Received January 21, 2021, accepted February 3, 2021, date of publication February 8, 2021, date of current version February 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3057586

Symmetric Cryptography With a Chaotic Map and a Multilayer Machine Learning Network for Physiological Signal Infosecurity: Case Study in Electrocardiogram

CHIA-HUNG LIN[1], JIAN-XING WU[1], PI-YUN CHEN[1], CHIEN-MING LI[2], NENG-SHENG PAI[1], AND CHAO-LIN KUO[3], (Member, IEEE)

[1]Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City 41170, Taiwan
[2]Division of Infectious Diseases, Department of Medicine of Chi Mei Medical Center, Tainan City 41710, Taiwan
[3]Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung City 80543, Taiwan

Corresponding authors: Pi-Yun Chen (chenby@ncut.edu.tw) and Neng-Sheng Pai (pai@ncut.edu.tw)

This work was supported by the Ministry of Science and Technology, Taiwan, under Grant MOST 108-2218-E-167 -00-MY2, Grant MOST 108-2221-E-167-005-MY2, and Grant MOST 109-2635- E-167-001, duration: August 1, 2019 – July 31, 2021.

ABSTRACT Digital physiological signals in telecare medicine information systems have been widely applied in remote medical applications, such as telecare, tele-examination, and telediagnosis, via computer networking transmission or wireless communication. However, these medical records need to ensure authorization demands in the channel model for human body communication and remote medical servers and enhance the confidentiality, recoverability, and availability of transmission data. Hence, this study proposes a symmetric cryptography scheme with a chaotic map and a multilayer machine learning network (MMLN) to achieve physiological signal infosecurity. A chaotic pseudorandom number generator within specific control parameters can dynamically produce unordered sequence numbers to set the secret keys for a regular secret key update, thereby improving the security of private cipher codes. The chaotic map is quickly iterated to produce a pseudorandom key stream for real-time applications, and the private cipher codes are selected using the initial and specific control parameters at the data emitter and receiver ends. A general regression neural network is used to map the high-dimensional input–output pair of cipher codes for substitution and permutation processes. Its adaptive MMLN with an optimization algorithm can rapidly train the random cipher code protocol to achieve an encryptor and a decryptor for a regular encrypted communication. Using the Massachusetts Institute of Technology–Beth Israel Hospital (MIT–BIH) Arrhythmia Database, 100 electrocardiogram fragments are used to verify the proposed model, and the peak signal-to-noise ratio (PSNR) as a quantitative quality metric is used to evaluate the visual quality after encryption and decryption processes for further diagnosis applications. Experimental results show that the proposed scheme has a higher mean PSNR (35.26 ± 3.77 dB) and shorter mean executing time (0.16 ± 0.01 s) compared with traditional cryptography protocol schemes.

INDEX TERMS Symmetric cryptography, chaotic map, general regression neural network, optimization algorithm, peak signal-to-noise ratio.

I. INTRODUCTION

In the human body communication (HBC) channel, physiological signals are obtained via biopotential electrodes and transducers over time, digitized by an analog-to-digital conversion (ADC), and stored in a memory unit. Signals, such as bioelectrical, biomagnetic, and bioacoustic signals, can be applied in healthcare and homecare applications for disease prevention, treatment cost reduction, and remote cardiac diagnosis [1], [2]. For example, an electrocardiogram (ECG) is commonly used to monitor the human heart's internal electrical activities for applications in computer-aided diagnosis

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wang.

systems. The raw data collected by ECG can be used to analyze heart rate variability (HRV), detect cardiac arrhythmia, diagnose cardiovascular diseases, recognize emotions, and screen obstructive sleep apnea [3]–[7]. For cardiac arrhythmia detection, various QRS waveforms are used to identify the normal beat (●), atrial premature beat (A), ventricular premature contraction (V), right/left bundle branch block beat (R/L), paced beat (P), and fusion of ventricular and normal beats (F) [6], [8], [9]. These symptom signals can be transmitted via wired (computer networks) or wireless communication for applications in remote cardiac diagnosis. For example, the IEEE 802.15 standard [10], [11] and physical layer security [12], [13] for signal transmission have defined the physical layer and media access control specification for wireless connection with a fixed, portable, or mobile device within an individual operating space in a body area network (BAN). However, the security and privacy of personal physiological data should be protected while being transmitted in public communication channel.

Hence, the Health Insurance Portability and Accountability Act has recommended communication networks as a medium to transmit digital physiological data with proper security and privacy to ensure confidentiality, integrity, and availability [14], [15], which is portrayed as a small-scale telecare medicine information system, as seen in Figure 1(a).

For communication techniques in telecare applications, a set of body sensors has been applied for pervasive and real-time healthcare monitoring; these sensors are used to collect patients' health states, such as vital signs, texts, images, and multimedia information. This wireless-based system consists of handheld mobile devices (smart phones or iPads) and remote sensors [16]–[19], which are either worn or implanted on the body for the monitoring of heart rate, blood pressure, oxygen saturation, temperature, and body motion states in a wireless BAN [11], [20]. These electronic medical records are private and confidential for be available by authorized people. For example, radio frequency identification (RFID) technology can link physical objects to the Internet for exchanging data and is also used for healthcare applications (industrial, scientific, and medical band; range: 1–12 m). This technology consists of a tag, reader, and backend server. Passive RFID has low storage and low computational capabilities and thus suffers from many security drawbacks and privacy issues, such as simple bitwise operations and pseudorandom number generators in RFID authentication protocols. A scalable pseudorandom mutual authentication scheme [21] is used to encrypt information with symmetric secret keys, random number generators, and hash functions. RFID tag authentication uses uniformly distributed random variables to produce random numbers for setting a secret key and then transmits data during communication transmission, which need to be independent and updated, resulting in a significant increase in signaling overhead and reduction of the overall throughput of the system. Its technique also has limited storage resources in the tag and low capacity of processing complex operations. In addition, similar with most electronics and network, the RFID system is susceptible to active and passive attacks. Hackers may take apart the knowledge about protocols and determine how its system operates to steal information, gain access, or tamper information.

In medical signal and image security, encryption algorithms with permutation and substitution methods or a combination of both have been proposed for digital medical records; these methods include (1) rearranging numerical / pixel positions and (2) changing numerical / pixel values [22]–[26]. The methods based on permutation cipher can rearrange their positions without changing the numerical / pixel values in an encrypted data sequence. By contrast, substitution cipher-based methods replace plain messages with letters, numbers, or specific symbols, which modify the numerical / pixel values in the entire encrypted data sequence by using the transformation function or combining the substitution and transposition methods. Methods, such as shift cipher, affine cipher, exclusive (XOR), Hill cipher, Playfair cipher, and hash function methods, can also combine a multi-round cryptography protocol to improve communication security [22], [26]. However, encrypted messages that use the permutation or substitution methods with fixed secret keys as constant control parameters in the symmetric cryptography protocol can easily be broken by active or passive hacker attacks, which intercept the content of messages to modify, steal, and copy by unauthorized actions, resulting in thefts and security threats. Hence, a secrecy performance evaluation of cryptography schemes and techniques is required to quantify secrecy performance metrics, such as the signal-to-interference-plus-noise ratio-based metric, bit error rate-based metric, and packet error rate-based metric, and fractional equivocation-based metric, which define the maximum secrecy rate (capacity), secrecy throughput, and secrecy outage probability at which the message is reliably recovered at the data receiver end [12], [13], [27], [28]. Combining the permutation and substitution process with chaotic secret keys [22]–[24], [29], [30] ensures the improved security of encrypted messages. Thus, to combat passive attacks, chaos-based dynamical systems or chaotic map- based methods have randomness and nonperiodicity to generate unordered sequences for setting unpredictable cryptography protocols.

One-dimensional chaotic map-based pseudorandom number generators, such as Arnold, sine, circle, tent, and logistic maps [29]–[33], has been designed to generate secret keys for protecting patients' digital medical data in wireless communication networks. Its technique uses the initial conditions and control (bifurcation) parameters to perform pure shuffling processes of row and columns for rearranging pixel positions or to modify the gray values of cluttered pixels, and has high security levels for gray and colored medical images. These chaotic map-based methods use different initial conditions and the specific control parameters to determine whether a dynamic system stabilizes at a constant value or periodic values or becomes chaotic behaviors. Its pseudorandom number generator offers a fast and easy way

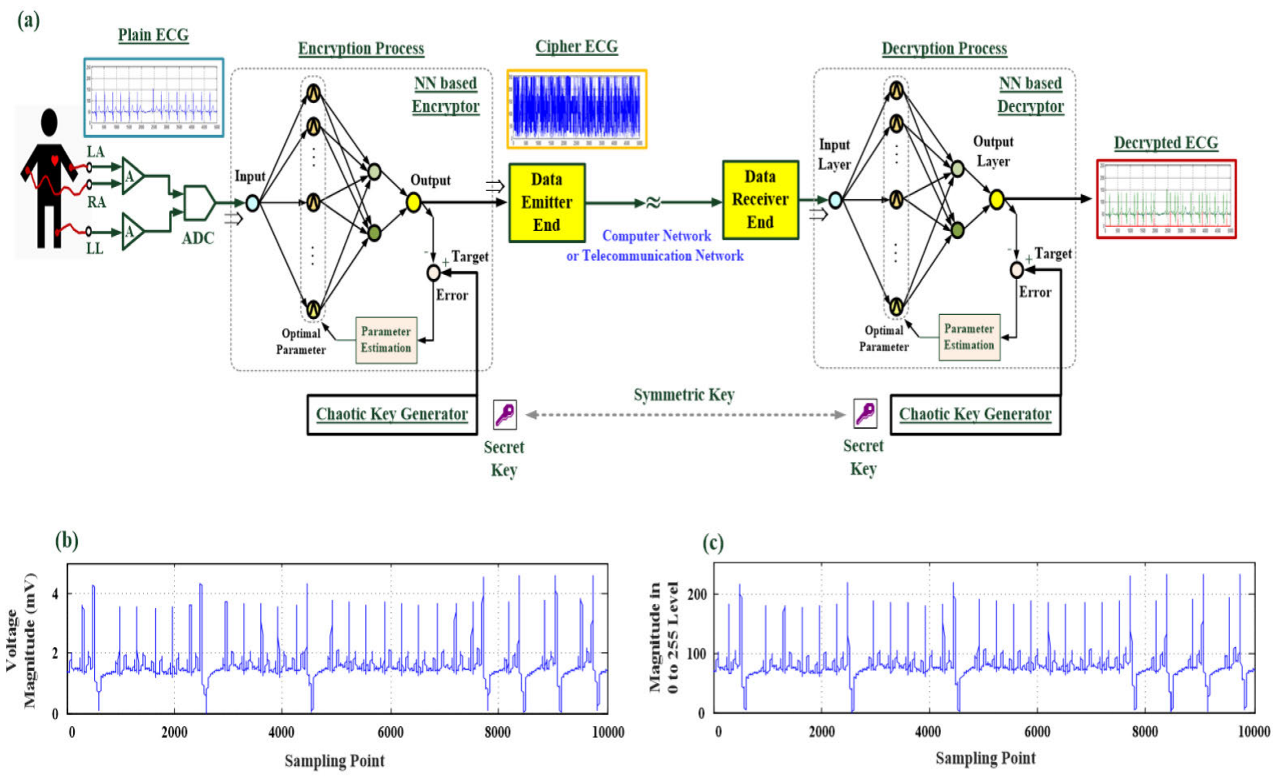


FIGURE 1. Telecare medicine information system and ECG sequence record (approximately 30 s of recording). (a) Architecture of bioelectrical signal security in a telecare medicine information system, (b) Original ECG raw data, (c) Encoded ECG data in 0–255 level.

to select the finite data length using chaotic iterations for setting secret keys as chaotic cipher codes, such as 8-bit, 56-bit (for data encryption standard), or 256-bit (for advanced encryption standard) key space. For example, a key is 8-bit long (key space = 2^8), with possible secret keys encoding from value 0 to value 255. To prevent any brute-force attack or statistical attack, a 256-bit key space is designed to randomly select from the possible key permutations. Thus, these unordered cipher codes can be used to train an encryptor and a decryptor using artificial neural network (ANN)-based models and optimization algorithms.

