**Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi**
*Bilecik Seyh Edebali University Journal of Science*

12(1), 196-205, 2025

**DOİ:** 10.35193/bseufbd.1491435
*e-ISSN: 2458-7575 (https://dergipark.org.tr/tr/pub/bseufbd)*

*Araştırma Makalesi - Research Article*

# Chaotic Image Encryption with Normal Sinus Rhythm ECG Signal and Chaoticity in ECG Signal

# Normal Sinüs Ritmi EKG Sinyali ile Kaotik Görüntü Şifreleme ve EKG Sinyalinde Kaotiklik

Zehra Gülru Çam Taşkıran[1*], Ramazan Cenker[2]

***Geliş / Received: 28/05/2024*** ***Revize / Revised: 04/08/2024*** ***Kabul / Accepted: 18/08/2024***

**ABSTRACT**

In this study, the use of ECG data in the field of secure communication was examined by using a chaotic encryption method that has proven its reliability in the literature. ECG data, the chaoticity of which is a controversial issue in the literature, was used directly instead of chaotic number sequences in this method, and a security analysis was made over the NPCR, UACI, and entropy values of the encrypted images. While NPCR and UACI values indicate the security of the system against plaintext attacks by revealing the dissimilarity rate at the pixel level between two images encrypted with different keys, the entropy value indicates the encryption performance by giving information about how close the encrypted image is to the random appearance. In addition, phase portraits and Lyapunov exponents were examined, and the chaotic components in ECG were shown. According to the results, it has been observed that the sequence of numbers obtained by determining the person, the phase shift samples count, and the time of ECG taken can be used as the key with this method. In addition to the periodicity of healthy ECG data, the chaotic properties it contains have been shown to be sufficient for encryption applications.

***Keywords- ECG Signal, Chaoticity, Image Encryption, Chaotic Encryption***

**ÖZ**

Bu çalışmada literatürde güvenilirliği kanıtlanmış kaotik bir şifreleme yöntemi kullanılarak EKG verilerinin güvenli iletişim alanında kullanımı incelenmiştir. Kaotikliği literatürde tartışmalı bir konu olan EKG verileri bu yöntemde kaotik sayı dizileri yerine doğrudan kullanılmış ve şifrelenmiş görüntülerin NPCR, UACI ve entropi değerleri üzerinden güvenlik analizi yapılmıştır. NPCR ve UACI değerleri farklı anahtarlarla şifrelenmiş iki görüntü arasındaki piksel düzeyindeki farklılık oranını ortaya koyarak sistemin düz metin saldırılarına karşı güvenliğini gösterirken, entropi değeri ise şifrelenmiş görüntünün rastgele görünüme ne kadar yakın olduğu hakkında bilgi vererek şifreleme performansını göstermektedir. Ayrıca faz portreleri ve Lyapunov üstelleri incelenerek EKG'deki kaotik bileşenler gösterilmiştir. Elde edilen sonuçlara göre kişi, faz kayması örnek sayısı ve EKG çekim zamanı belirlenerek elde edilen sayı dizisinin bu yöntemle anahtar olarak kullanılabileceği görülmüştür. Sağlıklı EKG verilerinin periyodikliğinin yanı sıra içerdiği kaotik özelliklerin de şifreleme uygulamaları için yeterli olduğu gösterilmiştir.

***Anahtar Kelimeler- EKG sinyali, Kaotiklik, Görüntü Şifreleme, Kaotik Şifreleme***

[1]*Sorumlu yazar iletişim: zgcam@yildiz.edu.tr (https://orcid.org/0000-0002-7996-7948)
*Elektronik ve Haberleşme Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, 34220, İstanbul, Türkiye*
[2]İletişim: ramazancenker@gmail.com (https://orcid.org/0000-0003-0740-2291)
*Elektronik ve Haberleşme Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, 34220, İstanbul, Türkiye*

## I. INTRODUCTION

The chaoticity of ECG signals is a controversial issue in the literature [1]. However, the generally accepted approach is that in case of arrhythmia, heart attack, tachycardia, and atrial fibrillation, ECG signals are chaotic, while healthy rhythm signals are periodic. In the literature, chaotic analyses have been made to recognize arrhythmia and atrial fibrillation and have been successful [2, 3]. Using chaotic methods while detecting R-peak in ECG signals shows that this signal carries chaotic components [4]. A similar study has been done for QRS detection [5]. In these cases, chaotic features are observed more dominantly in the signals. However, healthy rhythm signals also contain non-periodic components because the biomedical signal is a product of an interaction of a large number of different biological systems, the noise of the measurement mechanism, and the nature of the ECG itself. When Lyapunov exponents of healthy individuals' ECG signals are calculated, chaotically contradictory results are obtained. Chaotic signals produce positive Lyapunov exponents. It has also been shown that the exponents of ECG signals from healthy people are smaller than people with heart disease [6]. However, the adequacy of the chaotic components in it in terms of encryption security is open to examination. This study aims to examine whether these components in the ECG signals of healthy people can be used as cryptological keys.

