Received: November 23, 2020. Revised: February 15, 2021.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Transceiver Based on Independent Component Analysis (ICA) Algorithm

Dheyaa T. Al-Zuhairi[1]* **Abbas Salman Hameed[1]** **Isam Salah Hameed[1]**

[1]*College of Engineering, University of Diyala, Diyala, Iraq*
* Corresponding author's Email: dtaqq3@mail.missouri.edu

Abstract: In this paper, a system for the purpose of signals encryption using the technique of independent component analysis has been proposed. The proposed system mixes the original signal with arbitrary number of random signals in order to obtain a highly encrypted signal like noise. The number of random signals is indicated by an attached key signal preceding the encrypted signal. In order to increase the encryption strength, the number of random signals is changed at each signal transmission. An independent component analysis technique is utilized to separate signals and select the original signal by a designed selector. A set of parameters has been adopted to measure the encryption quality and decryption capability. Promising encryption results represented by up to - 48.35 dB for segmental spectral signal to noise ratio and 0.00037 correlation coefficient between the original and the encrypted signals are obtained. As well, an efficient signal decryption is achieved with 45.85 dB signal to noise ratio and nearly 1 correlation coefficient value between the original and reconstructed signals. In conclusion, the proposed system is a good candidate to be adopted in developing highly reliable security transceiver systems.

Keywords: Independent component analysis, Secure communication, Encryption, Blind source separation.

1. Introduction

Speech and voice communications under secured circumstances is too important due to the wide using of such communications, which are even more vulnerable. Thus, lifting information to a high level of security has become dramatically increasing demand [1]. Two main issues represented by privacy and security are very important to put concern about in most of communication systems. Therefore, cryptography comes to take the main role in safeguarding both of privacy and security concerns. By cryptography, transmitting information is done through masking data in a way that would make it hard to be accessed and only an approved receiver side is authorized to interpret encrypted signals [2].

Many techniques have been utilized for signals encryption. One of these techniques is chaotic cryptosystems. The chaotic systems produce a unique and randomness signals which are widely used as a key in the encryption algorithms [3]. This paragraph states most of the recent researches that used chaotic signal for speech encryption. Sathiyamurthi introduced a technique for speech signals encryption in which multi-level of speech samples shuffling based on five chaotic maps to increase security level [3]. Gathering more than one chaotic map leads to more robustness against encryption breaking attempts. The cryptosystem in [4] was built based on data scrambling in frequency domain. This scheme applied Discrete Cosine Transform (DCT) to obtain the frequency domain of speech segments. Then, the scheme added a random signal generated using Delay Ellipse Reflecting Cavity Map System (DE-RCM) to the DCT coefficients. The security level was improved by applying time scrambling depending on DE-RCM chaotic signal. However, applying amplitude and time scrambling in frequency domain then implementing inverse DCT on the generated coefficients lead to reduce the quality of reconstructed signal. In [5], Jawad presented a secured speech communication technique based on two stages by firstly scrambling the signal then masking it by chaotic maps in order to make key space large enough to increase security. However, the receiver cannot break the encryption without having the specific keys which were used to generate chaotic signals in the transmitter side to guarantee full transmitter - receiver synchronization. Kordov poposed another audio encryption technique [6]. This technique applies chaotic circle map and rotation equations composed with a chaotic bit-level permutations and substitutions for audio files encryption. In [7], Al-Hazaimeh applied a dynamic encryption algorithm on speech signals. In his technique, a 128-bit hash value was used to generate a dynamic key, then the encryption and decryption procedure was done using Lorenz chaotic map. Utilizing a dynamic key with Lorenz map intended to increase the security level. To secure speech samples against different eavesdropper attacks, Farsana, in [8], developed an encryption based on hyperchaotic system in quantum states. Bit-flip operation was used to encrypt rotated speech sample bits according to Controlled- Not gate accompanied by Hadamard transform depending on a Lü hyperchaotic generated key. Abdullah built a speech encryption method using Duffing map [9]. Upon the encryption side the original speech signal was masked by the chaotic signal. A slave chaotic map at the receiver side was used to achieve the synchronization process which leads to reconstruct the original signal. In [10], Zhao generated an encrypted speech by mixing the original audio signal with two key signals. Pseudo-random number generator was used to prepare the first key signal, while the second key signal was generated by a chaotic system. The decryption was carried out by assistance of Blind Source Separation technique (BSS).

Blind source means that both of source signals along with the criteria of mixing them is unknown. This makes it a challenging problem in case of the need to have such signals completely separated. Therefore, blind source separation (BSS) has become an important topic that aims to retrieve independent sources without knowing the way of mixing them. In short, Independent Component Analysis (ICA) is a method for facilitating the solution of BSS problem [11, 12].

Blind source separation has been widely exploited in the encryption techniques. In [13], Lin focused on the idea of splitting the original speech signal into frames which are then also divided into sub-frames (segments) from which key signals are derived based on segment length and numbers. Encryption was performed by mixing the signal segments and key signals along with the underdetermined mixing matrix. At the decryption side, information about original segments is necessary to generate key signals. In [14], Yang presented a cryptosystem based on sub-band decomposition independent component analysis (SDICA). The main idea in their work took into account that numerous signals are normally correlated or dependent while their sub bands components are statistically independent. After mutually sub bands signals mixing, the combination was mixed with the ciphers [14]. However, this method is also required to provide information regarding the mixing matrix in order to use it for sub bands components separation by ICA algorithm. Abbas, in [15], considered ICA in another suggested image cryptosystem. Arnold’s Cat Map (ACM) was used to modify the mixing matrix. By mixing both the original images with the generated mixing matrix, image encryption was performed. JADE ICA algorithm was used to decrypt the images. Khalane, in [16], proposed an image encryption algorithm which depends on scrambling various components derived from the original image. ICA as well as Non-Negative Matrix factorization decomposition techniques were used throughout encryption process. The encryption key includes decomposition method, components number, and component arrangement. To decrypt the image, the authorized user must be aware of all the secret keys exploited through encryption operation.

