Computers, Materials & Continua
DOI: 10.32604/cmc.2022.019951
Article

Tech Science Press

Secret Key Optimization for Secure Speech Communications

Osama S. Faragallah[1,*], Mahmoud Farouk[2] and Hala S. El-Sayed[3]

[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
*Corresponding Author: Osama S. Faragallah. Email: o.salah@tu.edu.sa

Received: 03 May 2021; Accepted: 23 June 2021

Abstract: This paper answers three essential questions for audio speech cryptosystems in time and discrete transform domains. The first question is, what are the best values of sub-keys that must be used to get the best quality and security for the audio cryptosystem in time and discrete transform domains. The second question is the relation between the number of sub-keys, the number of secret keys used, and the audio speech signal block's size. Finally, how many possible secret keys can be used to get the best quality and security results for the audio speech cryptosystem in time and discrete transform domains. An audio cryptosystem discussed before in recent research is applied to answer the three previous inquiries. Accurate simulation results and analysis answer all three questions; first, there is no specific, well-defined format or rule for sub-key values that must be used to get a better cryptosystem. For the second question, yes, there is a direct relationship between the number of applicable keys, number of available sub-keys, and block size of speech audio signal and formulated into a first-order equation. For the third question, each discrete transform domain has a specific acceptable range of sub-keys that imply a particular number of keys that can be used to get a better cryptosystem.

Keywords: Audio cryptosystem; chaotic baker map; secret key size

1 Introduction

Speech communications play essential roles in our daily life, and they cover several domains like military services, E-learning, banking services, social networks, phone conversations, and news broadcasting. As speech information passes through unsecured communication channels, there is a need to maintain this audio information secure before transmitting it via an insecure channel. Therefore, the employed cryptographic techniques must have the ability to transform the speech from intelligible format to unintelligible format. Also, it must have to ability to decipher it to a reasonable at the side of the receiver. There exist two speech encryption approaches; analogue and digital speech cryptosystems [1–6]. Nowadays, analogue audio encryption methods are more popular because it has characteristics of fewer bandwidth requirements. On the other hand, digital speech encryption methods require more bandwidth and complex implementation, but they provide more security.

This paper is trying to provide answers about three essential questions in the world of speech cryptosystem based on a comprehensive study which is an investigation and analysis using some advanced code and with statistics functions and analysis, then applying all together on a recently proposed cryptosystem discussed before in current research and proved its high degree of security [7].

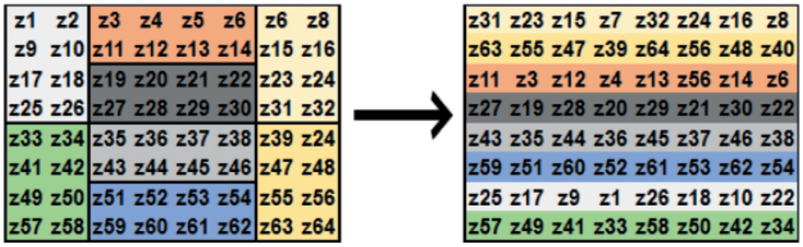
The main contribution points of this article can be listed as follows:

1. A better quality and efficient audio secure cryptosystem is obtained when changing the used sub-keys. However, there is no well-defined rule for how to choose values of sub-keys.
2. There is a direct relationship between the applicable number of sub-keys, audio speech block size, and functional secret keys.
3. Each transform domain has a specific range of sub-keys that must be used to get the best quality and security results, and not all transform domains have the same range of the number of sub-keys.

The remnant sections of this research are arranged as the following. Section 2 discusses the baker map. Section 3 discusses and presents the recent audio cryptosystem in [7]. Section 4 discusses the simulation results. Finally, Section 5 delivers the concluding remarks.

