Computers, Materials & Continua
DOI:10.32604/cmc.2022.019710
Article

Tech Science Press

Secure Audio Transmission Over Wireless Uncorrelated Rayleigh Fading Channel

Osama S. Faragallah[1,*], M. Farouk[2], Hala S. El-sayed[3] and Mohsen A.M. El-bendary[4]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[3]Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom, 32511, Egypt
[4]Department of Electronics Technology, Faculty of Technology and Education, Helwan University, Cairo, Egypt
[*]Corresponding Author: Osama S. Faragallah. Email: o.salah@tu.edu.sa

Received: 23 April 2021; Accepted: 08 June 2021

Abstract: Audio communications and computer networking play essential roles in our daily lives, including many domains with different scopes. Developments in these technologies are quick. In consequence, there is a dire need to secure these technologies up to date. This paper presents an efficient model for secure audio signal transmission over the wireless noisy uncorrelated Rayleigh fading channel. Also, the performance of the utilized multiple secret keys-based audio cryptosystem is analyzed in different transformation domains. The discrete cosine transform (DCT), the discrete sine transform (DST), and the discrete wavelet transform (DWT) are investigated in the utilized multiple secret key-based audio cryptosystem. Simulation results show consistent results with the wireless noisy channel. The performance of the proposed multiple secret keys-based audio cryptosystem can be ranked concerning the employed domain as DWT, DCT, and DST transform techniques. The simulation experiments proved that the presented multiple secret keys-based audio cryptosystem for audio signals transmitted over the wireless noisy uncorrelated Rayleigh fading channel achieves reliable and secure wireless link utilizing combined multi security layers.

Keywords: Audio communications; encryption; uncorrelated Rayleigh fading channel

1 Introduction

Audio communications have a pivotal role in our daily life, covering many domains like cell phone, military applications, electronic learning, online banking, social networks, landline phone conversation, and chatting conversation programs. Therefore, audio calls are widely utilized in our daily life, especially with audio cryptosystem calls. Essentially, any audio cryptosystem requires audio data to be transmitted in a non-clear form or encrypted form using a robust encryption algorithm. Otherwise, the audio cryptosystem cannot guarantee enough security against eavesdropping during the communication process. Moreover, it is mandatory to cancel and eliminate any residual intelligibility in the ciphered audio data to ensure sufficient protection against eavesdropping during audio communications [1–4].

As the cryptanalysis tools and activities have increased, it is crucial to encrypt audio files during the communication process through all known communication channels like the public telephone network, wireless network, radio communications and Internet calls. Any successful audio cryptosystem should own a strong encryption algorithm against attacks and eavesdroppers. Therefore, scientific research must focus on security enhancements for audio cryptosystems. They should quickly enhance the security of audio cryptosystems because of two reasons. First, there is rapid development in cryptanalysis and eavesdroppers' techniques. Second, there is a rapid increase in audio communication usage in a wide variety of daily lives [5–8].

Due to the wide-spreading of different wireless networks, security issues became vital to combat the various attacks. Several audio signals are susceptible, and they must be protected and secured from any attacks. Also, a communication system cannot give the required security level against hackers during communications, especially if the audio data over wireless channels is clear or not encrypted [7]. It is usually receivable for any unauthorized eavesdropper. For ensuring a high-security degree, efficient audio encryption/decryption techniques are required [8].

The secured wireless transmission model for sensitive audio signals is presented in this paper. Furthermore, the performance of the enhanced multiple secret keys-based audio cryptosystem is analyzed using different metrics over the wireless uncorrelated fading channel to prove its applicability with varying kinds of noises.

The paper rest has been organized as follows: the overview of the related work is presented in section 2. In section 3, the enhanced multiple secret keys-based audio cryptosystem description based on enhanced multiple key is presented. The computer simulation experiments for the enhanced multiple secret keys-based audio cryptosystem are explored in section 4. Finally, the conclusion is given in section 5.

2 Related Works

The recent presented audio security techniques have been discussed in this section. The audio security techniques include encryption tools, secret key based methods and data hiding based security techniques. The audio cryptosystems can be categorized into analog cryptosystems and digital cryptosystems. The analog methods of audio encryption can be categorized into time-domain (TD) methods and frequency domain methods like DCT, DST, and DWT [9–19]. The second type of audio cryptosystem is the digital cryptosystems. There are two examples of digital audio cryptosystems: the traditional Advanced Encryption Standard (AES) and the chaotic encryption using baker map-based techniques [20–23].

The chaotic baker map is used in 2019 as an efficient data randomizing tool for enhancing the error performance of low complex convolutional codes [24]. The chaotic baker map is employed in this presented research to improve the multiple secret keys audio cryptosystem. Although the problems of audio signals protection over the commercial channel have been discussed in [25], this research work proposed an efficient method for encrypting the speech using the variable-length encoding and the collatz conjecture. This speech encryption approach has a larger keyspace and significantly higher key sensitivity. Several metrics are considered for studying the performance of this proposed audio security technique, such as the computational cost, key sensitivity and security keyspace size [25].