In this paper, an encryption method based on BSS by ICA is presented. The proposed method provides encrypted signal through mixing it with flexible number of random signals which is impeded by a special key. Flexibility of random signals number is intended to obtain a valuable and strong encryption process. The receiver in the proposed system is designed with ICA technique greatly involved in it in order to have the original signal accurately separated and nominated. Unlike the previously proposed cryptosystems, this system does not require providing the receiver with any type of special information about the original mixing matrix. The rest of the paper is organized in three sections. Section 2 presents a full description of the proposed system and its structure, while the performance analysis of the system is discussed in Section 3. The final section summarizes a clear conclusion about the gist of the work.

2. System description and structure

The main aim for which this system is proposed is to achieve a high security for transmitting signals in communication systems. The high security level comes from shuffling the message signal with many unknown random signals at the transmitter side. At the receiver side, ICA technique is employed to efficiently extract the original signal. In this section, the proposed secure communication system parts, which are the transmitter and the receiver sides, are described as follows:

2.1 Transmitter design

Fig. 1 presents a full description of the transmitter side in which a detailed signal processing on the message signal until propagation can be observed. Firstly, M random signals are generated to be mixed later with the message signal. Hence, the total number of input signals is $M+1$. Mathematically, the original signal is denoted as $x(n)$ and the unknown random signals as $f_i(n), i = 1,2, \dots., M$. Index $n = 1,2, \dots, N$ refers to samples of signal of length N. The value of M is not restricted to a certain number. That is to say, the user has the ability to change M value before transmitting each part of data to add more security to the system. A key signal is attached with the transmitted signal to extract M value at the receiver side as illustrated later in this section. The message signal as well as the random signals are arranged in matrix B as follows:

$$B = \begin{bmatrix} x(1) & x(2) & \dots & x(N) \\ f_1(1) & f_1(2) & \dots & f_1(N) \\ \vdots & \vdots & \ddots & \vdots \\ f_M(1) & f_M(2) & \dots & f_M(N) \end{bmatrix} \quad (1)$$

To encrypt the data, matrix B is then multiplied with a random elements encryption matrix (A) of size $((M+1) \times (M+1))$. The result of the matrices multiplication is another matrix given by [17], [18]:

$$U = A\,B \quad (2)$$

Matrix U has $(M+1)$ rows and N columns. The next step is converting the matrix elements to be one vector data via parallel to serial convertor. Finally, a sinusoidal key signal is generated and inserted before the encrypted signal. The key signal is given by $\cos(2\pi CKt)$, where C is a constant and K represents the total number of signals (message signal and random signals $(K = M+1)$). The frequency of the key signal is denoted by F which is equal to $C\ K$. The value of K might be 2, 3,… . Because it not practical to send signals with very low frequencies, such as the values of K, the frequency of the key signal is chosen to be $F = C\ K$. The value of C is set to be 100 in this work, so F could be 100, 200, … . After inserting the key signal, the encrypted signal becomes ready to be transmitted. Each while during the transmitting, the number of the random signals is changed, hence a new key signal with different frequency is required to be inserted.

2.2 Receiver design

The proposed processing steps at the receiver side are shown in details in Fig. 2. First, the receiver antenna captures the transmitted signal which has the key signal in its early samples. The key signal is a single tone sinusoidal signal which stashes the total number of signals $(M+1)$ in its frequency. Fast Fourier Transform (FFT) is calculated for this early part of the received signal to obtain F which is directly divided by C to find the key (K). After getting the frequency of the key signal, phase-locked loop (PLL) is used to estimate the phase differences between the key part in the received signal and the receiver local oscillator. The output signal of the PLL is subtracted from the received signal, and the result signal has zeros at the key signal samples time indices. The key signal removal, shown in Fig. 2, utilizes the zeros in the early part of the PLL signal to cut the key signal part from the received signal. Because a new key signal with different frequency exists after each time period in the received signal, the key signal removal has also to recognize the encrypted data samples from the key signal samples. The key signal removal accomplishes this function by searching for zeros sequences coming to the key signal removal from subtracting the PLL signal from the received signal. Existing of a zeros sequence indicates that a new key signal is present. After the key signal removal step, the result signal is a serial vector data which is equivalent to the encrypted signal in the transmitter.

The next processing step to recover the message signal is ICA algorithm which needs a matrix as an input. As a result, a serial to parallel convertor is used to feed forward a matrix (Y) of $(M+1)$ rows to ICA stage. The following ICA operations are conducted for data separation [19]:

First, the covariance is computed for Y matrix to obtain [19]:

$$Y_C = MCOV(Y) \quad (3)$$

where $MCOV$ is the covariance matrix (see Appendix A) [20]. Then, the whitened data denoted by matrix S is written as [19]:

$$S = V\,\phi^{-0.5}\,\zeta^H\,Y_C \quad (4)$$

In Eq. (4), $\boldsymbol{\phi}$ is a diagonal matrix demonstrating eigenvalues of the matrix $\boldsymbol{Y_C}$, and $\boldsymbol{\zeta}$ is a matrix in which the columns are the corresponding