2 Baker Map

It is a 2D chaotic map used to provide some security and hiding original speech information in the permutation of speech information. It accomplishes this by rearranging pixels in the array matrix into new locations [8–14]. Moreover, it keeps all the superior features of chaotic systems, like non-predictability, randomness and small correlation [15–18]. There exist two kinds of baker map, generalized and discretized maps [19–21]. This paper focuses on discretized baker map. Some recent cryptosystems are using it. Fig. 1 illustrates the discretized baker map.



z1	z2	z3	z4	z5	z6	z6	z8
z9	z10	z11	z12	z13	z14	z15	z16
z17	z18	z19	z20	z21	z22	z23	z24
z25	z26	z27	z28	z29	z30	z31	z32
z33	z34	z35	z36	z37	z38	z39	z24
z41	z42	z43	z44	z45	z46	z47	z48
z49	z50	z51	z52	z53	z54	z55	z56
z57	z58	z59	z60	z61	z62	z63	z64

z31	z23	z15	z7	z32	z24	z16	z8
z63	z55	z47	z39	z64	z56	z48	z40
z11	z3	z12	z4	z13	z56	z14	z6
z27	z19	z28	z20	z29	z21	z30	z22
z43	z35	z44	z36	z45	z37	z46	z38
z59	z51	z60	z52	z61	z53	z62	z54
z25	z17	z9	z1	z26	z18	z10	z22
z57	z49	z41	z33	z58	z50	z42	z34

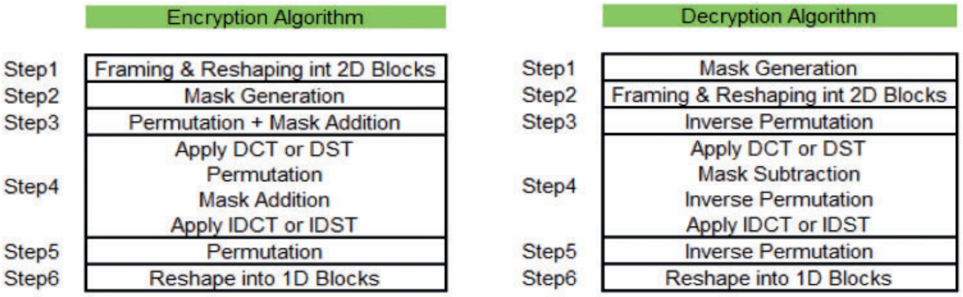
Figure 1: Discretized baker map

The pseudo-code for baker map can be presented as:

```
Input: 2D audio speech file X, row permutation matrix Bx, and column rearrangement matrix By
Output: Cipher Audio Speech File Y
read audio speech file
reshape into the two-dimension matrix
Initialize values for key used
Customized Function to construct matrix (mat) to hold operation into it, return its dimensions pr, pc
Loop1 start
    fill matrix (mat) with zeroes
    Shift +1 samples information and move samples information's positions by one (Permutation)
        loop2 start
          loop3 start
          loop4 start
          shift −1 and move samples information's positions by one in new matrix
          end loop4
          end loop3
              end Loop2
    write contents of filled matrix to output matrix
end loop1
reshape into one dimension
write speech file
```

3 Audio Cryptosystem

The audio cryptosystem used in recent research [7] can be represented as shown in Fig. 2, and it discussed the results based on time-domain (TD), discrete cosine transform (DCT) [22–25] and discrete sine transform (DST).



(a) Encryption Algorithm (b) Decryption Algorithm

Figure 2: Recent audio speech cryptosystem [7]

As depicted in Fig. 2, the encryption algorithm has the following steps:

a) Employ reformatting for the input audio signal via framing and reshaping from 1D to 2D segments.

b) Employ mask generation using the secret key and the baker map.

c) Employ the shuffling utilizing the baker map. First, audio samples are permuted, followed by substitution, to alter the audio sample amplitudes by summing their values to the mask's value.
d) Employ TD or transform domain like DCT or DST, followed by permutation using the baker map, then substitution by mask adding and finally employing the inverse transform (IDCT or IDST).
e) Employ permutation using the baker map.
f) Employ reshaping into a 1D format, a suitable format to store the audio information.