The data hiding concept is presented as a tool for protecting the audio signal in [26]. The authors in this research work proposed the watermarking technique to secure the audio signals. The DWT and singular value decomposition (SVD) techniques have been utilized in the proposed watermarking scheme; this proposed decentralized watermarking works based on distributing the audio signal watermark into the corners of the host signals for enhancing the robustness of this decentralized watermarking technique [26]. Furthermore, based on the LSB algorithm in [27], the steganography technique is proposed for image embedding into audio files. This approach contains two processes, the compression and encryption process of the image by the GMPR technique. Examples of data hiding techniques utilized as a tool for image and audio security have been presented in several research papers [26–28].

3 Enhanced Multiple Secret Keys-Based Audio Cryptosystem

The enhanced multiple secret keys-based audio cryptosystemis a combined encryption algorithm utilizing the baker map within the frequency domains. The permutation process increases the confusion of the presented multiple secret keys-based audio cryptosystem. Therefore, this research paper has utilized different transform techniques to test their performance within the presented multiple secret keys-based audio cryptosystem over the wireless uncorrelated Rayleigh fading channel. The enhanced multiple secret keys-based audio cryptosystem employs different transform domains like DCT, DST, and DWT.

3.1 Encryption Algorithm

In the following, the steps of the encryption algorithm of the enhanced multiple secret keys-based audio cryptosystem are presented.

Round 1: Framing and reshaping the audio signal from a 1D block into 2D blocks.

Round 2: Mask generation using the secret key; this is an essential step to modify the remaining non-permutated parts of the audio signal and enhance the security of the enhanced multiple secret keys-based audio cryptosystem. The mask is generated as follows:

The square matrix of size equal to the secret key size is filled with zero values. The first number of rows is equivalent to the number of sub-keys in the private key, filled with a value of 1. Zeros and ones masks are formed using the chaotic baker map permutations. This mask is combined with every audio block signal after reformatting to fill the silent periods of the audio signal and offer immunity against known-plaintext attacks.

Round 3: Permutation and substitution; the permutation utilizes the chaotic baker map to rearrange audio sample data in the audio matrix.

For each separate test, repeat permutation a number of rounds equals 3, 5 and 7. Then, permutation is followed by substitution to alter the remaining non-shuffled portions of the audio signal and increase the cryptosystem's security. Finally, the mask is added to the original audio signal in the encryption algorithm and subtracted in the decryption algorithm.

Round 4: Apply discrete transforms followed by permutation and then substitution; finally, apply the inverse of discrete transforms.

The main idea of employing the DCT, DST and DWT [29–31] is to increase diffusion and change the values of 1 introduced by masking in silent periods (all-zero blocks). Another shuffling operation is employed in the DCT, DST or DWT for the audio samples to improve the confusion and enhance the security before employing the inverse of the employed transform. This is followed by a substitution step, which changes the audio samples by combining their values to the mask's value. Finally, this step is followed by applying the inverse of transform domain IDCT, IDST or IDWT.

Round 5: Permutation using baker map is repeated a number of rounds equals 3, 5 and 7.

Round 6: Reshaping into a 1D format save audio data into a file. The output is the encrypted audio version.

3.2 Decryption Algorithm

In the following, the steps of the decryption algorithm of the enhanced multiple secret keys-based audio cryptosystem are presented.

Round 1: Mask generation using the secret key and baker map.

Round 2: Framing and reshaping into 2D blocks to form a readable format.

Round 3: Employ the inverse of permutation using the inverse of baker map. For each separate experiment, repeat this round a number of rounds equals 3, 5 and 7.

Round 4: Apply discrete transforms followed by the inverse of substitution and then the inverse of substitution; finally, apply the inverse of discrete transforms.

Round 5: Employ the inverse of substitution and the inverse of permutation. The inverse of substitution utilizes a subtract mask. The inverse of permutation employs the inverse of baker map with repeating the inverse permutation a number of rounds equals 3, 5 and 7.

Round 6: Reshaping into a 1D format save audio data into a file. The output is the decrypted audio version.

The encryption and decryption algorithms steps have been described in the above sections of the enhanced multiple secret keys-based audio cryptosystem. This enhanced multiple secret keys-based audio cryptosystem works using substitution and permutation of audio blocks using multiple secret keys in frequency domains. In addition, the enhanced multiple secret keys-based audio cryptosystem is based on utilizing the fifth private key created from the enhanced audio cryptosystem's original secret key. This adds another security layer for the enhanced multiple secret keys-based audio cryptosystem and enlarges the keyspace. Simulation experiments demonstrated that these modifications enhance the security of the audio transmission over the wireless uncorrelated fading channel. Therefore, the enhanced multiple secret keys-based audio cryptosystem is suitable for sensitive and classified phone calls. However, these enhancements are at the cost of increasing the time taken to execute the enhanced multiple secret keys-based audio cryptosystem.

