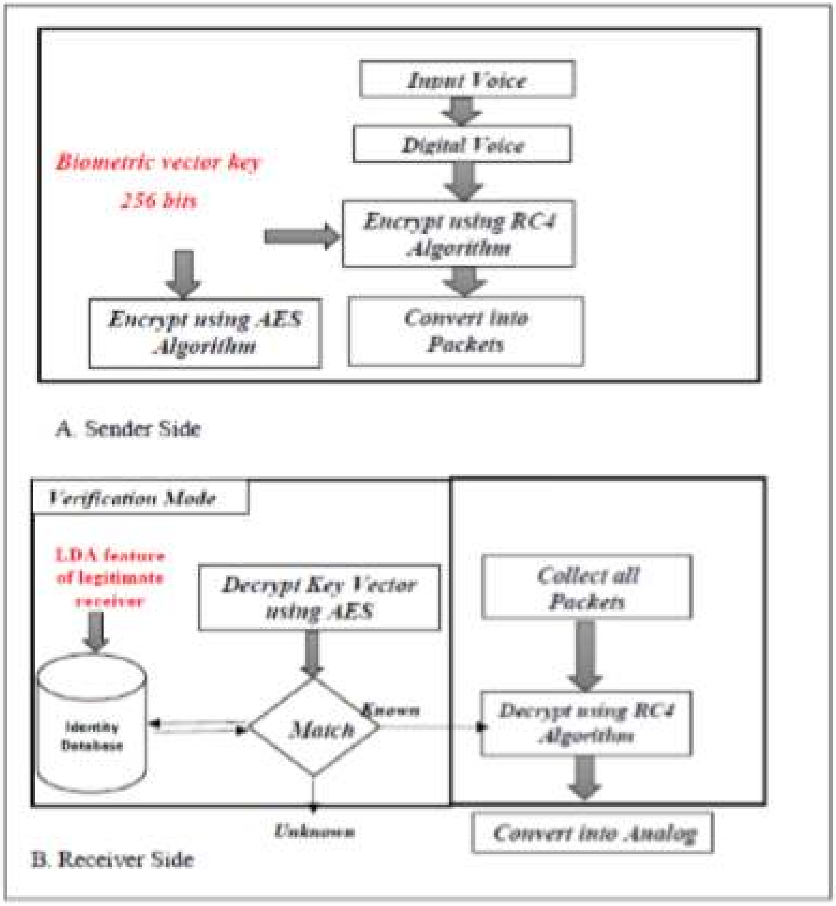

Figure 5: A: Illustrate VoIP Encryption at Sender Side. B: Illustrate VoIP Decryption at Receiver Side

7. 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 feature vector generated based face image have nineteen feature value as illustrated in figure 4 each of them have size $\approx 2^{7}$ so the key size of one key vector $\approx 2^{7} \times 19$ (2.432).

In our proposed system 2^{8} bits from generated random key used as secret key for RC4 algorithm. So, the key space of the proposed algorithm is 2^{256}.

8. Random Key Analysis

The statistical randomness tests by NIST was applied for 2 samples of key vectors generated based face image, there are five tests (Basic five Statistical Tests) which have been chosen to examine keys that are suitable to test the key depend on keys size. The basic five statistical tests (Frequency, Frequency within block, Run test, Discrete Fourier Transform, and Serial test). And all tests are passed successful by 100% as illustrated in Table I.

TABLE I: NIST Test Suite of the Proposed Key Generation based Face Image

Test. No.	Test Name	Result of Sample 1 (250 bit)	Result of Sample 2 (512 bit)
1	Frequency	SUCCESS	SUCCESS
2	Block Frequency	SUCCESS	SUCCESS
3	Runs	SUCCESS	SUCCESS
4	Discrete Fourier Transform	SUCCESS	SUCCESS
5	Serial	SUCCESS	SUCCESS

9. Encryption Quality

In the presented section, the quality related to the suggested encryption system is shown, such quality is on the basis of biometric-based key generation as well as light stream cipher algorithm. With regard to the encryption experimentations, 5-wave voice files are applied with various sizes. Figure 6 is showing a waveform related to original, decryption, and encryption voice signals. Also, in figure 6, the encrypted speech was distributed uniformly as well as unintelligible. It is distinctive from the original voice's waveform. Also, the waveform related to decryption voice has been identical to the original voice waveform.

