Akif Akgul*, Omer Faruk Boyraz, Karthikeyan Rajagopal, Emre Guleryuz, Mustafa Zahid Yildiz and Mustafa Kutlu

An unforced megastable chaotic oscillator and its application on protecting electrophysiological signals

https://doi.org/10.1515/zna-2020-0222
Received August 8, 2020; accepted September 13, 2020; published online September 30, 2020

Abstract: In this paper, we introduce a novel 3D chaotic oscillator which shows megastability without any external excitation. Some important dynamical properties of the proposed novel system were derived and investigated. Data protection application and its security analysis were realized for electrophysiological signals such as ECG, EEG and EMG on a microcomputer. This paper includes both encryption and data hiding processes for high security. Also a user interface was developed. For the encryption process, random numbers were generated by the megastable chaotic oscillator. These random numbers were tested with NIST-800-22 test which is the most widely accepted statistical test suite. The encrypted electrophysiological signals were analyzed by entropy, differential attacks, histogram, correlation, initial condition sensitivity, etc. The results of the analysis have shown that the proposed two level security method can be used in many fields as mobile. The most important feature of this paper is that both encryption and data hiding processes were implemented for electrophysiological signals. The experimental results verify that the proposed method has high security and is suitable for the protection of vital electrophysiological signals.

Keywords: chaos; data security; electrophysiological signals; microcomputer; nonlinear systems.

***Corresponding author: Akif Akgul**, Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54050 Serdivan, Sakarya, Turkey, E-mail: aakgul@sakarya.edu.tr, https://orcid.org/0000-0001-9151-3052

Omer Faruk Boyraz, Emre Guleryuz and Mustafa Kutlu, Department of Mechatronics, Faculty of Technology, Sakarya University of Applied Sciences, 54050 Serdivan, Sakarya, Turkey, E-mail: oboyraz@sakarya.edu.tr (O.F. Boyraz), emreguleryuz61@gmail.com (E. Guleryuz), mkutlu@sakarya.edu.tr (M. Kutlu)

Karthikeyan Rajagopal, Nonlinear Systems and Applications, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam, E-mail: rkarthiekeyan@gmail.com. https://orcid.org/0000-0003-2993-7182

Mustafa Zahid Yildiz, Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54050 Serdivan, Sakarya, Turkey, E-mail: mustafayildiz@sakarya.edu.tr

1 Introduction

The last two decades have seen a growing trend toward wired and wireless telecommunications technologies. They have become an important part of biomedical science with tele-healthcare. Electrophysiological signals (EEG, ECG, EEM) obtained from the patient via biopotential electrodes and converters are often used in the diagnosis. While, biosignals can be transmitted over public networks, according to the Health Insurance Portability and Accountability Act (HIPAA), all bio-signals transmitted over public networks must be protected [1]. Furthermore, these signals have recently been used in person recognition systems. However, the security and protection of diagnostic data is considered very important and must be protected when communicating through communication channels [2]. Since electrophysiological signals contain both personal and health information, it is very important to prevent and encrypt unauthorized access before they are transmitted via public media [3]. In addition, these encryption and decryption operations should be performed with minimal delay in a very short time. An example of this is to save the lives of patients with cardiovascular diseases without any delay [4].

Cryptography is a well-known data-protection technique [5, 6]. So far, many technologies have been developed to protect and store various data groups. Among these technologies, chaotic encryption is the most intuitive and effective way to obfuscate data [7, 8]. A chaotic system is sensitive to initial conditions, not periodically and randomly, and it has many features required for cryptography. But, chaos-based cryptology applications have some security drawbacks. In this article, using a megastable chaotic oscillator is realized to overcome those drawbacks by using a secure steganography application

with chaos-based encryption. In literature, studies which perform encryption and data hiding operations together are rare.

Chaos theory is an interesting branch of mathematics that is widely used in many fields of technology [9–12]. One of the applications of this theory is encryption of data such as audio, video, images and biomedical signals. Yildiz et al. encrypted 1–8 bits dorsal hand vein images in their study, encrypting vein images with a new chaos-based encryption algorithm and protect them in the database [11]. Zhang et al. utilised the compression detection and pixel permutation approaches. A medical image encryption and compression algorithm was proposed in their study. At the same time, this algorithm can simultaneously encrypt and compress medical images [13].

Chaos-based encryption is suitable for telemedicine applications [9, 14–20] because it facilitates data protection and guarantees confidentiality of patient-related information. Hao et al. proposed a chaotic map-based validation scheme for telecare drug information systems (TMIS) [21]. Lee et al. proposed an improved mobile health emergency system based on chaotic maps [2]. Parveen et al. have developed a chaos-based encryption technique using wavelet transform to encrypt EEG signals [22]. In their study, Lin et al. developed a two-dimensional chaotic-based virtual encryption algorithm and implemented EEG signals [19]. Lin et al. implemented the same encryption algorithm to encrypt ECG signals [20].

In this study, we are interested in proposing a new 3D chaotic oscillator that shows megastability out of any external excitement. Three different electrophysiological signals (EEG, EMG and ECG) received from humans were encrypted using a new chaotic system to secure them before being transmitted. Before the encryption, the identity of the patient (Name, ID Number) were hidden within these signals. In addition, an interface was designed to enable healthcare personnel to easily conceal data, encrypt and decrypt the received signal. The results of the analyzes confirm that the developed system provides high security for electrophysiological signals and minimizes the possibility of unauthorized access.

In Section 2, a novel 3D megastable oscillator (3DMO) is detailed and its dynamical analysis are performed. Electrophysiological signals and preprocessing are introduced in Section 3. In Sections 4 and 5 data hiding and cryptology application in electrophysiological signals are realized, respectively. Then, security analysis are implemented in Section 6. Also, a custom made user interface is designed in Section 7. The last section provides conclusions and draws future works.

2 3D megastable oscillator (3DMO) and its dynamical analysis

Many recent literatures have proposed chaotic oscillators with lattices of attractors and infinite number of equilibrium points [23–27] and some of them are unique with countable number of coexisting attractors named as “Megastable” after [28]. All the megastable oscillators discussed in the literatures show chaotic oscillations only when forced with an external excitation [29–32]. Hence in this paper, we are interested in proposing a new 3D chaotic oscillator which shows megastability without any external excitation. It is to be noted that such an oscillator was not discussed in the earlier literatures and hence the proposed system falls under category-2; as such an unforced megastable oscillator has not been investigated in the literature [33].

The mathematical model of the 3DMO is given by,

$$\begin{aligned} \dot{x} &= z \\ \dot{y} &= b * cos(z) - c * y \\ \dot{z} &= -dx + zcos(x) - ay \end{aligned} \tag{1}$$

where a, b, c, d are the system parameters. Using a computer search method, we could find the parameters as $a = 2.1$, $b = 0.7$, $c = 0.1$, $d = 0.3$ for which the system shows infinitely coexisting attractors as shown in Figure 1.