The presented audio cryptosystem adds another security layer by enlarging the secret keyspace. This is done by increasing the number of private keys used to five keys instead of only four keys by generating the fifth key (key 5). The size of key 5 equals one half the size of key 2. Also, mask four is developed to be handled with operations of key 4.

3.3 The Evaluating Model of the Enhanced Multiple Secret Keys-Based Audio Cryptosystem

In this section, the evaluating model of the presented enhanced multiple secret keys-based audio cryptosystem have been introduced. This model processes the audio files for performing the encryption process at the transmitter side as shown in Fig. 1. Also, it shows the operation of the encrypted audio file and the decryption process, as shown in Fig. 1 for decrypting the encrypted audio signal. The Rayleigh fading channel is utilized to test the performance of the presented audio cryptosystem and evaluate the quality of the received decrypted audio file.

The encrypted audio signal is prepared to send over the wireless uncorrelated Rayleigh fading channel through the following three steps: a- transmission process, b- segmentation to packets, and c- modulation. In Fig. 1, the proposed secured audio communication model is designed for testing the multiple secret keys-based audio cryptosystem over the wireless uncorrelated Rayleigh fading channel. This model has been designed for evaluating the performance of the enhanced multiple secret keys-based audio cryptosystem for securing the audio signals transmission in a free and open environment. This environment is represented in this proposed model of secure audio transmission by the wireless uncorrelated Rayleigh fading channel. In the simulation section, the presented guaranteed audio wireless transmission parameters are presented. These parameters are the length of the small packets, "transmitted packet length", the channel conditions simulation "SNR Values", the modulation and the utilized wireless communication channel.

4 The Computer Simulation Experiments

Several experiments are devoted to test and evaluate the effect of noise using uncorrelated fading channel on the received decrypted audio signal after passing through a wireless medium, with different SNR noise levels and at the same time re-run tests with the error-free channel. For evaluating the algorithms' performance, many metrics utilized, such as the spectral distortion (SD), Log-Likelihood Ratio (LLR), and the correlation coefficient (CC). There are two groups of experiments; the first experiment group tests the enhanced multiple secret keys-based audio cryptosystem concerning the different transform domains. The second experiment group tests evaluate the presented multiple secret keys-based audio cryptosystem as a security tool for securing the transmitted speech or audio signals over the wireless uncorrelated Rayleigh fading channel communication. The simulation setting parameters of the secured transmission model of the audio signals are presented in Tab. 1.

4.1 Uncorrelated Rayleigh Fading Channel Experiments Group

In this group of experiments, the enhanced multiple secret keys-based audio cryptosystem is tested over wireless uncorrelated Rayleigh fading channel with error-free and various SNR values using the different transform domains.

4.1.1 DCT Analysis

For decryption and according to the employed security metrics shown in Tab. 2 for CC, SD and LLR, the best performance of the enhanced multiple secret keys-based audio cryptosystemis achieved with SNR equals 35 dB, while the worst performance of the enhanced multiple secret keys-based audio cryptosystem is obtained with SNR equals 0 dB. This is generally expected as the noise level becomes lowest with the value of 35 dB and, as a result, better quality for the decrypted audio signal. Furthermore, it is shown from Tab. 2 that the enhanced multiple secret keys-based audio cryptosystem shows improved values of CC, SD and LLR with increasing the SNR of the uncorrelated Rayleigh fading channel.

4.1.2 DST Analysis

For decryption, according to employed security metrics shown in Tab. 3 for CC, SD and LLR, the best performance of the enhanced multiple secret keys-based audio cryptosystem is achieved with SNR equals 35, while the worst performance of the enhanced multiple secret keys-based audio cryptosystem is obtained with SNR equals 0 dB. This is usually expected as the noise level becomes lowest with a value of 35 dB and, as a result, better quality for the decrypted audio signal. This is generally expected as the noise level becomes lowest with a value of 35 dB and, as a result, better quality for the decrypted audio signal. It is shown from Tab. 3 that the performance of the enhanced multiple secret keys-based audio cryptosystem shows improved values of CC, SD and LLR with increasing the SNR of the uncorrelated Rayleigh fading channel. On the other hand, it is delivered from Tab. 3 that the DST-based enhanced multiple secret keys-based audio cryptosystem performs worse than the DCT-based enhanced multiple secret keys-based audio cryptosystem. Also, the received decrypted audio signal quality is lower than the DCT domain. Hence, these tabulated results demonstrate that the DCT transform achieves better performance over the uncorrelated Rayleigh fading channel than the DST transform.