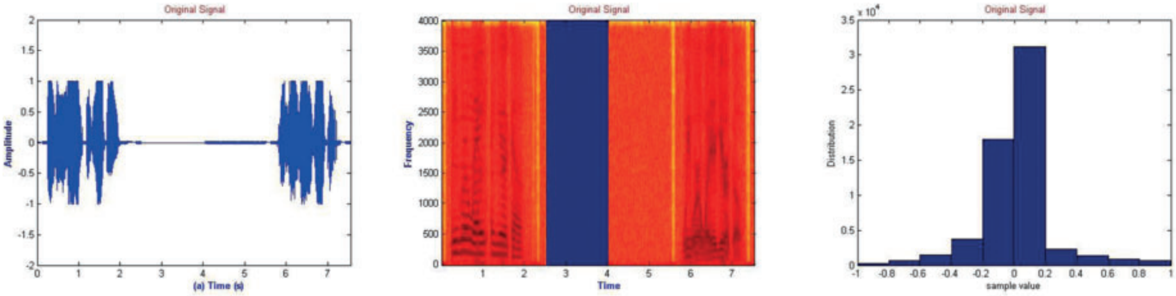
The decryption algorithm consists of the following steps:

a) First, employ mask generation using the secret key and the baker map.
b) Reformat the input audio signal via framing and reshaping from 1D to 2D segments.
c) Employ the inverse shuffling utilizing the baker map, in which audio information samples are rearranged to their original locations.
d) Employ TD or transform domain like DCT or DST, followed by inverse substitution. The inverse permutation using baker map, and finally employ the inverse transform (IDCT or IDST).
e) Employ the substitution (subtract mask) followed by the inverse permutation utilizing the baker map.
f) Employ reformatting for the audio signal via framing and reshaping from 2D to 1D segments,
g) Reshape into a 1D format, a suitable format to store the audio information.

In this paper, advanced code is added to the system to analyze, extend the study, and apply statistics functions to help in analysis for optimization's study.

4 Simulation Results

The hardware specification used in this simulation is an HP Pavilion g-series laptop with an intel® Core™ i3 CPU M370 2.40 GHz processor and 12 GB RAM. The simulation is done using Matlab (R 2017a). The used speech sample is the artificial speech that consists of four parts, as shown in Fig. 3 and Tab. 1.



(a) Plain speech (b) Spectrogram of plain speech (c) Histogram of plain speech

Figure 3: Illustration of the original speech signal, its spectrogram and histogram

Table 1: Specifications of audio speech sample

	Duration in s	Content	Speaker's sex
First part	2.5	The sentence "we were away years ago."	Female
Second part	1.5	Ideal silence without noise	Silence
Third part	1.5	Non-perfect silence with noise	Silence
Fourth part	2.5	The sentence "we were away years ago."	Male

The first and last parts are of the length of 2.5 s represent a female says the sentence "we were away years ago". A male says the same sentence in the fourth part. The third part consists of ideal silence without the noise of 1.5 s length and followed by part three of length 1.5 s of non-perfect silence with noise.

In the recent research introduced by Mosa et al. [7], a secret key used, let call it Key 1 with 13 sub-keys used, and the sum of sub-keys equals 64, which represents the audio speech block size used, with another two secret keys generated for testing by altering the positions of two sub-keys in the key, let call these two keys are Key 2 and Key3. In this research, a secret key with different sub-keys values will be used, termed as Key_1, with the same number of sub-keys of the same sum of sub-keys which is 64, another two keys Key_2 and Key_3, are generated by altering the positions of two sub-keys in the sub-key (key_1), for the testing purposes in this paper. The same code used by recent research [7] will be used and applied on the same sample speech signal and within the same testing environment.

4.1 TD Analysis

4.1.1 Values of Sub-keys

As shown from Tab. 2, Key 1, Key 2 and Key 3 represent keys used with recent research [7], while Key_1, Key_2 and Key_3 define keys used in this research. It is apparent from Tab. 2 that the keys used in this research exhibit best values for correlation coefficient (CC)'s values represented in Key_2 same as the value for key1 in recent research [7], For the values of spectral distortion (SD), it is evident that value for Key_3 represents the best value compared with values defined in recent research [7]. This means that better quality can be achieved for the audio cryptosystem by only changing the values of sub-keys.

The testing environment in terms of hardware, software, operating System specifications and Matlab for recent research [7] was not mentioned. Still, we will compare its results with its well-known testing environment as described.