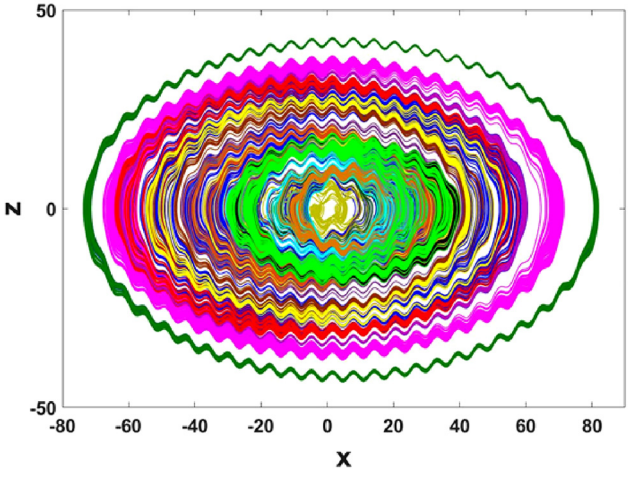

Figure 1: Coexisting attractors for the x initial values taken between −20 and 20 with steps of four and y initial values taken between −10 and 20 with steps of four.

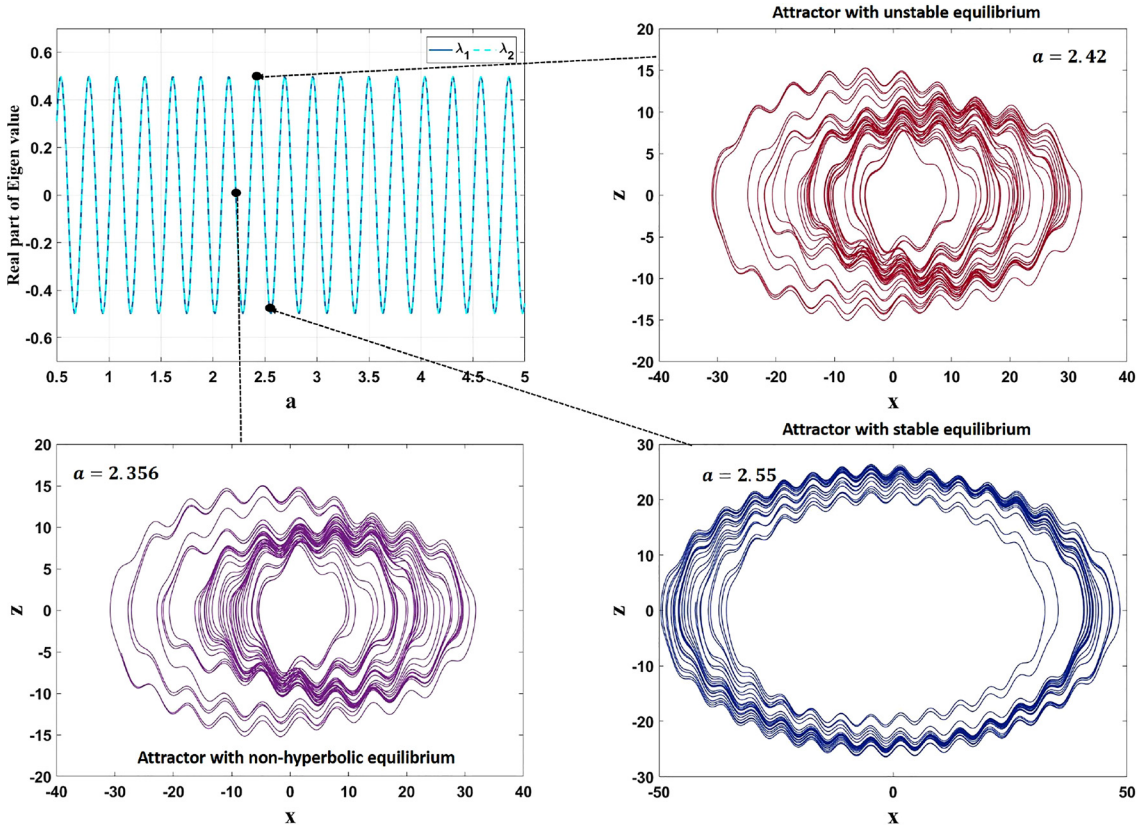

Figure 2: The real part of eigen values for various values of a. The chaotic attractors with stable, unstable and non-hyperbolic equilibriums are shown alongside the eigen values.

The equilibrium points of the system are calculated as $E = \left[-\frac{ab}{cd}, \frac{b}{c}, 0 \right]$. The Jacobian of the above system in its equilibria is:

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & -c & 0 \\ -d & a & \cos(ab/cd) \end{bmatrix} \tag{2}$$

The characteristic polynomial can be derived as:

$$\lambda^3 + \left(c - \cos\left(\frac{ab}{ca}\right)\right)\lambda^2 + \left(d - c\cos\left(\frac{ab}{cd}\right)\right)\lambda + cd \tag{3}$$

and the eigenvalues will be:

$$\lambda_{1,2} = \left(\sqrt{\cos\left(\frac{ab}{cd}\right)/2 + \left(\cos\left(\frac{ab}{cd}\right)^2 - 4d\right)} \right)/2 \tag{4}$$

$$\lambda_3 = -c$$

It can be easily noted from (4) that the third eigen value is always negative as $c > 0$ and hence the first two eigen values determine the stability of the system. Figure 2 shows the various eigen values for different values of parameter a and the 3DMO change between stable and unstable attractor and the chaotic attractors for stable, unstable and non-hyperbolic equilibriums are also shown in Figure 2.

According to the Routh-Hurwitz criterion, the real parts of all the roots of Eq. (3) are negative if and only if

$$\begin{gathered} c - \cos(ab/cd) > 0 \\ cd > 0 \\ \left(d - c\cos\left(\frac{ab}{cd}\right)\right)\left(c - \cos\left(\frac{ab}{cd}\right)\right) > 0 \end{gathered} \tag{5}$$

It can be seen from (5) that when $c < \cos\left(\frac{ab}{cd}\right)$, $d < c\cos\left(\frac{ab}{cd}\right)$ the system is unstable and stable for $c > \cos\left(\frac{ab}{cd}\right)$, $d > c\cos\left(\frac{ab}{cd}\right)$.

Bifurcation diagram of the 3DMO system and the Lyapunov spectrum are shown for parameter a between 0 and 6 in Figure 3. The system has chaotic behaviour approximately between 0 and 1, 1.9–2.6 and 3.1–6.

To show the megastable behaviour of the 3DMO system, we have plotted the bifurcation plots with respect to initial conditions by fixing the system parameters to = 2.1, b = 0.7, c = 0.1, d = 0.3 as shown in

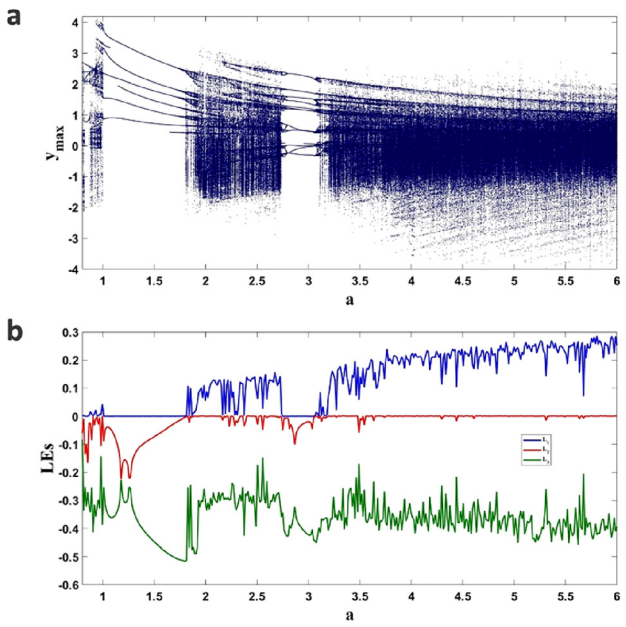

Figure 3: (a) Bifurcation of the 3DMO system with parameter a; (b) the corresponding Lyapunov spectrum.