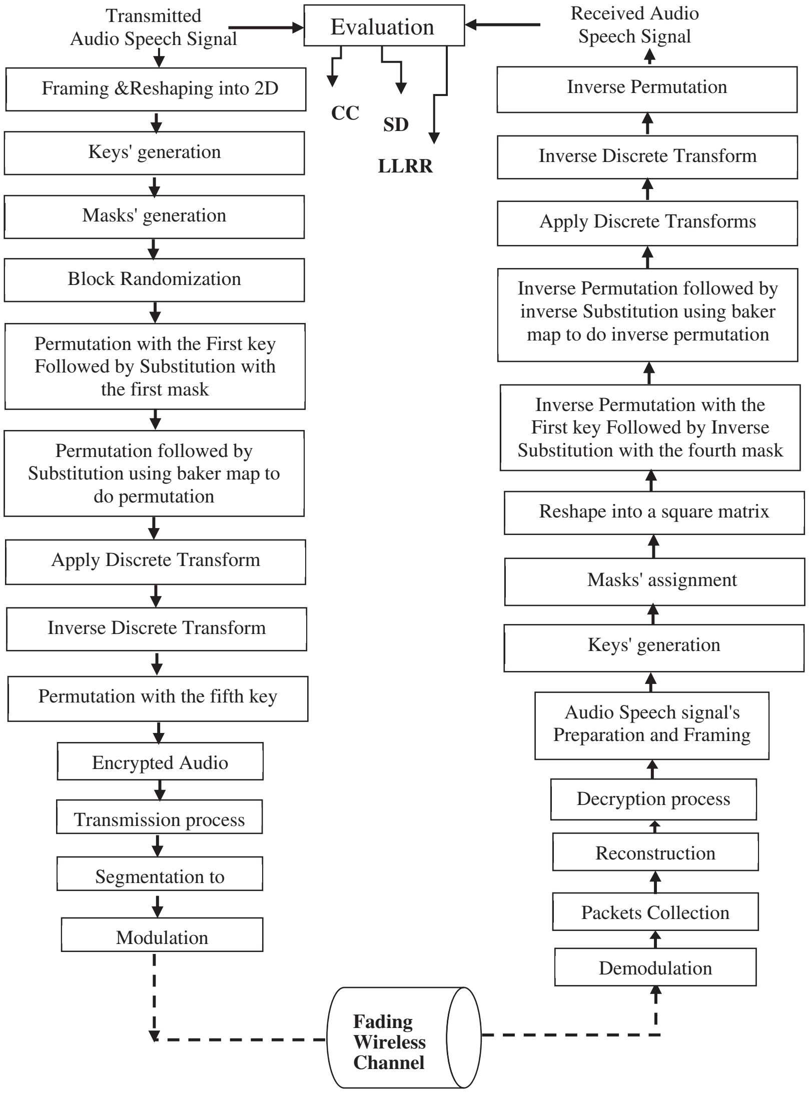
Transmitted
Audio Speech Signal
Evaluation
Received Audio
Speech Signal
CC
SD
LLRR
Framing &Reshaping into 2D
Keys' generation
Masks' generation
Block Randomization
Permutation with the First key Followed by Substitution with the first mask
Permutation followed by Substitution using baker map to do permutation
Apply Discrete Transform
Inverse Discrete Transform
Permutation with the fifth key
Encrypted Audio
Transmission process
Segmentation to
Modulation
Fading Wireless Channel
Inverse Permutation
Inverse Discrete Transform
Apply Discrete Transforms
Inverse Permutation followed by inverse Substitution using baker map to do inverse permutation
Inverse Permutation with the First key Followed by Inverse Substitution with the fourth mask
Reshape into a square matrix
Masks' assignment
Keys' generation
Audio Speech signal's Preparation and Framing
Decryption process
Reconstruction
Packets Collection
Demodulation

Figure 1: The encryption and decryption steps of the enhanced multiple secret keys-based audio cryptosystem model for performance evaluating over wireless uncorrelated Rayleigh fading channel

Table 1: Uncorrelated Rayleigh fading channel setting parameters

Parameter	Simulation values
Packet size	16384 bits/
Packet format	Standard packets without protection
FEC:- error control scheme	Not applicable
Modulation	BPSK modulation
Channel	Rayleigh fading channel
Channel conditions	Error-free and wireless channel
Signal to noise ratio (SNR)	SNR = [0–25 dB]
Transforms	DST & DCT & DWT techniques
Secret keys	5 Different secret keys utilized
Error control tech.	Not

Table 2: DCT results with error-free channel and various uncorrelated Rayleigh fading SNR values

Operation	Measure	Different evaluating metrics values with the various wireless Rayleigh fading channel SNR conditions					
		Error-free	0 dB	5 dB	15 dB	25 dB	35 dB
Encryption	CC	−0.00004	−0.00004	−0.00004	−0.00004	−0.00004	−0.00004
	SD	13.8795	13.8795	13.8795	13.8795	13.8795	13.8795
	LLR	0.4491	0.4491	0.4491	0.4491	0.4491	0.4491
Decryption	CC	0.9775	0.000686	0.0242	0.4239	0.5374	0.8968
	SD	1.384	50.6478	40.3216	17.7237	15.2594	7.4711
	LLR	0.0162	0.5608	0.5451	0.4615	0.3855	0.309

