



Transmission and Decryption of the Audio Signal Masked with ECG by FDM Method

I. Parlar¹ · M. N. Almali¹ · O. Atan¹ · A. C. Cabuker¹ · O. Silahtar¹

Received: 22 December 2021 / Accepted: 12 June 2022 / Published online: 4 July 2022
© The Author(s), under exclusive licence to Shiraz University 2022

Abstract

Today, the use of these methods as hybrids has provided the motivation to be a solution to important problems, since the existing methods are insufficient at some points in ensuring the security of personal data. In data security, the inability to decrypt and decrypt the signal to be encrypted retrospectively has always been the subject of research in terms of privacy. At this point, it was preferred to use the electrocardiography (ECG) signal, which is a signal that shows the vital signs of the human body and is also difficult to copy. In the study, firstly, the emulator circuit was obtained by using the mathematical model of the ECG signal. With this obtained signal, the audio signals are masked. The audio signal masked on the transmitter side and the signals providing synchronization were transmitted to the receiver side over a single channel using the frequency division multiplexing (FDM) method. Then, the sliding mode control (SMC) method was chosen for the synchronization of the ECG emulator circuits on the receiver and transmitter side. Histogram, spectral, mean square error (MSE), peak signal to noise ratio (PSNR), key space and key sensitivity, NSCR (number of sample change rate), UACI (unified average changing intensity) and PESQ (perceptual evaluation of speech quality) analyses were used to check the accuracy of the system. These analyses showed that the ECG encoding method has faster unit change, reduces synchronization time, minimizes losses and improves the security of the masked signal compared to other methods sent from two channels. Finally, use of an arrhythmia ECG signal for the synchronization signal on both the transmitter and receiver sides, the synchronization of this signal with the SMC method and the testing of a live audio recording in addition to the conversation, distinguishes the study from other existing studies and reveals its originality.

Keywords ECG emulator · FDM method · Sliding mode control · Security analytics · Spectral entropy · Encryption

1 Introduction

Some chaotic signals that can cause security problems, especially in the transmission channel, ECG signals with sudden amplitude changes, non-repeating, periodic and non-continuous chaotic behavior have been one of the biggest reasons for preference. In addition, when these signals are displayed in real time, they create a kind of chaotic signal behavior because they do not repeat themselves, especially in people with arrhythmia. During the human body, the heart rate can change instantaneously due to the increase and decrease in sleep or movements during exertion (Cilhoroz et al. 2021; Felber et al. 2008). These are important factors that can cause arrhythmia as well as increase the uniqueness of the signal (Chen et al. 2012; Chua 1992; Chua et al. 1993; Ebrahimi et al. 2020; Huang et al. 2016; Lorenz 1963; Quiroz-Juárez et al. 2019; Sprott

✉ I. Parlar
ishakparlar@yyu.edu.tr

M. N. Almali
mna1@yyu.edu.tr

O. Atan
oatan@yyu.edu.tr

A. C. Cabuker
alicancabuker@yyu.edu.tr

O. Silahtar
onursilahtar@yyu.edu.tr

¹ Department of Electrical and Electronics Engineering, Faculty of Engineering, Van Yuzuncu Yil University, 65090 Van, Turkey

2000). Therefore, one of our biggest motivations has been that the chaotic signals available in encrypted communication systems do not have fast amplitude changes to encrypt the data signal. Following this motivation, firstly, the emulator circuit was obtained by using the mathematical model of the ECG signal in this study. With this obtained signal, both masking and decoding of the audio signals were performed (Amr et al. 2019; Kakade et al. 2014; Li et al. 2020; Naskar et al. 2019). Since the ECG signal cannot be used simultaneously on both receiver and transmitter side in real time, the emulator circuit is preferred. It is ensured that these identical emulator circuits are located on the transmitter and receiver sides of the communication in the same way.

The emulator circuit acts as a chaotic oscillator that encodes and decodes audio signals. In order for the ECG emulator used throughout the system to work without delay on the receiver and transmitter side, synchronization of both emulators was provided by the SMC method (Xia et al. 2011). In addition, providing communication over a single channel using the FDM method has provided an advantage over existing two-channel communication systems. A guard band was created by calculating the frequency band gaps for each channel so that the audio signals do not overlap. These signals, which are intended to be transmitted to the receiver side, are precisely separated from each other with the help of analog filters. Assuming that the noise during acquisition of ECG signals is natural and that the variability of electrocardiograms depends on many factors (emotional state, diet, whether the person is making a physical exertion or resting, etc.), it is impossible to obtain an ECG signal the same way on both the transmitter and receiver side. The crucial aspects of transmitting the arrhythmia ECG masked audio signal with the FDM method can be described as follows:

- In the simulation, improvement of the FDM performance during encoding of both a conversation and a live recording with the proposed method.
- The presence of identical and arrhythmia ECG emulators on the receiver and transmitter side in chaotic communication has created an important advantage. In this way, it is aimed to contribute to the improvement of the overall performance of the system.
- Use of an arrhythmia ECG signal for the synchronization signal on both the transmitter and receiver sides, the synchronization of this signal with the SMC method and the testing of a live audio recording in addition to the conversation, distinguishes the study from other existing studies and reveals its originality.
- Compared to the chaotic signals used in classical coding, ECG is faster in coding due to its dynamic movement in case of arrhythmia. It also increases the

corruption of data to be encrypted and makes it difficult for unauthorized persons to access the data.

- ECG arrhythmia, which can occur in different types, further increases the analysis of data by unauthorized persons (İzci et al. 2020; Karataş 2021).
- Performing various security analyses and tests reveals the efficiency and performance of this study.

The remainder of the paper is arranged into several sections. Section 2 delineates the ECG system design and FDM method in detail. Section 3 explains the configuration and description of the proposed masking scheme and also theoretical analysis and system of synchronization. The proposed masking scheme is comprehensively explained to investigate the safety and quality of the masking in Sect. 4. Section 5 draws the main conclusions and future scope of the paper.

2 Methodology

2.1 ECG System Design

If the nonlinear variants x_1 – x_6 of the discretized (Barrio–Varea–Aragon–Maini) BVAM model are associated with natural pacemakers, the action potentials of the (sinoatrial) SA node, (atrioventricular) AV node and His–Purkinje complex are represented by coupled three oscillators. From the numerical integration of the ECG general system, it was seen that the variables x_1 , x_5 and x_2 , x_6 respectively, are not independent from each other due to symmetry. Thus, the system has become even smaller. The resulting equivalent system of equations is expressed as $x_2 = x_6$, which gives the result $x_1 = x_5$.