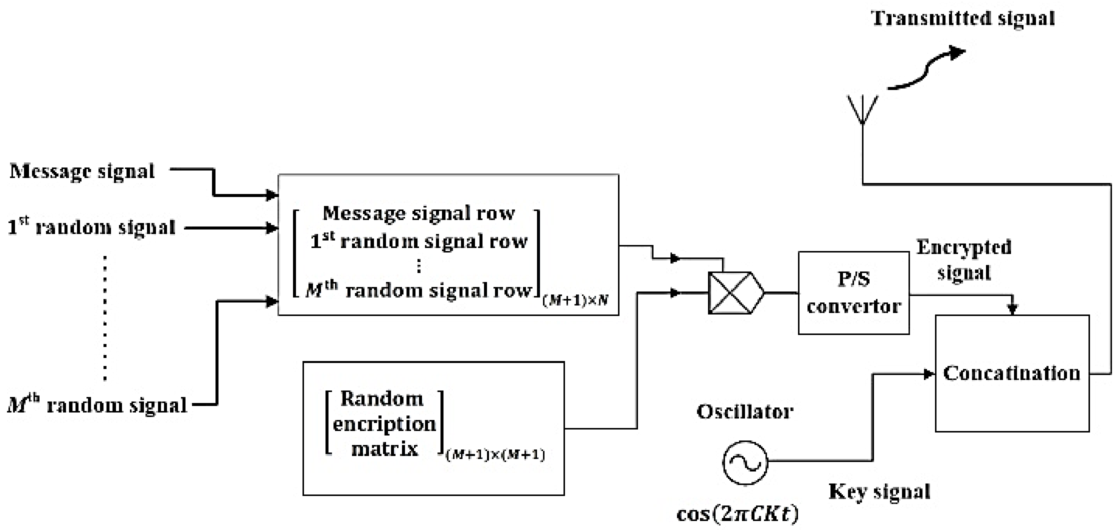

Figure. 1 Transmitter structure of the proposed system

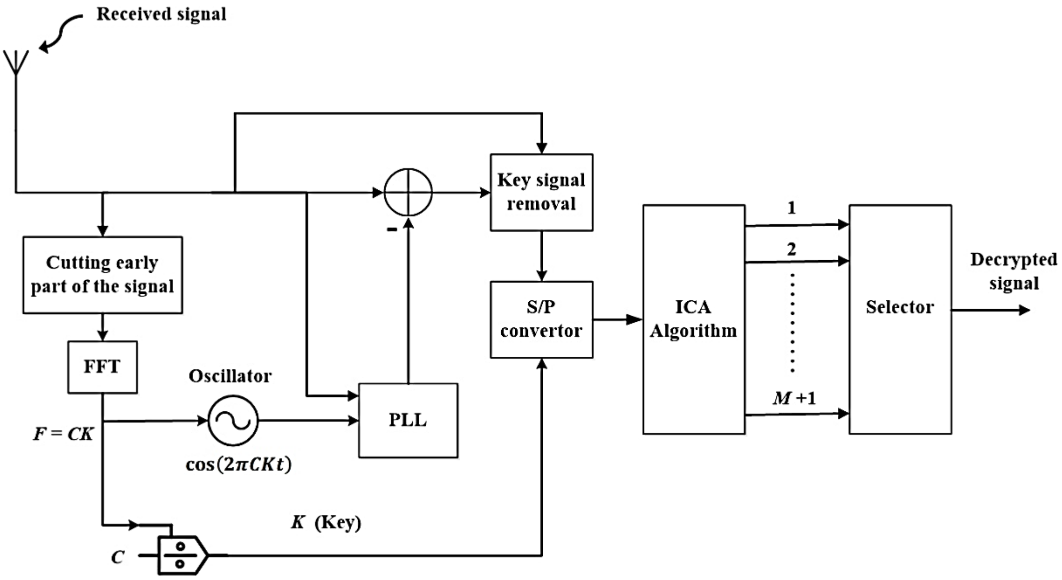

Figure. 2 Receiver structure of the proposed system

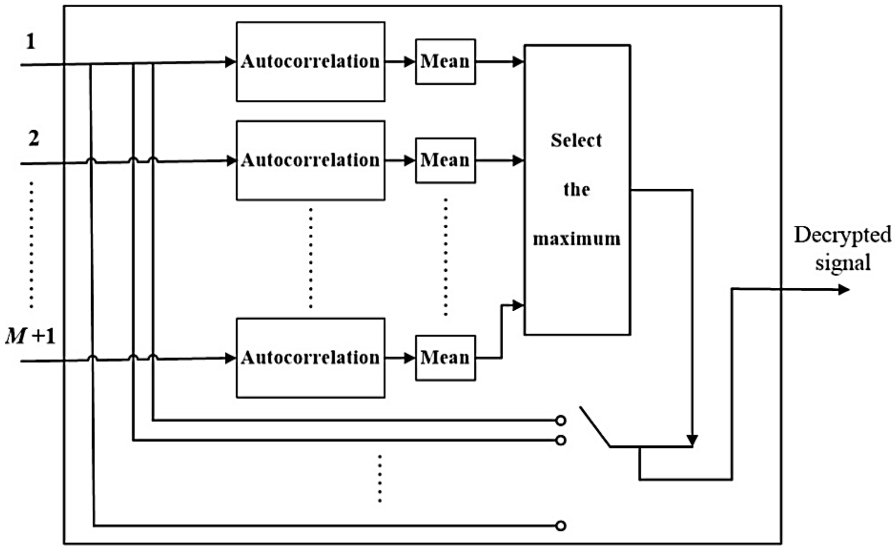

Figure. 3 Selector block diagram

eigenvectors. H denotes complex conjugate transpose.

$$P(n) = \sqrt{\sum_{i=1}^{M+1} \left(S_i(n)\right)^2} \quad (5)$$

$S_i(n)$ represents the n^{th} sample for the i^{th} column of the matrix S.

$$Q_i(n) = \prod_{n=1}^{N} P(n).S_i(n), \;\; i = 1,2,\dots,M+1 \quad (6)$$

$$Z = MCOV(Q) \quad (7)$$

The final step in ICA algorithm is [19]:

$$\tilde{B} = {Z_\lambda}^H \, S \quad (8)$$

where Z_λ is a diagonal matrix representing eigenvalues of the matrix Z.