Table 3: DST with error-free channel and various uncorrelated Rayleigh fading SNR values

Operation	Measure	Different evaluating metrics values with the various wireless Rayleigh fading channel SNR conditions					
		Error-free	0 dB	5 dB	15 dB	25 dB	35 dB
Encryption	CC	−0.0013	−0.0013	−0.0013	−0.0013	−0.0013	−0.0013
	SD	13.93	13.93	13.93	13.93	13.93	13.93
	LLR	0.4082	0.4082	0.4082	0.4082	0.4082	0.4082
Decryption	CC	0.9726	1.26E − 05	0.0186	0.2562	0.5049	0.8925
	SD	1.5818	48.844	41.8715	23.0499	16.2391	6.9576
	LLR	0.0163	0.5203	0.486	0.4747	0.451	0.2783

4.1.3 DWT Analysis

The performance evaluation of the enhanced multiple secret keys-based audio cryptosystem utilizing the DWT transform has been presented. The CC, SD and LLR metrics are employed for measuring the quality of encryption and decryption processes of the enhanced multiple secret keys-based audio cryptosystem. In addition, the various uncorrelated Rayleigh fading channel conditions are used through various SNR values. The results tabulated in Tab. 4.

Table 4: DWT with error-free channel and various uncorrelated Rayleigh fading SNR values

Operation	Measure	Different evaluating metrics values with the various wireless Rayleigh fading channel SNR conditions					
		Error-free	0 dB	5 dB	15 dB	25 dB	35 dB
Encryption	CC	0.0028	0.0028	0.0028	0.0028	0.0028	0.0028
	SD	15.4779	15.4779	15.4779	15.4779	15.4779	15.4779
	LLR	0.5301	0.5301	0.5301	0.5301	0.5301	0.5301
Decryption	CC	0.9789	0.006	0.0877	0.6759	0.7962	0.9237
	SD	1.3104	43.1353	34.6279	12.2944	9.3406	5.7236
	LLR	0.0113	0.7025	0.5598	0.3053	0.245	0.2213

As shown in Tab. 4, the DWT-based enhanced multiple secret keys-based audio cryptosystem performs better than the DCT and DST-based system. Moreover, the decrypted audio signal quality is improved with the DWT. These two previous computer simulation experiments prove the applicability of the enhanced multiple secret keys-based audio cryptosystem for securing the sensitive speech calls or audio files transmission over the wireless uncorrelated Rayleigh fading channel.

4.2 Results Analysis and Comparison

This section presents a comparison and analysis for security and quality metrics in decryption with different SNR values. Tab. 5 shows a comparison between the correlation coefficient (CC) values of different transform techniques. Fig. 2 shows the values of the CC between the original and received decrypted audio with different transform techniques and various SNR of the uncorrelated Rayleigh fading channel. For CC values, it is shown that the best values exist with the DWT for all SNR values. However, the worst values indicated with the DST for values of SNR equal 0 dB, 5 dB, 10 dB, 15 dB, 20 dB, and 25 dB. The worst value indicated with the DCT for SNR equals 25 dB.

Fig. 3 shows the values of the SD metric values of the enhanced multiple secret keys-based audio cryptosystem with the different transform techniques and various SNR values of the uncorrelated Rayleigh fading channels. In Fig. 3, the SD metrics values are drawn for the previous experiments for encrypted audio using the enhanced multiple secret keys-based audio cryptosystems. As shown from Fig. 3, with increasing the SNR values of the wireless uncorrelated Rayleigh fading channel, the quality of the received decrypted audio signal is improved. On the other hand, the DWT transform achieves better metrics values. For SD values, it is shown from Fig. 3 that the best values exist with the DWT for all SNR values. However, the worst values are indicated with the DCT and DST for different SNR values. Fig. 4 shows the LLR metric values of the enhanced multiple secret keys-based audio cryptosystem with different transform techniques and various SNR values of the uncorrelated Rayleigh fading channel. For LLR values shown in

Fig. 4, the best values exist with the DWT for SNR values equal 10 dB and 15 dB. The best values exist with the DST for SNR values equal 0 dB and 5 dB. However, the worst values are shown with the DWT for values of SNR equal 0 dB and 5 dB. The worst values exist with the DCT for SNR values equal 10 dB and 15 dB. The different metrics values are collected in Tab. 5. This table tabulates the values of the experiments using different transform techniques.