1) Mean Square Error (MSE):

MSE is a frequently calculate variance between two samples speech and it shows the measurement of the error with an estimate to the center of the mean of the value of speech samples, MSE is defined in equation (7). At most, it has already been used to evaluate the error that has happened due to the encryption and decryption process in the recovered speech data

$$MSE = \frac{1}{N}\sum_{i=0}^{N-1}(\hat{O}i - O\,i)^2 \qquad \textbf{(7)}$$

Where O represents the samples of the voice file, Ô represents the samples of encrypted or decrypted voice samples, and N represents the length of voice samples. When MSE equal to zero or near to zero it shows that the decryption process has a perfect decryption operation to recover the original voice samples. Table 2 shows the MSE measures of the tested decryption speech file.

2) Peak Signal-to-Noise Ratio (PSNR):

This is considered as the ratio between maximum possible powers related to signal as well as the power regarding the corrupting noise created from the encryption/decryption process. It is simply calculated by MSE, PSNR is defined in equation (8):

$$\mathrm{PSNR}_{\mathrm{db}} = 10\log(\frac{(MAX)^2}{MSE}) \qquad (8)$$

MSE indicates the Mean Square Error as well as MAX to the maximum possible value of the audio sample, which is equal to 65,535. A lower PSNR shows that decrees remaining intelligibility of voice signal, and a higher PSNR indicates to increase retuned voice signal. In the specific case, when the MSE is zero that means the original and returned voice signal is equal, In this case, the PSNR becomes infinite. Table 2 shows the PSNR measures of the tested decryption voice file.