Multimedia data consists of text, audio, video, graphics, and images. In recent years, there has been rapid development in multimedia, including video, image, and audio. With the increasing use of multimedia data over the internet, the demand for secure multimedia data arises. Chaos-based methods have recently become attractive to secure image content. Based on some unique properties such as sensitivity to initial conditions, non-periodicity, convergence, and control parameters, chaos has become the latest trend in image encryption. The basic requirement in chaotic encryption algorithms is a good encryption scheme and keys that will be produced with sufficient length and sufficient complexity, that is, chaotic sequences. In the chaotic encryption algorithms proposed in the literature, time series produced by dynamic systems such as Lorenz, Rössler, and Henon maps, which are generally defined by ordinary differential equations, are used as the key [7-10].

The use of ECG signals in the field of information security is quite limited. In general, studies have been conducted for the secure transmission and storage of ECG signals [11-13]. In this study, unlike these, the use of the ECG signal instead of the chaos signal in chaotic coding methods is examined.

In a study using ECG signals for a similar purpose, a dynamic key based on ECG signal was created and used by continuously measuring the distance between the QRS waves [14]. The results obtained in this study are insufficient in terms of plain-text security. In a different study, residual signals were obtained by filtering long-term trends for key generation from ECG signals. Because it has been determined that there are chaotic components in short-term changes in the ECG. The P wave represents the depolarization impulse of the atrium; the QRS complex represents ventricular depolarization, while the T wave represents the repolarization of the ventricles. The R-peak, the most noticeable feature of the ECG waveform, is often used to represent the heartbeat. These keys are created by using the time delays between these waves [15]. In a similar study, finite-length keys were created by using some distinguishing features in the ECG signal [16].

In the mentioned studies, time-invariant metrics of the person's ECG were obtained and these constants were used as keys in encryption. Chaotic components in the ECG were not used intentionally, but their existence was emphasized in all studies. In this study, unlike the mentioned studies, the focus was directly on these chaotic components. For the encryption method used, 3 different chaotic series are needed. Instead of producing personalized series using a different dynamic system with ECG metrics, different series were created by shifting the person's ECG signal at different phase shifts and encryption was performed by using these series directly instead of the chaotic series. The ECG signals used were obtained from the MIT-BIH Normal Sinus Rhythm Database [17]. In this way, it was examined whether the chaotic components contained in the ECG were sufficient in terms of encryption security, whether healthy ECG data constituted personal biometric data, and whether the phase shift count was a key in this encryption method.

## II. USED CHAOTIC IMAGE ENCRYPTION ALGORITHM

A chaotic encryption algorithm, which has been proven to be reliable before in the literature, was chosen to check the suitability of the data to be used [18]. The encryption algorithm used basically consists of 4 steps: Histogram Equalization, Row Rotation, Column Rotation, XOR Operation. The flow chart of the encryption algorithm is given in Figure 1.

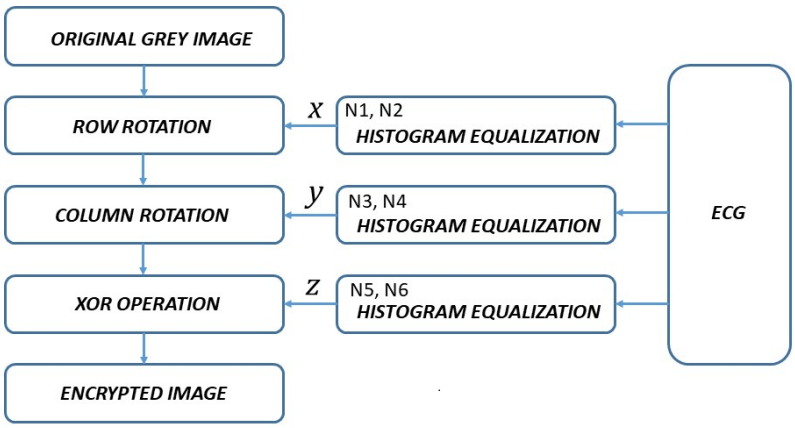



**Figure 1.** The flow chart of the encryption algorithm.

### *A. Histogram Equalization*

As seen in Figure 2, it is clear that the histograms of 3 different chaotic signals, called $x$, y, $z$, have an inhomogeneous distribution. For higher security, the histogram needs to be equalized. If there is a gray image of size $M \times N$, $M$ represents the number of rows and $N$ represents the number of columns. The histogram is then equalized using Eq. 1.

$$x = integer(x \times N2) mod N \tag{1a}$$

$$y = integer(y \times N4) mod M \tag{1b}$$

$$z = integer(z \times N6) mod 256 \tag{1c}$$

Here, $N2$, $N4$, $N6$ is a large random number usually greater than 10000. For simplicity, $N2$, $N4$, and $N6$ can also be considered equal. Figure. 1(g), (h), and (i) show the equalized histogram using random numbers $N2$ = $N4$ = $N6$ =100000, $M$ = $N$ = 256. The aim here is to approximate the 3 series to be used to a uniform distribution. In this algorithm, the equivalence of the odd and even distributions in $x$ and $y$, and the approximation of $z$ to a random distribution in the range of pixel values in the grayscale image, as much as possible are essential.