The matrix $\tilde{B}$ is the output of ICA algorithm, and it is equivalent to matrix B in the transmitter side. However, the $(M+1)$ output vectors of $\tilde{B}$ have a random order that is different from the order in which these signals arranged at the transmitter input. In order to estimate the desired signal and get rid of the other random signals, a selector is proposed as shown in Fig. 3. In fact, auto-correlation of random signals is an impulse signal which has a considered value only at delay of zero sample index, while the regular signals have significant correlation values at most of the delay samples as can be seen in Fig. 4. Hence, the mean of the correlation of the desired signal is usually the highest in the proposed system as considering only one message signal mixed with random signals every time. The proposed selector adopts this idea to select the wanted signal by calculating auto-correlation and mean then choose the maximum which is corresponding to the right order of the decrypted message signal.

3. Performance analysis

In this section, the performance of the proposed system is discussed and analysed. The simulation is conducted using MATLAB. For testing the proposed system efficiency in terms of encryption strength and original signal reconstruction, Signal to Noise Ratio (SNR), Segmental Spectral Signal to Noise Ratio (SSSNR), Peak Signal to Noise Ratio (PSNR), and Correlation coefficient (CC) parameters are used as measurement criteria. Then, the results are compared with other encryption techniques found in [3-5, 7] and [9]. For simulation data, five speech signals were arbitrarily selected from the well-known TIMIT database.

3.1 Parameters definition

The quantitative parameters used to evaluate the statistical performance of the proposed system are defined in this subsection:

3.1.1. SNR

SNR is a vital parameter in evaluating encryption and decryption quality. In the case of encrypted signal, the lower the SNR is, the better its residual intelligibility. On the other hand, a high SNR value refers to a good quality of the decrypted signal [21]. Mathematically, SNR is the ratio between the original speech signal and the difference between it and the decrypted signal. SNR is given by the following equation [21]:

$$\text{SNR} = 10 \log_{10} \frac{\sum_{n=1}^{N} x^2(n)}{\sum_{n=1}^{N} (x(n)-d(n))^2} \quad (9)$$

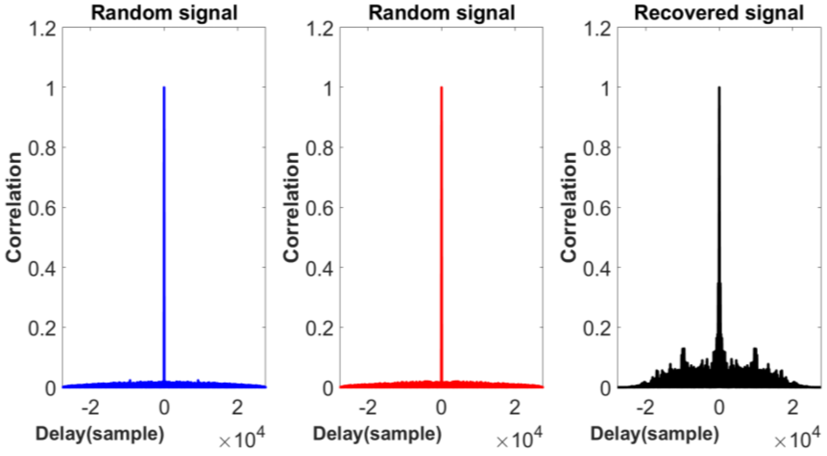

Figure. 4 Auto-correlation of ICA output (two random and one audio signals)

where $x(n)$ is the original speech signal and $d(n)$ is the decrypted speech signal.

3.1.2. SSSNR

SSSNR is an encryption strength indicator parameter which is inversely proportional to the encryption quality; as long as SSSNR is of lower values, encryption strength is of higher level [5].

$$\mathrm{SSSNR} = 10\log_{10}\frac{\sum_{r=1}^{R}|X(r)|}{\sum_{r=1}^{R}[|X(r)|-|D(r)|]} \qquad (10)$$

where $X(r)$ & $D(r\ )$ are the discrete Fourier transform of the original and recovered speech respectively.

3.1.3. PSNR

PSNR is another parameter for signal quality calculation. It takes in consideration original speech signal maximum power component and divides it by the power of residual signal obtained from the difference between the original and the decrypted signals. So, higher PSNR is preferred to ensure a high quality signal decryption. The PSNR is written as [22]:

$$\mathrm{PSNR} = 10\ \log_{10}\frac{N\,[max(|x(n)|)]^2}{\sum_{n=1}^{T_s}(x(n)-d(n))^2} \qquad (11)$$

3.1.4. CC

CC is a well-known parameter that evaluates the correlation between two signals in order to specify their similarity amount. Hence, a CC value of one means that the two signals are identical while CC values close zero refer to a weak relation between the compared signals [21]. The CC is given as follows [4], [21]:

$$\mathrm{CC} = \frac{COV(x,d)}{\sqrt{V(x)V(d)}} \qquad (12)$$

where COV and V, defined below, are the covariance and the variance, respectively.

$$V(x) = \frac{1}{N}\sum_{n=1}^{N}(x(n)-\bar{x})^2 \qquad (13)$$

$$COV(x,d) = \frac{1}{N}\sum_{n=1}^{N}(x(n)-\bar{x})\big(d(n)\ -\bar{d}\big) \qquad (14)$$

where $\bar{x}$ and $\bar{d}$ are the mean of x and d, respectively.