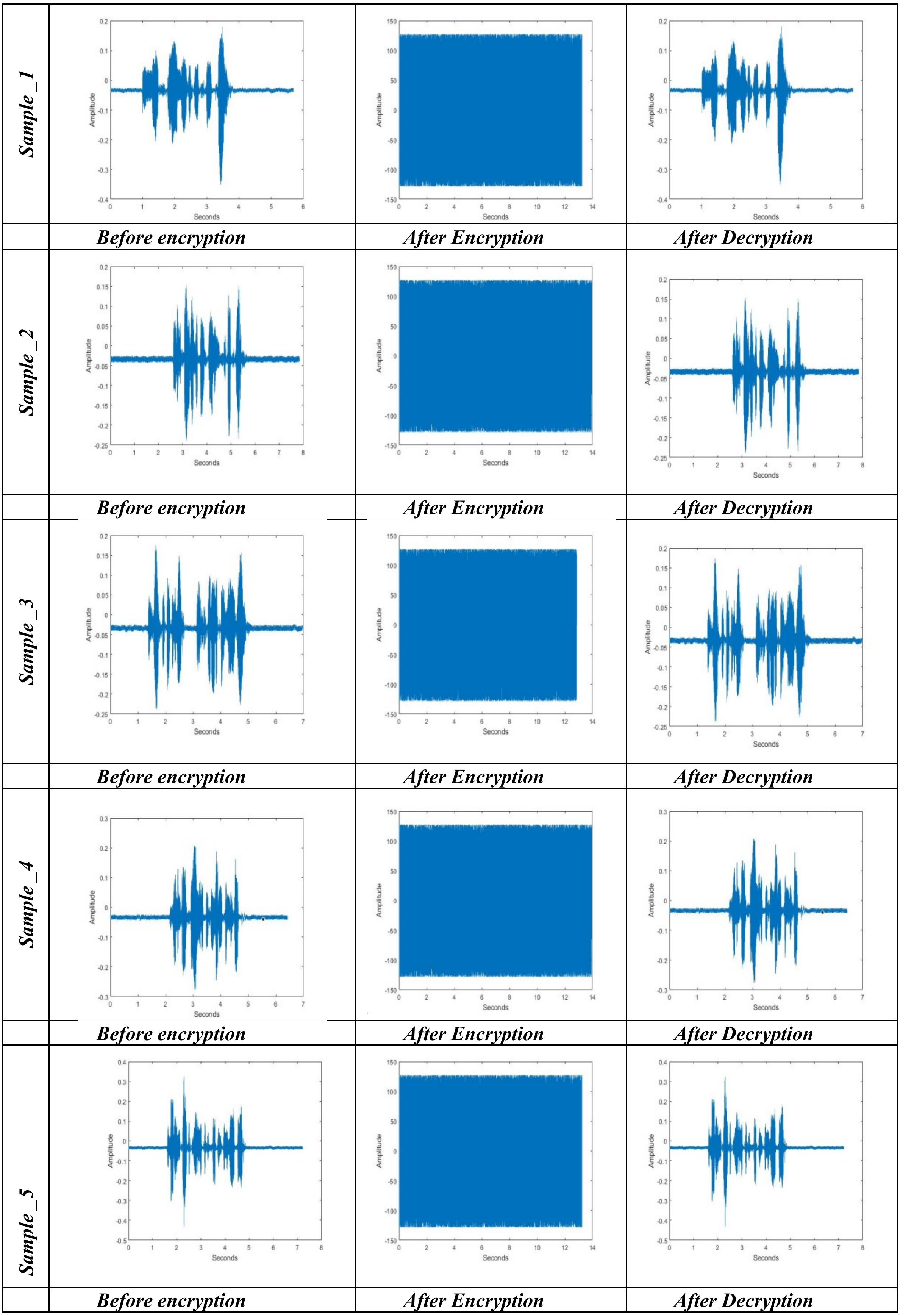

Figure 6: Shows a Waveform of an Original, Encryption and Decryption Voice Signals

10. Time Analysis

Another significant aspect with regard to an excellent algorithm of encryption is the algorithm's execution speed. The algorithm's speed performance might be impacted via many variables, containing the compiler utilized as well as the programming level. The encryption and decryption times are fast for five different voice samples of different sizes. By implementing AES with 256-bit long key size instead of the RC4 algorithm in the proposed system. One can see that the time required for computations based RC4 is faster than AES. Thus the proposed system is appropriate used for real time systems. Table II includes the time related to the decryption and encryption process regarding the Encryption VoIP based on Generated Biometric Key for RC4 Algorithm and Encryption VoIP based on Generated Biometric Key for AES Algorithm. Also, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) between original and decrypted signals and tabulated in Table II.

TABLE II: Comparison of Encryption Time between Proposed System Method & AES based biometric key, Add to MSE & PSNR Measures of The Tested Decryption Voice File of Our System

		Time analysis for Encryption and Decryption					
Voice File	**Size in kilobytes**	***Encryption VoIP based on Generated Biometric Key for RC4 Algorithm***		***Encryption VoIP based on Generated Biometric Key for AES Algorithm***		**MSE of decrypted Speech of Proposal**	**PSNR of Decrypted Speech of Proposal**
		Encryption	***Decryption***	***Encryption***	***Decryption***		
Sample1	178 KB	0.015 Sec	0.02 Sec	0.032 Sec	0.023 Sec	0	Infinity
Sample2	525 KB	0.031 Sec	0.015 Sec	0.056 Sec	0.023 Sec	0	Infinity
Sample3	622 KB	0.032 Sec	0.015 Sec	0.064 Sec	0.024 Sec	0	Infinity
Sample4	910KB	0.040 Sec	0.020 Sec	0.072 Sec	0.035 Sec	0	Infinity
Sample5	12500KB	0.169 Sec	0.168Sec	0.174 Sec	0.170 Sec	0	Infinity

11. COMPARISON OF PERFORMANCE METRICS WITH RELATED WORK

In this section, the proposal is compared with other works, first comparison depends on key space, the second depends on MSE and PSNR, and the third depends on consumed timed through encryption process, Table III, Table IV and Table V show these comparisons.

As it shown in Table III, the proposal the key space size of the proposal is 2^{256} , while in [6] is 2^{238} , and in [7] is 2^{319}. It's obvious from Table III that key space of proposal is better than [6] and less than [7].

Also the proposal is compared with [7] and [8] regarding to the MSE and PSNR values between original and decrypted signal, Table IV shows average of MSE equal to 0, and average PSNR value of the proposal , which indicates the perfect retuned of voice signal.

Finally, the proposal is compared with [7]and by estimating time of encryption for 12500KB voice data , it's obvious from Table V that time of proposal is better than time obtained by [7]. Then compared with [9] also according to time of encryption while [9] takes approximately between 0.4 and 0.9 to encrypt data file of 1 KB. It's obvious from Table V that time of proposal is better than time obtained by [9].