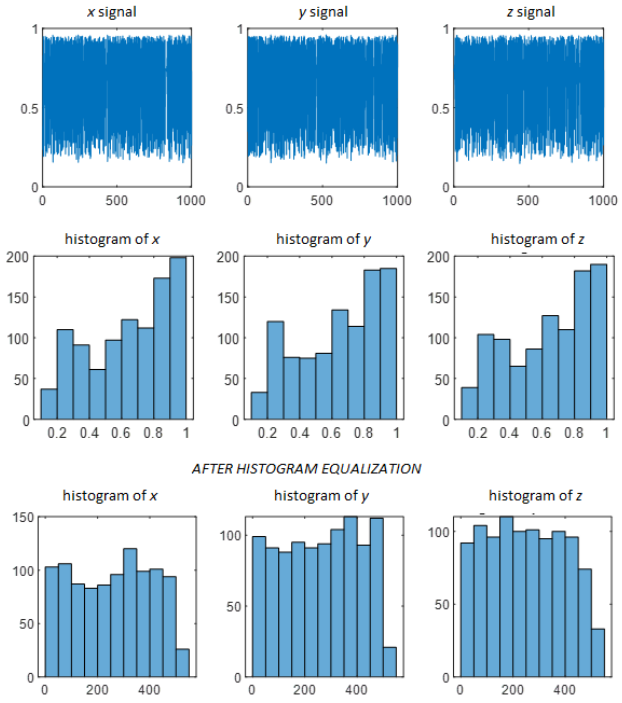



**Figure 2.** ECG signal histogram equalization.

### *B. Row Rotation*

Row rotation is performed for image pixel permutation. Since there are $M$ pixel elements in a row, a $M$ length chaotic sequence is used to rotate the row of a gray image of size $M \times N$. To increase the security, according to the randomly determined $N1$ number of the $x$-sequence obtained using the ECG signal, a total of $M$ elements are taken from the $N1$st ($N1 = 500$) element. In the selected row, when the key value corresponding to the row number is even, the entire row is rotated to the left, and when it is odd, the entire row is rotated to the right.

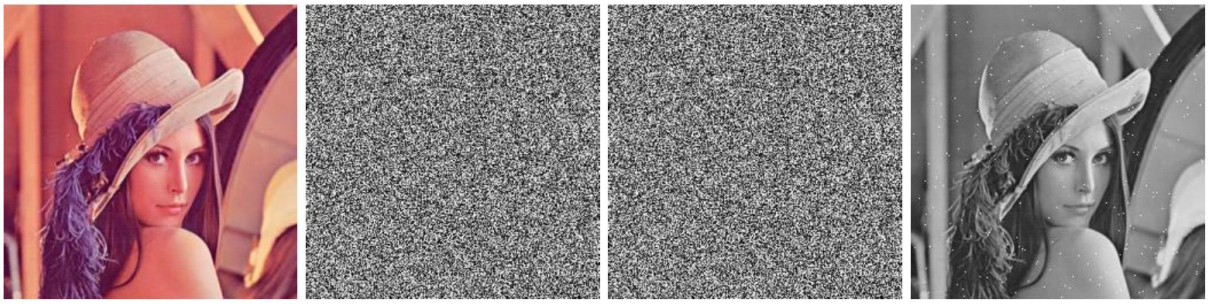
### *C. Column Rotation*

This step is performed after the row rotation is complete. Since there are $N$ pixel elements in a column, a $N$ length of the chaotic sequence is used to rotate the column of a gray image of size $M \times N$. To increase the security, according to the randomly determined $N3$ number of the $y$-sequence obtained by using the ECG signal, a total of $N$ elements are taken from the $N3$rd ($N3 = 600$) element. In the selected column, when the key value corresponding to the number of columns is even, it is rotated up and if the value is odd, it is rotated down.

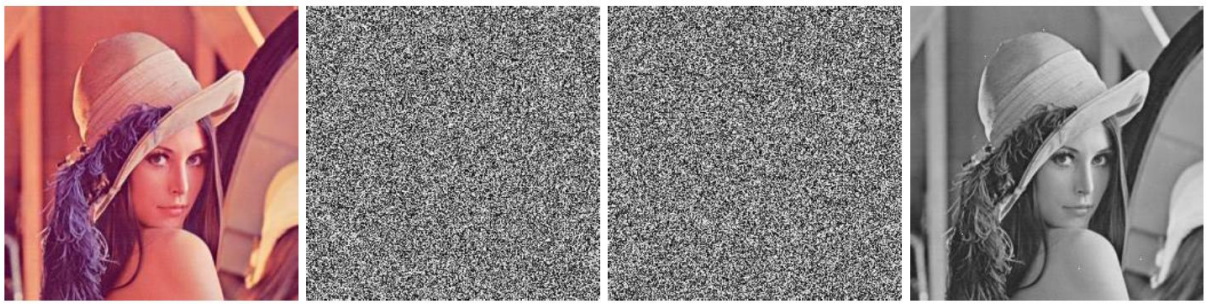
### *D. XOR Operation*

The last step of the encryption process is the XOR operation. The XOR operation changes the pixel value to the new value, and the new value cannot be reversed without knowing the key obtained using the ECG signal. First, random number $N5$ value is entered, and $M \times N$ image is converted to $1 \times MN$ image. After that, the row-column rotated image ais XORed with the ECG signal (starting from the $N5$th ($N5 = 700$) element of the sequence), and finally, the encrypted image is obtained.