Each pair of cryptography protocol is a cipher codes as the "ordered sequence numbers (0_255) referring to the nonordered sequence numbers (chaotic cipher codes) for encryption process, or the non-ordered sequence numbers referring to the ordered sequence numbers (0_255) for decryption process. In this study, a general regression neural network (GRNN)-based [34]–[37] multilayer machine learning network (MMLN) is used to establish nonlinear mapping between high-dimensional feature space and complex input and output relationships for nonlinear curve-fitting applications. These nonlinear mapping feature patterns with a finite number of training patterns will cause practical difficulties in an estimator design using traditional ANN, such as multilayer perceptron neural network (MPNN). MPNN-based estimators use the back- propagation algorithm to adjust the overall network connecting weights to reduce the generalization error and complete the complexity input and output mapping relationships. However, MPNN's model performance is significantly affected by the numbers of hidden nodes and layers, initialized random connecting weights, learning rates, and convergent condition [34]–[37]. This complexity model will increase the computational time consumption and design cycle. The proposed GRNN model uses the number of input–output pairs of training patterns to establish the architecture of MMLN, including input nodes in the input layer, hidden nodes in the pattern layer, and outputs nodes in the output layer. Hence, GRNN can rapidly construct a multilayer connecting network, as shown in Figure 1(a). For a regular secret key update, to produce a new cryptography protocol with the logistic map function [30], [33], [38], GRNN-based models with an optimization algorithm, such as the particle swarm optimization (PSO) search algorithm [34]–[36], [39], can rapidly adjust the network parameters to minimize the generalization error and achieve the near global minimum, which will be trained for implementing an encryptor and a decryptor for physiological signal infosecurity. Its adaptive scheme has a fast operation time in the learning and recall stages at a regular secret key update. The adaptive training scheme of the proposed model can overcome the shortcomings of permutation or substitution methods with fixed secret keys. Through methodology verification using the Massachusetts Institute of Technology–Beth Israel Hospital (MIT–BIH) database [40], we will suggest promising parameters, including chaotic control and PSO parameters, to model the encryptor and decryptor for online applications. For 100 ECG fragments, peak signal-to-noise ratio (PSNR) [41], [37] is used to evaluate the decrypted performance of the proposed symmetric cryptographic method. Experimental results indicate that we can obtain good-quality decrypted ECG signals without hacker attacks and noise, with a mean PSNR $\geq$ 30 dB. Hence, the recoverable ECG signal is reliable and lossless for further disease diagnostic applications.

The remainder of this article is organized as follows: Section II describes the methodology, including ECG signal collection, chaotic secret key generation, encryptor and decryptor modeling, and recovery quality evaluation. Section III describes encryptor and decryptor training, experimental tests with MIT–BIH ECG data, and performance comparison with traditional cryptographic methods. Section IV concludes the study.

II. METHODOLOGY

A. ECG RAW DATA ENCODING

An ECG signal is a sequence record used to determine the heart's electrical activities as indications for chest pain, suspected myocardial infarction, cardiac electrophysiology, and medication monitoring [6], [42], [43]. Its record can be performed as a short-duration tracing or continuous monitoring by 12-lead ECG measurements, including limb leads (leads I to III), augmented limb leads (leads aVR, aVL, and aVF), and precordial leads (leads V_1 to V_6) [44]. In each ECG raw data, each beat is labeled by two cardiologists in accordance with the Association for the Advancement of Medical Instrumentation standard. After ADC, we converted the discrete values of ECG raw data

into positive values (unsigned data) as

$$ECG = ECG_{org} + abs(\arg\min(ECG_{org})), \tag{1}$$

where ECG$_{org}$ is the ECG raw data, argmin(•) is the function to find the minimal value, and abs(•) is the function to return the absolute value. Then, with a resolution of 8 bits to encode an "ECG raw data" once in 256 levels for the encryption process (8 bits), the voltage scale can be represented from value 0 to value 255 as

$$\Phi_{01} = ECG\frac{(2^8-1)}{V_{FSR}} \tag{2}$$

$$\Phi_{01} = \left[\phi_{01,1}, \quad \phi_{01,2}, \quad \phi_{01,3}, \quad \cdots, \quad \phi_{01,N}\right] \tag{3}$$

where V_{FSR} is the full-scale range of voltage magnitude (V_{FSR} = 5.0 mV in this study), N is the number of sampling points in ECG sequence data, and Φ_{01} is the "plain sequence data." Figures 1(b) and 1(c) show the ECG sequence data (approximately 30 s of recording) from original ECG signal to encoded signal. These sequence data could be used to evaluate the performance of the proposed symmetric cryptographic method.

B. CHAOTIC SECRET KEY GENERATION

For data substitution and permutation, the discrete chaotic dynamic manner, such as sine, circle, tent, and logistic maps [18]–[24], has been proposed to generate one-dimensional random numbers in nonperiodic chaotic sequences. Its generation process has a randomness function, and its chaotic trajectories are controlled by initial condition and control parameters. For example, a logistic map is used to generate a nonperiodic chaotic

sequence c_n between 0 and 1 and can be presented as

$$c_{n+1} = r \cdot c_n(1 - c_n), \quad n = 0, 1, 2, \ldots, n_c \tag{4}$$

where parameter r is the control (bifurcation) parameter; c_0 is the initial condition, as $0< c_0 <1$; and n_c is the sequence length. With the bifurcation parameter ($0< r \leq 4$) and initial condition ($c_0 = 0.5$), Figures 2(a) and 2(b) show the bifurcation diagram from 0 to 4 and the chaotic trajectories over 2 × 10^4 iteration numbers, respectively. The figures also show that amplitude and frequency are highly random. The Lyapunov exponent (LE) is used to observe the adequate interval of control parameters.

$$LE_t = \frac{1}{n_c}\sum_{n=1}^{n_c}\log(abs(r_t - 2r_t c_n))(\text{dB}) \tag{5}$$

$$r_t = r_{t-1} + \Delta r, \ \Delta r = 0.0010, t = 1, 2, 3, \ldots, n_r \tag{6}$$

where r_0 is the initial control parameter, n_r is the number of control parameters, and n_c is the number of sequence length. As shown in Figure 2(c), given the parameters $r_0 = 3.500$, $n_r = 501$, and $n_c = 2 \times 10^4$, the estimated values of the $LE = -1.3274$ dB can be used to validate the chaotic phenomenon [40]. With the control parameter values in the range of 3.8320–4.0000, the dynamic behavior will become more chaotic in nature and suggests that the control parameters must be set in this specific range.

Hence, in consideration of this specific range of control parameters (as indicated by the red dash-line box), the generated sequence values are in interval (0, 1) and then transformed into unsigned integer numbers by multiplying the sequence value c_n with 255, resulting in sequence

values ranging from value 0 to value 255.

$$sc_n = \text{mod}(round(255 \cdot c_n), 256), \quad n = 1, 2, \ldots, n_c \tag{7}$$

where round(•) is the function to return the nearest integer, and function mod(•) is the modulo operation. Hence, in this study, the chaotic key generator (CKG) can be implemented as follows:

Step 1) random sequence numbers $sc_n, n = 1, 2, \ldots, n_c$, are generated using the logistic map function with the different initial condition c_0 and specific control parameters within the interval (3.8320, 4.0000).

Step 2) Nonordered sequence numbers (no repeating) are selected in 256 data length to set the secret keys (SK), $SK = [ck_1, ck_2, ck_3, \ldots, ck_{256}], k = 1, 2, 3, \ldots, 256.$

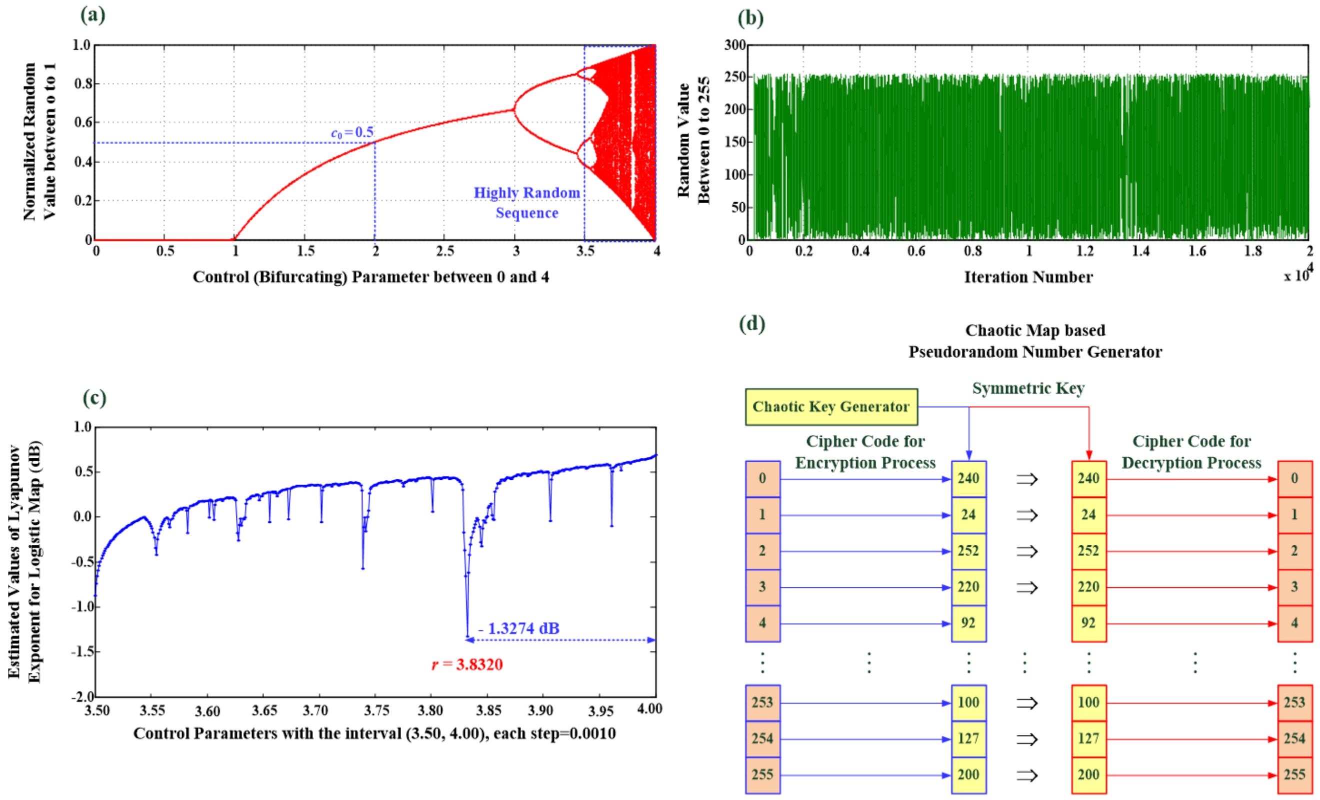


FIGURE 2. Chaotic map. (a) Bifurcation diagram of logistic map, (b) Chaotic trajectories over 2 × 10^4 iteration numbers, (c) Estimated values of Lyapunov exponent versus control parameters with interval (3.50, 4.00), (d) Two pairs of cipher codes as secret keys for encryption and decryption processes.