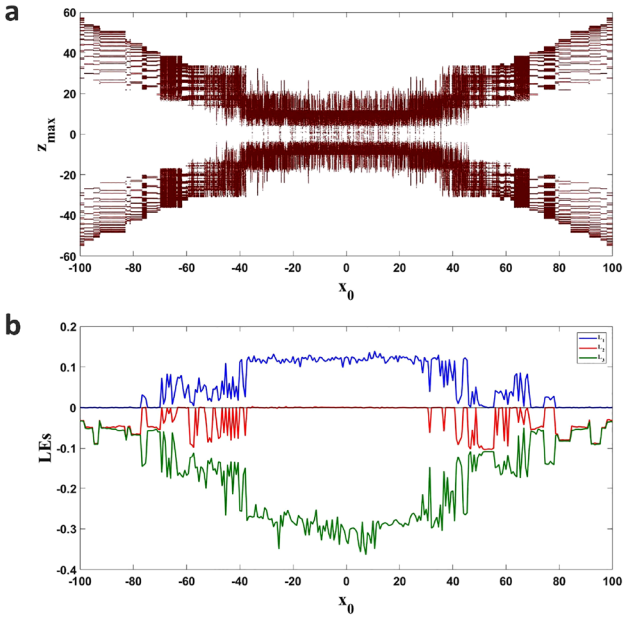

Figure 4: (a) Bifurcation of the 3DMO system with parameter x_0; (b) The corresponding Lyapunov spectrum.

Figure 4a. We could identify the growing amplitude of the state 'z' as the initial condition of state 'x' is increased/decreased which confirms that the radius of the system grows as in Figure 1. Also, the 3DMO system shows chaotic attractor for a wide range for $x_0 \in [-80.80]$ which can be confirmed from the Lyapunov spectrum shown in Figure 4b.

3 Electrophysiological signals and preprocessing

EEG is one of the methods used to determine normal and abnormal functions of the living human brain. Electrical recordings obtained from the surface of the brain from the outer surface of the head indicate that the brain has a continuous electrical activity. The electrical activity of brain skull is between 0 and 200 uV and its frequency is between 1 and 50 Hz. The electrical activity of the brain is affected by changes in the level of arousal such as coma, sleep/wake, epilepsy, some psychoses and brain death [34]. Biomedical EEG signals have been used since the 1950s to monitor patients with coma, dementia and long-term memory problems. It is also used to assess brain death to legally prove that a patient will not recover from life support equipment.

ECG is a method based on recording the possible electric changes in the heart [35]. ECG signals with a frequency range of 0.1–100 Hz, and usually a maximum amplitude of 1 mV provide some information for the diagnosis of heart disease.

The EMG signal is an electrical electrophysiological signal representing the activity of the corresponding motor unit of the contracting muscle and is a potential source for the human-machine interface [36]. The amplitude of the EMG signal is between 0 and 10 mV peaks or 0–1.5 mV (rms) while the frequency is in the range of 50–500 Hz.

Electrophysiological data are specific to the patient, but when admitted to a hospital, they are routinely transmitted over an insecure channel prior to diagnosis. When the same data is collected for telemedical purposes, it is required by law to protect the patient's biomedical health information from unauthorized access before being transmitted over an insecure channel. It is equally important that the applied protection approach does not change the patient's data to influence the later diagnosis. Furthermore, a powerful encryption algorithm must be stored to protect personal signals from illegal access or modification of attacks.

Figure 5 shows the ECG signal from the physiobank database. The signal ranging from 1 to −0.8 mV was converted into eight bit data for encryption. Figure 5 shows also the conversion of ECG data to eight bits. The signal ranging from 0 to 256 μV was converted into eight bit data for encryption.

4 Data hiding in electrophysiological signals

The name, surname and ID number information received from the participants of electrophysiological signals is

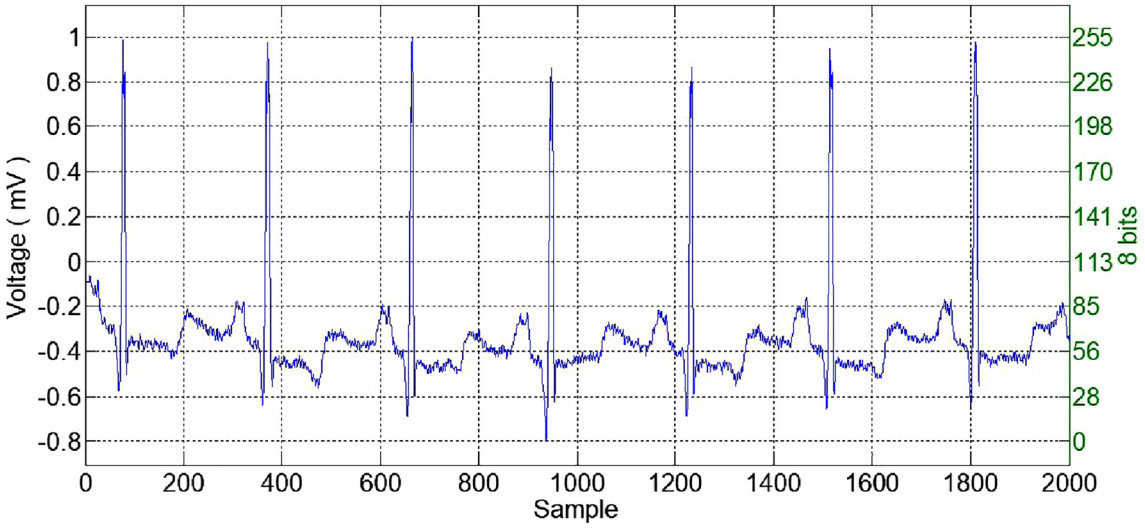

Figure 5: An example ECG signal received from Physiobank and the converted to eight bits before encryption.

an important credential; therefore, it is concluded that this information should be hidden in the signals. The reason why encryption precedes is that it requires identity information which is not recognized on the encrypted signal. Steganography is one of the methods for securely storing and transmitting personal information in a computer environment. The purpose of steganography is to obscure the existence of important personal information. Steganography hides the data that is to be hidden in the object without changing the structure of the data to be hidden. The hidden data is not displayed by unauthorized persons because they are invisible to the naked eye. In this study, least significant bit (LSB) method was selected from the algorithms commonly used to hide data in electrophysiological signals to increase the encrypted data capacity. As a result of this method, data hidden in electrophysiological signals are minimized to hide maximum information at the same time. This attempts to minimize algorithmic complexity.