The original versions of the used benchmark image Lena, its encrypted versions with 3 and 10 phase shifts of Subject 1, and the decrypted version are given in Fig. 3. In order to compare the encryption patterns, the Lorenz system, known in the literature for its dominant chaotic feature, was used [19]. The benchmark image Lena, encrypted with two different chaotic sequences obtained by slightly changing the initial conditions, and the decrypted Lena are given in Figure 3.a. The Lena images encrypted with two different ECG sequences obtained from the 3 and 10 phase shift spaces of Subject 1 and the decrypted version are given in Figure 3.b.



a. Image examples obtained by using chaotic Lorenz system.



b. Image examples obtained by using ECG signals of Subject 1.

**Figure 3.** Original image, two encrypted images with different keys, and decrypted image.

## III. SECURITY ANALYSIS

It has been investigated whether it is appropriate to use ECG signals directly as a chaotic sequence in encrypting benchmark images frequently used in the literature. Some common metrics are used to evaluate the security of the algorithm used.

Using a computer equipped with an Intel(R) Core (TM) i5-8265U 1.80 GHz CPU; all simulations were performed by Matlab R2022a. The security of the encrypted images was examined by making analyzes with the healthy human ECG data, the chaoticity of which is controversial. Long-term ECG recordings of 3 healthy subjects referred to the Arrhythmia Laboratory at Beth Israel Hospital in Boston were used for analysis [17]. The subjects do not have a dominant arrhythmia or infarction. Two metrics are used to evaluate the sensitivity of plain-text attacks, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). It is expressed as in Eq. 2, NPCR is defined as the percentage of different pixel numbers between two encrypted images. UACI; $M \times N$ is defined as the mean intensity of the differences between the two encrypted images as in Eq. 3. Here $C1$ and $C2$ are two different encrypted images encrypted using different keys [20]. Each of these metrics is obtained by comparing all values of two images encrypted with different keys but the same method, pixel by pixel. To build a near-ideal image encryption algorithm, NPCR values must be greater than 99% and UACI values must be around 33% [21].

$$NPCR = \frac{\sum D(i,j)}{M \times N} 100\% \tag{2a}$$

$$D(i,j) = \begin{matrix} 1 \; if \; C1(i,j) \neq C2(i,j) \\ 0 \; if \; C1(i,j) = C2(i,j) \end{matrix} \tag{2b}$$

$$UACI = \frac{1}{M \times N} \sum \frac{|C1(i,j) - C2(i,j)|}{255} 100\% \tag{3}$$

The information entropy value is a measure of the randomness of the given data. For a good image encryption algorithm, the encrypted image should have equiprobable gray levels. For example, for a gray-scale image of 256 levels, if each gray level is assumed to be equiprobable, the image entropy will be theoretically equal to 8 bits. It is desired that this value be as close as possible to 8 for cryptological applications, in the sense that the probability of all pixel values is equal. It is calculated as in Eq. 4 where $n$ represents the total number of symbols, $Si$ is the pixel value and $P$ ($Si$) represents the probability of occurrence of $Si$ [22].

$$H(s) = \sum_{i=0}^{n-1} P(S_i) \log_2 \frac{1}{P(S_i)} \tag{4}$$

## IV. SIMULATION RESULTS

To obtain the 3 different number sequences required for the used encryption algorithm, the time series consisting of ECG data was shifted by a different number of samples, and phase-shifted spaces were formed. For this purpose, to create a new sequence within the collected one-dimensional ECG data, the previous sequence is shifted at the specified phase shift count [23]. This shifting process is performed twice, resulting in 3 different sequences.