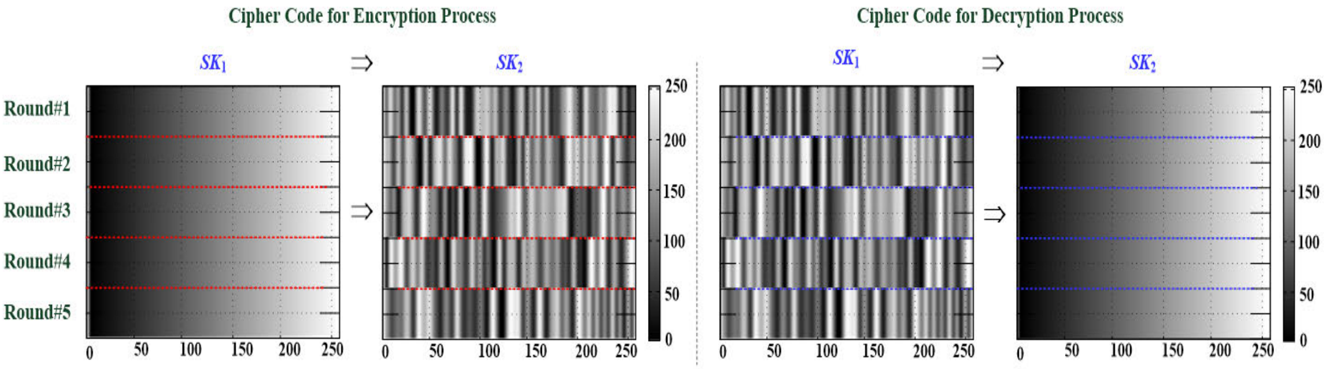


FIGURE 3. Randomness chaotic secret keys with five rounds of preliminary tests for regular secret key update.

Step 3) two pairs of cipher codes are set for encryption and decryption stage, as shown in Figure 2(d), and are defined as follows:

- cipher codes for encrypted keys: $SK_1 = [0, 1, 2, \ldots, 255]$ refers to $SK_2 = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$
- cipher codes for decrypted keys: $SK_1 = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$ refers to $SK_2 = [0, 1, 2, \ldots, 255]$.

For example, with the *CKG*, we can randomly generate five rounds of cipher codes with different initial conditions and control parameters for encryption and decryption. As shown in Figure 3, five pairs of cipher codes are different for setting symmetric SK and can be changed for regular secret key update duration communication authentication. Hence, these unpredictable randomness chaotic SK with strong cryptographic permits can be preliminarily validated for physiological signal infosecurity.

C. GRNN BASED ENCRYPTOR AND DECRYPTOR

After SK generation, we can obtain two pairs of cipher codes to train the GRNN-based encryptor and decryptor, as cipher code protocol following:

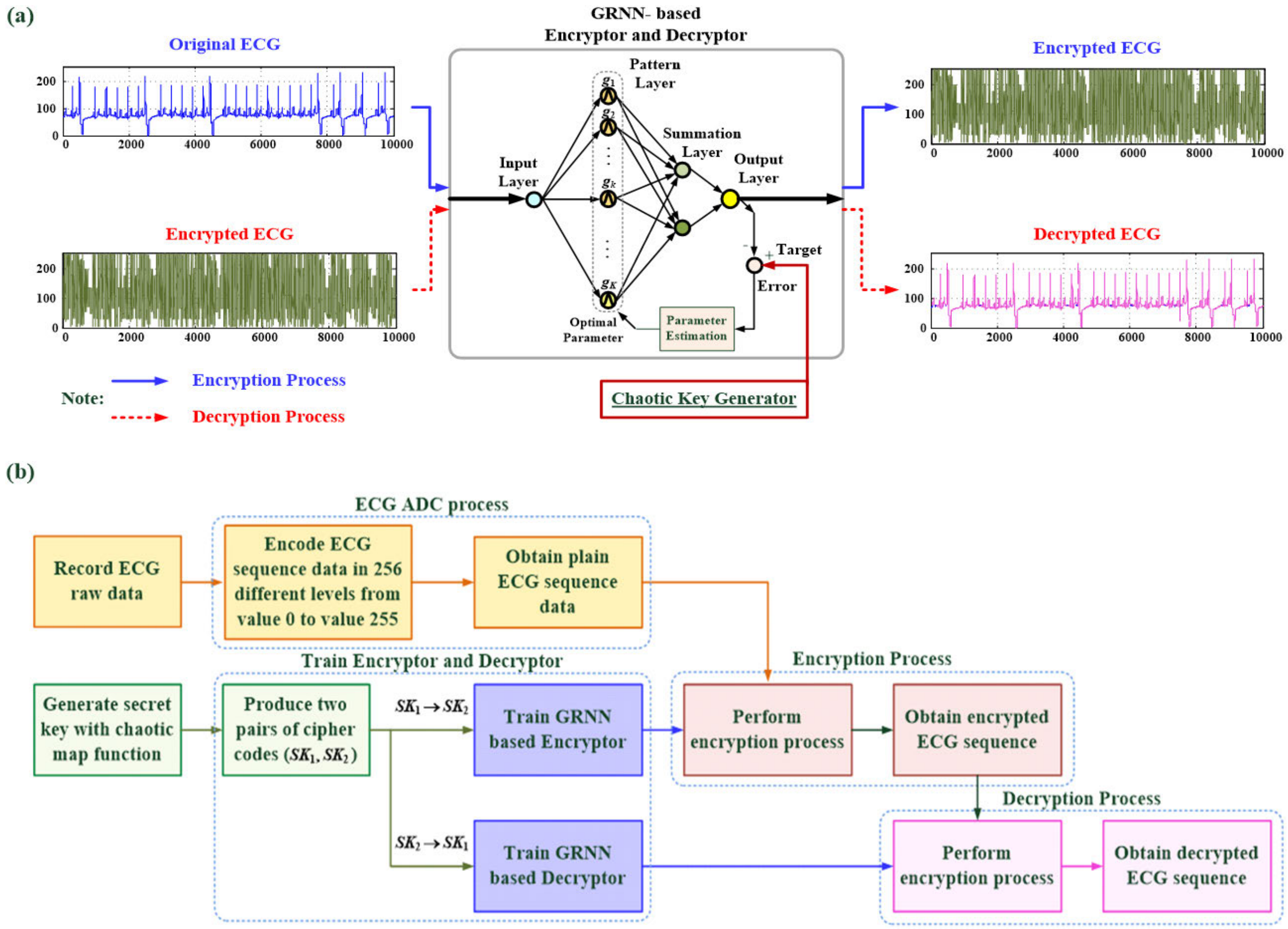


FIGURE 4. (a) Architecture of GRNN-based encryptor and decryptor, (b) Flowchart of cryptography protocol for ECG signal infosecurity, including the ECG ADC, encryptor and decryptor training, and ECG sequence encryption and decryption processes.

- first pair of cipher codes for encryption: the input-output pair is $SK_1 = [0, 1, 2, \ldots, 255]$ referring to $SK_2 = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$, where SK_2 is randomly produced by *CKG*.
- second pair of cipher codes for decryption: the input–output pair is $SK_2 = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$ referring to $SK_1 = [0, 1, 2, \ldots, 255]$.

In this study, two GRNNs, which consist of an input layer, a pattern layer, a summation layer, and an output layer, were used to create an encryptor and a decryptor, as shown in Figure 4(a), with one input and corresponding one output. The number of pattern nodes is determined by the dimension of the cipher code vector; thus, 256 pattern nodes are set in the pattern layer. Each GRNN-based model is a nonlinear regression model that maps the nonlinear relationship between SK_1 and SK_2 (for encryption process) or SK_2 and SK_1 (for decryption process) as a nonlinear curve-fitting application. Then, the optimization method is used to refine the network parameter in the pattern layer, thus improving the model performance. To create a curve- fitting model, the nonlinear regression algorithm can be expressed as follows:

Step 1) two cipher codes are used to set the connecting matrix W^{IP} of encryptor and decryptor between the input and pattern layers, respectively, as

$$\bullet \text{ for encryption process}: W^{IP} = [w_{k1}]^T = [\frac{k-1}{255}]^T \tag{8}$$

$$\bullet \text{ for decryption process}: W^{IP} = [w_{k1}]^T = [\frac{ck_k}{255}]^T \tag{9}$$

In the above equations, K is the number of pattern nodes; $k = 1, 2, 3, \ldots, K$, $K = 256$ in this study, and the dimension of the matrix W^{IP} is $K \times 1$. Then, the connecting matrix $W^{PS} = [w_{kj}]$, $j = 1, 2$ is set between the pattern and summation layers, as

$$\begin{aligned}\bullet \text{ for encryption process}: W^{PS} &= [\, w_{k1},\ w_{k2}\,]^T \\ &= [\frac{ck_k}{255}, 1]^T \end{aligned} \tag{10}$$

$$\begin{aligned}\bullet \text{ for decryption process}: W^{PS} &= [\, w_{k1},\ w_{k2}\,]^T \\ &= [\frac{k-1}{255}, 1]^T \end{aligned} \tag{11}$$

where two nodes in the summation layer, and the dimension of the matrix W^{PS} is $K \times 2$.

Step 2) the training data Φ_1 or Φ_2 are fed to the pattern layer, and the output of the pattern layer is calculated as follows:

$$g_k = \exp[-\sum_{k=1}^{K} \frac{(\phi_{ik} - w_{k1})^2}{2\sigma_k^2}], \quad i = 1, 2 \tag{12}$$

$$\begin{cases} \phi_{1k} = \dfrac{k-1}{255} \\ \phi_{2k} = \dfrac{ck_k}{255} \end{cases}, \quad k = 1, 2, 3, \ldots, 256 \tag{13}$$

where $\Phi_1 = [\phi_{11}, \phi_{12}, \ldots, \phi_{1k}, \ldots, \phi_{1K}]$ is the training data for an encryptor; $\Phi_2 = [\phi_{21}, \phi_{22}, \ldots, \phi_{2k}, \ldots, \phi_{2K}]$ is the training data for a decryptor; σ_k is the smoothing parameter, $k = 1, 2, 3, \ldots, K$, and all smoothing parameters in the pattern layer are equal to the same value σ. The optimal smoothing parameter σ_{opt} can be obtained using the optimization method.

Step 3) the output of the pattern layer is fed to the summation layer, and the output y_k in the output layer is computed as

$$y_k = \sum_{k=1}^{K} w_{k1} g_k \Big/ \sum_{k=1}^{K} w_{k2} g_k \tag{14}$$

The final output of GRNN can be computed by

$$Y_k = 255 y_k \tag{15}$$

In Equation (13), given an optimal smoothing parameter σ_{opt}, the GRNN can increase the prediction accuracy; hence, it requires the refinement of the optimal parameter to

minimize the mean squared error (MSE).

$$MSE = \frac{1}{K} \sum_{k=1}^{K} (Y_k - T_k)^2 \leq \varepsilon \tag{16}$$

where T_k is the desired target for the kth training data, and ε is the specified tolerance error (convergent condition) to terminate the training stage.