Here, β , C and H are parameters of the system. Finally, the system has become simpler by being reduced to a four-component (ordinary differential equations) ODE systems that are viewed as below (Quiroz–Juárez et al. 2019):

$$\begin{aligned}\dot{x}_1 &= x_1 - x_2 - Cx_1x_2 - x_1x_2^2 \\ \dot{x}_2 &= Hx_1 - 3x_2 + Cx_1x_2 + x_1x_2^2 + \beta(x_4 - x_2) \\ \dot{x}_3 &= x_3 - x_4 - Cx_3x_4 - x_3x_4^2 \\ \dot{x}_4 &= Hx_3 - 3x_4 + Cx_3x_4 + x_3x_4^2 + 2\beta(x_2 - x_4)\end{aligned}\quad (1)$$

Since the ECG signal is a composite of waves of different amplitudes from different parts of the heart, the ECG signal is thought to be a linear mix of electrical activations of the main pacemakers of different strengths. In this way, signals very similar to ECG signals can be produced with variables x_i . Also, α_i coefficient shows the behavior of ECG emulator system. Control parameters of arrhythmia ECG emulator for $H = 2.7126$, $C = 1.35$ and $\beta = 4$. These specified values constitute limits approach of the

arrhythmia ECG signal. Otherwise, the ECG signal without arrhythmia reduces the performance of the system. Signals that closely resemble ECG signals can be generated by an adequate linear combination of the variables x_i on depend time (t) (Gois et al. 2009):

$$ECG(t) = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 \quad (2)$$

This chaotic emulator provides an advantage in encryption operations as it has faster output responses than the Sprott chaotic (Gupta et al. 2019).

2.2 Frequency Division Multiplexing Method

Frequency division multiplexing method enables the transmission of signals over a single channel in the communication to be made with the receiver and transmitter. On the basis of frequency division multiplexing, it is based on placing the signals on the frequency band without overlapping each other by performing double sideband amplitude modulation. The signals placed in the frequency band are separated by high-grade filters on the receiver side and returned to their original state (Rao 2018; Wu 2010; Rajabpour-Moghaddam et al. 2014).

In the study, masked audio signal and synchronization signals (x_1, x_2, x_3, x_4) were transmitted from a single channel using different carrier signals for synchronization of ECG emulator circuits. In double sideband amplitude modulation, $x_1 - 2.5kHz, x_2 - 7.5kHz, x_3 - 12.5kHz, x_4 - 17.5kHz$, the masked audio signal is modulated with $35kHz$ carrier signals. The mathematical expression of double sideband amplitude modulation is as follows:

$$\begin{aligned} m(t) * c(t) &= V_m \cdot \cos(W_m(t)) * V_c \cdot \cos(W_c(t)) \\ &= ((V_m V_c)/2)[\cos(W_m + W_c) + \cos(W_m - W_c)] \end{aligned} \quad (3)$$

3 Configuration and Description of the Proposed Masking Scheme

The general purpose of this system is to communicate between the receiver and the transmitter over a single channel for reduces noise with 8th-order Chebyshev type II filter.

On the transmitter side; the ECG signal (x_1) received from the master ECG emulator circuit is received as a chaotic response. The frequency modulator then generates a unique key for the system based on the chaotic movement of the ECG signal. Encryption is performed by adding the generated key to the audio. The encrypted audio signal and x_1, x_2, x_3 and x_4 , which will provide synchronization, are transmitted over the same channel by frequency division

multiplexing method. The frequency division multiplexing method allows signals to be transmitted with the help of amplitude modulation. Signals are transmitted using carrier signals with specific frequencies.

On the receiver side; the received signals are separated by analog filters according to their frequency. Signals separated on the receiver side enter a controller, ensuring the synchronization of the emulator circuits on the receiver and transmitter side, and the password on the audio is removed.

In order to remove unauthorized users' access to data in the communication channel, the masked signal c was obtained by masking the message signal m , the chaotic signal together with the k switch. Mathematical expression of c masking signal is as follows:

$$c = f(m, k) \quad (4)$$

The masked signal obtained from the frequency division multiplexing channel was decoded after synchronization with the SMC. It is seen that \hat{m} given in Eq. (5) is approximately equal to the message signal given in Eq. (4).

$$\hat{m} = f(c, k) \quad (5)$$

The detailed step-by-step description of the proposed masking scheme encryption is given in the flowchart shown in Fig. 1.

In the proposed encryption diagram in Fig. 1, the ECG signal, which has chaotic dynamics from the ECG master circuit, produces an analog key in frequency modulation since it has a fast heart arrhythmia feature. The audio signal is encrypted with this generated analog key. As in chaotic communication, the oscillators (ECG) on the receiver and transmitter side must be synchronized in real time in order to perform the decoding process. Therefore, it is necessary to send signals to ensure synchronization from the ECG master circuit. In order to send these signals over the same channel, frequency division multiplexing method was used. On the receiver side, the signals transmitted with certain carrier frequencies are separated with the help of analog filters. Then, the synchronization between the two ECG circuits was ensured and the original data was reached by removing the analog switch from the ECG slave circuit from the signal. The synchronization of the proposed system was carried out with sliding mode modulation.

3.1 Synchronization with Sliding Mode Control

There are many SMC applicable in the field of hyperchaotic communication in the literature (Al-sawalha et al. s; Azar et al. 2018; Rajagopal et al. 2017). In this section, synchronization of identical hyperchaotic systems is performed using sliding mode control and Lyapunov stability