**Table 1.** Effect of Raw ECG Data From Different People on NPCR and UACI

| Phase Shift Count | Subjects | NPCR | UACI |
|---|---|---|---|
| 1 | Subject 1&2 | 99,6368 | 33,9043 |
| | Subject 1&3 | 99,6140 | 33,4521 |
| | Subject 2&3 | 99,6384 | 33,4144 |
| 10 | Subject 1&2 | 99,6185 | 33,6864 |
| | Subject 1&3 | 99,6307 | 33,4053 |
| | Subject 2&3 | 99,5972 | 33,3632 |
| 17 | Subject 1&2 | 99,6216 | 33,6640 |
| | Subject 1&3 | 99,6094 | 33,3917 |
| | Subject 2&3 | 99,6017 | 33,4743 |

Firstly, the NPCR and UACI values of the same images encrypted using ECG signals belonging to different people were compared to examine whether ECG signals could be secure keys and the results are presented in Table 1. Since all these data were collected from healthy people, it was proven that images encrypted with 2 different signals accepted as periodic in the literature, were different from each other. UACI was obtained as 33.9043% at most. This shows that individual ECG data can be applied to chaotic encryption methods as biometric keys. Here, it is seen that although it is accepted as a periodic signal, it contains a randomness that can be used for

encryption. Despite the different phase shift numbers, it is seen that NPCR and UACI values give a value that confirms secure encryption every time. As a result of the tests carried out with the method used, it was understood that ECG keys have high sensitivity in image encryption, and healthy ECG signals belonging to different people create different keys. This proves that the chaotic components in the ECG create sufficient randomness, that people's ECGs create a unique biometric series, and that an image encrypted with one cannot be encrypted with the other.

After observing that individuals produce different keys from each other, different spaces were obtained by shifting the ECG data taken from the same person at different times by different sample numbers, and the same analyzes were made for these samples. As can be seen in Table 2, different spaces obtained with different signals yielded successful results in terms of encryption security as they produce completely different time series. In this way, it has been shown that although healthy ECG data are accepted periodic in the literature, ECG data taken from the same person at different times does not produce the same key. Even when the number of phase shifts is the same, encryptions made with samples taken at different times are completely secure. It constantly produces safe keys with the ECGs of even healthy people. This shows that besides the periodicity of the ECG signal, the components it contains create a continuous randomness.

**Table 2.** Effect of Raw ECG Data Generated with Different Sample Shifts on NPCR and UACI

| Subject | Phase Shift Count | | NPCR | UACI |
|---|---|---|---|---|
| Subject 1 | 1 | 10 | 99,5773 | 33,2148 |
| | 10 | 10 | 99,5514 | 33,2321 |
| | 17 | 10 | 99,5422 | 33,1516 |
| Subject 2 | 1 | 10 | 99,5331 | 33,6405 |
| | 10 | 10 | 99,5285 | 33,7338 |
| | 17 | 10 | 99,5850 | 33,5854 |

The information entropy values for all encrypted images were also calculated and given in Table 3. It is seen that the ($S$) values are quite close to the ideal value of 8. That means that the amount of unpredictable randomness in encrypted images is extremely close to the ideal value, meaning that successful encryption has been performed.

**Table 3.** Entropy Values of the Obtained Encrypted Images with Raw ECG Data

| Subject | Phase Shift Count | | |
|---|---|---|---|
| | 1 | 10 | 17 |
| Subject 1 | 7,9849 | 7,9856 | 7,9845 |
| Subject 2 | 7, 9842 | 7,9845 | 7,9831 |
| Subject 3 | 7,9871 | 7,9869 | 7,9868 |

Since the used chaotic encryption algorithm deals with numerical values in decimals with high precision, it is necessary to control whether encryption performance is achieved only by noise on the signal. For this reason, the Low Pass FIR filter is used to remove high-frequency noises in ECG signals obtained from the database. The stopband attenuation of the FIR filter is at 60 Db. A notch filter has been applied to eliminate network noises. In addition, the maximum fluctuation was tried to be minimized for all frequencies with the Parks-McClellan algorithm [24]. The analyzes performed in the previous steps were also repeated for the refiltered ECG signals.

The NPCR and UACI results of the encryptions with the filtered signals taken from the subjects in different phase-shifted spaces are given in Table 4. It is seen that the results obtained are very close to the results obtained with the original ECG data.

The NPCR and UACI data obtained for the filtered data of the same individuals taken at different times are given in Table 5. Accordingly, it has been shown that secure encryption continues even when the data is filtered, that is, the components that can be called random or chaotic are not only caused by noise, they are in the nature of the ECG.

**Table 4.** Effect of Filtered ECG Data From Different People on NPCR and UACI

| Phase Shift Count | Subjects | NPCR | UACI |
|---|---|---|---|
| 1 | Subject 1&2 | 99,5651 | 33,4999 |
| | Subject 1&3 | 99,5789 | 33,4520 |
| | Subject 2&3 | 99,6445 | 33,5592 |
| 10 | Subject 1&2 | 99,6124 | 33,3905 |
| | Subject 1&3 | 99,6017 | 33,4610 |
| | Subject 2&3 | 99,6216 | 33,4637 |
| 17 | Subject 1&2 | 99,5880 | 33,3792 |
| | Subject 1&3 | 99,5865 | 33,4532 |
| | Subject 2&3 | 99,6017 | 33,5665 |

**Table 5.** Effect of Filtered ECG Data Generated with Different Sample Shifts on NPCR and UACI

| Subject | Phase Shift Count | | NPCR | UACI |
|---|---|---|---|---|
| Subject 1 | 1 | 10 | 99,6246 | 33,5080 |
| | 10 | 10 | 99,6277 | 33,4162 |
| | 17 | 10 | 99,6231 | 33,4896 |
| Subject 2 | 1 | 10 | 99,5331 | 33,5339 |
| | 10 | 10 | 99,6231 | 33,4143 |
| | 17 | 10 | 99,6124 | 33,3777 |

The entropy values of images encoded using filtered signals are given in Table 6. Again, values very close to the ideal value of 8 can be used to evaluate the encryption performance.