Even when comparing values presented in recent research [7] with values presented in this paper, both results are obtained in a different testing environment. For example, it is apparent from Tab. 3 that key3 used in recent research [7] exhibits the best value for correlation coefficient (CC) among values represented in this paper. Also, the value of spectral distortion (SD) for Key_3 has the best value compared with values defined in recent research [7]. This is evidence that better quality can be achieved for the audio cryptosystem by changing the sub-keys values even in a different testing environment. In summary, with TD, there is no specified or well-defined rule for choosing values of sub-keys to get the best quality and security for the audio cryptosystem.

Table 2: TD analysis of values of sub-keys with the same testing environment

DCT		Encryption	
		CC	SD
Recent system in [7]	Key 1	−0.00180	21.26570
	Key 2	0.00250	21.40520
	Key 3	0.00640	21.37230
This research study	Key_1	0.00094	21.37000
	Key_2	−00180	21.35400
	Key_3	0.00160	21.72900

Table 3: TD analysis of values of sub-keys with different testing environment

DCT		Encryption	
		CC	SD
Recent system in [7]	Key 1	0.01000	15.18290
	Key 2	0.01370	15.59480
	Key 3	−0.000140	16.63680
This research study	Key_1	0.00094	21.37000
	Key_2	−0.00180	21.35400
	Key_3	0.00160	21.72900

4.1.2 Number of Sub-keys – Secret Key Size & Audio Speech Block Size

In the search for the best number of sub-keys that give the best quality for audio speech cryptosystem, the secret key must adhere to the following rules:

- The sum of sub-keys values in the secret key must equal to block size of the audio speech signal.
- Any sub-keys value must be divisible by the audio speech block's size.
- The maximum number of available secret keys = (audio speech block's size – 4), because the following conditions will make the secret key easy to be broken so that it will be ignored:
- The number of sub-keys <> block size/2, so will ignore the secret key that consists of sub-keys with same equal values, in case of block size equals 64, will forget the secret key with 32 sub-keys, each sub-key value is 2.
- Values of all sub-keys must not be the same, so will ignore the secret key with sub-key values of the same values; in the case of block size equals 64, will ignore the secret key with 64 sub-keys because all sub-key values will be of a value 1.
- Also, if the secret key with only one sub-key of a value equals block size in case of block size equals 64, we will ignore the secret key with one sub-key because the secret key will be only one sub-key, and its value is 64.
- Finally, we will ignore the secret key with only two sub-keys; each value equals block size/2 if block size equals 64. Likewise, we will ignore the secret key consisting of only two sub-keys sub-key with a value of 32.

From these conditions, the number of applicable secret keys is formulated in the following equation:

$$\text{Number of secret keys} = (\text{Block size - 4}) \tag{1}$$

where, Block size > 4

Tab. 4 represents the relation between audio speech signal block size in byte and the number of available secret keys used with this audio speech signal; this equation can be applied on all block sizes starting from 4 and multiples of 64 bytes. For block size equals or less than 4 bytes, the number of secret keys will be zero, so it will not be considered and not be applicable in this research. For example, tests executed in this paper use an audio speech block size of 64 bytes, so there is up to 60 secret keys, for keys with the number of sub-keys equals 1, 2, 32 or 64 are not applicable according to Eq. (1) and will not be used in simulation tests.

Table 4: Relation between block size of the speech signal and number of sub-keys

Audio speech signal block size in bytes	4	8	16	32	64	128	256	512	1024
Number of applicable secret keys	0	4	12	28	60	124	252	508	1020

For the encryption algorithm, the experimental results demonstrate that the best value for correlation coefficient (CC) is for a key with the number of sub-keys equals to five and worst for the key consisting of 53 sub-keys. For spectral distortion (SD), the best value for a key consists of 34 sub-keys and the worst value for a key consists of 63 sub-keys. For the Log-Likelihood Ratio (LLR), the best value for a key consists of 20 sub-keys and the worst value for a key consists of 60 sub-keys. In conclusion, the best values are obtained using a key with a number of sub-keys not greater than 34 sub-keys. The correlation coefficient (CC) has the same value for all possible keys for the decryption algorithm. The SD has the best value for a key with 63 sub-keys and the worst value for a key with 23 sub-keys, and LLR has the best value with a key of 63 sub-keys and the worst value with 48 sub-keys.