D. PSO OPTIMIZATION METHOD

In this study, the PSO algorithm [34]–[36], [39] was used to tune the optimal smoothing parameter, σ_{opt}, through an iterative computation and minimize the *MSE*, as

$$\begin{cases} \Delta\sigma_g(p+1) = \Delta\sigma_g(p) \\ + \cdots c_1 rand_1(\sigma best_g - \sigma(p)) \\ + c_2\, rand_2(\sigma best - \sigma_g(p)) & (17) \\ c_1 = (b_1 - a_1)\dfrac{p}{p_{\max}} + a_1,\ c_2 = (b_2 - a_2)\dfrac{p}{p_{\max}} + a_2 & (18) \\ \sigma_g(p+1) = \sigma_g(p) + \Delta\sigma_g(p+1) & (19) \end{cases}$$

where $\sigma_g(p)$ is the gth particle at the pth search stage and particle population size, $g = 1, 2, 3, \ldots, G$; $\sigma best$ is the global best in the particle population; $\sigma best_g$ is the individual best at the pth search stage, $p = 1, 2, 3, \ldots, p_{max}$; c_1 and c_2 are the adaptive acceleration factors that vary with the iterative computation; p_{max} is the maximum iteration number, as the term $p/p_{\max}$ is used to control the acceleration factors; and $rand_1 \in(0, 1)$ and $rand_2 \in (0, 1)$. As second and third terms in Equation (17), a_1, b_1, a_2, and b_2 are constant values, of which the experienced values are c_1 from 2.5 to 0.5 and c_2 from 0.5 to 2.5 [34]–[36], [39]. By monotonously varying c_1 and c_2, Equation (17) gradually narrows down the search region and approaches the optimal solution σ_{opt} as fine-tuning the smoothing parameter at each search stage. After achieving the convergent condition, we terminated the iterative computations, and then fed the plain ECG $\Phi_{01} = [\phi_{01,1}, \phi_{01,2}, \ldots, \phi_{01,n}, \ldots, \phi_{01,N}]$ or encrypted ECG $\Phi_{02} = [\phi_{02,1}, \phi_{02,2}, \ldots, \phi_{02,n}, \ldots, \phi_{02,N}]$ to the encryptor and decryptor, respectively, perform the encryption or decryption tasks, as follows:

$$g_k = \exp[-\sum_{k=1}^{K} \frac{(\phi_{0i,n} - w_{k1})^2}{2\sigma_{opt}^2}], \quad i = 1, 2 \tag{20}$$

$$y_{in} = 255(\sum_{k=1}^{K} w_{k1} g_k \Big/ \sum_{k=1}^{K} w_{k2} g_k), \quad i = 1, 2 \tag{21}$$

where $Y_1 = [y_{11}, y_{12}, \ldots, y_{1n}, \ldots, y_{1N}]$ is the ECG-encrypted sequence; $Y_2 = [y_{21}, y_{22}, \ldots, y_{2n}, \ldots, y_{2N}]$ is the ECG-decrypted sequence; and connecting-weight values w_{k1} and w_{k2} are set using Equations (8) and (10) for encryption process and Equations (9) and (11) for decryption process. The flowchart of the cryptography protocol is shown in Figure 4(b); it includes the ECG ADC, encryptor and decryptor training, and ECG sequence encryption and decryption processes.

E. EVALUATION OF THE DECRYPTION PERFORMANCE

After ECG encryption and decryption, the *PSNR* index [41], [37] is used to evaluate the distortion degree between the plain ECG $\Phi_{01} = [\phi_{01,1}, \phi_{01,2}, \phi_{01,3}, \ldots, \phi_{01,N}]$, and decrypted ECG $Y_2 = [y_{21}, y_{22}, y_{23}, \ldots, y_{2N}]$, as

$$MSE_{ECG}(\Phi_{01}, Y_2) = \frac{1}{N} \sum_{n=1}^{N} (\phi_{01,n} - y_{2n})^2, \tag{22}$$

$$\begin{aligned} PSNR(\Phi_{01}, Y_2) &= 10 \cdot \log(\frac{MAX_{ECG}^2}{MSE_{ECG}}) \\ &= 20 \cdot \log(\frac{MAX_{ECG}}{\sqrt{MSE}_{ECG}}), \end{aligned} \tag{23}$$

$$Index = \begin{cases} 0, & 0 < PSNR < 30dB \\ 1, & PSNR \geq 30dB \end{cases} \tag{24}$$

where MAX_{ECG} is the maximum value in sequence Y_2, as $MAX_{ECG} = \max(Y_2)$. Index *PSNR* (in dB), *PSNR* > 0 dB, indicates the similarity degree between the plain ECG and decrypted ECG, which is also an index for human perception of recovery quality. When the *PSNR* has a high value, the plain ECG and decrypted ECG are similar. After the encryption and decryption processes, the larger the *PSNR* value, the smaller the loss is, which means that the proposed decryptor has a good recovery quality without involving noise interferences or any hacker attack. If the *PSNR* index is higher than 30 dB, then *Index* has value "1." The value 0 dB $< PSNR <$ 30 dB reflects an ECG sequence with the active attack, transformation errors, or transmission noises, as *Index* with value "0" implies the bad quality of decrypted ECG. Hence, the *PSNR* index offers a quantitative indication to evaluate the recovery quality for inspecting cardiac arrhythmias and diseases from the decrypted ECG sequence.

III. EXPERIMENTAL RESULTS AND DISCUSSION

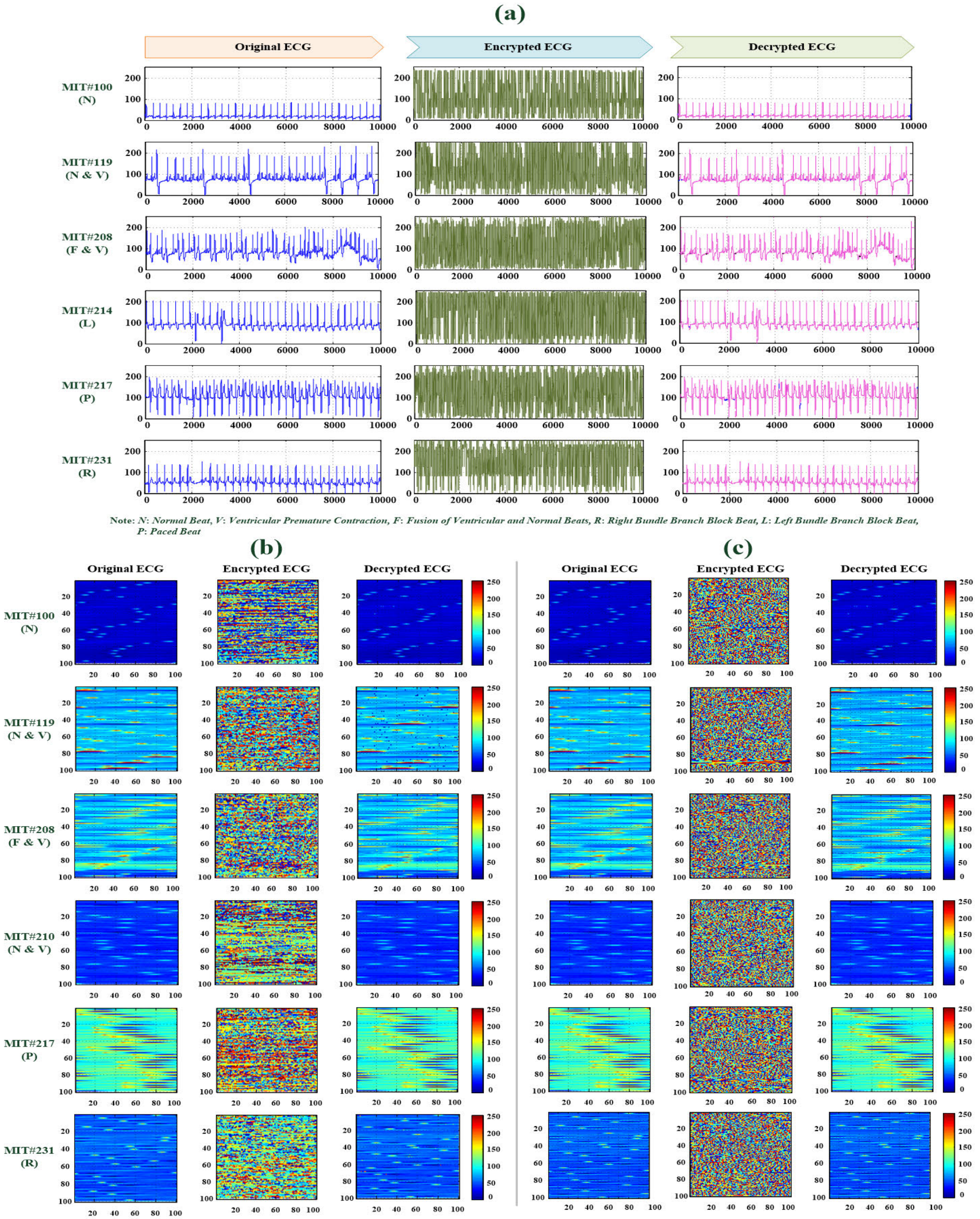
This section presents the experiment results to validate the effectiveness of the proposed symmetric cryptography protocol for ECG infosecurity in computer networks (IEEE 802.3 standard [45]) or wireless communication networks (IEEE 802.15 standard[10]), including (1) the ECG ADC process, (2) the encryptor and decryptor training, (3) the ECG encryption and decryption processes, and (4) recovery quality evaluation. The proposed GRNN-based encryptor and decryptor were designed on a tablet PC using a high-level graphical programming language in LabVIEW and MATLAB software (NI$^{\text{TM}}$, Austin, Texas, USA). Experimental ECG records were collected from archived files from MIT#100 to MIT#234 in the MIT–BIH arrhythmia database [40], including 22 women (aged 23 to 89 years) and 25 men (32 to 89 years); approximately 60% of these records was obtained from inpatients and 20 major classes. Some typical classes are shown in the left- hand side of Figures 5(a) and 5(b), which are represented in vector or matrix forms, respectively, including •, V, A, R, L, F, and P. The feasibility of the proposed cryptographic methods was validated. Details are provided in the subsequent sections.

A. GRNN-BASED ENCRYPTOR AND DECRYPTOR TRAINING

In the ECG cryptography protocol, at the data emitter end, before transiting the cipher ECG data, we could randomly generate the nonperiodic chaotic sequences using the *CKG* with control parameters within the interval, $r \in (3.8320, 4.0000)$ and initial condition, $c_0 = 0.5$, and select nonordered 256 numbers in 256 data length (no repeating) for setting the secret keys. Authorized persons at both data emitter and receiver end can mutually agree on specific control parameter to generate the two pairs of chaotic secret keys. Then, we could obtain the ordered sequence $SK_1 = [0, 1, 2, \ldots, 255]$, referring to the nonordered sequence $SK_2 = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$ for the encryption process; SK_2 referred to SK_1 for the decryption process, as shown in the randomness chaotic secret keys in Figure 3. Two GRNNs were used to train an encryptor and a decryptor at the data emitter end and data receiver end, respectively. Hence, an encryptor and a decryptor had one input node in input layer, 256 pattern nodes in pattern layer, two summation nodes, and one output node in output layer, as shown in Figure 4(a). Then, the PSO algorithm was used to find the optimal smoothing parameter, σ_{opt}, by using the adaptive acceleration factors (as in Equation (18)), particle population size $G = 10$–30, convergent condition, $\varepsilon \leq 10^{-2}$, and a maximum iteration number of $p_{max} = 50$. In the training stage, given $G = 10$, 20, and 30, we randomly produced multi-smoothing parameters (multi particles) in the search space and monotonously to minimize the generalization error by refining the optimal parameter.

As shown in Figures 6(a) and 6(d), the near-optimal smoothing parameters, $\sigma_{opt} = 0.0238$ and 0.0289, were guaranteed to minimize the MSE for training the encryptor and decryptor, respectively, as shown by the convergent curves in Figures 6(b) and 6(e). When the particle population size was increased from 10 to 30 particles, the numerical computations and mean CPU executing time increases, as shown in Figures 6(c) and 6(f), respectively. For the same convergent condition, the iteration computing process required < 15 iterative computations (150_450 numerical computations) and a CPU executing time of < 15 s to achieve the convergent condition. In addition, two MPNNs were used to train the encryptor and decryptor, respectively; each MPNN topology (1-20–20-1) consists of an input layer, two hidden layers (20 hidden nodes in the first and second hidden layers), and output layer. The back-propagation algorithm was used to adjust the network parameters (440 parameters) to minimize the MSE [36]–[37], with the randomly initializing network parameters, learning rates η of 0.1 –0.5, desired convergent condition $\varepsilon \leq 10^{-2}$, and maximum iteration number of 400. With the gradual increase in the learning rates from 0.1 to 0.5, the iteration computation processes took 100 –400 iterative computations to reach the convergent condition, as shown in the solution lists in Figures 7(a) and 7(c). The optimal solution lists were also monotonously decreased to minimize the MSE and were guaranteed to reach the convergent condition. Regarding the learning speed and generalization capability, we suggested selecting the learning rate $\eta \geq 0.5$ for training the MPNN-based estimator. Their iteration computations would take approximately < 20 s CPU execution time to determine the optimal network parameters and required iteration computations < 100, as shown in Figures 7(b) and 7(d). However, the MPNN model needed a trial-and-error procedure to determine the adequate network connecting topology and parameters for training the encryptor and decryptor.