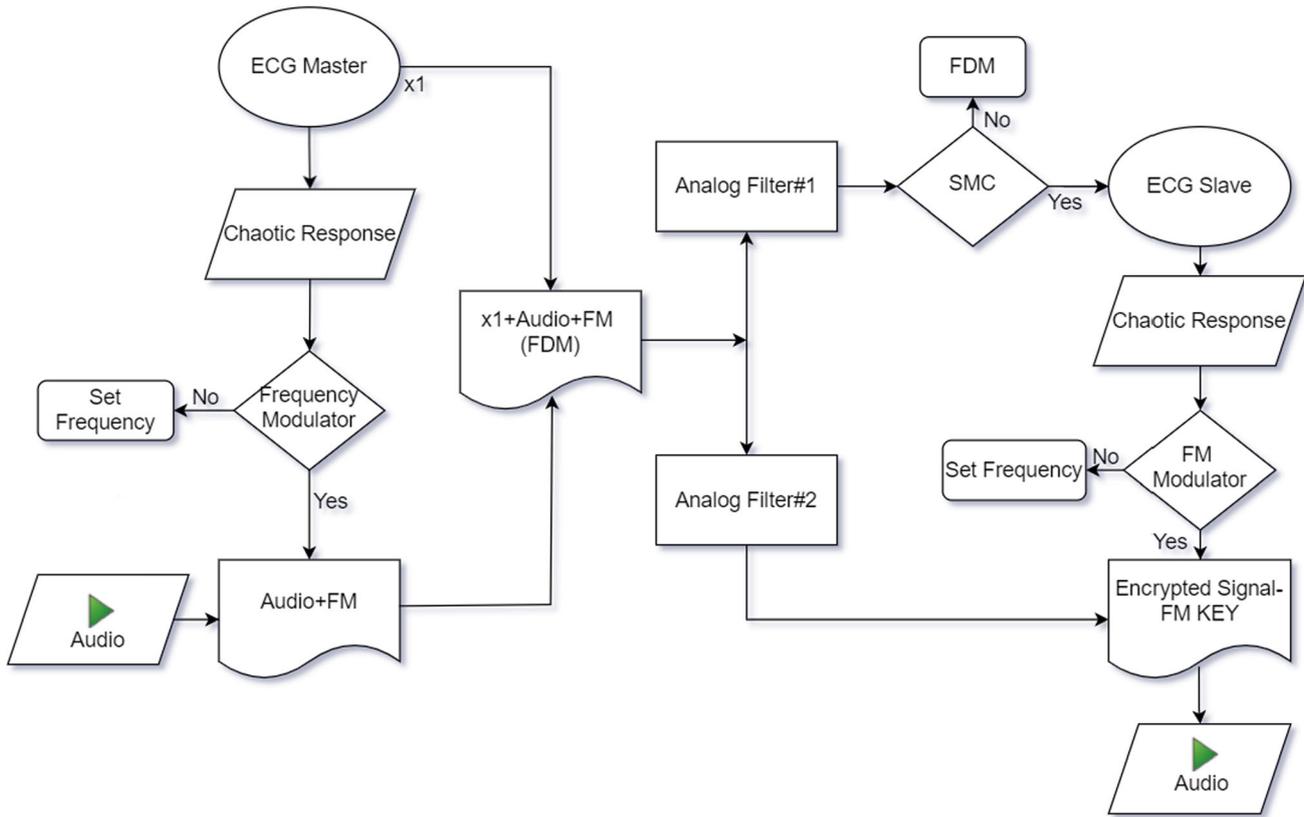


Fig. 1 Flowchart of the proposed masking scheme

theory (Hahn 1967). Let the hyperchaotic system be formulated as follows:

$$\dot{x} = Ax + f(x, t) \tag{6}$$

where $x \in R^n$ the state of the system, $A \in R^n \times R^n$ is the matrix of the system parameters, and $f : R^n \rightarrow R^n$ is the nonlinearity function of the system. This system is chosen as master or drive system. Also slave or response system is described as follows in Eq. (7). The general structure of the frequency division multiplexing-based ECG chaotic masking system is shown in Fig. 2.

$$\dot{y} = Ay + g(y, t) + \Delta g(y, t) + d(t) + u \tag{7}$$

$\Delta g(y, t)$ is the uncertain term which represents unmodeled dynamics or variations and $d(t)$ is external bounded disturbance. In this study, $\Delta g(y, t) + d(t) = 0$ is assumed. Also $u \in R^n$ is the control input, $g : R^n \rightarrow R^n$ is the nonlinear part of the slave system, and $y \in R^n$ is the state of the system. The nominal form in Eqs. (6) and (7) can be obtained from Eq. (1). Additionally main subject of this section is synchronization of two identical systems in Eqs. (6) and (7) for different initial conditions. Control input in Eq. (7) is designed to provide for the following condition: $\lim_{t \rightarrow \infty} \|e(t)\| \rightarrow 0$ where $e(t) = [e_1(t), e_2(t), e_3(t), e_4(t)]^T$ such that $e_i(t) = y_i - x_i$ for $i \in \{1, 2, 3, 4\}$. In

(Hahn 1967; Nagamalai et al. 2011; Meghanathan et al. 2012), the error dynamics and control parameters are obtained as;

$$\dot{e} = Ae + \eta(x, y) + u \tag{8}$$

where $\eta(x, y) = g(y, t) - f(x, t)$. Then, the control input u is defined as (Vaidyanathan et al. 2011);

$$u(t) = -\eta(x, y) + Bv(t) \tag{9}$$

where B is a constant gain vector selected such that (A, B) is controllable. Substituting Eq. (9) into (8), the error dynamics are obtained as;

$$\dot{e} = Ae + Bv \tag{10}$$

which is a linear time-invariant control system with single input v . Sliding surface is chosen as;

$$s = Ce = c_1e_1 + c_2e_2 + c_3e_3 + c_4e_4 \tag{11}$$

where $C = [c_1, c_2, c_3, c_4]$ is a constant vector. Equation (10) satisfies the following conditions when in sliding surface (s).

$$s(e) = 0 \text{ and } \dot{s}(e) = 0 \tag{12}$$

Using Eqs. (10) and (11), (12) is rewritten as;