3.2 Simulation results and discussion

For the proposed system simulation, many speech signals are selected to test the encryption solidity. Each time, a speech signal is mixed with three random like-noise signals by different weighting via a random matrix. At the receiver side, the signals are segregated using ICA algorithm, and the original speech signal is selected by the proposed selector.

Graphically, Fig. 5 depicts the results of encryption and decryption process. The original signal and its spectrogram are located in the upper portion of the figure. The center portion of the figure shows the encrypted signal along with its equivalent spectrogram which clearly imply a highly veiled

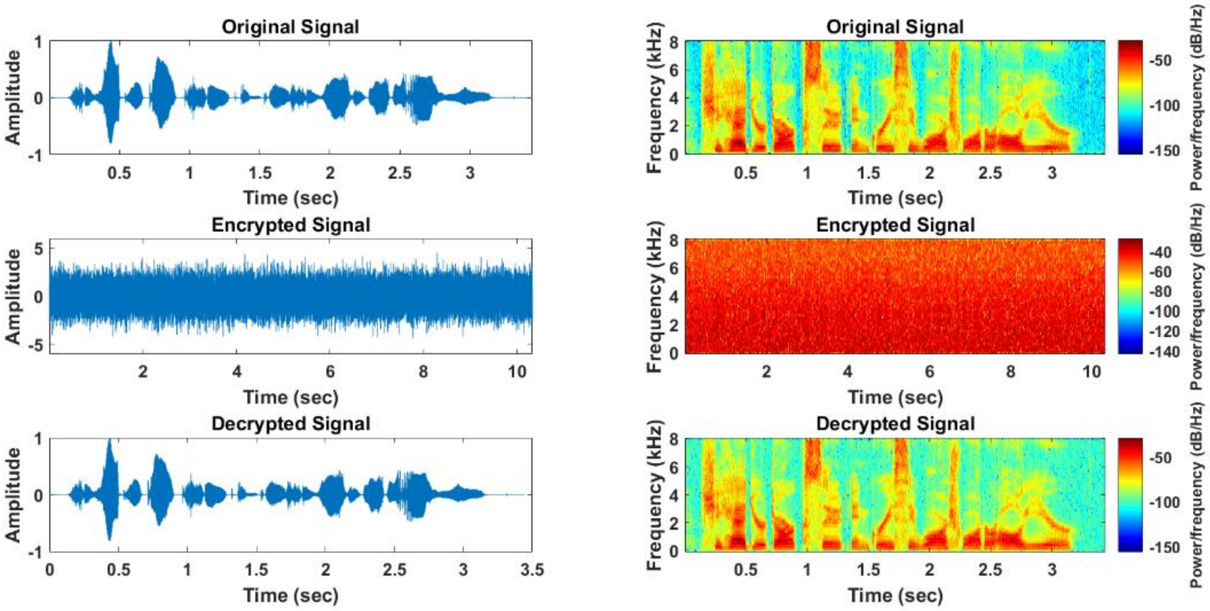

Figure. 5 Illustration of signal encryption and decryption. (Left) Time domain signals, and (Right) Corresponding spectrogram

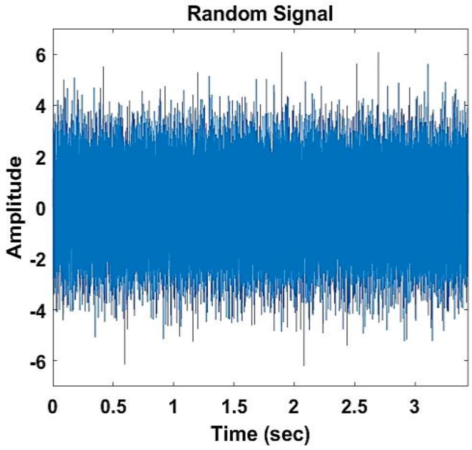

Figure. 6 A sample of random signals used for encryption

signal. As a normal speech signal, the spectrogram of the original signal indicates low frequency components concentration while the encrypted signal components are uniformly distributed over the entire frequency range in its spectrogram. The original signal is successfully reconstructed as can be observed in the bottom portion of Fig. 5. Visually, it seems that the original signal and the decrypted signal have the same waveform and spectrogram. More quantitative measurements regarding the encryption and decryption performance are included later in this section. An example of the random signals used throughout the encryption is shown in Fig. 6.

Fig. 7 demonstrates the absolute value of the correlation between the original and both of the encrypted and decrypted signals. Firstly, the original and encrypted signals correlation verifies the encryption strength as it has no sharp peak value and all the correlation values approach to zero. On the other hand, it can be inferred from the original and the decrypted signals correlation that the original signal is correctly constructed since a peak correlation value equal to one is apparently shown in the figure. Because the message signal is mixed with random signals for encryption purpose, the simulation was conducted 100 times for each message signal and the values shown in the coming tables represent the average results. For a five selected signals, Table 1 shows SNR, SSSNR, and CC results of the encrypted signals. The observed results appear to confirm low levels of SNR, SSSNR and CC parameters. Numerically, the values are ranging from -35.26 to -27.79, - 48.35 to - 42.51, and - 0.00037 to -0.0016 for SNR, SSSNR and CC, respectively. The obtained low-level results of quantitative parameters are due to using the fully random signals and mixing matrix in the encryption process. This kind of encryption leads to a significant divergence between the original and the encrypted signals.