In summary, for online nonlinear curve-fitting applications and computation resource reduction, the PSO algorithm with adaptive acceleration factors and particle population size $G = 20$ is suggested to train the encryptor and decryptor, which could rapidly search the optimal smoothing parameter (<6 iterative computations and <6 s CPU executing time, as shown in Figures 6(c) and 6(f), respectively). Hence, the proposed symmetric cryptography protocol could quickly change the secret keys with the chaotic-map function through an authorized person, and the GRNN-based encryptor and decryptor could also be quickly retrained using the PSO algorithm for on line infosecurity applications.



Note: *N*: *Normal Beat*, *V*: *Ventricular Premature Contraction*, *F*: *Fusion of Ventricular and Normal Beats*, *R*: *Right Bundle Branch Block Beat*, *L*: *Left Bundle Branch Block Beat*, *P*: *Paced Beat*

FIGURE 5. Experiment results in vector and matrix forms for seven typical classes. (a) Experiment results in vector forms, including ECG encoding from value 0 to value 255, ECG encryption, and ECG decryption for seven typical classes, (b) Results of ECG encryption and decryption using the proposed GRNN-based encryptor and decryptor, (c) Results of ECG encryption and decryption using a chaotic synchronization system with a fuzzy rule-based controller.

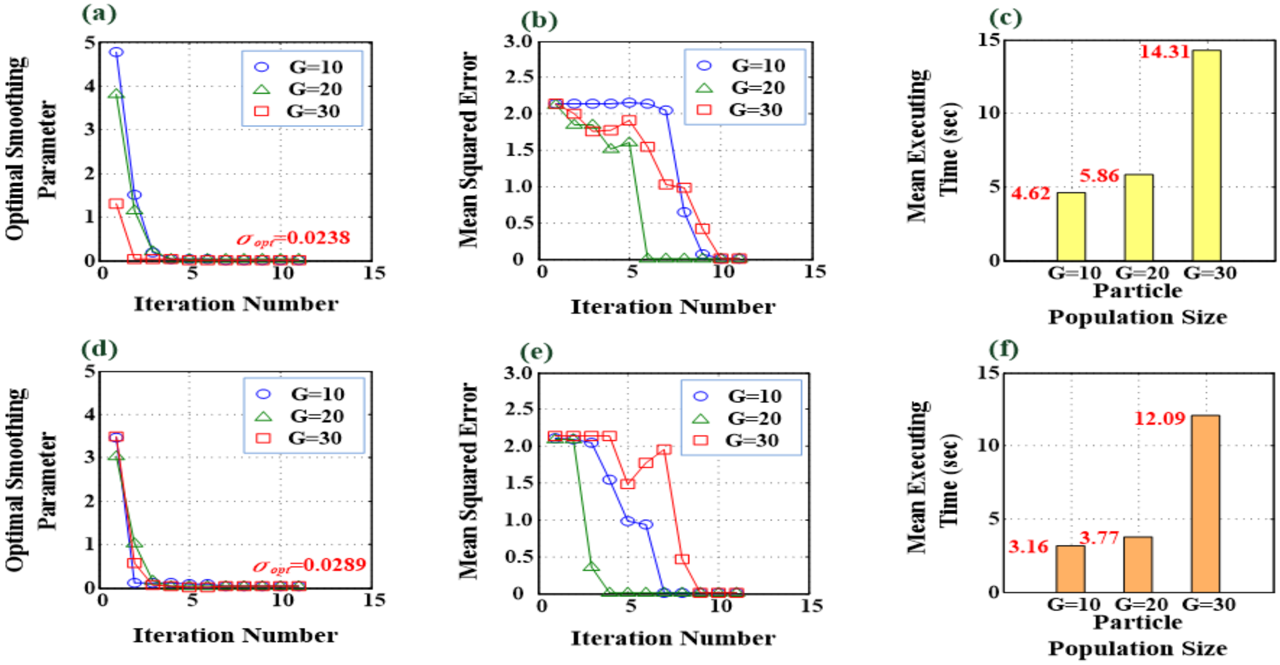


FIGURE 6. Solution lists of the GRNN based encryptor and decryptor. (a) and (b) Solution lists for training encryptor, (c) Mean executing time for training encryptor, (d) and (e) Solution lists for training decryptor, (f) Mean executing time for training decryptor.

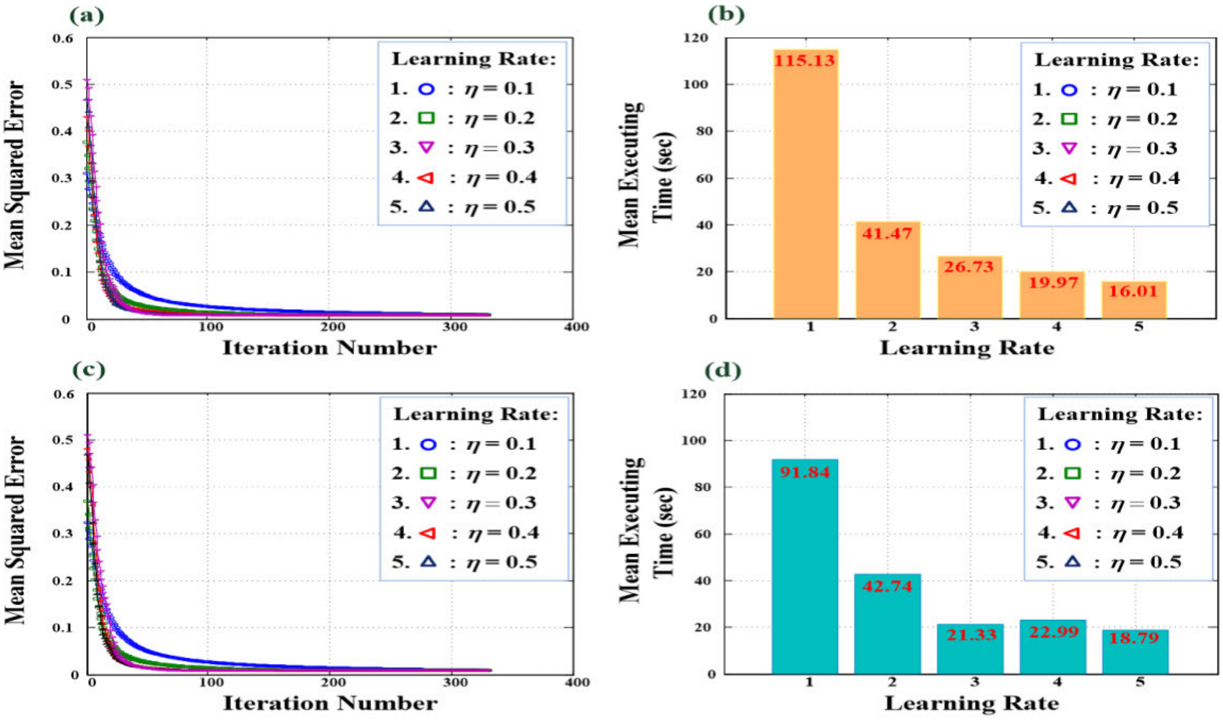


FIGURE 7. Solution lists of the MPNN-based encryptor and decryptor. (a) and (b) Solution lists and mean execution time for training the encryptor. (c) and (d) Solution lists and mean executing time for training the decryptor.

B. EXPERIMENTAL RESULTS OF ECG ENCRYPTION AND DECRYPTION

In the ECG encryption process, approximately 30 s-long raw data with 10,000 sampling points (333.33 Hz sampling rate) were used to verify the proposed encryptor and decryptor, which might contain typical classes, such as ventricular arrhythmias, bundle branch ectopic beats, fusion, and paced ectopic beats (•, V, A, R, L, F, and P). As shown in Figure 5,

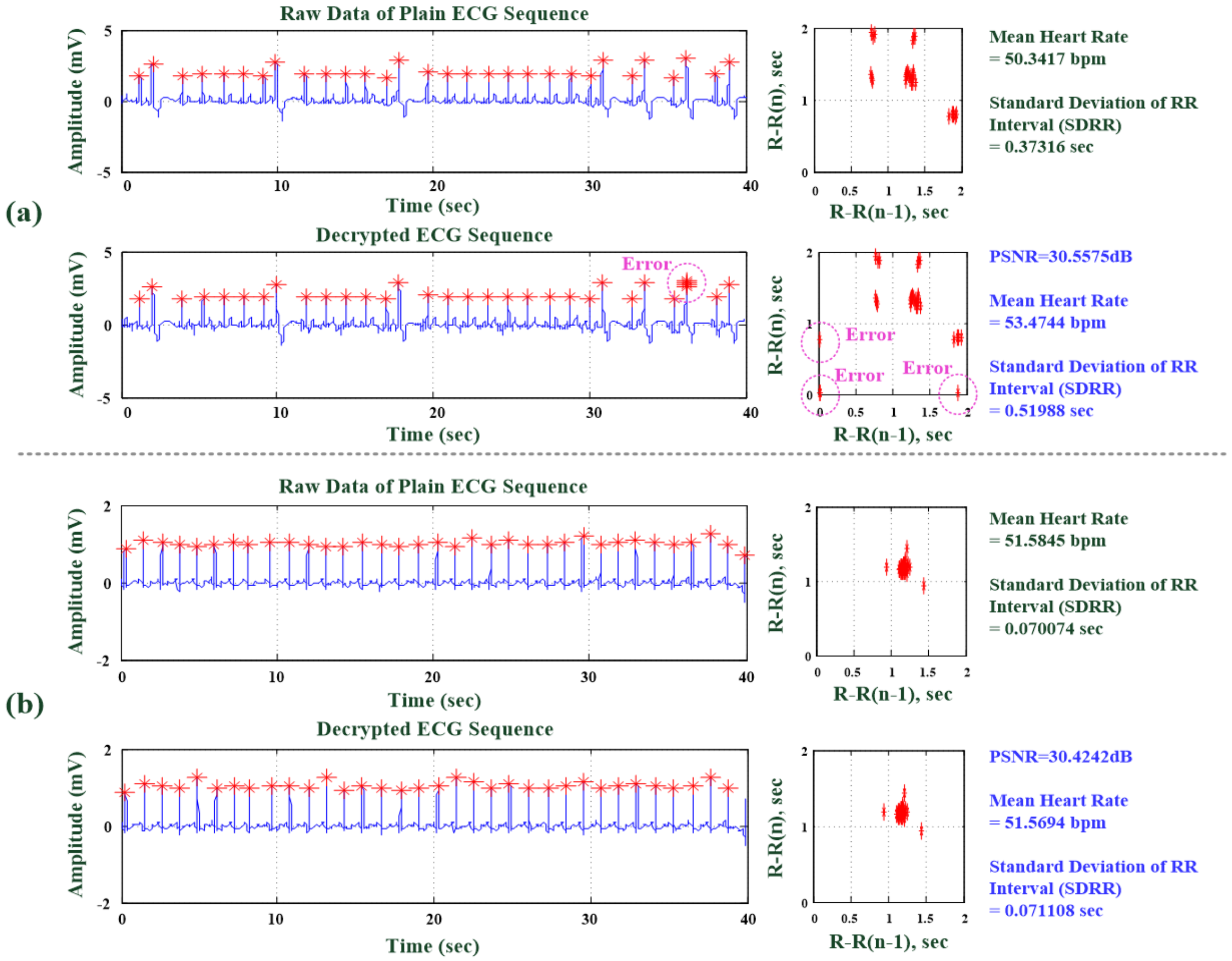


FIGURE 8. **Heart rate analysis for paced ectopic beats and normal heart beats. (a) Heart rate analysis for the ventricular premature contraction (V). (b) Heart rate analysis for the normal heart beat (•).**