Table 5: Metrics values of different techniques over the wireless noisy uncorrelated Rayleigh fading channel with SNR variations for original and decrypted version

Metrics		The proposed algorithms with metrics values with different SNR channel					
		DCT		DST		DWT	
		SNR	Value	SNR	Value	SNR	Value
CC_Dec. Original & decrypted audio	Channel SNR	0 dB	0.0006	0 dB	0.00001	0 dB	0.006
		5 dB	0.0242	5 dB	0.0186	5 dB	0.0877
		10 dB	0.0631	10 dB	0.0599	10 dB	0.2502
		15 dB	0.4239	15 dB	0.2562	15 dB	0.6759
		20 dB	0.5374	20 dB	0.5449	20 dB	0.7962
		25 dB	0.8768	25 dB	0.8725	25 dB	0.9337
Spectral Distortion (SD) Decryption process	Channel SNR	0 dB	50.648	0 dB	48.844	0 dB	43.1353
		5 dB	40.322	5 dB	41.8715	5 dB	34.6279
		10 dB	39.107	10 dB	36.4781	10 dB	25.7108
		15 dB	17.724	15 dB	23.0499	15 dB	12.2944
		20 dB	15.259	20 dB	16.2391	20 dB	9.3406
		25 dB	7.4711	25 dB	6.9576	25 dB	5.7236
LLR-Dec. Decryption process	Channel SNR	0 dB	0.5608	0 dB	0.5203	0 dB	0.7025
		5 dB	0.5451	5 dB	0.486	5 dB	0.5598
		10 dB	0.4743	10 dB	0.4825	10 dB	0.4782
		15 dB	0.4615	15 dB	0.4747	15 dB	0.3053
		20 dB	0.3855	20 dB	0.451	20 dB	0.245
		25 dB	0.309	25 dB	0.2783	25 dB	0.2213
Average processed time (ms)		0.1045		0.0935		0.1325	

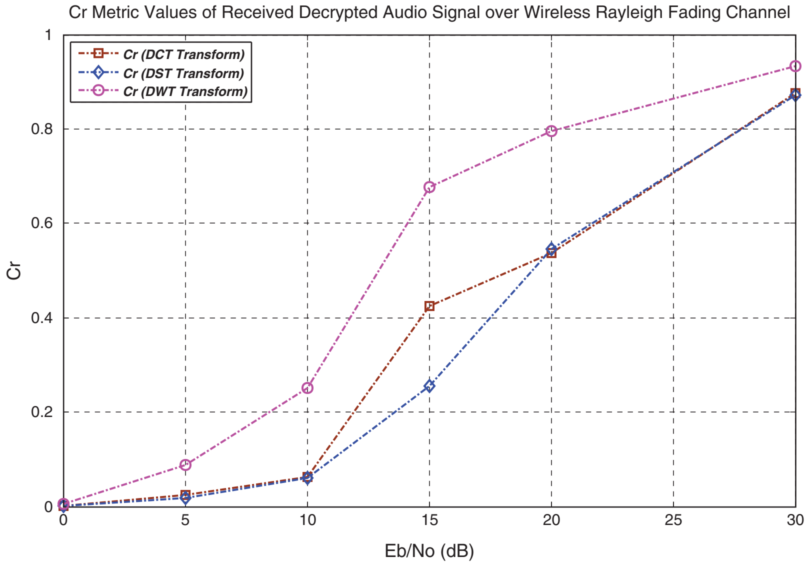

Figure 2: CC *vs.* SNR for the enhanced multiple secret keys-based audio cryptosystem over the wireless noisy uncorrelated Rayleigh fading channel

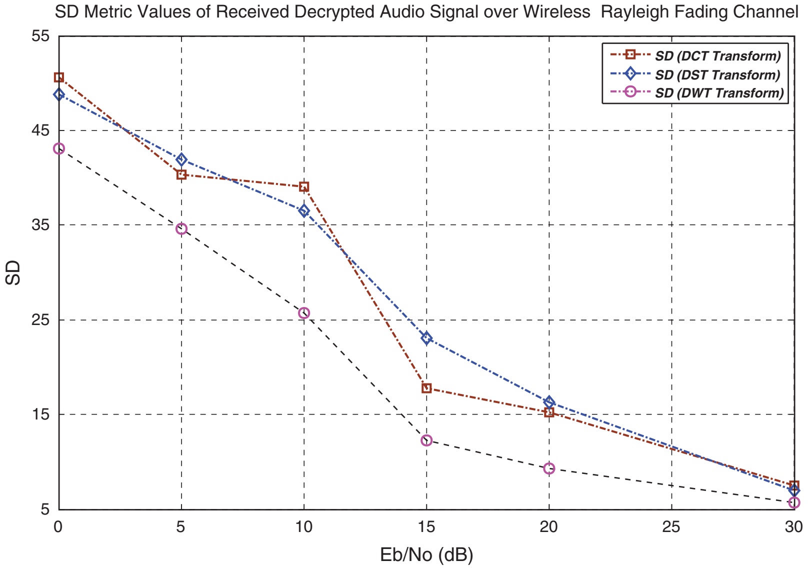

Figure 3: SD *vs.* SNR for the enhanced multiple secret keys-based audio cryptosystem over the wireless noisy uncorrelated Rayleigh fading channel

In Tab. 5, the metrics of the received decrypted audio signal quality are tabulated. These metrics demonstrate the suitability of this enhanced multiple secret keys-based audio cryptosystem for securing the audio signals transmission over the wireless uncorrelated Rayleigh fading channel. Hence, this high-level audio security tool can achieve reliable wireless links to transmit high-sensitive audio signals. The DWT transform technique achieves good decrypted audio quality compared to the other utilized methods. The presented secured model for sensitive speech calls or audio signals transmitted over the wireless uncorrelated Rayleigh fading channel is applicable and can provide combined layers of security due to the secret key enlarging and security-enhancing utilizing the chaotic baker map.