In decryption, it seems clear form Table 2 that the high recorded levels of quantitative parameters are a great evidence of a high-quality decryption. These results range from 41.54 to 45.85, and 60.42 to 67.88 for SNR and PSNR, respectively. These results reflect the high quality of the decrypted signal. Moreover, all the correlation coefficient values approach to one which represents the identification between the original and the reconstructed signals. As a result of the obtained encryption and decryption parameters values mentioned above, the proposed system has a high level of signal encoding and an accurate signal retrieval capability. However, this performance accomplishment does not require information about the encryption manner to be sent from the transmitter to the receiver.

At the receiver side, wrong estimation of the key gives entirely wrong results. To test the sensitivity of the proposed system to the key value estimation, a speech signal is mixed with three random signals at

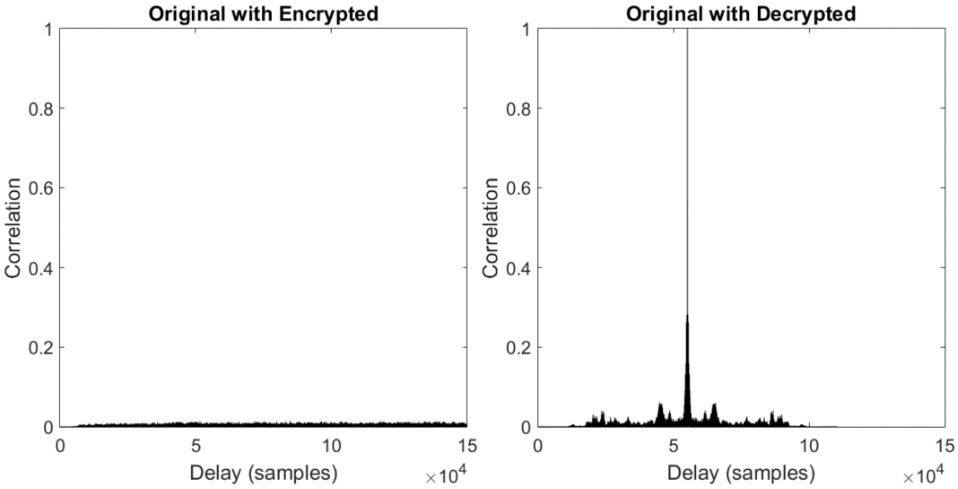

Figure. 7 Correlation of the encrypted and the decrypted signals with the original signal

the transmitter. At the receiver, the key was incorrectly chosen to be less than the correct value by one. Fig. 8 shows the original signal as well as the decrypted signal which seem totally different. The decrypted signal is random and it looks like a noise signal as can be seen from its spectrogram. The cross-correlation between the original and reconstructed signals depicted in Fig. 8 exhibits the mismatch between these signals. Table 3 shows the SNR, and CC values relating to wrong key estimation at the receiver. The low values of the results, represented by (-8.03 ~ - 5.22) dB for SNR and (0.0036 ~ 0.0047) for CC, confirm the observations in Fig. 8 discussed above. The reason why the receiver cannot reconstruct the original signal in case of wrong key estimation is the incorrect signal splitting through the serial to parallel convertor which leads to collapse the mixed signals statistical independence. However, ICA algorithm needs independent mixed signals as an input to successfully separate them.

A performance comparison with other algorithms is listed in Table 4. It is clearly shown that in terms of encryption, the proposed system overcomes the other techniques when SSSNR and CC are taken as encryption quality measurements. Among the previous listed works, SSSNR was found in [5] of about - 20.78 dB, whereas the proposed work recorded a range of (- 48.35 ~ - 42.51) dB. From the same table, the best CC parameter value was obtained in [7] and it was 0.0018. However, the proposed system achieved CC value up to - 0.00037 which indicates how far the divergence between the encrypted and original signals.

Table 1. Dissimilarity measurement between original and encrypted signals

Signal Name	SNR	SSSNR (dB)	CC
SA1	-34.48	- 44.66	0.00068
SI733	-27.79	- 48.25	- 0.0016
SI1088	-33.04	- 48.35	- 0.00037
SX11	-31.55	- 42.51	0.00066
SX319	-35.26	- 46.24	0.00071

Table 2. Similarity measurement between original and decrypted signals

Signal Name	SNR (dB)	PSNR (dB)	CC
SA1	43.86	62.83	1
SI733	45.85	67.88	0.99999
SI1088	45.33	64.59	1
SX11	41.54	61.28	0.9999
SX319	42.26	60.42	0.9999

Table 3. Sensitivity measurements for key estimation

Speech file	SNR (dB)	CC
SA1	- 6.53	0.0039
SI733	- 8.03	0.0036
SI1088	- 6.02	0.0045
SX11	- 6.41	0.0047
SX319	- 5.22	0.0044

Similarly, the proposed system decryption performance represented by SNR and CC in Table 4 is better than the others. For SNR values, the proposed system outperforms other techniques by at