Algorithm 1 Hide data algorithm pseudo code

1: Start
2: Text = [name, surname, id number]
3: binary text = ascii (text)
4: **for** i = 1: length of binary text **do**
5: binary signal = decimal to binary (Signal (i))
6: binary signal (8) = binary text (i)
7: **end for**
8: Hidden_data_signal = binary to decimal (binary_signal)
9: End

Algorithm 1 gives the LSB method for embedding the most trivial bite for hiding contact information in electrophysiological signals. First, the text consisting of the first name, last name, and ID number is converted to numerical values in binary according to the American Standard Code for Information Interchange (ASCII) code. The binary numerical values of ECG, EEG and EMG signals are converted into eight bites. The eighth bit of these eight bit binary values is synchronized with the binary value from the text data. This process continues up to the length of the text data binary value. This means personal data is hidden in electrophysiological signals.

Figure 6 shows the general flow diagram of the system. Electrophysiological signals taken from Physiobank database were transferred to the microcomputer and converted into eight bits by preprocessing. The personal data obtained from the patients were transferred to the system over the interface and hidden in eight-bit signals using the LSB method. In this way, the personal data of the patient were hidden within their physiological signals. Finally, the electrophysiological signals of the patient were encrypted by passing through the eXclusive (XOR) bit operator with random numbers generated from the 3DMO system and securely stored in the database.

Mean squared error (MSE) and peak signal-to-noise ratio (PSNR) analysis of the original signal and the data hiding signal are shown in Table 1. As the purpose of data type authentication with the LSB encrypting method is to keep the original signal intact, MSE and PSNR analyses measure the quality of data hiding. The MSE is an average quadratic error analysis and its percentage should be very low in a data-hidden signal. This does not disturb the original electrophysiological signal. PSNR indicates noise and quality levels and is inversely proportional to, and

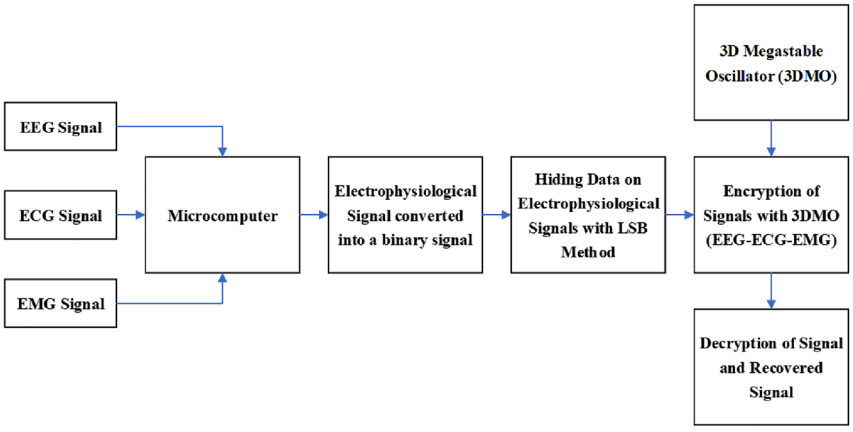

Figure 6: The general flow diagram of the system.

Table 1: MSE–PSNR analysis of data hidden and original signals.

	MSE	PSNR
ECG	0.1356	61.1848
Encrypted ECG		
EEG	0.0540	61.4098
Encrypted EEG		
EMG	0.1321	61.0069
Encrypted EMG		

almost 0 causes the original signal to be corrupted after data hiding. The values calculated in Table 1 were calculated using Eqs. (6) and (7).

$$\mathrm{MSE}\,(I, I_0) = \frac{1}{M} x \sum_{y=1}^{M} \sum_{x=1}^{N} [I - I_0] \tag{6}$$

$$\mathrm{PSNR} = 20x \log_{10}\left(\frac{255}{\sqrt{\mathrm{MSE}\,(I, I_0)}}\right) \tag{7}$$

In Eq. (6), M refers to the length of the binary value according to the ASCII code of text information consisting of the person's name, last name and ID number data. The value of the I and I_0 refer data hidden signal and the value of the hidden signal, respectively.

In the analysis of the data hidden in the electrophysiological signals of 2000 data shown in Table 1, it was concluded that the original signal was not distorted by giving very close results to 0 MSE. At the same time, the PSNR results in Table 1 show that the PSNR will be a maximum of 80 in 2000 data of eight bits.

5 Cryptology application in electrophysiological signals

Chaos-based random numbers were used to encrypt in many engineering applications as pseudo and true random numbers [37–41]. In this paper, random numbers were generated with chaotic signals from the 3D Megastable oscillator. The generated random numbers were tested by subjecting to the internationally valid NIST-800-22 test.

Algorithm 2 Random number generator algorithm pseudo code.

1: Start
2: Entering system parameters
3: Entering initial condition
4: Determination of the appropriate value of Δh (0.05)
5: Solving the chaotic system using RK-4 algorithm and obtaining time series
6: **for** i = 1: 2000*8/16 **do**
7: $x_{rng}(16*(i-1)+1{:}16*(i-1)+16) = decimaltobinary\,(round\,(mod\,(x\,(i), 0.00065535)* 100000000), 16)$
8: **end for**
9: Ready to use 2000*8 random number
10: End

Algorithm 2 specifies the so-called random number code, which is generated on the basis of chaotic systems. According to the algorithm, the parameter and start values of the 3D Megastable Oscillator are first entered into the system. After entering the system as step interval value 0.05, the values of the 3D chaotic system used by the differential equation solution method are determined in Runge–Kutta 4. With the x phase of the 3D chaotic system whose values are determined, a 16-bit random number sequence is generated at each step. Since the data requested for encryption is 2000 pieces and the electrophysiological signals hidden in the data are eight bits, a random sequence of numbers of 2000*8 is obtained.

The NIST-800-22 test [10] was used to measure the complexity of random numbers generated. It is a security

Table 2: NIST-800-22 test results for generated random numbers from chaotic system.

Statistical tests	*p*-value	Result
Frequency monobit test	0.5312	Successful
Block-frequency test	0.6571	Successful
Run test	0.1545	Successful
Longest-run test	0.5664	Successful
Binary matrix rank test	0.7982	Successful
Discreate Fourier transform test	0.5741	Successful
Non-overlapping templates test	0.7759	Successful
Overlapping temp templates test	0.5241	Successful
Maurier's universal statistical test	0.1123	Successful
Linear complexity test	0.0815	Successful
Serial test-1	0.9142	Successful
Serial test-2	0.7533	Successful
Approximate entropy test	0.2456	Successful
Cumulative sums (forward) test	0.1908	Successful
Random excursion test ($x = -4$)	0.9165	Successful
Random excursion variant test($x = -9$)	0.8875	Successful

testing tool performed by the National Institute of Standards and Technology [11, 13]. The NIST-800-22 test contains 16 tests. In order for the generated random numbers to pass the NIST-800-22 test successfully, it must pass all 16 tests. The names of the tests are given in the table [14].

In this test, the most important parameter, the *p*-value, is considered as a measure of the complexity of the random number sequence that enters the test. If the *p*-value is a really complex series, it is close to 1, not 0. For the tests to be successful, these *p*-values must be greater than 0.01 [15–18].

In Table 2, random numbers generated from the status variables of the chaotic system were tested NIST-800-22 to measure their randomness. The results indicated that the *p*-values found in each of the 16 tests in the NIST 800-22 test were greater than 0.01. So after the NIST 800-22 test, which was made by passing all 16 tests, it was determined that it was random.

Algorithm 3 Signal encryption algorithm pseudo code.