$$\dot{s}(e) = C[Ae + Bv] = 0 \tag{13}$$

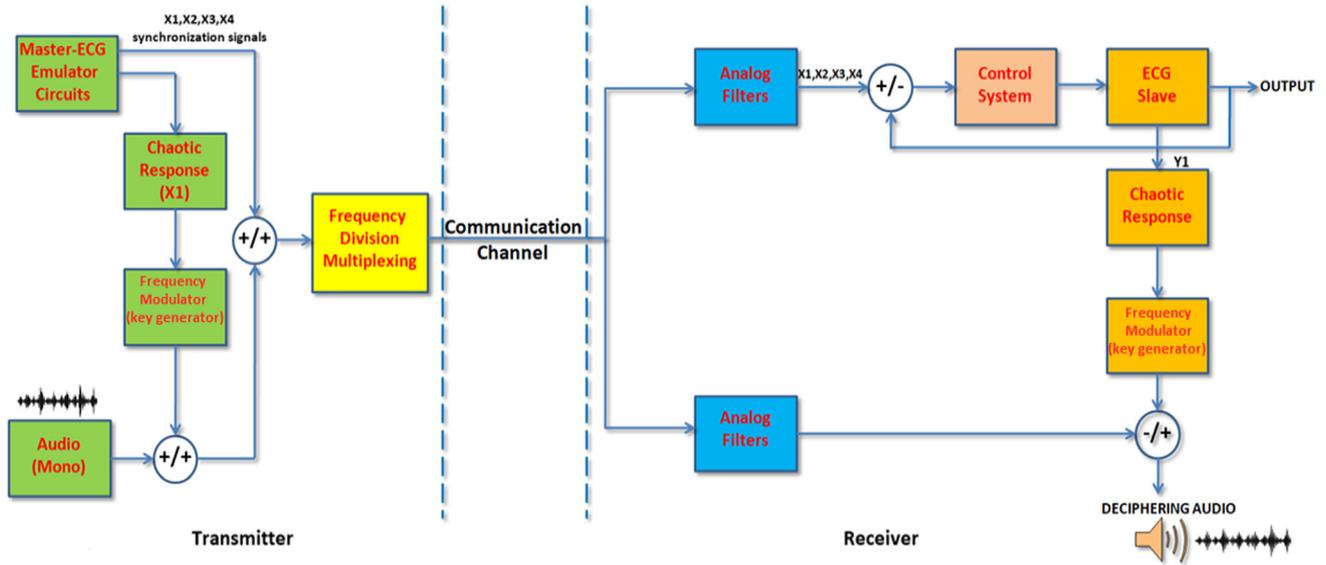


Fig. 2 Chaotic masking system scheme for audio transmission

Solving Eq. (13), the equivalent control law is obtained as follows;

$$v_{eq}(t) = -(CB)^{-1}CAe(t) \tag{14}$$

where C and B matrices must be chosen such that $CB \neq 0$. Using Eqs. (14), (15) is rewritten as;

$$\dot{e} = [I - B(CB)^{-1}C]Ae \tag{15}$$

where C and B are chosen such that the system matrix $[I - B(CB)^{-1}C]$ satisfies Hurwitz condition. Thus, Eq. (15) is globally asymptotically stable. The constant plus proportional rate reaching law is used to design sliding mode controller as follows, where $sgn(\cdot)$ denotes the sign function and constants $q > 0, k > 0$ are chosen.

$$\dot{s} = -q \cdot sgn(s) - ks \tag{16}$$

Finally, control input $v(t)$ is obtained as shown.

$$v(t) = -(CB)^{-1}[C(kI + A)e + q \cdot sgn(s)] \tag{17}$$

The controller designed above is simulated using MATLAB/Simulink. In the simulation, 4th-order Runge–Kutta method is used with the step size of 0.001s. In order for the MATLAB/Simulink program to provide fast and effective results, the step size interval is selected as 0.001 s by default. Increasing the step size value allows the simulation to be carried out quickly, but makes it difficult to observe how efficiently the controller is working. The time interval determined as the limitations of their approach is the most optimal value. Also initial conditions are chosen as; $x(0) = [x_1(0)x_2(0)x_3(0)x_4(0)] = [-0.10.20. 10.1]$ and $y(0) = [y_1(0)y_2(0)y_3(0)y_4(0)] = [-0.30.20.001 -0.5]$ then

$C = [11 - 2 - 2], B = [11 - 1 - 2]^T, q = 0.3$ and $k = 0.85$ are chosen. Simulation results are obtained as in Fig. 3. The results showed that the master and slave systems are synchronous and the synchronization system is stable.

4 Result Analysis and Performance Evaluation

There are many methods in the literature to investigate the safety and quality of the masking and encryption method applied to the sound signal (Almali et al. 2016; Sheu et al. 2010). Some of the most decisive analyses among these methods were used in this study;

- Histogram analysis
- Spectral entropy
- PSNR tests and MSE values
- Key space and key sensitivity analysis
- NSCR and UACI analysis
- PESQ analysis

In this section, comparisons of masking and decrypting processes applied on the audio signal were done.

In the comparison, it was observed that the audio signals were completely disturbed and the audio signal itself was obtained after the synchronization achieved while decrypting. The original, masked and decrypted form of speech is given in Fig. 4. As can be seen in the deciphering processes in Fig. 5, it was observed that the masking continued until the entire synchronization process. Synchronization takes place in a very short time. Thus, data loss on the receiver side is low.