**Table 6.** Entropy Values of the Obtained Encrypted Images with Filtered ECG Data

| Subject | Phase Shift Count | | |
|---|---|---|---|
| | 1 | 10 | 17 |
| Subject 1 | 7,9895 | 7,9891 | 7,9899 |
| Subject 2 | 7, 9892 | 7,9896 | 7,9885 |
| Subject 3 | 7,9895 | 7,9882 | 7,9893 |

In order to compare the obtained numerical values, the metrics of Lena image encrypted with the same method using Lorenz system can be used. The NPCR value of Lena images encrypted with 2 different chaotic sequences obtained by slightly changing the initial conditions in Lorenz system was obtained as 99.6002 and UACI value as 33.3708. The entropy values of the encrypted images used were 7.9898 and 7.9999. It has been observed that the encryption performances obtained using a proven chaotic sequence in the literature or an ECG signal are approximately equal.

## V. CHAOTICITY ANALYSIS

Although there is not a universally accepted definition for a time series to be chaotic, the common approach in the literature is Lyapunov analysis. Lyapunov exponents are a measure of the rate at which infinitesimally adjacent trajectories in the phase space of a dynamical system separate from each other with each iteration or unit of time. Dynamical systems with a positive largest Lyapunov exponent are described as chaotic since the trajectory does not converge to a single point [25]. The largest Lyapunov exponents (LLE) calculated in different phase-shifted spaces of the ECG signals used with the method proposed by Wolf are given in Table 7 [23]. Accordingly, all of the filtered signals give positive exponents. In the original signals, it is not possible to calculate with this method for the time series containing all the samples used, and all exponents go to $-\infty$ due to divergence. The largest exponent values calculated for the sample before the divergence are given in parentheses and they are also seen to be positive. In other words, it is clearly seen by Lyapunov analysis that the signals are chaotic.