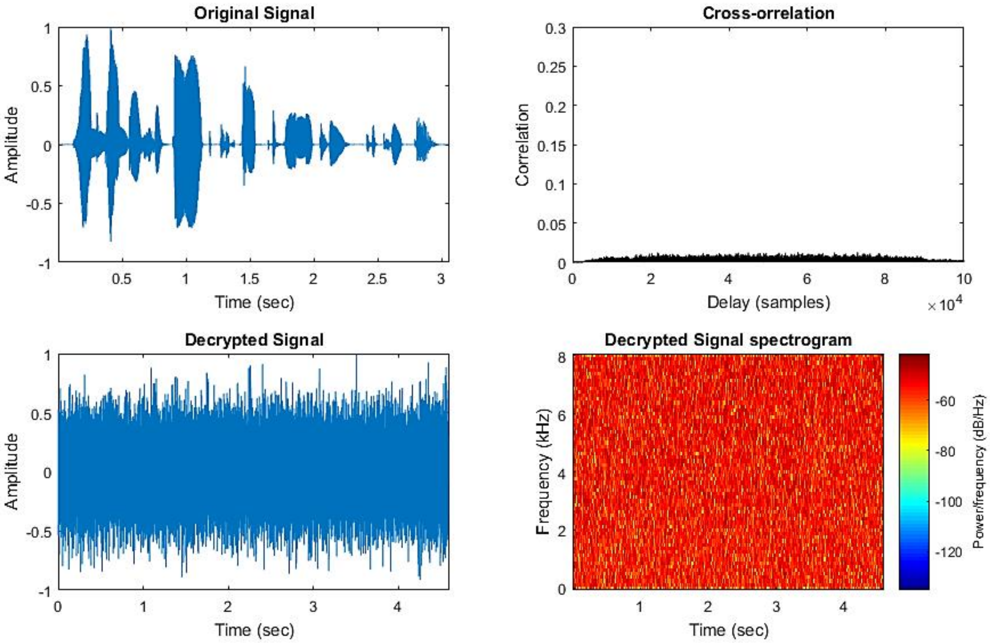

Figure. 8 Signal reconstruction in case of wrong key estimation

Table 4. Performance comparison with other algorithms

Reference	Encrypted		Decrypted		Encryption pre-information
	SSSNR (dB)	CC	SNR (dB)	CC	
[3]	NA	0.0119~ 0.0384	32.57~34.71	0.999~1	Required
[4]	NA	- 0.022	NA	0.986	Required
[5]	- 20.78	NA	NA	1	Required
[7]	NA	0.0018 ~ 0.00064	NA	0.96241~0.99114	Required
[9]	NA	0.04128	30	0.9999	Required
Proposed	- 48.35 ~ - 42.51	- 0.00037 ~ - 0.0016	41.54 ~ 45.85	0.99999~1	Not required

least 7 dB. Regarding the CC parameter, most of the values including ours reached one which refers to the high quality signal reconstruction.

It was noticed that sending key information is of necessary to correctly reconstruct original signals in common cryptosystems. Encryption pre-information are required in the all algorithms mentioned in Table 4 as well as the ICA based cryptosystems in [10,13-16] which need providing criteria of mixing matrix information at their receiver side. However, this work is proceeding above techniques as it does not required sending any information about the mixing matrix.

4. Conclusion

This work proposes a secure transceiver based on independent component analysis. The acoustic and statistical evaluations of the findings have shown reliable observations. Acoustically, audiometry tests show that the encrypted signal includes nothing but noise while retrieved signal at the receiver side is clearly heard. Acoustic test has also been underpinned by the valuable statistical results obtained from measuring important parameters. Numerically, The results have given high encryption quality supported by up to - 48.35 dB for segmental spectral signal to noise ratio and 0.00037 correlation coefficient between the original and the encrypted signals. Additionally, an efficient signal reconstruction at decryption stage is acquired with 45.85 dB signal to noise ratio and almost 1 correlation coefficient. The proposed system is highly sensitive to the number of random signals used in the encryption process. Therefore, decryption side results in signals that are far from the original speech signal when a wrong key is estimated. A correlation value around 0.004 between the original and decrypted signals is obtained by considering two random signals instead of the three signals originally used in the encryption. Finally, the proposed cryptosystem has the merits of simplicity, encryption strength and needless to provide the receiver with information about the encoding mechanism which most cryptosystems require. As a future work, orthogonal chaotic signals can be used as random signals in the encryption. Thereby, the algorithm would lead to more authentic results since signals' independency has already been considered by the orthogonal behavior.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; methodology, Dheyaa T. Al-Zuhairi; software, Abbas Salman Hameed; validation, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; formal analysis, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; investigation, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; resources, Isam Salah Hameed; data curation, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; writing—original draft preparation, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; writing—review and editing, Dheyaa T. Al-Zuhairi, Abbas Salman Hameed, and Isam Salah Hameed; visualization, Dheyaa T. Al-Zuhairi, and Abbas Salman Hameed; supervision, Dheyaa T. Al-Zuhairi; project administration, Abbas Salman Hameed.

References

[1] H. Beker and F. PIPER, *Secure Speech Communications*, Academic, London, U.K. 1985.

[2] J. Fridrich, "Symmetric Ciphers Based On Two-Dimensional Chaotic Maps", *International Journal of Bifurcation and Chaos,* Vol. 8, No. 6, pp. 1259–1284, 1998.

[3] P. Sathiyamurthi and S. Ramakrishnan, "Speech Encryption Using Chaotic Shift Keying for Secured Speech Communication", *EURASIP Journal on Audio, Speech, and Music Processing*, Vol. 1, No. 20, pp. 1-11, 2017.

[4] Z. Habib, J. Khan, J. Ahmad, M. Khan, and F. Khan, "Secure Speech Communication

Algorithm Via DCT and TD-ERCS Chaotic Map", In: *Proc. of 4th International Conf. on Electrical and Electronic Engineering (ICEEE)*, Ankara, Turkey, pp. 246-250, 2017.

[5] A. Jawad, H. Abdullah, and S. Hreshee, "Secure Speech Communication System Based On Scrambling and Masking by Chaotic Maps", In: *Proc. of International Conf. on Advance of Sustainable Engineering and its Application*, Kut, Iraq, pp. 7-12, 2018.

[6] Kordov, Krasimir. "A novel audio encryption algorithm with permutation-substitution architecture", *Electronics*, Vol. 8, No. 5 pp. 1-15, 2019.