Fig. 3 Synchronization of identical hyperchaotic system

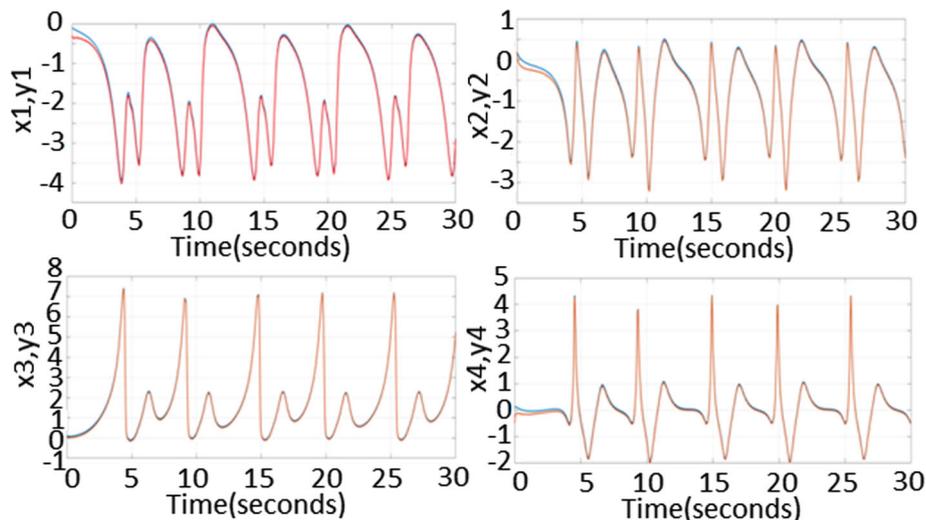


Fig. 4 Original/Masked/Decrypted audio signals

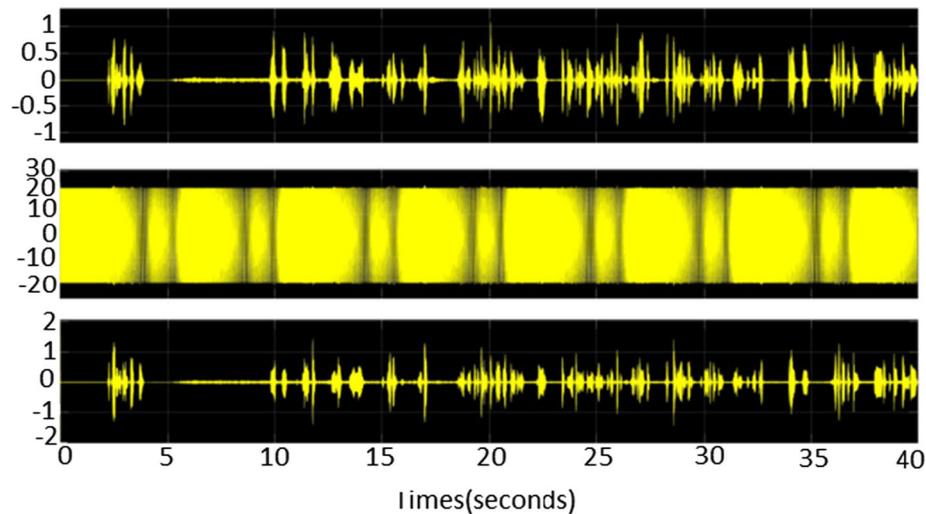
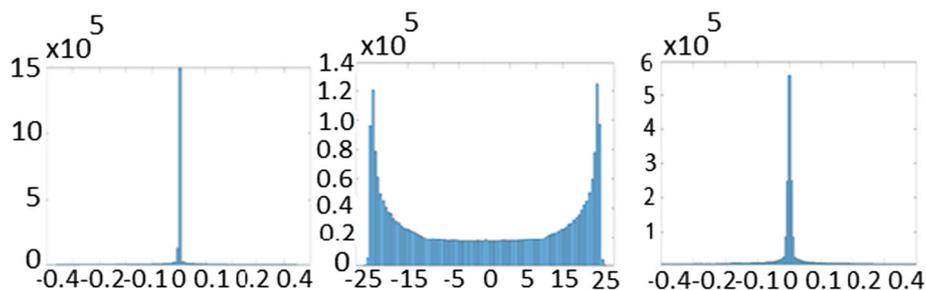


Fig. 5 Speech-Original/Masked/Decrypted Histogram Analysis



4.1 Histogram Analysis

Histogram analysis enables the determination of the accuracy of the encryption process by starting from the distribution of the data. If the distribution of the data is far from

the original data, it is understood that the encryption process is done in a robust way.

The histograms of the original, masked and decoded signals are given in Fig. 5. It has been observed that the distribution of the data in the masked audio signal in the histograms is different from the original signal.

4.2 Spectral Entropy

Spectral entropy is used to detect the region and movement of silences and speech activities in sound data. Thus, it turns out whether the data compared belong to the same voice data or not (Toh et al. 2005). In spectral entropy graphics, the entropies of the audio signals decrypted with the original audio signals appear to follow each other locally, in both value and motion. In spectral entropy applications, it is assumed that the speech spectrum is more organized during speech segments than noise segments. Thus, vocal speech regions cause low entropy. Spectral entropy of the signal is shown in Fig. 6.

4.3 PSNR Tests and MSE Values

The peak signal-to-noise ratio, often abbreviated as PSNR, is used for the ratio between the maximum power of a signal and the interfering noise power that affects the accuracy of its representation.

There is an inverse proportion between PSNR and MSE values. The reason for the high PSNR value between the original and the masked signal is because of the lower MSE than the decrypted signal (Lagmiri et al. 2018). PSNR and MSE test values are indicated in Tables 1, 2, 3. The mean

Table 1 PSNR and MSE test of audio signals

Different Cases	PSNR	MSE
Original/Decrypted	64.7718	0.1472
Original/Masked	23.99	16.09

square error calculated for the X and Y vectors is expressed as:

$$MSE = \frac{1}{n} \sum_{i=1}^n (X[i] - Y[i])^2 \tag{18}$$

PSNR values for the encrypted audio signal (Y) and the original audio signal (X) can be calculated as follows:

$$PSNR = 10 * \log_{10} \left(\frac{MAX^2}{MSE} \right) \tag{19}$$

where MAX is the maximum values of the given signals.

4.4 Key Space and Key Sensitivity Analyzes

The width of the key space plays a critical role for a secure encryption method. (Alvarez et al. 2006). Even small changes in keys used in key sensitivity analysis, encryption