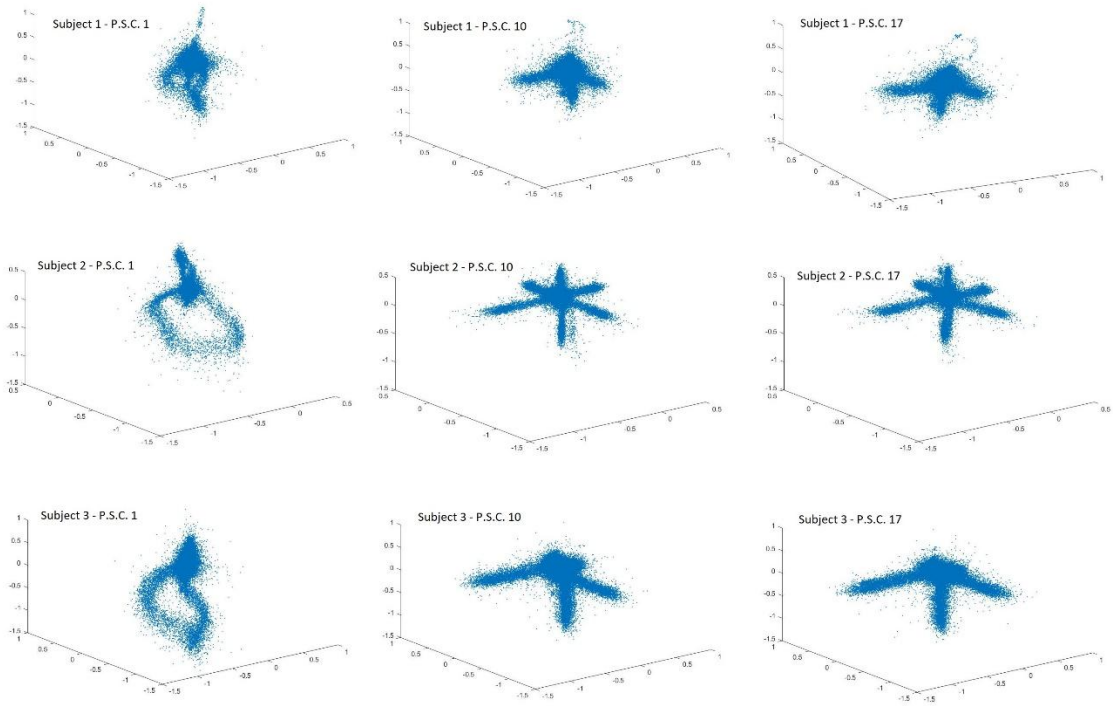



**Figure 4.** Phase portraits of raw ECG signals.

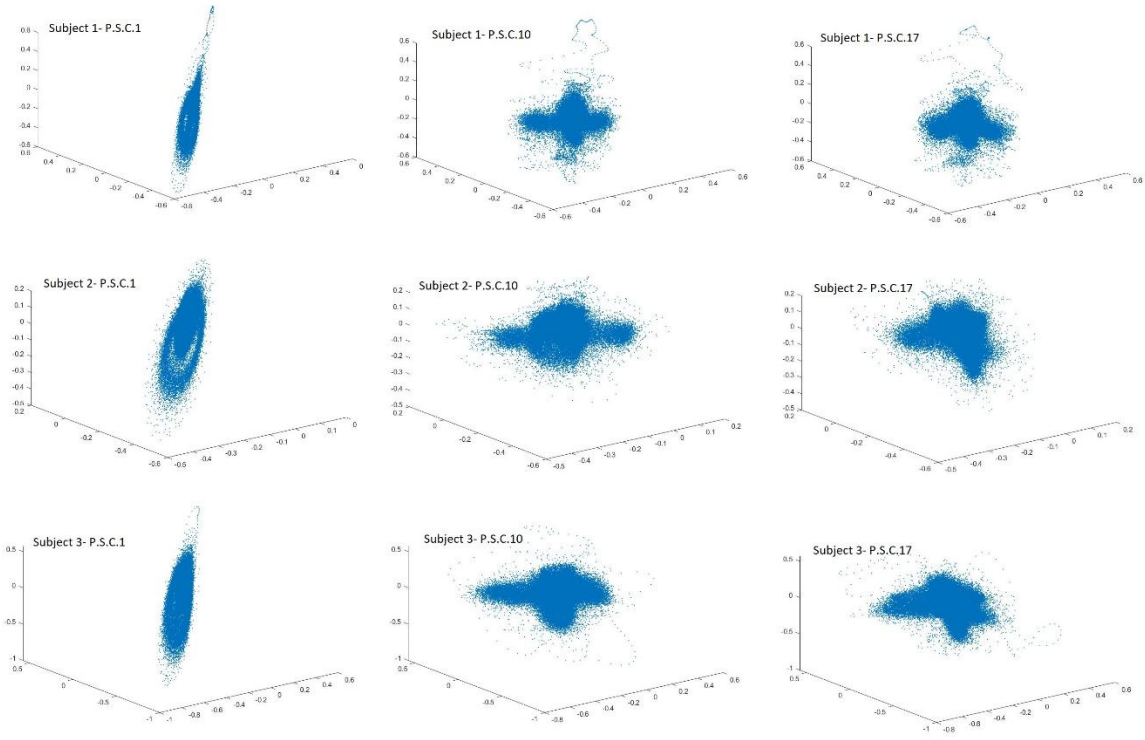



**Figure 5.** Phase portraits of filtered ECG signals.

**Table 7.** The Largest Lyapunov Exponents of ECG Signals

| Subject | Phase Shift Count | LLE of Raw ECG | LLE of Filtered ECG |
|---|---|---|---|
| Subject 1 | 1 | -∞ (1.3347) | 1.2074 |
| | 10 | 1.7746 | 0.663 |
| | 17 | -∞ (2.5629) | 0.7245 |
| Subject 2 | 1 | -∞ (2.2889) | 1.0992 |
| | 10 | -∞ (2.6308) | 0.5139 |
| | 17 | -∞ (2.7224) | 0.4915 |
| Subject 3 | 1 | -∞ (4.2213) | 2.8335 |
| | 10 | -∞ (4.4326) | 2.901 |
| | 17 | -∞ (4.8424) | 3.0148 |

Phase portraits can be drawn and their attractors compared to visually check the chaotic signals. Phase portraits formed by the original ECG signals can be observed in Figure 4, and phase portraits formed by the filtered ECG signs in Figure 5. Orbits formed outside the dominant periodic orbit can be observed through these phase portraits.

## VI. CONCLUSION

This study has tested whether the ECG data can be used in chaotic encryption methods by calculating NPCR, UACI values, which are a measure of security against plain-text attacks, and the entropy of the encrypted image. In addition, the chaoticity of normal rhythm ECG signals was also examined with phase portraits, and Lyapunov exponents. In a chaotic encryption method, which is known to be reliable in the literature, ECG data was substituted for chaotic number sequences, and according to the simulation results, although normal ECG signals cannot be defined as chaotic, they allow secure encryption when used in chaotic encryption methods. Not only the ECG data of different people, but also the data of the same person recorded at different times, or the ECG data subjected to different phase shifts, provide different secure sequences. The collected ECG data can also be used for secure encryption when used raw or filtered to remove noise. It has been shown that the periodic ECG signals of individuals can be used as a continuous chaotic key generator.