In conclusion, decryption with TD gives the best values when the number of sub-keys equals 63. So, in summary, to get the best quality for encryption with TD, use the number of sub-keys not greater than 34 sub-keys and the best quality for decryption when the number of sub-keys is 63. Also, the keys with the number of sub-keys 5, 6 and 7 sub-keys give the best quality for the audio cryptosystem.

For optimization and analysis, detailed statistics functions are applied. The secret keys that consist of sub-keys not greater than 34 sub-keys, or keys with the number of sub-keys equal 5, 6 and 7, give the best results for better security and quality for audio cryptosystem in TD.

4.1.3 Number of Applicable Secret Keys

In the search for the possible applicable number of keys that can be used in TD that give best results for audio cryptosystem, will apply permutation and probability law [26], and Eq. (1), and all its governing presented conditions on the number of sub-keys that give best quality and security results driven from the previous sub-section which are 5, 6 and 7 sub-keys. From Tab. 5, there are approximately 5880 possible applicable keys from the region of the best keys that offer the best quality for audio speech cryptosystem with the TD. There are 120, 720 and 5040 secret keys generated from sub-keys sizes 5, 6 and 7, respectively, considering that some secret keys are repeated.

Table 5: TD analysis of values of the available number of secret keys that give best quality results

Number of applicable Sub-keys	5	6	7	
Number of possible keys	120	720	5040	5880

4.2 DCT Analysis

4.2.1 Values of Sub-key

It is apparent from Tab. 6 that the keys used in recent research [7] exhibit the best values for both correlation coefficient (CC) and spectral distortion (SD) represented by Key 3 even when comparing values presented in recent research [7] with values presented in this paper in which both results obtained in a different testing environment.

It is apparent from Tab. 7 that key_1 and key_2 used in this research exhibit the best value for correlation coefficient (CC) and spectral distortion (SD), among other values in Tab. 7. This is evidence that better quality can be achieved for the audio cryptosystem by changing the sub-keys values. In summary, with the DCT, there is no specified or well-defined rule for choosing values of sub-keys to get the best quality and security for the audio cryptosystem.

Table 6: DCT analysis of values of sub-keys with the same testing environment

DCT		Encryption	
		CC	SD
Recent system in [7]	Key 1	0.00300	15.73610
	Key 2	0.00160	15.83900
	Key 3	−0.00002	15.84580
This research study	Key_1	0.00065	15.83010
	Key_2	0.00140	15.83810
	Key_3	0.00270	15.684470

Table 7: DCT analysis of values of sub-keys with different testing environment

DCT		Encryption	
		CC	SD
Recent system in [7]	Key 1	0.00230	14.25500
	Key 2	0.00240	14.21920
	Key 3	0.00270	14.05680
This research study	Key_1	0.00065	15.83010
	Key_2	0.00140	15.83010
	Key_3	0.00270	15.68470

4.2.2 Number of Sub-keys – Secret Key Size & Audio Speech Block Size

For the encryption algorithm's analysis, the best value for correlation coefficient (CC) is for a key with the number of sub-keys equals 21 and the worst for a key consists of 52 sub-keys. For spectral distortion (SD), the best value for a key consists of 3 sub-keys, and the worst value for a key consists of 34 sub-keys. For the Log-Likelihood Ratio (LLR), the best value for a key consists of 3 sub-keys and the worst value for a key consists of 51 sub-keys. In conclusion, the best values for encryption with the DCT are using a key with the number of sub-keys not greater than 21 sub-keys. Also, it is better to consider a key with three sub-keys as the best choice for the best quality for encryption.

For decryption analysis, the correlation coefficient best value (CC) is for a key with a number of sub-keys equals eight and the worst for a key consists of 63 sub-keys. The SD has the best value for a key with three sub-keys and the worst value for 63 sub-keys. The LLR has the best value with a key of 7 sub-keys and the worst value with 61 sub-keys. In conclusion, the decryption with DCT gives the best values when the number of sub-keys is with a lower number of sub-keys in the range of {3–8} sub-keys, while it gives the worst results with the number of sub-keys equals 63 sub-key.

Also, it is seen that a key with sub-keys = 3, 4, 6 and 7 sub-keys give the best results, but will consider only sub-keys = 6 and 7, as 3 and 4 sub-keys represents weak keys easily to be broken or known. Several sub-keys not higher than 15 will give the best results for both encryption and decryption with cryptosystem in DCT, and in specific, with the number of sub-keys equal 6 and 7 sub-keys.