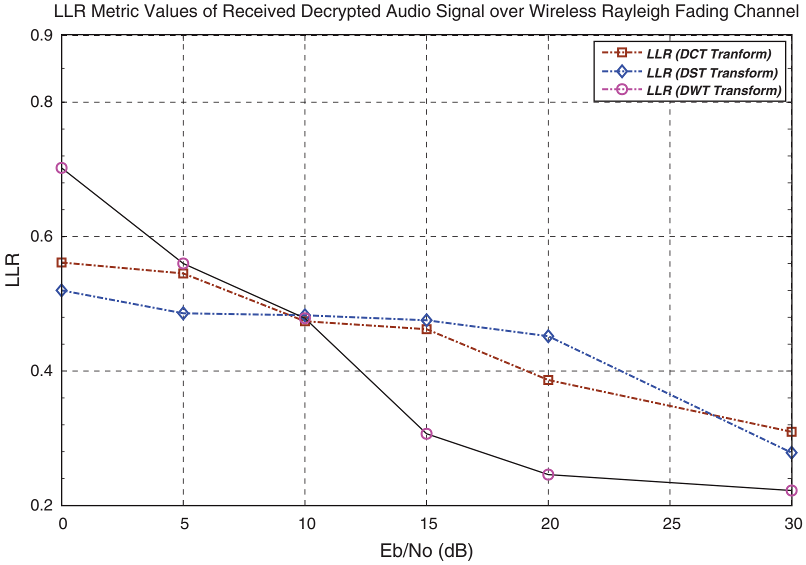

Figure 4: LLR *vs.* SNR for the enhanced multiple secret keys-based audio cryptosystem over the wireless noisy uncorrelated Rayleigh fading channel

5 Conclusions

This paper presents an efficient model for guaranteed audio signal transmission over the wireless noisy uncorrelated Rayleigh fading channel. Also, the performance of the utilized enhanced multiple secret keys-based audio cryptosystem is analyzed with different transform domains like DCT, DST and DWT using chaotic baker map and multiple secret keys. Simulation results show consistent results with the wireless uncorrelated Rayleigh fading channel. The DWT-based enhanced multiple secret keys-based audio cryptosystem outperforms better than the DCT and DST-based systems. Also, the decrypted audio signal quality is improved with the DWT. The achieved results proved the applicability of the enhanced multiple secret keys-based audio cryptosystem for transmitting sensitive speech calls or audio signals over the wireless uncorrelated Rayleigh fading channel.

Acknowledgement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

Funding Statement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Mohammed, B. AlKasasbeh and F. AlAdwan, "An improved secure SIP registration mechanism to avoid VoIP threats," *International Journal of Cloud Applications and Computing*, vol. 6, no. 2, pp. 25–36, 2016.

[2] O. S. Faragallah and H. S. El-Sayed, "Secure opto-audio cryptosystem using XORing mask and hartley transform," *IEEE Access*, vol. 9, pp. 25437–25449, 2021.

[3] L. Hongjun, A. Kadir and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik—International Journal for Light and Electron Optics*, vol. 127, no. 19, pp. 7431–7438, 2016.

[4] Z. Wei, B. Zhao, B. Liu, J. Su, L. Xu *et al.,* "A novel steganography approach for voice over IP," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 4, pp. 601–610, 2014.

[5] A. Castiglione, A. De Santis, A. Castiglione, F. Palmieri and U. Fiore, "An energy-aware framework for reliable and secure end-to-end ubiquitous data communications," in *2013 5th Int. Conf. on Intelligent Networking and Collaborative Systems*, Xi'an, China, pp. 157–165, 2013.

[6] O. M. Al-Hazaimeh, "A new approach for complex encrypting and decrypting data," *International Journal of Computer Networks & Communications*, vol. 5, no. 2, pp. 95–103, 2013.

[7] F. E. Abd El-Samie, A. Shafik, H. S. El-Sayed, S. M. Elhalafawy, S. M. Diab *et al.,* "Sensitivity of automatic speaker identification to SVD digital audio watermarking," *International Journal of Speech Technology*, vol. 18, no. 4, pp. 565–581, 2015.

[8] P. Amit, P. Mohapatra and J. Zambreno, "Securing multimedia content using joint compression and encryption," *IEEE Multimedia*, vol. 20, no. 4, pp. 50–61, 2013.

[9] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map," *Multimedia Tools and Applications*, vol. 79, pp. 17817–17835, 2020.