1: Start
2: **for** i = 1: length of hidden data signal **do**
3: Encrypted signal = XOR (hidden data signal, random number)
4: **end for**
5: End

Algorithm 3 provides the encryption algorithm for electrophysiological signals hidden in data. According to the algorithm, the signal which hides the data is XOR processed by an eight bit random number sequence generated in Algorithm 2. As a result of this algorithm, data hidden and encrypted signals are shown in Figures 7 and 8, respectively.

6 Security analysis of encrypted electrophysiological signals

The bit values of encrypted data must be evenly distributed for a good encryption [17]. The data must have a proper histogram to be resistant against statistical attacks. The histogram of the encrypted data indicates that the value of each bit is the same and the values are properly distributed, indicating that the randomness has been achieved.

In Figure 9 histogram analysis of encrypted ECG, EEG and EMG signals are performed by histogram analysis of ECG, EEG and EMG signals with data hidden in the data. Data is weighted only in hidden signals, while encrypted signals have a homogeneous distribution.

There are strong correlations with non-encrypted signals. In a well-encrypted image, the correlation results should be scattered. The dispersion of the correlation results indicates a uniform variability of the values and the randomness.

There is strong correlation when the correlation maps of ECG, EEG and EMG signals are hidden in Figure 10. There is a numbness between adjacent pixels. In encrypted electrophysiological signals, the correlation was low and the distribution was homogeneous.

The knowledge of entropy is a mathematical theory derived from Shannon [22, 20]. It is a feature that defines randomness and uncertainty in data and is used to measure the same distribution of values in the data. The entropy value is calculated using Eq. (8) [19].

$$H(s) = \sum_{i=0}^{2^M-1} P(s_i) \log_2 \frac{1}{P(s_i)} \tag{8}$$

$$\mathrm{NPCR} = \frac{1}{M} \sum_{i=1}^{M} Dif(i) * 100\% \tag{9}$$

$$\mathrm{Dif}(i) = \begin{cases} 1 & C_1(i) \neq C_2(i) \\ 0 & C_1(i) = C_2(i) \end{cases} \tag{10}$$

$$\mathrm{UACI} = \frac{1}{M} \frac{\sum_{i=1}^{M} |C_1(i) - C_2(i)|}{255} \mathrm{Dif}(i) * 100\% \tag{11}$$

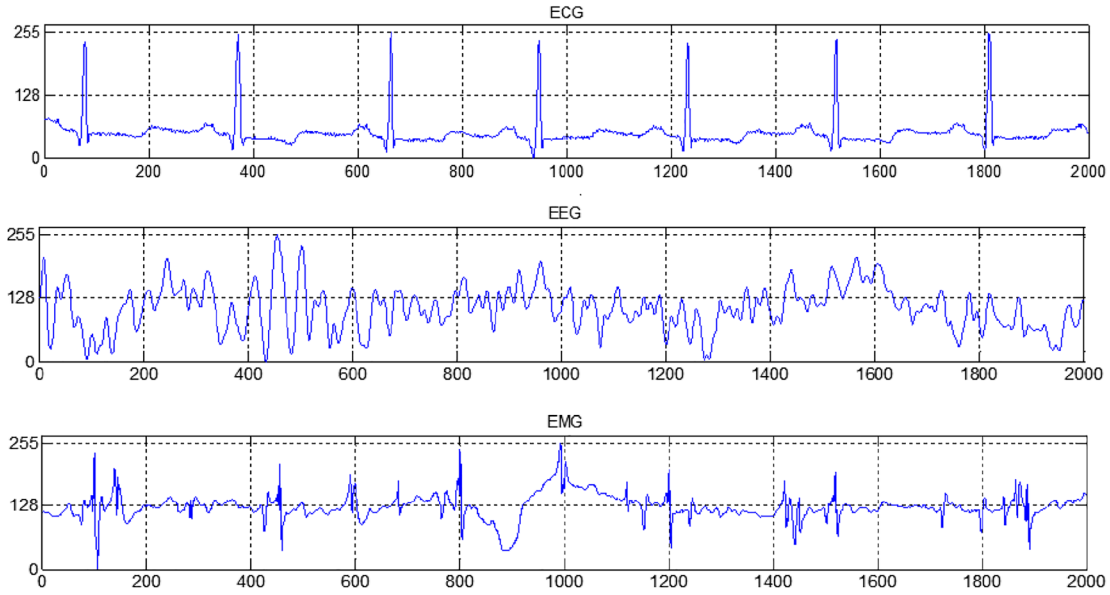

Figure 7: Data hidden electrophysiological signals.

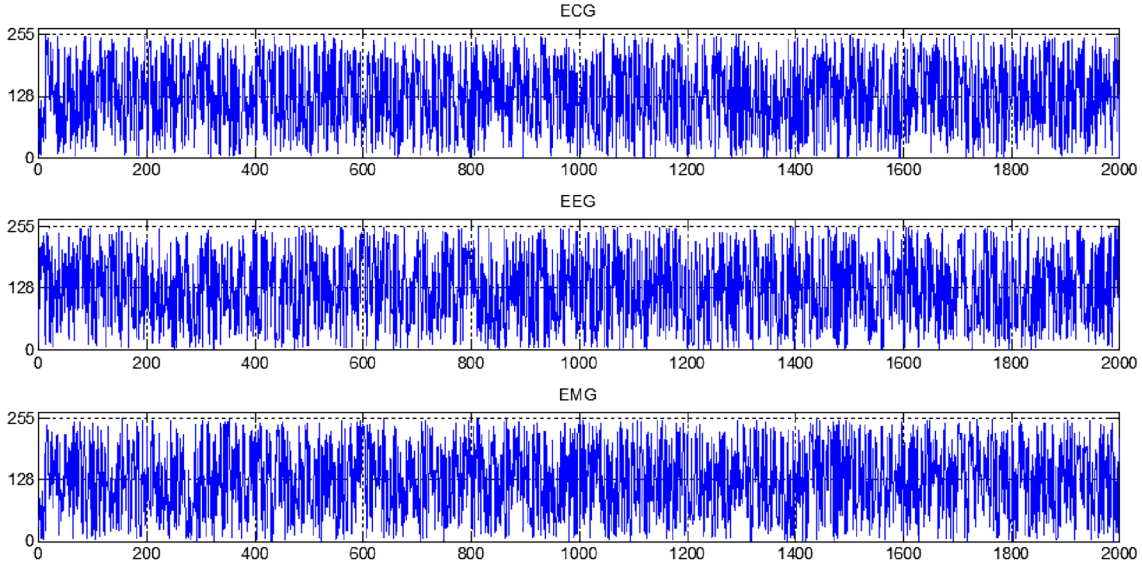

Figure 8: Encrypted electrophysiological signals.

In the equations, M represents the total number of values in the data, C_1 represents the values of unencrypted data, C_2 represents the values of the encrypted data. The Number of Changing Pixel Rate (NPCR) shows the number of changed values between encrypted and unencrypted data, and the Unified Averaged Changed Intensity (UACI) shows the average value of the changed values [24]. In previous studies, the fact that NPCR is greater than 99.6% and UACI is close to or greater than 30% has been accepted as an indication of good encryption.