4.2.3 Number of Applicable Secret Keys

In the search for a possible applicable number of keys used in DCT, we will apply permutation and probability law [26] and Eq. (1) on the number of sub-keys that give the best quality and security results from the previous sub-section, which are 6 and 7 sub-keys.

From Tab. 8, there are a total approximate number of 5760 possible applicable keys from the region of the best keys that offer the best quality for audio speech cryptosystem with DCT, and there are 720 and 5040 secret keys that can be generated from sub-keys sizes 6 and 7 respectively, considering that some secret keys are repeated.

Table 8: DCT analysis of values of the available number of secret keys that give best quality results

Number of applicable Sub-keys	6	7	
Number of possible keys	720	5040	5760

4.3 DST Analysis

4.3.1 Values of Sub-key

It is apparent from Tab. 9 that the Key_3 exhibits the best values for both correlation coefficients (CC) and spectral distortion (SD) even when comparing values presented in recent research [7] with values presented in this paper in which both results obtained in a different testing environment.

It is apparent from Tab. 10 that Key_3 and Key1 exhibit the best value for correlation coefficient (CC) and spectral distortion (SD), respectively, among other values presented in Tab. 10. This is evidence that better quality can be achieved for audio cryptosystem by merely changing sub-keys values even in a different testing environment. In summary, with DST, there is no specified or well-defined rule for choosing values of sub-keys to get the best quality and security for the audio cryptosystem.

Table 9: DST analysis of values of sub-keys with the same testing environment

DCT		Encryption	
		CC	SD
Recent system in [7]	Key 1	0.00340	15.41160
	Key 2	0.00400	15.33220
	Key 3	0.00120	15.39330
This research study	Key_1	0.00230	15.49430
	Key_2	0.000834	15.411
	Key_3	−0.0032	15.5731

Table 10: DST analysis of values of sub-keys with different testing environment

DCT		Encryption	
		CC	SD
Recent system in [7]	Key 1	0.00130	16.30530
	Key 2	0.00110	15.31230
	Key 3	−0.00120	14.16670
This research study	Key_1	0.00230	15.49430
	Key_2	0.000834	15.41100
	Key_3	−0.0032	15.57310

4.3.2 Number of Sub-keys – Secret Key Size & Audio Speech Block Size

For the encryption algorithm's analysis with DST, the best value for correlation coefficient (CC) is for a key with a number of sub-keys equals six and the worst for a key consists of 60 sub-keys. Likewise, for spectral distortion (SD), the best value for a key consists of 3 sub-keys and the worst value for a key consists of 33 sub-keys. Finally, for the Log-Likelihood Ratio (LLR), the best value for a key consists of 6 sub-keys and the worst value for a key consists of 24 sub-keys. Therefore, it is concluded that the best values for encryption with DST when using a key with the number of sub-keys is in the range {3–6} sub-keys. Also, we can consider a key with six sub-keys as the best choice for the best quality of encryption.

For the decryption analysis, the correlation coefficient (CC) best value is for a key with a number of sub-keys equals four and the worst for a key consists of 63 sub-keys. SD has the best value for a key with four sub-keys and the worst value for 63 sub-keys. The LLR has the best value with a key of 8 sub-keys and the worst value with 28 sub-keys. It is concluded that decryption with DST gives the best values when the sub-keys are in the range {4–8} sub-keys. In summary, a key with four sub-keys is the best choice for the best quality for decryption.

Also, the key with sub-keys in the range {3–12} sub-keys gives the best combined results. Sub-keys of 5 and 6 provide the best results.

4.3.3 Number of Applicable Secret Keys

In the search for a possible applicable number of keys that can be used in DST, will apply permutation and combination law [26] and represented in Eq. (1) on the number of sub-keys that give best quality and security results driven from the previous sub-section, which are 5 and 6 sub-keys.

From Tab. 11, there are approximately840 possible applicable keys from the region of the best keys that offer the best quality for audio speech cryptosystem with DST. Also, 120 and 720 secret keys can be generated from sub-keys sizes 5 and 6, considering that some secret keys are repeated.