the specific fragments in seven archived files (MIT#100, MIT#119, MIT#208, MIT#210, MIT#214, MIT#217, and MIT#231 [40]) were randomly selected to validate the feasibility of the proposed cryptography protocol. For example, in consideration of seven ECG fragments (represented as vector (1 × 10,000) and matrix (100 × 100) forms in the left-hand side of Figures 5(a) and 5(b)), the seven plain ECG sequences had been encoded from value 0 to value 255 using Equations (2) and (3). The middle part results in Figures 5(a) and 5(b) showed the encrypted ECG in vector and matrix forms; the plain and encrypted ECGs were not related at all in visual inspection and did not indicate any information about plain ECG data as looking like noise signals. The right-hand side results in Figures 5(a) and 5(b) showed the decrypted ECGs with the decrypted SK, which indicated that the plain and decrypted ECGs were almost identical. The proposed GRNN-based encryptor and decryptor could recover the plain ECG without hacker attacks and transmission noises in the vector and matrix forms, as the recovery quality was 35.48, 31.80, 32.10, 29.13, 34.31, 34.13, and 36.81 dB for seven ECG fragments, respectively. The mean $PSNR = 33.39$ dB ≥ 30.00 dB was obtained to qualify the recovered quality for all testing ECG fragments after the decryption process. This finding indicated that the recoverable ECGs were reliable and lossless and can be used for further time-domain heart rate analysis and cardiac arrhythmia diagnostic applications, such as the mean heart rates and standard deviation of the R–R interval for V and •beats presented in Figure 8. The decrypted ECG sequences presented recovery qualities of 30.5575 and 30.4242 dB (slight errors), respectively, to measure the beat-to-beat changes within the duration of the R–R (peak-to-peak) intervals in the time domain, where the R–R intervals, as R-R(n) and R-R($n-$ 1), $n = 1, 2, 3, \ldots, N$, can be calculated using the R-peak detection algorithm [6], [46]. For the HRV analysis, the mean heart rates and the mean and standard deviation of the R–R interval can be obtained from the decrypted ECG in the timing series. The decrypted ECG sequence offers

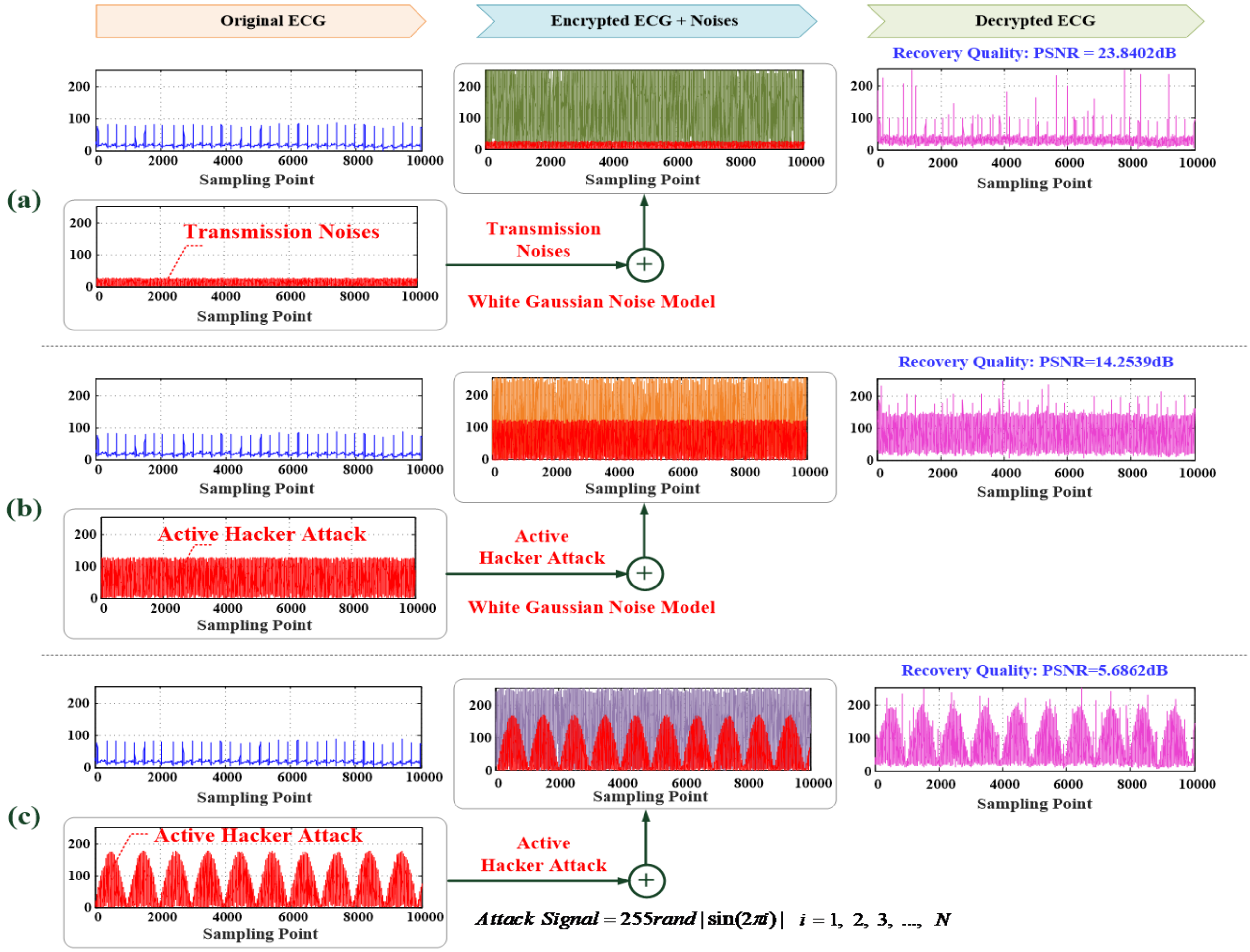


FIGURE 9. Scenario studies for suffering transmission noises and active hacker attacks.

promising messages to plot the R–R interval histogram for visually inspecting normal and ectopic beats to classify the classes.

However, ciphering ECG sequences can suffer from transmission noises and hacker attacks at any routing patch, as shown in Figures 9(a), 9(b), and 9(c), respectively. In these cases, the encrypted ECG could not appropriately recover the well quality of the original plain messages for clinical diagnostic applications. The *PSNR* declined in the range of 0–30 dB, with 23.8402 dB for transmission noises and 14.2539 and 5.6862 dB for active hacker attacks. The *PSNR* index indicates the value "0" as the warning sign for authorized people and required retransmission of cipher messages from the data emitter end and data receiver end under the transmission control protocol (TCP) system [45]. For the random selection of 100 ECG fragments without interferences, the experimental results exhibited well recoverability, as shown in Table 1. The mean $PSNR = 35.26 \pm 3.77$ dB was used to evaluate the recovered capability before and after encryption and decryption for overall ECG fragments. The mean CPU execution time for completing the encryption and decryption processes was 0.16±0.01 s. Hence, the feasibility of the proposed symmetric cryptographic methods was validated.

C. COMPARISON WITH THE TRADITIONAL CRYPTOGRAPHIC METHODS

In this study, a chaotic synchronization system (CSS) was also applied to ECG encryption and decryption [47]–[49]. The CCS could randomly change the positions and amplitude values in the matrix form of ECG data and mix their relations between the plain and cipher ECG, as shown in Figure 5(c). A CSS consists of a master chaotic system (MCS), a slave chaotic system (SCS), and a controller. The controller was used to synchronize the trajectories of the MCS and SCS, as seen in the synchronization control responses in Figures 10(a) to 10(b), such as the proportional–integral–derivative (PID) controller, sliding mode controllers, optimization method (such as PSO algorithm), and fuzzy rule-based controller, which were used to control the CSS parameters to achieve a two-system synchronization at approximately 4,000

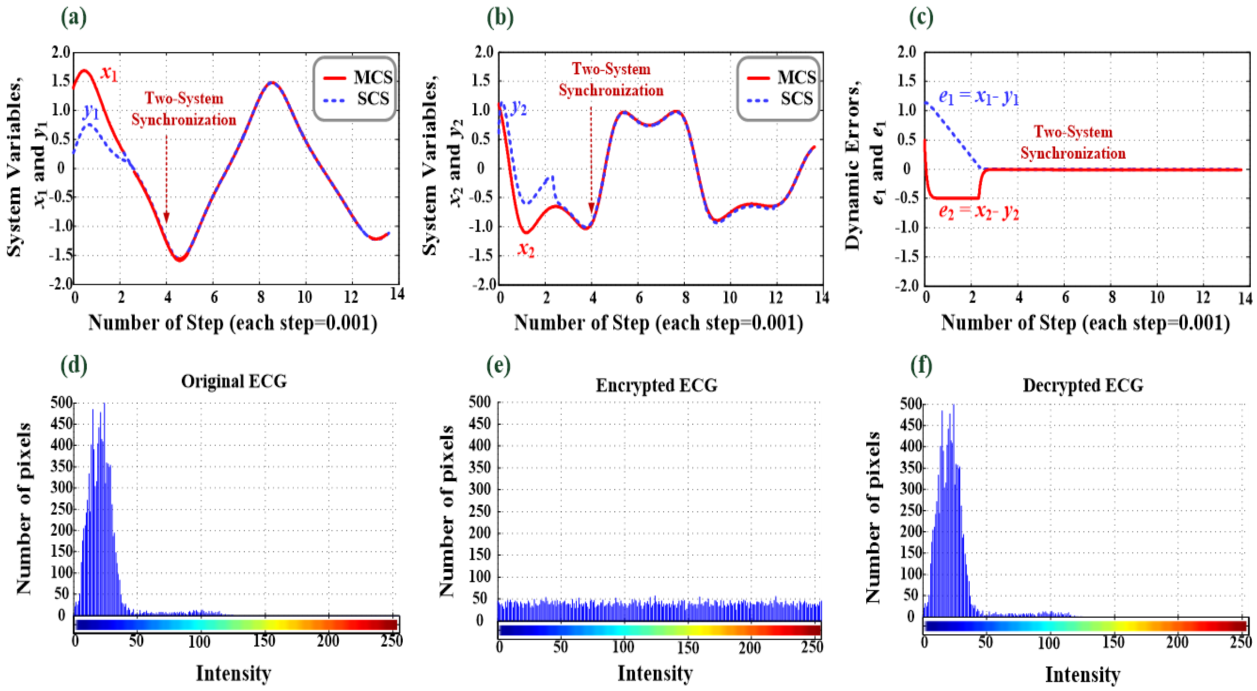


FIGURE 10. Experimental results for CSCS control responses and histogram plots. (a) and (b) Response of CSCS synchronization control, (c) Response of dynamic errors, (d) Plain ECG histogram, (e) Encrypted ECG histogram, (f) Decrypted ECG histogram.

TABLE 1. Experimental results of recoverability evaluation for the proposed GRNN-based encryptor and decryptor.

