IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 November 2023, accepted 1 January 2024, date of publication 8 January 2024, date of current version 22 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3351373

RESEARCH ARTICLE

Information Security and Artificial Intelligence–Assisted Diagnosis in an Internet of Medical Thing System (IoMTS)

PI-YUN CHEN[1], YU-CHENG CHENG[1], ZI-HENG ZHONG[1], FENG-ZHOU ZHANG[1], NENG-SHENG PAI[1], CHIEN-MING LI[2], AND CHIA-HUNG LIN[1]

[1]Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung 41170, Taiwan
[2]Division of Infectious Diseases, Department of Medicine, Chi Mei Medical Center, Tainan 710, Taiwan

Corresponding authors: Pi-Yun Chen (chenby@ncut.edu.tw) and Chia-Hung Lin (eechl53@gmail.com)

This work was supported in part by the National Science and Technology Council (NSTC), from August 2022 to July 2024, under Contract NSTC 111-2221-E-167-034 and Contract NSTC 112-2221-E-167-015; and in part by the National Chin-Yi University of Technology, from January 2023 to November 2023, under Contract NCUT 23-R-CE-009.

ABSTRACT The internet of medical thing system (IoMTS) comprises the fifth-generation (5G) networking technology that collects and shares digital data from signal- or image-capturing devices through computer and wireless communication networks. This framework enables healthcare professionals to gain immediate visibility into a patient's condition and facilitates communication with patients and family members. Recently, artificial intelligence (AI)- based methods are being increasingly applied to preprocess digital data and extract features. The key physiological parameters and feature patterns can then be incorporated into AI- based tools to help monitor, detect, and diagnose applications. However, these digital data contain patients' privacy and may be restricted to authorized users. In a public channel, IoMTS must ensure information security for protection against hacker attacks. Hence, in this study, a symmetric encryption and decryption protocol was designed to ensure infosecurity of biosignals and medical images and assist in specific purposes in disease diagnosis. For a symmetric cryptography scheme, this study proposed a key generator combining a chaotic map and Bell inequality and generating unordered numbers and unrepeated 256 secret keys in the key space. Then, a machine learning - based model was employed to train the encryptor and decryptor for both biosignals and image infosecurity. After secure - data transmission, a case study is conducted for classifying medical images. Here, a classifier based on a convolutional neural network (CNN) is used for AI- assisted breast tumor diagnosis. In addition, for biosignal infosecurity, raw data were collected from a radar millimeter-wave (mm-Wave) sensing firmware for detecting vital signs. The experimental results are validated for heartbeat signals, respiratory signals, and mammography images, demonstrating the effectiveness and feasibility of the proposed encryption, decryption, and AI-assisted diagnosis methods.

INDEX TERMS Internet of medical thing (IoMTS), symmetric encryption and decryption protocol, convolutional neural network (CNN), radar millimeter-wave (mm-Wave), vital signs detection.

I. INTRODUCTION

An internet of medical things system (IoMTS) integrates various measurement instruments, imaging devices, and information management systems [1], [2], [3], [4]. In addition, it uses the fifth-generation (5G) communication systems [5] to remotely and timely transmit digital data to multiple institutions and facilitate multiparty consultations of disease status among the hospitals, patients, and their family members. For measurement instruments, physiological data can be transmitted from various sensors through ZigBee, WiFi, or Bluetooth wireless communication

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

protocols (IEEE 802.11 Wireless Networking Protocol [6]). The HIPAA (Health Insurance Portability and Accountability Act) Security Rule defines that transmitting data through wireless communication protocols can ensure data confidentiality and integrity and facilitate AI- assisted diagnosis [2], [7], [8]. The IoMTS framework uses the picture archiving and communication system (PACS) as its management system, a medical imaging technology used for storage, processing, and transmission of medical images [7], [8]. Digital medical images from different imaging devices can be securely stored in a database in the DICOM (digital imaging and communications in medicine) format. Moreover, medical images can be transformed into various formats (e.g., JPEG, JPEG Lossless, and JPEG 2000 formats) and transmitted in real time over a communication network, such as X-ray images, computed tomography (CT) images, magnetic resonance imaging (MRI), and mammography [3], [9], [10], [11]. In public channels, to ensure a proper security level in IoMTS against the active-hacker and passive-hacker attacks, digital data transmissions must be protected using loophole detection, and secure communications protocols must be reinforced. Therefore, we intend to design an intelligent cryptography scheme for biosignals and medical - image infosecurity, ensuring data confidentiality, integrity, and availability. In addition, we ensured that the scheme boasts the additional benefit of assisting in disease diagnosis, such as cardiac arrhythmia, cardiopulmonary diseases, and cancer detection.