While the entropy value in the unencrypted data in the table is far from eight which is the number of the data in bit, this value is very close to eight in the encrypted data. As the result of the encryption, the entropy value is close to the maximum values, which means that the encrypted data has good frequency values. In addition, it has been shown

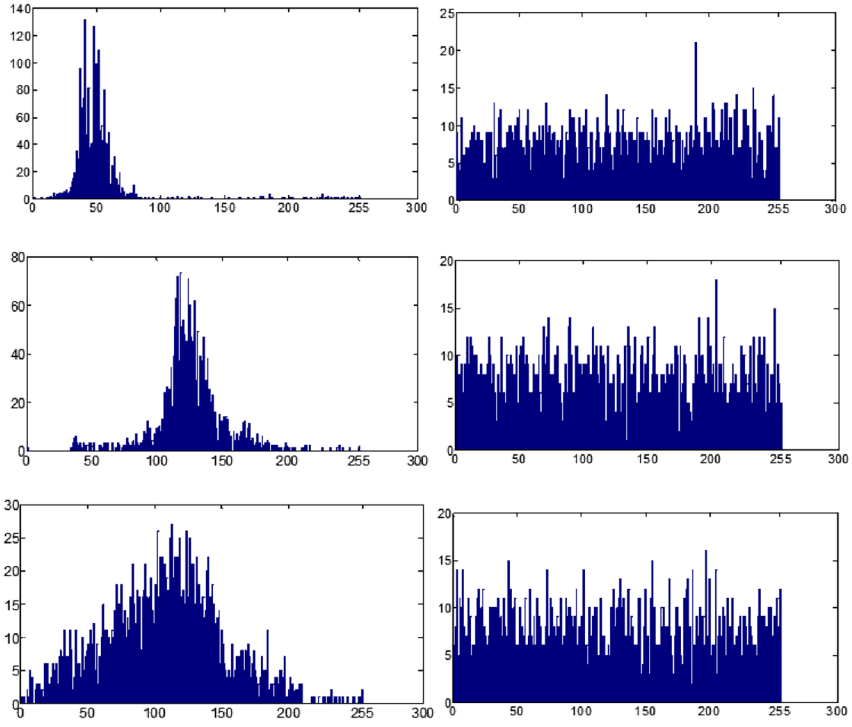

Figure 9: Histogram analysis of original and encrypted ECG, EEG and EMG signals.

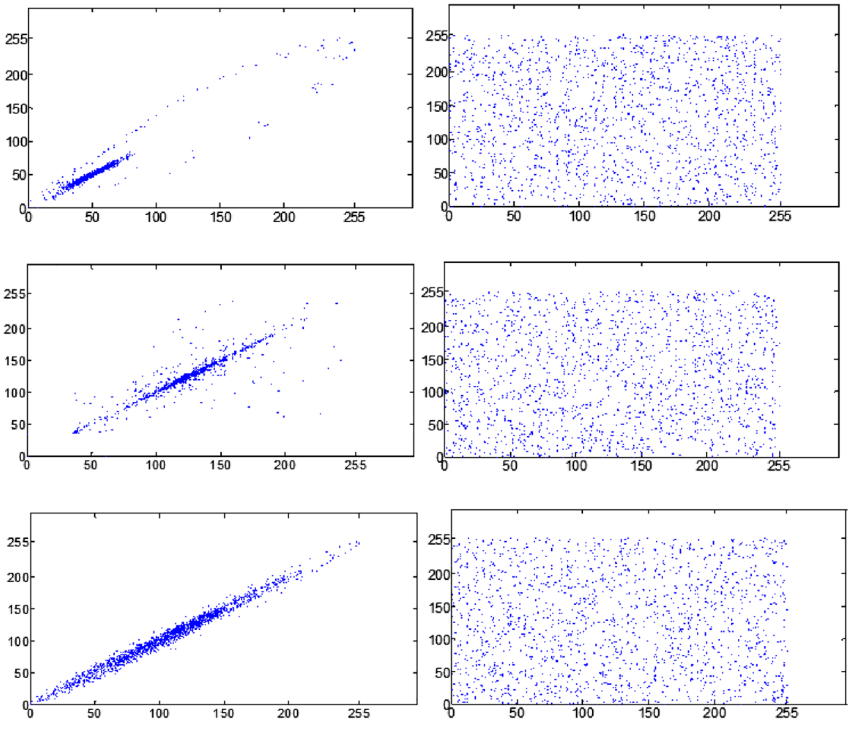

Figure 10: Correlation analysis of original and encrypted ECG, EEG and EMG signals.

Table 3: Entropy, UACI and NPCR analysis of original and encrypted electrophysiological signals.

	Entropy	UACI	NPCR
ECG	5.4686	0.3536	0.9975
Encrypted ECG	7.9934		
EEG	7.3816	0.3283	0.9970
Encrypted EEG	7.9860		
EMG	6.3197	0.3222	0.9964
Encrypted EMG	7.9808		

that NPCR and UACI encryption analyzes were successfully passed in Table 3.

7 Graphical user interface design

The recording of electrophysiological signals from the person into the database facilitates the work of health workers with an interface designed as given Figure 11. This designed interface retrieves the person's name and ID number information from the user and enters it into the system. The retrieve text button transforms the person's information into a text sequence. The signal type received by the person is then selected and transmitted to the interface in the voltage unit. The hide data button hides a text sequence in the signal information converted to eight bites. In the final phase, the electrophysiological signal is encrypted with random numbers from the chaotic system by pressing the encrypt data button. The encrypted data is securely stored in the database with the name entered by the user. The process of storing a sample ECG data in the database is displayed in the interface environment.

Figure 12 shows the process of decrypting the signal stored in the database in an encrypted form to give contact information to the screen. First, the encrypted data which will be decrypted in the database is transferred to the interface via the import data button in the interface.

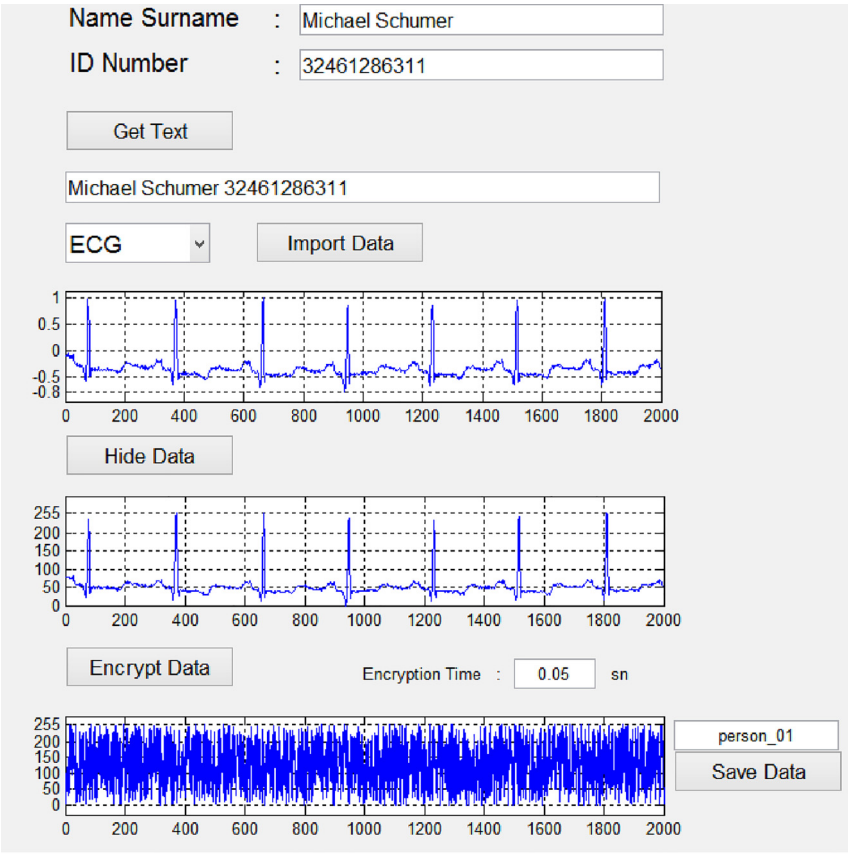

Figure 11: Graphical user interface main screen.