Record Number	Major Beat Classes							Mean *PSNR* (dB)	Executing Time (sec)
	•	V	A	R	L	F	P		
10	○	×	×	×	×	×	×	43.58 ± 4.05	0.15 ± 0.01
10	○	○	×	×	×	×	×	33.18 ± 1.32	0.17 ± 0.02
10	○	×	○	×	×	×	×	39.21 ± 3.56	0.17 ± 0.02
10	×	○	×	○	○	×	×	33.18 ± 2.03	0.17 ± 0.02
10	×	×	×	○	×	×	×	35.48 ± 0.59	0.18 ± 0.02
10	×	×	×	×	○	×	×	35.22 ± 1.09	0.17 ± 0.02
10	×	○	×	×	○	×	×	32.49 ± 1.82	0.17 ± 0.02
10	×	×	×	×	×	○	×	33.98 ± 1.42	0.17 ± 0.02
10	×	×	×	×	×	×	○	36.02 ± 1.89	0.15 ± 0.01
10	×	×	×	×	×	○	○	30.28 ± 1.43	0.17 ± 0.01
100							Average	35.26 ± 3.77	0.16 ± 0.01

TABLE 2. Experimental results of recoverability evaluation for the CSCS based encryptor and decryptor.

Record Number	Major Beat Classes							Mean *PSNR* (dB)	Executing Time (sec)
	•	V	A	R	L	F	P		
10	○	×	×	×	×	×	×	29.82 ± 0.12	20.21 ± 0.74
10	○	○	×	×	×	×	×	34.02 ± 0.01	18.81 ± 1.87
10	○	×	○	×	×	×	×	33.40 ± 0.02	21.11 ± 1.12
10	×	○	×	○	○	×	×	30.54 ± 0.03	21.89 ± 3.29
10	×	×	×	○	×	×	×	33.45 ± 0.01	21.94 ± 1.45
10	×	×	×	×	○	×	×	33.25 ± 0.05	20.32 ± 0.60
10	×	○	×	×	○	×	×	32.77 ± 0.02	21.35 ± 0.08
10	×	×	×	×	×	○	×	32.15 ± 0.01	19.64 ± 0.12
10	×	×	×	×	×	×	○	31.25 ± 0.03	18.21 ± 1.06
10	×	×	×	×	×	○	○	31.24 ± 0.01	20.45 ± 0.30
100							Average	32.19 ± 1.41	20.39 ± 1.24

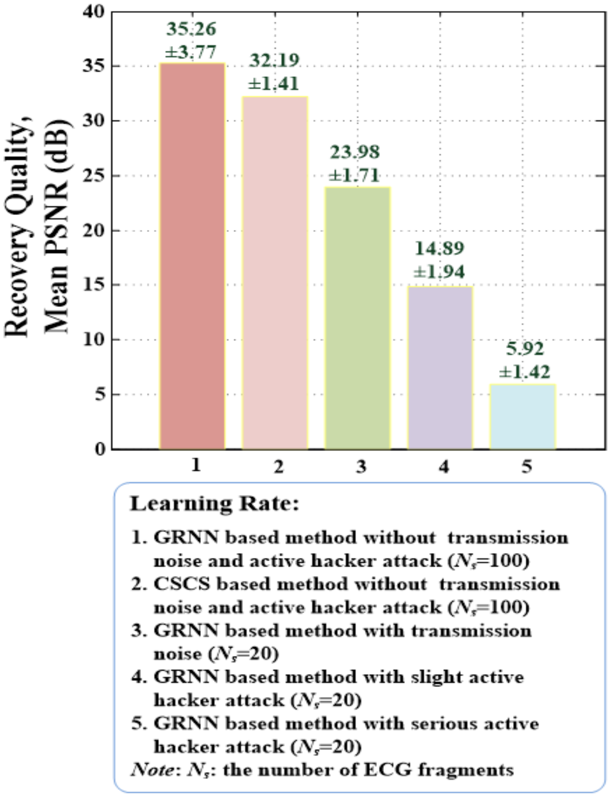


FIGURE 11. Mean *PSNR* (dB) for ECG decryption with and without transmission noises and active hacker attacks.

computations (each step = 0.001). The response of dynamic errors between MCS and SCS decreased and approached zero, as shown in Figure 10(c). Hence, a CSS and a fuzzy rule-based controller were integrated into a chaotic synchronization cryptographic system (CSCS) for ECG encryption and decryption. For the same 100 ECG fragments, as shown in the experimental results in Table 2, the mean $PSNR$ = 32.19 ± 1.41 dB was also greater than 30.00 dB and was achieved for recovering the cipher ECG. The mean execution time for completing the entire cryptographic processes was 20.39 ± 1.24 s. Experimental results indicated that the CSCS with a fuzzy rule-based controller had promising feasibility for the issue of physiological signal infosecurity. Figures 10(d)–10(f) showed that compared with that of plain and decrypted ECG, the histogram plot of encrypted ECG was fairly uniform and flat (as shown in Figure 10(e)) when using the CSCS method. This finding indicates that the plain and encrypted ECG were uncorrelated and perceptually different in the proposed method and the CSCS method, as shown in the middle part of Figures 5(b) and 5(c).

However, the CSCS method using a fuzzy rule-based controller needed to assign suitable system parameters (Duffing–Holmes system was used in this study, MCS and SCS parameters, $a = -1.00$, $b = 0.25$, and disturbance = $0.3\cos(t)$), fuzzy controller parameters, and initial conditions. For example, the CSS system parameters needed to assign specific constraint constant values in accordance with the desired control object, and the fuzzy rule-based controller required a trial-and-error procedure to determine the suitable membership functions and control rules. In this study, we had two input variables with 14 input membership functions and one output variable with seven output membership functions, representing seven fuzzy partitions as negative big, negative medium, negative small, zero, positive small, positive medium, and positive big. Overall, 49 fuzzy rule-based controllers were used to adjust the control parameters and achieve MCS and SCS synchronization. Thus, in contrast to the CSCS control scheme, the proposed GRNN-based method could reduce the CPU execution time and computational resources and obtained promising results for physiological signal infosecurity. In addition, the GRNN-based and CSCS- based methods have good recovery quality without transmission noises and active hacker attacks, and the decrypted ECGs can be interpretable for diagnostic applications, as presented by the mean $PSNR \geq 30$ dB, and $0< PSNR <30$ dB for transmission noises and slight / serious active attacks, as shown in Figure 11.

IV. CONCLUSION

In this study, GRNN-based encryptor and decryptor were proposed for application in physiological signal infosecurity in a small-scale computer networks or wireless communication networks. After the digital signaling process, an ECG signal sequence was encoded in values ranging from 0 to 255, and then these digital data were randomly permutated by chaotic secret keys, which were produced by a logistic map function. Before transiting ECG fragments at the data emitter end, authorized people could quickly set the random secret keys with the logistic map function; subsequently, the two GRNN-based MMLNs (as identical architecture) were used to train an encryptor and decryptor using two pairs of symmetric cryptography protocols. After encrypting the ECG fragment, the visual uncorrelation between the plain and cipher ECG was presented in vector or matrix forms. Through selected 100 ECG fragments from the MIT–BIH database, the mean PSNR = 35.26± 3.77dB was used to qualify the recovery quality of the decryption process for physiological signal infosecurity, which required a mean CPU execution time of 0.16 ± 0.01 s (less than CSCS's execution time) to complete encryption and decryption. With the same ECG fragments, the proposed method surpassed the CSCS method in terms of recovery quality and computational speed. We also suggested the learning parameters for training GRNN with the PSO algorithm, including specific particle population size ($G = 20$), maximum iteration number ($p_{max} = 25$), and convergent condition ($\varepsilon \leq 10^{-2}$), to model the encryptor and decryptor. Its adaptive learning scheme did not require the following: (1) specific system parameter assignment, (2) inference control rule assignment, (3) inference membership function assignment, and (4) too many numerical operations in the encryption and decryption processes for online application. Hence, the proposed cryptography protocol provides a promising model to speed up the encryption and decryption operations and enhances the confidentiality, recoverability, and availability of physiological signal infosecurity in tele- examination and telediagnosis applications; the method can also be applied to biomagnetic and bioacoustic signals.

ABBREVIATIONS

HBC	Human Body Communication
BAN	Body-Area Network
WBAN	Wireless BAN
RFID	Radio Frequency Identification
ISM	Industrial Scientific Medical
ECG	Electrocardiogram
MITBIH	Massachusetts Institute of Technology–Beth Israel Hospital
ADC	Analog-to-Digital Conversion
XOR	Exclusive
SINR	Signal-to-Interference-and-Noise Ratio
BER	Bit Error Rate
PER	Packet Error Rate
FE	Fractional Equivocation
PSNR	Peak Signal-to-Noise Ratio
ANN	Artificial Neural Network
GRNN	General Regression Neural Network
MMLN	Multilayer Machine Learning Network
MPNN	Multilayer Perceptron Neural Network
PSO	Particle Swarm Optimization
LE	Lyapunov Exponent
CKG	Chaotic Key Generator
SK	Secret Key
MSE	Mean Squared Error
HRV	Heart Rate Variability
RR	Peak- to-Peak
TCP	Transmission Control Protocol
CSS	Chaotic Synchronization System
MCS	Master Chaotic System
SCS	Slave Chaotic System
PID	Proportional–Integral–Derivative
CSCS	Chaotic Synchronization Cryptographic System
.●	Normal Beat
A	Atrial Premature Beat
V	Ventricular Premature Contraction Beat
R	Right Bundle Branch Block Beat
L	Left Bundle Branch Block Beat
P	Paced Beat
F	Fusion of Ventricular and Normal Beats

REFERENCES

[1] J. Gao, H. Zhang, P. Lu, and Z. Wang, "An effective LSTM recurrent network to detect arrhythmia on imbalanced ECG dataset," *J. Healthcare Eng.*, vol. 2019, pp. 1–10, Oct. 2019.

[2] R. Madhusudhan and C. S. Nayak, "A robust authentication scheme for telecare medical information systems," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15255–15273, Jun. 2019.

[3] C. Y. Song, K. B. Liu, X. Zhang, L. L. Chen, and X. C. Xian, "An obstructive sleep apnea detection approach using a discriminative hidden Markov model from ECG signals," *IEEE Trans. Biomed. Eng.*, vol. 63, no. 7, pp. 1532–1542, Jul. 2016.

[4] D. W. Jung, S. H. Hwang, Y. J. Lee, D.-U. Jeong, and A. S. Park, "Apnea–hypopnea index prediction using electrocardiogram acquired during the sleep-onset period," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 2, pp. 295–301, Feb. 2017.

[5] M. A. Quiroz-Juarez, O. Jimenez-Ramirez, R. Vazquez-Medina, E. Ryzhii, M. Ryzhii, and J. L. Aragon, "Cardiac conduction model for generating 12 lead ECG signals with realistic heart rate dynamics," *IEEE Trans. Nanobiosci.*, vol. 17, no. 4, pp. 525–532, Oct. 2018.

[6] C.-H. Lin, C.-D. Kan, J.-N. Wang, W.-L. Chen, and P.-Y. Chen, "Cardiac arrhythmias automated screening using discrete fractional-order integration process and meta learning based intelligent classifier," *IEEE Access*, vol. 6, pp. 52652–52667, 2018.

[7] X. Wang, Y. Guo, J. Ban, Q. Xu, C. Bai, and Shanliang Liu, "Driver emotion recognition of multiple-ECG feature fusion based on BP network and D–S evidence," *IET Intell. Transp. Syst.*, vol. 14, no. 8, pp. 815–824, 2020.

[8] X. Zhai and C. Tin, "Automated ECG classification using dual heartbeat coupling based on convolutional neural network," *IEEE Access*, vol. 6, pp. 27465–27472, 2018.

[9] T. Teijeiro, P. Felix, J. Presedo, and D. Castro, "Heartbeat classification using abstract features from the abductive interpretation of the ECG," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 2, pp. 409–420, Mar. 2018.

[10] *Part 15.1, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*, IEEE Standards Association, IEEE Standard 802.15.1-2005, Jun. 2011, doi: 10.1109/IEEESTD.2002.93621.

[11] M. A. Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, pp. 93–101, Mar. 2012.

[12] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[13] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017.