TABLE III: Comparison of Key Space between the Proposal and other Related Work

	Key Space
The Proposed algorithm	2^{256}
[6]	2^{238}
[7]	2^{319}

TABLE IV:Comparison of MSE and PSNR between the Proposal and other Related Work

	Average of MSE of decrypted signal	**Average of PSNR of decrypted signal**
The Proposed algorithm	0	infinity
[7]	0	infinity
[8]	—	284.5251

TABLE V: Comparison of Time encryption between the Proposal and other Related Work

File size in kilobytes	Time encryption of proposal	Time encryption of [7]	Time encryption of [9]
12500KB	0.169 Sec	5.000 Sec	1630.85Sec

12. Conclusion

As there is more necessity for transmission of high-security over un-secured channels, integrating the biometrics along with the cryptosystems is considered as a secure channel to pass confidential data. The main objective of this research is to encrypt and decrypt VoIP using stream cipher and while the strength of any stream cipher method depends on the strength of the key, so in this work propose an approach to generate cryptographic key using face image biometric by employ LDA for extracting the features of face image. The generated keys are tested by using the NIST statistical tests the result showed the success of all five basic tests, as shown in tables 1.In addition key space of generated key is large enough to resist all kinds attacks. The waveform of encryption voice file is different totally from the waveform of original voice file. also the experimental results are showing that the waveform of the decryption voice is identical to the original voice waveform as illustrated in Figure 6 In addition, the experimental work shows that the proposed system offers secrecy to speech data with voice cipher is unintelligible and the recovered voice has perfect quality with MSR equal to zero and PSNR equal to infinity.

References

[1] M. Ibrahem & H. Kassim, “VoIP Speech Encryption System Using Stream Cipher with Chaotic Key Generator”, Journal of Fundamental and Applied sciences, 2018.

[2] S. Bhuvaneshwari &. P. Arul," Generating a Biometric Iris Key for VoIP Security, International Journal of Electronics Communication and Computer Engineering, 2016.

[3] S. Anwarul & S. Dahiya, “A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy”, Proceedings of ICRIC, 2020.

[4] M. Abdullah & Z. Khaleefah” Design a Hybrid Cryptosystem Based Chaos and Sharing for Digital Audio”, Iraqi Journal of Computers, Communication and Control & System Engineering (IJCCCE), 2017

[5] M. Singh & N. Sharma," A Proposed Security Framework for VoIP", International Journal of Computer Science and Mobile Computing, 2015.

[6] E.Hato & D.Shihab," Lorenz and Rossler Chaotic System for Speech Signal Encryption ", International Journal of Computer Applications, 2015

[7] E. Albahrani," A New Audio Encryption Algorithm Based on Chaotic Block Cipher", Annual Conference on New Trends in Information & Communications Technology Applications, 2017.

[8] S. Yousif, "A new speech cryptosystem using DNA encoding, genetic and RSA algorithms", International Journal of Engineering & Technology, 2018.

[9] H. Kakaei & et al," A Novel Fast and Secure Approach for Voice Encryption Based on DNA Computing ", 3DR EXPRESS, 2018.

[10] Z. Hussein& A. Rahma," Modified the RC4 Stream Cipher Algorithm Based on Irreducible Polynomial ", Eng. &Tech.Journal, 2015.

[11] J. Saadoon & I. Mohammed," ARSMS: A Hybrid Secured SMS Protocol for Smart Home using AES and RC4 ", International Journal of Computer Science and Network Security, 2018.

[12] S. Hameed, I. Mahmood," A Modified Key Scheduling Algorithm for RC4 “, Iraqi Journal of Science, 2016.

[13] A. Aboshosha & et al," EA Based Dynamic Key Generation in RC4 Ciphering Applied to CMS", International Journal of Network Security, 2015.

[14] M. Abd Zaid & S. Hassan," Lightweight RC4 Algorithm ", Journal of AL-Qadisiyah for computer science and mathematics, 2019.

[15] P.Arul & .A.Shanmugam," GENERATE A KEY FOR AES USING BIOMETRIC FOR VOIP NETWORK SECURITY, Journal of Theoretical & Applied Information Technology, 2009.

[16] A. Agarwal & et al" Secured Audio Encryption using AES Algorithm “, International Journal of Computer Applications, 2019.

[17] MUCT Face images dataset, Available on URL: http://www.milbo.org/muct/.