Fig. 6 Spectral entropies of speech

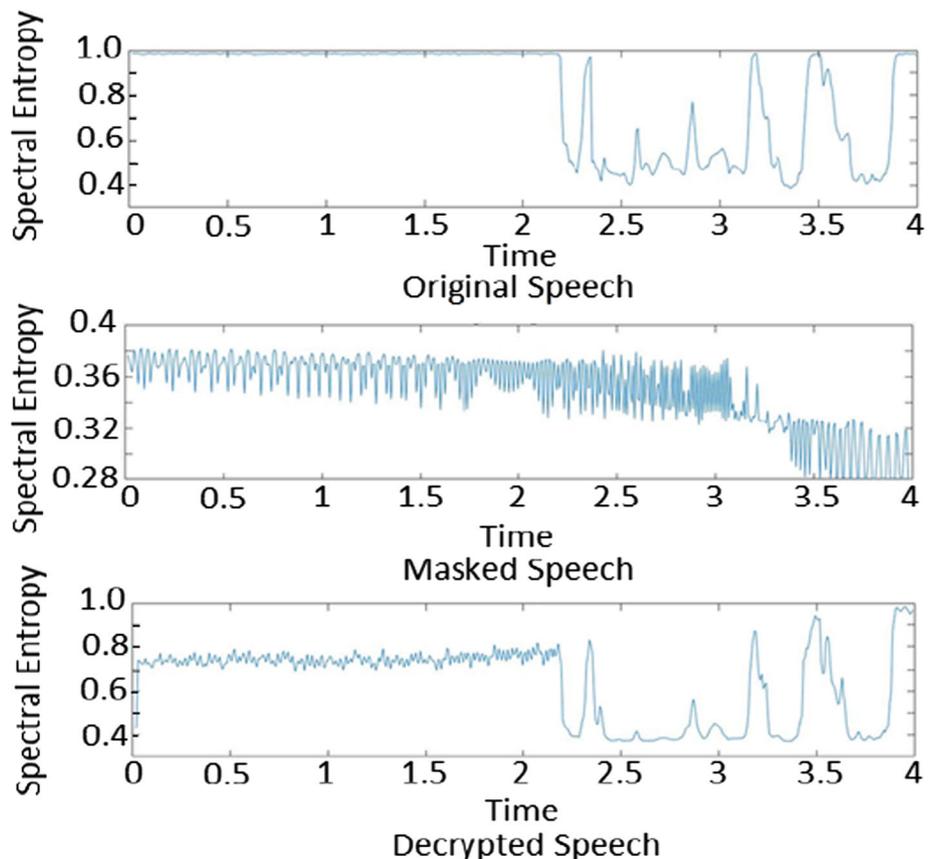


Table 2 Key space analysis

	Lima et al. (2015)	Farsana et al. (2016)	Belmeguenai et al. (2017)	Kate et al. (2018)	Naskar et al. (2019)	Ours
Key space size	2^{256}	2^{477}	2^{512}	2^{512}	2^{256}	2^{512}

Table 3 Key sensitivity analysis

Proposed method	Correct key	Modified key	Figure of modified key	Correlation coefficient	Number of signal change rate
The control parameter u	u	$u + 0.001$	Fig. 4	0.00016	100%

and decryption can lead to very different results in encryption and decryption processes. In a secure encryption, it should produce a secure encryption for very small changes in keys. (Atalay et al. 2019; Çavuşoğlu 2016).

4.5 NSCR and UACI Analysis

The encryption method used for security against potential attacks is an important parameter. This security measure is calculated with NSCR and UACI tests (Ahmad et al. 2016; Çavuşoğlu 2016; Abdelfatah 2020). During the execution of these tests, two different audio signals must be encrypted with the same key. These mixed audio signals can be found by the equations given below:

$$NSCR = \sum_i \frac{D_i}{N_s} \times 100\% \quad i = 1, 2, \dots, \dots, N \quad (20)$$

$$UACI = \frac{1}{N_s} \left[\frac{\sum_i x_i - x'_i}{65535} \right] \quad (21)$$

$$\text{here } D_i = \begin{cases} 1, & x_i \neq x'_i \\ 0, & \text{otherwise} \end{cases} \quad (22)$$

The NSCR and UACI analysis values obtained for the encrypted signal of the original signal (x_i) and the encrypted signal of the modified signal (x'_i) are shown in Table 4. The proposed scheme appears to have better resistance to a different attack.

4.6 PESQ Analysis

PESQ is a popular analysis method that automatically evaluates speech quality. It has been determined that the Audio-1 signal used in this study has a moderate performance. In addition, since it does not provide enough data

for the Audio-1 file, it is an expected result to obtain a middle level of performance.

4.7 Comparative Study

The advantages of the proposed arrhythmia ECG chaotic attractor method compared to other methods are evaluated in this section. The most common security parameters such as correlation, key space and key sensitivity, PSNR, UACI, NSCR and PESQ were used for performance comparison.

The values shown in Table 5 show how low the similarity is between the original audio signal and the encrypted audio signal.

Table 6 shows these comparisons against other methods. It has been observed that the proposed method has the lowest correlation coefficient value between the original audio signal and the encrypted audio signal. When PSNR, UACI and NSCR values are examined, it is determined that the proposed method has a stronger encryption.

5 Conclusion and Future Scope

In this study, speech pattern (Audio-1) which was taken from Cambridge University publishing Face2Face with mutual dialogues (Redston et al. 2013) is masked with the help of a signal received from a ECG chaotic emulator. The masked audio signal and a second ECG chaotic signal that will synchronize the system are transmitted on a single channel. The FDM method was used to transmit two signals through a single channel. In this method, the signals are placed on the frequency spectrum using DSB-SC amplitude modulation. In addition, shielding tapes have been created to avoid overlapping between the signals. The chaotic behavior of the ECG signal ensured that the audio signal was reliably encoded. As can be seen in histogram analysis, it was observed that there was no similarity between the distribution of the original audio signal and the masked audio signal data and only the amplitude difference

Table 4 NSCR and UACI analysis of audio signals

Audio file	NSCR	UACI
Audio-1	100%	37.11%

Table 5 PSNR and correlation coefficient between the original and encrypted audio signals

Audio file	Size	Duration (Sec.)	Correlation coefficient	Speed(s/KB)	PSNR
Audio-1	1.294 KB	10	0.00016	0.0077	64.7718

Table 6 Comparison with other methods

Method	Correlation coefficient	Key space	PSNR	UACI	NSCR	RMS	CF
Lima et al. (2015)	0.0021	2^{256}	–	33.29%	99.9992%	–	4.8
Farsana et al. (2016)	0.00023	2^{447}	–	–	–	–	–
Belmeguenai et al. (2017)	–0.0011	2^{512}	47.98	–	–	–	–
Kordov et al. (2019)	0.0038	2^{149}	4.39	–	99.996%	–	–
Naskar et al. (2019)	0.000207	2^{256}	–	–	99.9989%	0.6	4.8
Ours	0.00016	2^{512}	64.7718	37.11%	100%	–	–

occurred between the original audio signal and the decoded audio signal. The reason for this difference is many of filters used on the FDM side (Atan 2020; Bagheri et al. 2009; Gao et al. 2016; Garcia-Hernandez et al. 2013; Sathiyamurthi et al. 2017; Liu et al. 2007). The synchronization time was realized in a very short time such as 0.02 s with SMC.

It has been observed that the ECG emulator circuit performs faster and more secure encryption than the Sprott chaotic oscillator. Spectral entropy was used to track the region and movement of audio signals. In spectral entropy simulations, it has been observed that the original and decrypted audio signals were in the same ranges and follow each other. When spectral entropies of original and masked signals were compared, it was determined that the ranges and movements were different from each other. For the audio signal used in the study, MSE values among the original/decrypted signals are desired to be close to zero, and among the original/masked signals, the value being as far from zero as possible is an expression of the successful decrypted process. In this process, simulation worked 15 s. For these reasons, when all parameters are evaluated in total against various differential attacks, it is seen that the proposed method exhibits a strong behavior. Finally, it was concluded that the proposed system is reliable and successful in encryption. In this way, a theoretical contribution was made to the literature. In addition, the use of a single channel to transmit the masked audio signal and the synchronization signal to the receiving side will provide practical benefits in communication systems.