[14] *Health Insurance Portability and Accountability Act of 1996*, United State Department of Health and Human Services, Washington, DC, USA, 1996, vol. 104, p. 191.

[15] P. Mathivanan, A. B. Ganesh, and R. Venkatesan, "QR code–based ECG signal encryption/decryption algorithm," *Cryptologia*, vol. 43, no. 3, pp. 233–253, 2019.

[16] M. Aziz and M. Al-Akaidi, "Security issues in wireless ad hoc networks and the application to the telecare project," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Cardiff, U.K., Jul. 2007, pp. 491–494.

[17] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[18] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, pp. 23514–23526, 2019.

[19] M. Mohamed Alhejazi, E. Mohammed AL-Dahasi, and N. Abbas Saqib, "A new remote user authentication scheme for E-health-care applications using steganography," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–10.

[20] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *J. Med. Syst.*, vol. 40, p. 117, Mar. 2016.

[21] P. Dass and H. Om, "A secure authentication scheme for RFID systems," *Procedia Comput. Sci.*, vol. 78, pp. 100–106, 2016.

[22] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion–substitution based gray image encryption scheme," *Digit. Signal Process.*, vol. 23, pp. 894–901, Mar. 2013.

[23] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," *Multimedia Syst.*, vol. 20, no. 1, pp. 45–64, Feb. 2014.

[24] S. Anwar and S. Meghana, "A pixel permutation based image encryption technique using chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27569–27590, Oct. 2019.

[25] P.-Y. Chen, J.-X. Wu, C.-M. Li, C.-L. Kuo, N.-S. Pai, and C.-H. Lin, "Medical image infosecurity using hash transformation and optimization-based controller in a health information system: Case study in breast elastography and X-ray image," *IEEE Access*, vol. 8, pp. 61340–61354, 2020.

[26] P.-Y. Chen, J.-X. Wu, C.-M. Li, C.-L. Kuo, N.-S. Pai, and C.-H. Lin, "Symmetric cryptography with shift 2^{n-1}, hash transformation, optimization-based controller for medical image infosecurity: Case study in mammographic image," *IEEE Photon. J.*, vol. 12, no. 3, Jun. 2020, Art. no. 4100115.

[27] M. F. Zia and J. M. Hamamreh, "An advanced non-orthogonal multiple access security technique for future wireless communication networks," *RS Open J. Innov. Commun. Technol.*, no. 2, pp. 1–11, Dec. 2020, doi: 10.46470/03d8ffbd.19888ce7.

[28] J. P. Lemayian and J. M. Hamamreh, "A novel small-scale nonorthogonal communication technique using auxiliary signal superposition with enhanced security for future wireless networks," *RS Open J. Innov. Commun. Technol.*, no. 2, pp. 1–11, Nov. 2020, doi: 10.46470/03d8ffbd.86b0d106.

[29] W. San-Um and N. Chuayphan, "A lossless physical-layer encryption scheme in medical picture archiving and communication systems using highly-robust chaotic signals," in *Proc. 7th 2014 Biomed. Eng. Int. Conf.*, Fukuoka, Japan, Nov. 2014, pp. 1–5.

[30] A. N. K. Telem, C. M. Segning, G. Kenne, and H. B. Fotsin, "A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network," *Adv. Multimedia*, vol. 2014, Dec. 2014, Art. no. 602921.

[31] A. N. K. Telem, C. M. Segning, G. Kenne, and H. B. Fotsin, "A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network," *Adv. Multimedia*, vol. 2014, Dec. 2014, Art. no. 602921.

[32] M. Kumar, S. Kumar, R. Budhiraja, M. K. Das, and S. Singh, "A cryptographic model based on logistic map and a 3-D matrix," *J. Inf. Secur. Appl.*, vol. 32, pp. 47–58, Feb. 2017.

[33] L. A. Demidova and A. V. Gorchakov, "A study of chaotic maps producing symmetric distributions in the fish school search optimization algorithm with exponential step decay," *Symmetry*, vol. 12, no. 5, p. 784, 2020.

[34] T.-L. Yang, C.-H. Lin, W.-L. Chen, H.-Y. Lin, C.-S. Su, and C.-K. Liang, "Hash transformation and machine learning-based decision-making classifier improved the accuracy rate of automated Parkinson's disease screening," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 28, no. 1, pp. 72–82, Jan. 2020.

[35] T.-L. Yang, P.-J. Kan, C.-H. Lin, H.-Y. Lin, W.-L. Chen, and H.-T. Yau, "Using polar expression features and nonlinear machine learning classifier for automated Parkinson's disease screening," *IEEE Sensors J.*, vol. 20, no. 1, pp. 501–514, Jan. 2020.

[36] J.-X. Wu, P.-Y. Chen, C.-M. Li, Y.-C. Kuo, N.-S. Pai, and C.-H. Lin, "Multilayer fractional-order machine vision classifier for rapid typical lung diseases screening on digital chest X-ray images," *IEEE Access*, vol. 8, pp. 105886–105902, 2020.

[37] H. Chougrad, H. Zouaki, and O. Alheyane, "Deep convolutional neural networks for breast cancer screening," *Comput. Methods Programs Biomed.*, vol. 157, pp. 19–30, Apr. 2018.

[38] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-Boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.

[39] T.-H.-S. Li, C.-Y. Liu, P.-H. Kuo, N.-C. Fang, C.-H. Li, C.-W. Cheng, C.-Y. Hsieh, L.-F. Wu, J.-J. Liang, and C.-Y. Chen, "A three-dimensional adaptive PSO-based packing algorithm for an IoT-based automated e-Fulfillment packaging system," *IEEE Access*, vol. 5, pp. 9188–9205, 2017.

[40] *MIT-BIH Arrhythmia Database*. Accessed: Jan. 2018. [Online]. Available: https://www.physionet.org/ Physiobank/database/mitdb/

[41] M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," *IET Image Process.*, vol. 10, no. 11, pp. 830–839, Nov. 2016.

[42] S. G. Al-Kindi and R. Tafreshi, "Real-time detection of myocardial infarction by evaluation of ST-segment in digital ECG," *J. Med. Imag. Health Informat.*, vol. 1, no. 3, pp. 225–230, Sep. 2011.

[43] S. Gutta and Q. Cheng, "Joint feature extraction and classifier design for ECG-based biometric recognition," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 2, pp. 460–468, Mar. 2016.

[44] I. Jekova, V. Krasteva, R. Leber, R. Schmid, R. Twerenbold, T. Reichlin, C. Müller, and R. Abächerli, "A real-time quality monitoring system for optimal recording of 12-lead resting ECG," *Biomed. Signal Process. Control*, vol. 34, pp. 126–133, Apr. 2017.

[45] (2019). *IEEE 802 LAN/MAN Standards Committee*. [Online]. Available: http://grouper.ieee.org/groups/802/

[46] M. Andreu Climent, M. D. L. S. Guillem, D. Husser, F. Castells, J. Millet, and A. Bollmann, "Poincare surface profiles of RR intervals: A novel noninvasive method for the evaluation of preferential AV nodal conduction during atrial fibrillation," *IEEE Trans. Biomed. Eng.*, vol. 56, no. 2, pp. 433–442, Feb. 2009.

[47] C.-L. Kuo, "Design of an adaptive fuzzy sliding-mode controller for chaos synchronization," *Int. J. Nonlinear Sci. Numer. Simul.*, vol. 8, no. 4, pp. 631–636, Jan. 2007.

[48] Y.-Y. Hou, H.-C. Chen, J.-F. Chang, J.-J. Yan, and T.-L. Liao, "Design and implementation of the sprott chaotic secure digital communication systems," *Appl. Math. Comput.*, vol. 218, no. 24, pp. 11799–11805, Aug. 2012.

[49] H. Tirandaz and S. S. Aminabadi, "Chaos synchronization and parameter identification of a finance chaotic system with unknown parameters, a linear feedback controller," *Alexandria Eng. J.*, vol. 57, pp. 1519–1524, Sep. 2018.

CHIA-HUNG LIN was born in Kaohsiung City, Taiwan, in 1974. He received the B.S. degree in electrical engineering from the Tatung Institute of Technology, Taipei City, Taiwan, in 1998, and the M.S. and Ph.D. degrees in electrical engineering from National Sun Yat-Sen University, Kaohsiung City, in 2000 and 2004, respectively.

He is currently a Professor with the Department of Electrical Engineering, Kao-Yuan University, Kaohsiung City, from 2004 to 2017. He is also a Professor with the Department of Electrical Engineering and a Researcher with the Artificial Intelligence Application Research Center, National Chin-Yi University of Technology, Taichung City, Taiwan, where has been since 2018. His research interests include neural network computing and its applications in power system and biomedical engineering, biomedical signal and image processing, healthcare, hemodynamic analysis, and pattern recognition.

JIAN-XING WU was born in 1985. He received the B.S. and M.S. degrees in electrical engineering from the Southern Taiwan University of Science and Technology, Tainan, Taiwan, in 2007 and 2009, respectively, and the Ph.D. degree in biomedical engineering from National Cheng Kung University, Tainan City, Taiwan, in 2014.

He is currently a Postdoctoral Research Fellow with the X-ray and IR Imaging Group, National Synchrotron Radiation Research Center, Hsinchu City, Taiwan, from 2014 to 2017. He is also a Postdoctoral Research Fellow with the Department of Niche Biomedical LLC, California Nano Systems Institute, UCLA, Los Angeles, USA, from 2017 to 2018. He is currently an Assistant Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan, where has been since 2019. His research interests include artificial intelligence applications in electrical engineering and biomedical engineering, biomedical signal processing, medical ultrasound, and medical device design, and X-ray microscopy.

PI-YUN CHEN received the Ph.D. degree from the Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Yunlin, Taiwan, in 2011.

She is currently an Associate Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan. She is also the Chief of the Department of Electrical Engineering, National Chin-Yi University of Technology, where has been since 2019. Her current research interests include neural network computing and its applications, fuzzy systems, and advanced control systems.

CHIEN-MING LI was born in 1959. He received the B.S. degree in science from National Taiwan University, Taipei, Taiwan, in 1982, the M.D. degree from National Cheng Kung University, Tainan, Taiwan, in 1990, and the Ph.D. degree in biomedical engineering from National Cheng Kong University, Tainan, Taiwan, in 2014.

He is currently an Infectious Disease Specialist with the Chi Mei Medical Center, and an Associate Professor with the Medical College of National Cheng Kung University, Tainan, Taiwan. His research interests include medical applications of pattern recognition and MATLAB, computer-assisted diagnosis and treatment of infectious disease.

NENG-SHENG PAI received the B.S. and M.S. degrees from the Department of Automatic Control Engineering, Feng Chia University, Taichung, Taiwan, ROC, in 1983 and 1986, respectively, and the Ph.D. degree from the Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan, ROC, in December 2002.

He is currently a Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan, ROC. He was the Chairman of the Department of Electrical Engineering, from 2004 to 2007 and was also the Chairman of the Computer Center of the National Chin-Yi University of Technology from 2013 to 2017. His current research interests include fuzzy systems, artificial intelligence, imagine processing, advanced control systems, and microprocessor systems.

CHAO-LIN KUO (Member, IEEE) received the B.S. degree from the Department of Automatic Control Engineering, Feng Chia University, Taichung, Taiwan, in 1998, the M.S. degree from the Institute of Biomedical Engineering, National Cheng Kung University, Tainan, Taiwan, in 2000, and the Ph.D. degree from the Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan, in 2006.

He is currently an Associate Professor with the Institute of Maritime Information and Technology, National Kaohsiung Marine University, Kaohsiung City, Taiwan, from 2011 to 2017. He is currently a Professor with the Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung City, Taiwan, where has been since 2017. He is also the Chief of the Department of Maritime Information and Technology, where has been since 2018. His current research interests include artificial intelligence applications in electrical engineering and ocean engineering, intelligent control systems, fuzzy systems, and embedded systems and its applications.