Medical images and records and personal information are increasingly digitalized in PACS and may be attacked by the passive- or active-hacker attacks. In 2018–2022 years, 500 ransomware attacks were detected that targeted medical institutions worldwide; possibly, 12,961 organizations have been subjected to passive hacking attacks. The total amount paid in ransoms exceeded US$1.2 billion, and losses due to the resulting downtime of the medical system reached US$92 billion [12]. In 2019 years, dozens of hospitals in Taiwan were also victims of ransomware attacks. Hackers simultaneously attacked multiple medical institutions and encrypted files in multiple formats, preventing access to medical images. Hence, in 2018 years, the U.S. FDA (Food and Drug Administration) promulgated relevant regulations to strengthen medical cybersecurity and protect networked medical devices [13]. Since then, studies have been committed to developing information security and AI-assisted diagnosis systems [9], [14]. These systems help clinicians safely use relevant digital data and reduce the time required for diagnosis.

For information security, many studies have developed digital encryption technologies, such as Rivest–Shamir–Adleman (RSA), data encryption standard (DES), and advanced encryption standard (AES) methods [15], [16], [17], [18], [19], [20]. The RSA method is an asymmetric encryption algorithm in which a long length of secret keys (binary format) has a higher security level, and the secret keys need not be transmitted to authorized people (with public keys). The RAS-based cryptography schemes can be applied to digital signature authentication. However, RSA requires complex operations for producing secret keys and performing encryption and decryption processes; moreover, it is used for encrypting small amounts of data. The DES is a block-symmetric encryption algorithm that encrypts and decrypts digital data using XOR, permutation, substitution, and transposition operations, and its secret keys and cipher life cycles are short. Due to its slow computational operations, the DES-based cryptography scheme is unsuitable for signal- and image-based encryption; the AES is also a symmetric encryption algorithm that applies substitution, row shifting, and column mixing operations to the encryption process and achieves decryption process through reverse operations. It follows fast computational operation and is secure and resource-efficient. Studies on AI-assisted diagnosis applications have applied machine learning (ML) and deep learning (DL) methods to classify medical images, digital signals, and text [2], [7], [8], [21], [22], [23], [24], [25], [26], [27].

In this study, we intend to establish an AI-assisted secure system for biosignals and medical images in human vital-signs detection (VSD) and rapid breast lesions screening in an IoMTS, as seen in Figure 1. In physiological signals measurements, a radar millimeter- wave (mm-Wave) sensing firmware (76–81GHz mm- Wave radar, 4-GHz Bandwidth) and Raspberry Pi-Hat board (ARM® Cortex®-R4F-Based Radio Control System) were used for VSD applications using the frequency- modulated continuous-wave (FMCW) control mode. This is integrated into a sensing system with the Doppler effect and FMCW for a short range ($<$1.0 m), and contactless measurements are performed in heartbeat and respiratory pulsation signals. These physiological signals can be used to estimate the heart rate (HR) and respiratory rate (RR), with the primary advantage in high-frequency sensing firmware that prevents receiving unwanted signals; additionally, it can avoid misjudgment caused by intermodulation signals and has some advantages, such as low cost, lightweight, and portability. For AI-assisted diagnosis in image classification, conventional ML-based methods, such as back-propagation neural networks (BPNN) and support vector machines (SVM), cannot automatically extract feature patterns from an image; manual labeling and feature-extraction processes are required before classifier training. Conversely, DL-based methods, such as convolutional neural networks (CNNs), can automatically extract feature patterns and facilitate classification model training [21]. The CNN comprises multiple convolutional layers and kernel convolutional windows with combinations of different weighted values that allow for automatic denoising, sharpening objects, and feature extraction processes. These convolutional operations with different weighted values of kernel windows can enhance the depth of feature patterns, thereby improving the ability of pattern recognition. Finally, the maximum pooling (Max-pooling) operations are used