The next step of this research is to increase data security in future studies on new types of heart arrhythmias caused by diseases such as Covid-19 (Akkus et al. 2021). In addition, by combining existing methods with hybrid methods, it is to ensure the optimum data security in terms of both simulation and application.

Acknowledgements The authors thank the associate editor and the anonymous reviewers for their constructive comments and useful suggestions.

Authors' Contribution All the authors made significant contributions to the work. İP was involved in writing—reviewing and editing, MNA helped in supervision, conceptualization, methodology, ÖA contributed to visualization, investigation. ACÇ was involved in writing—original draft preparation, validation, OS helped in writing—original draft preparation, data curation.

Funding This research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

- Abdelfatah RI (2020) Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. *IEEE Access* 8:69894–69907. <https://doi.org/10.1109/ACCESS.2020.2987197>
- Ahmad J, Hwang SO (2016) A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed Tools Appl* 75(21):13951–13976. <https://doi.org/10.1007/s11042-015-2973-y>
- Akkus O, Bal T, Yagoobi H, Bekler O, Akkus G, Cabalak M (2021) Electrocardiographic findings and cardiac safety of hydroxychloroquine+azithromycin in hospitalized patients with COVID-19. *Cukurova Med J* 46(2):691–698
- Almali MN, Dikici Z (2016) The simulation of sound signal masking with different chaotic oscillations and its circuit application. *Turk J Electr Eng Comput Sci* 24(5):4284–4293
- Al-sawalha MM (2020) Synchronization of different order fractional-order chaotic systems using modify adaptive sliding mode control. *Adv Differ Equ* 2020(1):1–1. <https://doi.org/10.1186/s13662-020-02876-7>
- Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurcation Chaos* 16(8):2129–2151. <https://doi.org/10.1142/S0218127406015970>

- Amr S, Hussein HED, Ramadan N, El-Shafai W, El-Hanafy W, El-Samie A, Fathi E (2019) Chaotic encryption of ECG signals with a random Kernel approach. *Menoufia J Electr Eng Res* 28:115–121
- Atalay NS, Doğan Ş, Tuncer T, Akbal E (2019) Image encryption methods and algorithms. *Dicle Univ Eng Fac J Eng* 10(3):815–831
- Atan Ö (2020) Effects of variable-order passive circuit element in Chua circuit. *Circ Syst Signal Process* 39:2293–2306. <https://doi.org/10.1007/s00034-019-01271-2>
- Azar AT, Serranot FE, Vaidyanathan S (2018) Sliding mode stabilization and synchronization of fractional order complex chaotic and hyperchaotic systems. In: *Mathematical Techniques of Fractional Order Systems*, pp. 283–317. Elsevier. <https://doi.org/10.1016/B978-0-12-813592-1.00010-6>
- Bagheri A, Moghaddam JJ (2009) Decoupled adaptive neuro-fuzzy (DANF) sliding mode control system for a Lorenz chaotic problem. *Expert Syst Appl* 36(3):6062–6068. <https://doi.org/10.1016/j.eswa.2008.06.123>
- Belmeugeni A, Ahmida Z, Ouchtati S, Dejmi R (2017) A novel approach based on stream cipher for selective speech encryption. *Int J Speech Technol*. <https://doi.org/10.1007/s10772-017-9439-8>
- Cavusoglu U (2016) Design and implementation of chaos based hybrid symmetric and asymmetric encryption algorithms (doctoral thesis, unpublished). Sakarya University, Institute of Science, Sakarya, Turkey
- Chen CK, Lin CL, Chiang CT, Lin SL (2012) Personalized information encryption using ECG signals with chaotic functions. *Inf Sci* 193:125–140. <https://doi.org/10.1016/j.ins.2012.01.016>
- Chua LO (1992) The genesis of Chua's circuit. Electronics Research Laboratory, College of Engineering, University of California, Berkeley, CA, USA
- Chua LO, Wu CW, Huang A, Zhong GQ (1993) A universal circuit for studying and generating chaos. I. Routes to chaos. *IEEE Trans Circ Syst I Fund Theory Appl* 40(10):732–744. <https://doi.org/10.1109/81.246149>
- Cilhoroz B, Zaleski A, Taylor B, Fernhall B, Chen MH, Thompson P, Pescatello L (2021) The ambulatory blood pressure and heart rate variability responses following sudden vigorous physical exertion among firefighters with hypertension. *Turk J Sports Med* 56(3):98–105. <https://doi.org/10.47447/tjism.0492>
- Ebrahimi Z, Loni M, Daneshmand M, Gharehbaghi A (2020) A review on deep learning methods for ECG arrhythmia classification. *Exp Syst Appl*: X 7:100033. <https://doi.org/10.1016/j.eswax.2020.100033>
- Farsana F, Gopakumar K (2016) A novel approach for speech encryption: Zaalavsky map as pseudo random number generator. In: 6th International conference on advances in computing & communications, ICACC 2016, 6-8 September 2016, Cochin, India. <https://doi.org/10.1016/j.procs.2016.07.302>
- Felber DD, Ackermann-Liebrich U, Schindler C, Barthélémy JC, Brändli O, Gold DR, Gaspoz JM (2008) Effect of physical activity on heart rate variability in normal weight, overweight and obese subjects: results from the SAPALDIA study. *Eur J Appl Physiol* 104(3):557–565
- Gao F, Lee T, Cao WJ, Lee XJ, Deng YF, Tong HQ (2016) Self-evolution of hyper fractional order chaos driven by a novel approach through genetic programming. *Expert Syst Appl* 52:1–15. <https://doi.org/10.1016/j.eswa.2015.12.033>
- García-Hernández JJ, Parra-Michel R, Feregrino-Uribe C, Cumplido R (2013) High payload data-hiding in audio signals based on a modified OFDM approach. *Expert Syst Appl* 40(8):3055–3064. <https://doi.org/10.1016/j.eswa.2012.12.021>
- Gois SR, Savi MA (2009) An analysis of heart rhythm dynamics using a three-coupled oscillator model. *Chaos, Solit Fract* 41(5):2553–2565. <https://doi.org/10.1016/j.chaos.2008.09.040>
- Gupta V, Mittal M, Mittal V (2019) R-peak detection based chaos analysis of ECG signal. *Analog Integr Circ Sig Process*. <https://doi.org/10.1007/s10470-019-01556-1>
- Hahn W, Stab Th (1967) *Mot*. Springer, New York
- Huang P, Li B, Guo L, Jin Z, & Chen Y (2016) A robust and reusable ecg-based authentication and data encryption scheme for ehealth systems. In: 2016 IEEE global communications conference (GLOBECOM) (pp 1–6). IEEE. <https://doi.org/10.1109/GLOCOM.2016.7841541>
- İzci E, Değirmenci M, Özdemir MA, Akan A (2020) ECG arrhythmia detection with deep learning. In: 2020 28th signal processing and communications applications conference (SIU), pp 1–4. <https://doi.org/10.1109/SIU49456.2020.9302219>
- Kakade M, Singh J (2014) Memristors SPICE modeling. *Ijetee Com* 4(8):343–346
- Karataş F (2021) ECG simulator design FPGA-based with VHDL (Master's thesis, Institute of Science and Technology)
- Kate HK, Razmara J, Isazadeh J (2018) A Novel fast and secure approach for voice encryption based on DNA computing. *3D Res* (2018) 9:17. 3D Research Center, Kwangwoon University and Springer-Verlag GmbH Germany, part of Springer Nature. <https://doi.org/10.1007/s13319-018-0167-x>
- Kordov K (2019) A novel audio encryption algorithm with permutation-substitution architecture. *Electron MDPI* 2019(8):530. <https://doi.org/10.3390/electronics8050530>
- Lagmiri SN, Bakhous H (2018) Audio encryption algorithm using hyperchaotic systems of different dimensions. In: CS & IT conference proceedings (Vol. 8, No. 15). CS & IT conference proceedings. <https://doi.org/10.5121/csit.2018.81507>
- Li H, Hua Z, Bao H, Zhu L, Chen M, Bao B (2020) Two-dimensional memristive hyperchaotic maps and application in secure communication. *IEEE Trans Industr Electron*. <https://doi.org/10.1109/TIE.2020.3022539>
- Lima JB, da Silva NEF (2015) Audio encryption based on the cosine number transform. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-015-2755-6>
- Liu Y, Mikhael WB (2007) A blind maximum likelihood carrier frequency offset correction approach for OFDM systems over multipath fading channels. *Circ Syst Signal Process* 26(1):43–54. <https://doi.org/10.1007/s00034-005-0922-0>
- Lorenz EN (1963) Deterministic nonperiodic flow. *J Atmos Sci* 20(2):130–141
- Meghanathan N, Nagamalai D, Chaki N (2012) Advances in computing and information technology. Proceedings of the second international conference on advances in computing and information technology (ACITY), July 13–15, 2012, Chennai, India, vol 1. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-642-31513-8>
- Nagamalai D, Renault E, Dhanuskodi M (eds) (2011) Advances in digital image processing and information technology: first international conference on digital image processing and pattern recognition, DPPR 2011, Tirunelveli, Tamil Nadu, India, September 23–25, 2011, Proceedings, vol 205. Springer Science & Business Media
- Naskar PK, Paul S, Nandy D, Chaudhuri A (2019) DNA encoding and channel shuffling for secured encryption of audio data. *Multimed Tools Appl* 78:25019–25042. <https://doi.org/10.1007/s11042-019-7696-z>
- Quiroz-Juárez MA, Jiménez-Ramírez O, Vázquez-Medina R, Breña-Medina V, Aragón JL, Barrio RA (2019) Generation of ECG signals from a reaction-diffusion model spatially discretized. *Sci Rep* 9(1):1–10. <https://doi.org/10.1038/s41598-019-55448-5>