## KAYNAKLAR

[1] Glass, L. (2009). Introduction to controversial topics in nonlinear science: Is the normal heart rate chaotic?. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *19*(2).
[2] Gupta, V., Mittal, M., & Mittal, V. (2020). Chaos theory: an emerging tool for arrhythmia detection. *Sensing and Imaging*, *21*(1), 10.
[3] Gorshkov, O., & Ombao, H. (2021). Multi-chaotic analysis of inter-beat (RR) intervals in cardiac signals for discrimination between normal and pathological classes. *Entropy*, *23*(1), 112.
[4] Gupta, V., Mittal, M., & Mittal, V. (2019). R-peak detection using chaos analysis in standard and real time ECG databases. *Irbm*, *40*(6), 341-354.
[5] Gupta, V., & Mittal, M. (2019). QRS complex detection using STFT, chaos analysis, and PCA in standard and real-time ECG databases. *Journal of The Institution of Engineers (India): Series B*, *100*(5), 489-497.
[6] Casaleggio, A., & Braiotta, S. (1997). Estimation of Lyapunov exponents of ECG time series—the influence of parameters. *Chaos, Solitons & Fractals*, *8*(10), 1591-1599.
[7] Liu, Y., Tong, X., & Ma, J. (2016). Image encryption algorithm based on hyper-chaotic system and dynamic S-box. *Multimedia Tools and Applications*, *75*, 7739-7759.
[8] Akgül, A., Yıldız, M. Z., Boyraz, Ö. F., Güleryüz, E., Kaçar, S., & Gürevin, B. (2020). Doğrusal olmayan yeni bir sistem ile damar görüntülerinin mikrobilgisayar tabanlı olarak şifrelenmesi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *35*(3), 1369-1386.
[9] Abundiz-Pérez, F., Cruz-Hernández, C., Murillo-Escobar, M. A., López-Gutiérrez, R. M., & Arellano-Delgado, A. (2016). A fingerprint image encryption scheme based on hyperchaotic Rössler map. *Mathematical Problems in Engineering*, *2016*.
[10] Murillo-Escobar, M. A., Cardoza-Avendaño, L., López-Gutiérrez, R. M., & Cruz-Hernández, C. (2017). A double chaotic layer encryption algorithm for clinical signals in telemedicine. *Journal of medical systems*, *41*, 1-17.
[11] Mathivanan, P., Ganesh, A. B., & Venkatesan, R. (2019). QR code–based ECG signal encryption/decryption algorithm. *Cryptologia*, *43*(3), 233-253.

[12] Algarni, A. D., Soliman, N. F., Abdallah, H. A., & Abd El-Samie, F. E. (2021). Encryption of ECG signals for telemedicine applications. *Multimedia Tools and Applications*, *80*, 10679-10703.
[13] Sufi, F., & Khalil, I. (2008). Enforcing secured ecg transmission for realtime telemonitoring: A joint encoding, compression, encryption mechanism. *Security and Communication Networks*, *1*(5), 389-405.
[14] Wang, H., Bai, T., Pang, Y., Wang, W., Lin, J., Li, G., ... & Jiang, X. (2018). The dynamic encryption method based on ecg characteristic value. In *Communications, Signal Processing, and Systems: Proceedings of the 2016 International Conference on Communications, Signal Processing, and Systems* (pp. 431-438). Springer Singapore.
[15] Zheng, G., Fang, G., Shankaran, R., & Orgun, M. A. (2015). Encryption for implantable medical devices using modified one-time pads. *IEEE Access*, *3*, 825-836.
[16] Huang, P., Li, B., Guo, L., Jin, Z., & Chen, Y. (2016, December). 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.
[17] Goldberger, A. L., Amaral, L. A., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., ... & Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. *circulation*, *101*(23), e215-e220.
[18] Hossain, M. B., Rahman, M. T., Rahman, A. S., & Islam, S. (2014, May). A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. In *2014 International Conference on Informatics, Electronics & Vision (ICIEV)* (pp. 1-6). IEEE.
[19] Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of atmospheric sciences*, *20*(2), 130-141.
[20] Ye, G., Zhao, H., & Chai, H. (2016). Chaotic image encryption algorithm using wave-line permutation and block diffusion. *Nonlinear Dynamics*, *83*, 2067-2077.
[21] Loukhaoukha, K., Nabti, M., & Zebbiche, K. (2013, May). An efficient image encryption algorithm based on blocks permutation and Rubik's cube principle for iris images. In *2013 8th International workshop on systems, signal processing and their applications (WoSSPA)* (pp. 267-272). IEEE.
[22] Kumari, M., Gupta, S., & Sardana, P. (2017). A survey of image encryption algorithms. *3D Research*, *8*, 1-35.
[23] Wolf, A., Swift, J. B., Swinney, H. L., & Vastano, J. A. (1985). Determining Lyapunov exponents from a time series. *Physica D: nonlinear phenomena*, *16*(3), 285-317.
[24] McClellan, J. H., & Parks, T. W. (2005). A personal history of the Parks-McClellan algorithm. *IEEE signal processing magazine*, *22*(2), 82-86.
[25] Stefanski, A., Dabrowski, A., & Kapitaniak, T. (2005). Evaluation of the largest Lyapunov exponent in dynamical systems with time delay. *Chaos, Solitons & Fractals*, *23*(5), 1651-1659.