[7] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol", *International Journal of Electrical and Computer Engineering*, Vol. 10, No. 5, pp. 4824-4834, 2020.

[8] F. J. Farsana and K. Gopakumar, "Speech Encryption Algorithm Based on Nonorthogonal Quantum State with Hyperchaotic Keystreams", *Advances in Mathematical Physics*, Vol. 2020, pp. 1-12, 2020.

[9] H. Abdullah, "Secure Speech Transmission Using Chaotic System", *U.P.B. Sci. Bull., Series C*, Vol. 82, No. 2, pp. 115-126, 2020.

[10] H. Zhao, S. He, Z. Chen, and X. Zhang, "Dual key speech encryption algorithm based underdetermined BSS", *The Scientific World Journal*, Vol. 2014, pp. 1-7, 2014.

[11] Hyvärinen and E. Oja, "Independent Component Analysis: Algorithms and Applications", *Neural Networks*, Vol. 13, No. 4-5, pp. 411–430, 2000.

[12] A. Tharwat, "Independent Component Analysis: An Introduction", *Applied Computing and Informatics*, pp. 1-16, 2018. DOI: 10.1016/j.aci.2018.08.006.

[13] Q. Lin, F. Yin, T. Mei, and H. Liang, "A Blind Source Separation Based Method for Speech Encryption", *IEEE Transactions on Circuits and Systems I*, Vol. 53, No. 6, pp. 1320-1328, 2006.

[14] Z. Yang, G. Zhou, Z. Wu, and J. Zhang, "New Method for Signal Encryption Using Blind Source Separation Based on Subband Decomposition", *Progress in Natural Science*, Vol. 18, No. 6, pp.751-755, 2008.

[15] N. A. Abbas, "Image encryption based on independent component analysis and arnold's cat map", *Egyptian Informatics Journal*, Vol. 17, No. 1, pp. 139-146, 2016.

[16] V. Khalane, S. Suralkar, and U. Bhadade, "Image Encryption Based on Matrix Factorization", *International Journal of Safety and Security Engineering*, Vol. 10, No. 5, pp. 655-661, 2020.

[17] K. Mohanaprasad, A. Singh, K. Sinha, and T. Ketkar, "Noise Reduction in Speech Signals Using Adaptive Independent Component Analysis (ICA) For Hands Free Communication Devices", *International Journal of Speech Technology*, Vol. 22, No. 1, pp. 169-177, 2019.

[18] L. Van, P. Huang, and T. Lu, "Cost-Effective and Variable-Channel Fastica Hardware Architecture and Implementation for EEG Signal Processing", *Journal of Signal Processing Systems*, Vol. 82, No. 1, pp. 91-113, 2016.

[19] K. Zhang and L. Chan, "ICA by PCA Approach: Relating Higher-Order Statistics to Second-Order Moments", In: *Proc. of International Conf. on Independent Component Analysis and Signal Separation*, Heidelberg, Germany, pp. 311-318, 2006.

[20] A. Awad and D. Awad, "Efficient Image Chaotic Encryption Algorithm with No Propagation Error", *ETRI Journal*, Vol. 32, No. 5, pp. 774-783, 2010.

[21] S. Sheela, K. Suresh, and D. Tandur, "A Novel Audio Cryptosystem Using Chaotic Maps and DNA Encoding", *Journal of Computer Networks and Communications*, Vol. 2017, No. 1, pp.1-12, 2017.

[22] M. Dewasthale and R. Kharadkar, "High Performance Self Tuning Adaptive Filter Algorithm for Noise Cancellation in Speech", *Journal of Intelligent & Fuzzy Systems*, Vol. 32, No. 4, pp. 3167-3176, 2017.

Appendix A

$$MCOV(\boldsymbol{Y}) =$$
$$\begin{bmatrix} E[(\boldsymbol{Y_1}-E[\boldsymbol{Y_1}])(\boldsymbol{Y_1}-E[\boldsymbol{Y_1}])] & E[(\boldsymbol{Y_1}-E[\boldsymbol{Y_1}])(\boldsymbol{Y_2}-E[\boldsymbol{Y_2}])] & \dots & E[(\boldsymbol{Y_1}-E[\boldsymbol{Y_1}])(\boldsymbol{Y_{M+1}}-E[\boldsymbol{Y_{M+1}}])] \\ E[(\boldsymbol{Y_2}-E[\boldsymbol{Y_2}])(\boldsymbol{Y_1}-E[\boldsymbol{Y_1}])] & E[(\boldsymbol{Y_2}-E[\boldsymbol{Y_2}])(Y_2-E[Y_2])] & \dots & E[(\boldsymbol{Y_2}-E[\boldsymbol{Y_2}])(\boldsymbol{Y_{M+1}}-E[\boldsymbol{Y_{M+1}}])] \\ \vdots & \vdots & \ddots & \vdots \\ E[(\boldsymbol{Y_{M+1}}-E[\boldsymbol{Y_{M+1}}])(\boldsymbol{Y_1}-E[\boldsymbol{Y_1}])] & E[(\boldsymbol{Y_{M+1}}-E[\boldsymbol{Y_{M+1}}])(\boldsymbol{Y_2}-E[\boldsymbol{Y_2}])] & \dots & E[(\boldsymbol{Y_{M+1}}-E[\boldsymbol{Y_{M+1}}])(\boldsymbol{Y_{M+1}}-E[\boldsymbol{Y_{M+1}}])] \end{bmatrix}$$

where $E[.]$ represents the expectation and $\boldsymbol{Y_i}$, $i \in (1,2,\dots,M+1)$, is the i^{th} rows in $\boldsymbol{Y}$ matrix.