- Rajabpour-Moghaddam K, Maymandi-Nejad M, Ghomash HK (2014) A 24-channel implantable neural recording based on time and frequency-division multiplexing. *Analog Integr Circ Sig Process* 79(3):493–506. <https://doi.org/10.1007/s10470-013-0182-z>
- Rajagopal K, Guessas L, Vaidyanathan S, Karthikeyan A, Srinivasan A (2017) Dynamical analysis and FPGA implementation of a novel hyperchaotic system and its synchronization using adaptive sliding mode control and genetically optimized PID control. *Math Probl Eng*. <https://doi.org/10.1155/2017/7307452>
- Rao RP (2018) Real time audio signal processing through DSB-SC using Simulink. *Int J Sci Dev Res (IJS DR)* 3(6):52–55
- Redston C, Clementson T, Cunningham G (2013) *Face2face Upper intermediate teacher's book with DVD*. Cambridge University Press
- Sathiyamurthi P, Ramakrishnan S (2017) Speech encryption using chaotic shift keying for secured speech communication. *EUR-ASIP J Audio, Speech, Music Process* 2017(1):1–11. <https://doi.org/10.1186/s13636-017-0118-0>
- Sheu LJ, Chen WC, Chen YC, Weng WT (2010) A two-channel secure communication using fractional chaotic systems. *World Acad Sci, Eng Technol* 65:1057–1061
- Sprott JC (2000) A new class of chaotic circuit. *Phys Lett A* 266(1):19–23. [https://doi.org/10.1016/S0375-9601\(00\)00026-8](https://doi.org/10.1016/S0375-9601(00)00026-8)
- Toh AM, Togneri R, Nordholm S (2005) Spectral entropy as speech features for speech recognition. *Proc PEECS* 1:92
- Vaidyanathan S, Sampath S (2011) Global chaos synchronization of hyperchaotic Lorenz systems by sliding mode control. In: *International conference on digital image processing and information technology*, 156–164. https://doi.org/10.1007/978-3-642-24055-3_16
- Wu D (2010) Application research on frequency-division multiplexing to chaos secret communication. In: *2010 international conference of information science and management engineering (Vol. 1, pp 139–142)*. IEEE. . <https://doi.org/10.1109/ISME.2010.180>
- Xia Y, Yang H, Fu M, Shi P (2011) Sliding mode control for linear systems with time-varying input and state delays. *Circ Syst Signal Process* 30(3):629–641. <https://doi.org/10.1007/s00034-010-9237-x>