[10] Y. Wu and B. P. Ng, "Speech scrambling with hadamard transform in frequency domain," in *6th Int. Conf. on Signal Processing, 2002*, vol. 2, pp. 1560–1563, 2002.

[11] G. Manjunath and G. V. Anand, "Speech encryption using circulant transformations," in *Proc. IEEE Int. Conf. on Multimedia and Expo*, vol. 1, pp. 553–556, 2002.

[12] A. Musheer, B. Alam and O. Farooq, "Chaos based mixed keystream generation for voice data encryption," *International Journal on Cryptography and Information Security*, vol. 2, no. 1, pp. 36–45, 2012.

[13] S. S. Nassar, N. M. Ayad, H. M. Kelash, H. S. El-Sayed, M. A. M. El-Bendary *et al.,* "Efficient audio integrity verification algorithm using discrete cosine transform," *International Journal of Speech Technology*, vol. 19, no. 1, pp. 1–8, 2016.

[14] J. Daemen and V. Rijmen, "Rijndael/aes," in *Encyclopedia of Cryptography and Security*. Berlin/Heidelberg, Germany: Springer, pp. 520–524, 2005.

[15] E. M. Elshamy, E. M. El-Rabaie, O. S. Faragallah, O. A. Elshakankiry, F. E. Abd El-Samie *et al.,* "Efficient audio cryptosystem based on chaotic maps and double random phase encoding," *International Journal of Speech Technology*, vol. 18, no. 4, pp. 619–631, 2015.

[16] C. Sanchez-Avila and R. Sanchez-Reillol, "The Rijndael block cipher (AES proposal): A comparison with DES," in *Proc. IEEE 35th Annual 2001 Int. Carnahan Conf. on Security Technology*, London, UK, pp. 229–234, 2001.

[17] O. S. Faragallah, "Secure audio cryptosystem using hashed image LSB watermarking and encryption," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2009–2023, 2018.

[18] S. E. Borujeni and M. Eshghi, "Chaotic image encryption system using phase-magnitude transformation and pixel substitution," *Telecommunication Systems*, vol. 52, no. 2, pp. 525–537, 2013.

[19] L. Zheng, X. Li and Z. Dong, "Enhancing security of frequency domain video encryption," in *Proc. of the 12th annual ACM Int. Conf. on Multimedia*, New York, USA, pp. 304–307, 2004.

[20] L. Wen-Nung and C. Li-Chun, "Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification," *IEEE Transactions on Multimedia*, vol. 8, no. 1, pp. 46–59, 2006.

[21] G. Unnikrishnan and K. Singh, “Double random fractional Fourier-domain encoding for optical security,” *Optical Engineering*, vol. 39, no. 11, pp. 2853–2859, 2000.

[22] S. E. Borujeni, “Speech encryption based on fast Fourier transform permutation,” in *7th IEEE Int. Conf. on Electronics, Circuits and Systems (ICECS 2000)*, vol. 1, pp. 290–293, 2000.

[23] M. A. M. El-Bendry and A. E. A. Azm, “Complexity considerations: Efficient image transmission over mobile communications channels,” *Multimedia Tools and Applications*, vol. 78, pp. 16633–16664, 2019.

[24] D. Renza, S. Mendoza and D. M. Ballesteros, “High-uncertainty audio signal encryption based on the Collatz conjecture,” *Journal of Information Security and Applications*, vol. 46, pp. 62–69, 2019.

[25] A. Singha and M. A. Ullah, “Development of an audio watermarking with decentralization of the watermarks,” *Journal of King Saud University, Computer and Information Sciences*, 2020. https://doi.org/10.1016/j.jksuci.2020.09.007.

[26] S. T. Abdulrazzaq, M. M. Siddeq and M. A. Rodrigues, “Novel steganography approach for audio files,” *SN Computer Science*, vol. 1, pp. 1–13, 2020.

[27] J. Chaharlang, M. Mosleh and S. Rasouli-Heikalabad, “A novel quantum steganography-steganalysis system for audio signals,” *Multimedia Tools and Applications*, vol. 79, pp. 17551–17577, 2020.

[28] F. J. Farsana and K. Gopakumar, “Speech encryption algorithm based on nonorthogonal quantum state with hyperchaotic keystreamsm,” *Advances in Mathematical Physics*, vol. 2020, pp. 1–12, 2020.

[29] S. F. El-Zoghdy, H. S. El-sayed and O. S. Faragallah, “Transmission of chaotic-based encrypted audio through OFDM,” *Wireless Personal Communications*, vol. 113, pp. 241–261, 2020.

[30] E. Mosa, N. W. Messiha and O. Zahran, “Chaotic encryption of speech signals in transform domains,” in *Int. Conf. on Computer Engineering & Systems*, Cairo, Egypt, pp. 300–305, 2009.

[31] P. Mohit and D. Nitnawwre, “Performance improvement of OFDM system using PAPR reduction,” *Performance Improvement*, vol. 3, no. 1, pp. 23–27, 2012.