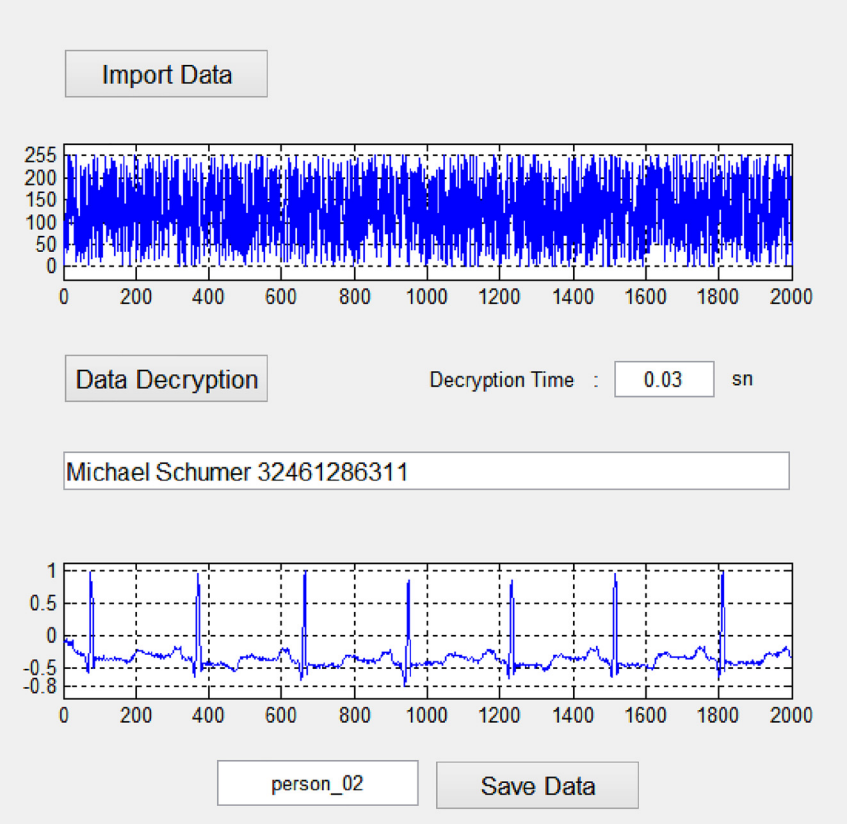

Figure 12: Graphical user interface screen.

While the process of encrypting the signal and storing the person's information in the signal took 50 ms, it took only 30 ms to retrieve the original signal and the hidden personal data from the encrypted signal.

8 Conclusion

In this paper, a novel 3D chaotic oscillator which shows megastability without any external excitation was introduced with some dynamical analysis. It is to be proved that such an oscillator was not shown in the earlier literatures. This paper includes both encryption and data hiding processes for high security in electrophysiological signals. ECG, EEG and EMG signals were utilized for personal data hiding and cryptology applications on a microcomputer. In the cryptology application, random numbers were obtained via the novel 3D megastability chaotic oscillator. These random numbers were tested with NIST-800-22 and they successfully passed from all NIST-800-22 tests.

The encrypted electrophysiological signals which hide data with LSB technique were done security analysis such as MSE, PSNR, entropy, differential attacks, histogram, correlation and initial condition sensitivity. An input parameter error (for example, 10^{-12}initial condition error) does not allow signals to be decrypted. The results have proved that the security analysis are successful. These analysis gave superior encryption results, and the electrophysiological signals were completely recovered when the correct initial condition parameter was applied. Also, a user interface is developed to ease of use. This study set out to assess the feasibility of realising to secure transfer the electrophysiological signals. The results of the analysis have shown that the proposed two-level security method can be used in many fields as mobile in the future.

Author contribution: All the authors have accepted responsibility for the entire content of this submitted manuscript and approved submission.

Research funding: This work is supported by the Scientific and the Research Council of Turkey (TUBITAK) under Grant No. 117E284. Karthikeyan Rajagopal was partially supported by Institute of Research and Development, Defence University, Ethiopia with grant CND/DEC/2018-2.

Conflict of Interest: None.

Ethical approval: Not required.

References

[1] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: conveying the utility of