Table 11: DCT analysis of values of the available number of secret keys that give best quality results

Number of applicable Sub-keys	5	6	
Number of possible keys	120	720	840

5 Conclusions

Values of sub-keys and the number of sub-keys used in any audio speech cryptosystem play an essential role in how much the audio system is secure and qualified. It is concluded from tests and simulation results that better quality and more audio secure cryptosystem is obtained when changing the used sub-keys. However, there is no well-defined rule for how to choose values of sub-keys. Also, there is a direct relationship between the applicable number of sub-keys, audio speech block size, and functional secret keys. Finally, each transform domain has a specific range of sub-keys that must be used to get the best quality and security results, and not all transform domains have the same range of the number of sub-keys. This conclusion will help in future research, especially which may be for comparison issues and optimizations.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia for supporting this research work.

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] S. B. Sadkhan and N. A. Abbas, "Performance evaluation of speech scrambling methods based on statistical Approach," *Atti Della Fonadzione Giorgio Ronchi*, vol. 66, no. 5, pp. 601–6014, 2011.

[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] 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, no. 1, pp. 241–261, 2020.

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

[5] 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.

[6] O. S. Faragallah, M. Farouk, H. S. El-sayed and M. A. M. El-bendary, "Secure audio transmission over wireless uncorrelated rayleigh fading channel," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1604–1615, 2021.

[7] E. Mosa, N. W. Messiha, O. Zahran and F. E. Abd El-Samie, "Chaotic encryption of speech signals," *International Journal of Speech Technology*, vol. 14, no. 4, pp. 285–196, 2011.

[8] O. S. Faragallah, M. A. AlZain, H. S. El-sayed, J. F. Al-Amri, W. El-Shafai *et al.,* "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.

[9] X. Tong, "Design of an image encryption scheme based on a multiple chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 7, pp. 1725–1733, 2013.

[10] M. Bhaskar and T. Mandal, "A multilevel security scheme using chaos based encryption and steganography for secure audio communication," *International Journal of Research in Engineering and Technology (IJRET)*, vol. 2, no. 10, pp. 399–403, 2010.

[11] O. S. Faragallah, A. Afifi, I. F. Elashry, E. A. Naeem, H. M. El-Hoseny *et al.,* "Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform," *Optical and Quantum Electronics*, vol. 53, no. 305, pp. 1–26, 2021.

[12] 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.

[13] A. M. Elshamy, A. N. Z. Rashed, A. E. A. Mohamed, O. S. Faragallah, Y. Mu *et al.,* "Optical image encryption based on chaotic baker map and double random phase encoding," *Journal of Lightwave Technology*, vol. 31, no. 15, pp. 2533–2539, 2013.

[14] O. S. Faragallah, H. S. El-sayed, A. Afifi and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 137, no. 6, pp. 106333, 2021.

[15] S. Rajesh, V. Paul, V. G. Menon and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 393, 2019.

[16] W. Xingyuan and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[17] O. S. Faragallah, M. A. AlZain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai *et al.,* "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 77, no. 3–4, pp. 1–25, 2020.

[18] O. S. Faragallah, W. El-Shafai, A. Afifi, I. Elashry, M. A. AlZain *et al.,* "Efficient three-dimensional video cybersecurity framework based on double random phase encoding," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 253–367, 2021.

[19] S. Thakur, A. K. Singh, S. P. Ghrera and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for telehealth applications," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3457–3470, 2019.

[20] O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E. M. El-Rabaie *et al.,* "Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, pp. 1215–1239, 2022.

[21] R. Roman, J. Lopez and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, no. 4, pp. 680–698, 2018.

[22] J. Chaharlang, M. Mosleh and S. Rasouli-Heikalabad, "A novel quantum steganography-steganalysis system for audio signals," *Multimedia Tools and Applications*, vol. 79, no. 25–26, pp. 17551–17577, 2020.

[23] 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, no. 20, pp. 62–69, 2019.

[24] M. A. M. El-Bendry and A. E. A. Azzm, "Complexity considerations: Efficient image transmission over mobile communications channels," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16633–16664, 2019.

[25] 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.

[26] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz-logistic chaotic map," *Multimedia Tools and Applications*, vol. 79, no. 25–26, pp. 17817–17835, 2020.