homomorphic encryption and multiparty computation," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, 2012.
[2] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 1, pp. 34–41, 2008.
[3] M. Ahmad, O. Farooq, S. Datta, S. S. Sohail, A. L. Vyas, and D. Mulvaney, "Chaos-based encryption of biomedical EEG signals using random quantization technique," in *2011 4th International Conf. on Biomedical Engineering and Informatics (BMEI)*, vol. 3, Shanghai, China, IEEE, 2011, pp. 1471–1475.
[4] F. Sufi, F. Han, I. Khalil, and J. Hu, "A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 515–524, 2011.
[5] R. S. Douglas, *Cryptography: Theory and Practice*, Chapman and Hall/CRC, Ontario, Canada, 2005.
[6] L. Moysis, A. Tutueva, K. Christos, and D. Butusov, "A chaos based pseudo-random bit generator using multiple digits comparison," *Chaos Theory Appl.*, vol. 2, no. 2, pp. 58–68, 2020.
[7] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, 2017.
[8] Arshad, S. Shaukat, A. Ali, E. Amna, S. S. Aziz, and A. Jawad, "Chaos theory and its application: An essential framework for image encryption," *Chaos Theory Appl.*, vol. 2, no. 1, pp. 15–20, 2020.
[9] C.-F. Lin, C.-H. Chung, and J. H. Lin, "A chaos-based visual encryption mechanism for clinical EEG signals," *Med. Biol. Eng. Comput.*, vol. 47, no. 7, pp. 757–762, 2009.
[10] S. Thakur, K. S. Amit, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimed. Tools. Appl.*, vol. 78, no. 3, pp. 3457–3470, 2019.
[11] M. Z. Yildiz, O. F. Boyraz, E. Guleryuz, A. Akgul, and I. Hussain, "A novel encryption method for dorsal hand vein images on a microcomputer," *IEEE Access*, vol. 7, pp. 60850–60867, 2019.
[12] G. Chen, "Chaos theory and applications: a new trend," *Chaos Theory Appl.*, vol. 3, no. 1, pp. 1–2, 2021.
[13] L.-B. Zhang, Z.-L. Zhu, B.-Q. Yang, W.-Y. Liu, H.-F. Zhu, and M.-Y. Zou, "Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach," *Math. Probl. Eng.*, vol. 2015, p. 940638, 2015.
[14] C.-F. Lin, W.-T. Chang, H.-W. Lee, and S.-I. Hung, "Downlink power control in multi-code CDMA for mobile medicine," *Med. Biol. Eng. Comput.*, vol. 44, no. 5, p. 437, 2006.
[15] C.-F. Lin, W.-T. Chang, and C.-Y. Li, "A chaos-based visual encryption mechanism in JPEG2000 medical images," *J. Med. Biol. Eng.*, vol. 27, no. 3, pp. 144–149, 2007.
[16] C.-F. Lin, C.-H. Chung, Z.-L. Chen, C.-J. Song, and Z.-X. Wang, "A chaos-based unequal encryption mechanism in wireless telemedicine with error decryption," *WSEAS Trans. Syst.*, vol. 7, no. 2, pp. 49–55, 2008.
[17] C.-F. Lin, and C. Y. Li, "A DS UWB transmission system for wireless telemedicine," *WSEAS Trans. Syst.*, vol. 7, no. 7, pp. 578–588, 2008.
[18] C.F. Lin, "A Ka band WCDMA-based LEO transport architecture in mobile telemedicine," *Telemed. 21st Century*, 2008. https://ci.nii.ac.jp/naid/10025029096.
[19] C.-F. Lin, "Chaos-based 2D visual encryption mechanism for ecgmedical signals," *Int. J. Comput. Res.*, vol. 18, nos 3/4, p. 341, 2011.
[20] C.-F. Lin and B. S. H. Wang, "A 2D chaos-based visual encryption scheme for clinical EEG signals," *J. Mar. Sci. Technol.*, vol. 19, no. 6, pp. 666–672, 2011.
[21] X. Hao, J. Wang, Q. Yang, X. Yan, and P. Li, "A chaotic map-based authentication scheme for telecare medicine information systems," J. Med. Syst., vol. 37, no. 2, p. 9919, Jan. 2013.
[22] S. Parveen, S. Parashar, and Izharuddin, "Technique for providing security in medical signals," in *2011 International Conf. on Multimedia, Signal Processing and Communication Technologies*, Aligarh, India, IEEE, 2011, pp. 68–71.
[23] Y. Tang, H. R. Abdolmohammadi, A. J. M. Khalaf, Y. Tian, and T. Kapitaniak, "Carpet oscillator: a new megastable nonlinear oscillator with infinite islands of self-excited and hidden attractors," *Pramana*, vol. 91, no. 1, p. 11, 2018.
[24] Y.-X. Tang, A. J. M. Khalaf, K. Rajagopal, V.-T. Pham, S. Jafari, and Y. Tian, "A new nonlinear oscillator with infinite number of coexisting hidden and self-excited attractors," *Chin. Phys. B*, vol. 27, no. 4, p. 040502, 2018.
[25] Z. Wei, Y. Li, B. Sang, Y. Liu, and W. Zhang, "Complex dynamical behaviors in a 3D simple chaotic flow with 3D stable or 3D unstable manifolds of a single equilibrium," *Int. J. Bifurcat. Chaos*, vol. 29, no. 07, p. 1950095, 2019.
[26] Y. Li, Z. Wei, W. Zhang, M. Perc, and R. Repnik, "Bogdanov–takens singularity in the hindmarsh–rose neuron with time delay," *Appl. Math. Comput.*, vol. 354, pp. 180–188, 2019.
[27] Z. Wei, V. -T. Pham, A. J. M. Khalaf, J. Kengne, and S. Jafari, "A modified multistable chaotic oscillator," *Int. J. Bifurcat. Chaos*, vol. 28, no. 07, p. 1850085, 2018.
[28] J. C. Sprott, S. Jafari, A. J. M. Khalaf, and T. Kapitaniak, "Megastability: coexistence of a countable infinity of nested attractors in a periodically-forced oscillator with spatially-periodic damping," *Eur. Phys. J. Spec. Top.*, vol. 226, no. 9, pp. 1979–1985, 2017.
[29] K. Rajagopal, J. P. Singh, B. K. Roy, and A. Karthikeyan, "Dissipative and conservative chaotic nature of a new quasi-periodically forced oscillator with megastability," *Chin. J. Phys.*, vol. 58, pp. 263–272, 2019.
[30] P. Prakash, K. Rajagopal, J. P. Singh, and B. K. Roy, "Megastability, multistability in a periodically forced conservative and dissipative system with signum nonlinearity," *Int. J. Bifurcat. Chaos*, vol. 28, no. 09, p. 1830030, 2018.
[31] P. Prakash, K. Rajagopal, J. P. Singh, and B. K. Roy, "Megastability in a quasi-periodically forced system exhibiting multistability, quasi-periodic behaviour, and its analogue circuit simulation," *Int. J. Electron. Commun.*, vol. 92, pp. 111–115, 2018.
[32] H. Jahanshahi, K. Rajagopal, A. Akgul, N. N. Sari, H. Namazi, and S. Jafari, "Complete analysis and engineering applications of a megastable nonlinear oscillator," *Int. J. Nonlin. Mech.*, vol. 107, pp. 126–136, 2018.
[33] J. C. Sprott, "A proposed standard for the publication of new chaotic systems," *Int. J. Bifurcat. Chaos*, vol. 21, no. 09, pp. 2391–2394, 2011.
[34] J. R. Ira, "A primer for eeg signal processing in anesthesia," *Anesthesiology*, vol. 89, no. 4, pp. 980–1002, 1998.
[35] C. Saritha, V. Sukanya, and Y. N. Murthy, "ECG signal analysis using wavelet transforms," *Bulg. J. Phys.*, vol. 35, no. 1, pp. 68–77, 2008.

[36] T.-T. Pan, P.-L. Fan, H. K. Chiang, R.-S. Chang, and J.-A. Jiang, "Mechatronic experiments course design: a myoelectric controlled partial-hand prosthesis project," *IEEE Trans. Educ.*, vol. 47, no. 3, pp. 348–355, 2004.

[37] M. Alcin, K. Ismail, M. Tuna, V. Metin, and I. Pehlivan, "A novel high speed artificial neural network–based chaotic true random number generator on field programmable gate array," *Int. J. Circ. Theor. Appl.*, vol. 47, no. 3, pp. 365–378, 2019.

[38] S. Vaidyanathan, I. Pehlivan, L. G. Dolvis, et al., "A novel ANN-based four-dimensional two-disk hyperchaotic dynamical system, bifurcation analysis, circuit realisation and FPGA-based TRNG implementation," *Int. J. Comput. Appl. Technol.*, vol. 62, no. 1, pp. 20–35, 2020.

[39] K. İsmail, M. Tuna, İ. Pehlivan, C. B. Fidan, and M. Alçın, "Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator," *Analog Integr. Circuits Signal Process.*, vol. 102, no. 2, pp. 445–456, 2020.

[40] M. Tuna, A. Karthikeyan, K. Rajagopal, M. Alcin, and K. İsmail, "Hyperjerk multiscroll oscillators with megastability: analysis, FPGA implementation and a novel ANN-ring-based true random number generator," Int. J. Electron. Commun., vol. 112, p. 152941, 2019.

[41] A. Akif, C. Arslan, and B. Arıcıoğlu, "Design of an interface for random number generators based on integer and fractional order chaotic systems," Chaos Theory Appl., vol. 1, no. 1, pp. 1–18, 2019.