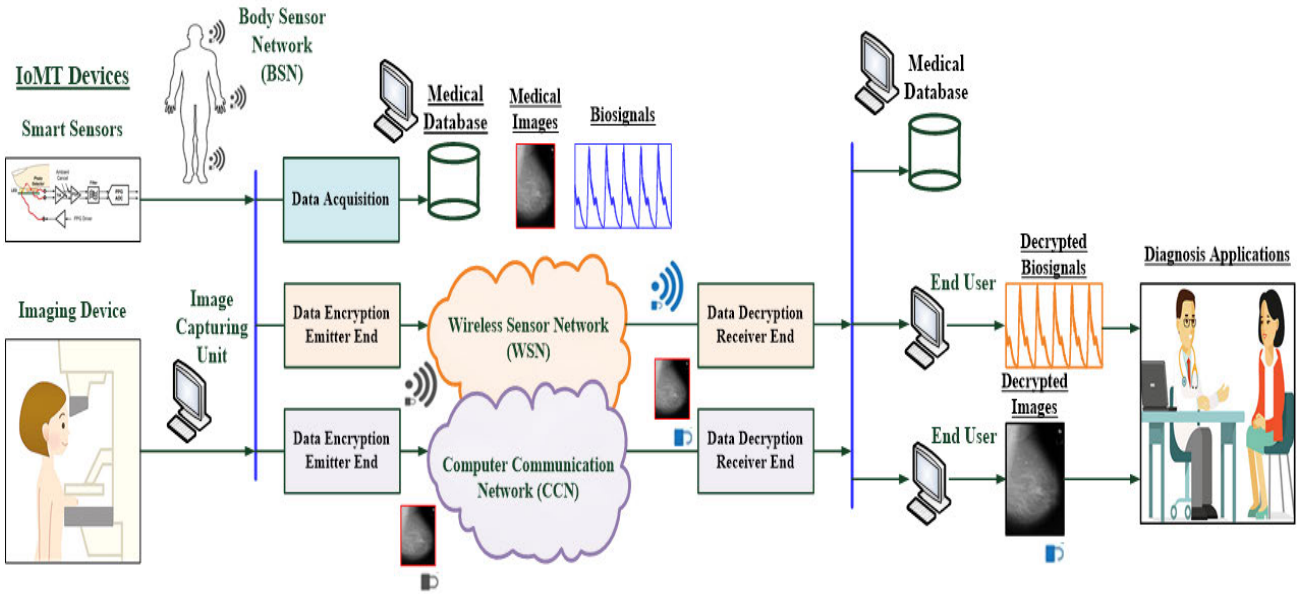

FIGURE 1. System framework for achieving information security and AI-assisted diagnosis in an IoMTS.

in pooling layers for extracting specific features. Hence, the sizes of feature patterns are downscaled, reducing the number of feature parameters by approximately one-fourth, while maintaining their depth. Overall, a CNN can establish a small-scale structure network. In addition, even if using limited number of training datasets to train a classifier, the training scheme of CNN can typically be adjusted to attain favorable generalizability, such as the numbers of convolutional layers and kernel convolutional windows. Therefore, CNN-based classifier's image- classification ability is superior to other conventional ML-based methods.

Therefore, we established an AI- assisted system in information security and diagnosis applications that comprises two parts: encryption–decryption and image- classification schemes. In encryption–decryption scheme, a combining chaotic map and quantum-based key generator was introduced to produce the two-round pseudorandom numbers, which we used to select the secret keys for encryption and decryption processes for biosignals and medical-image infosecurity [28], [29], [30], [31], [32]. In the first round, the one-dimensional (1D) chaotic map based on sine-power mathematical equation, as the so-called sine-power chaotic map (SPCM), which has more complex chaotic behaviors and a wider chaotic range [33], [34] for generating pseudorandom number seeds. The dynamic chaotic behaviors exhibit a bifurcation characteristic diagram and have a lower regularity level and high non-linearity for generating the time-series dynamic map. The bifurcation diagram is a period-doubling cascade attractor with different system control parameters which can produce an infinite sequence of period-doubling logistic map by iteration computations and also produce perturbation trajectories for creating random movement states similar to the perturbation trajectories of photon propagations. These perturbation trajectories include the usual polarization state pairs, e.g., rectilinear vertical (+90°) and horizontal (0°) bases with encoding values of "1" and "0" and diagonal bases of −45° and +45° with encoding values of "1" and "0" [28]. In the second round, according to these perturbation trajectories, any two bases can be conjugated to each other, and thus Bell inequality [35], [36], [37] can be applied to superimpose these bases (movement states) to produce the second-round random numbers, as the quantum-based key generator.

Thus, this two-round key generator (SPCM+ quantum-based key generator) can produce 256-bit unordered and unrepeated random numbers in a 256-bit key space to set the symmetric secret keys for authorized persons (clinicians or users in the medical environment). Next, two general regression neural networks (GRNNs) were used for training an encryptor and a decryptor for biosignals and medical images, such as electrocardiogram (ECG), photoplethysmography (PPG), chest X-ray, and mammography images [20], [22], [23], [24], [25], [26], [27], [28], [29]. The decrypted biosignals and medical images can be used to estimate HR and RR and identify diseases and breast lesions. In image classification, datasets of breast mammography were used to train a CNN-based classifier comprising multiple convolutional layers with multiple kernel convolutional windows (100×100, 50×50, and 25×25 windows), multiple Max-pooling layers (cascaded "convolutional operation" + "Max-pooling operation"), a flattening process layer, and a classification layer. This cascaded classification scheme was applied to manually or automatically extract feature patterns from the region of interest (ROI) and then sequentially feed the feature pattern into a CNN-based classifier for image classification [22], [23], [24], [25], [26], [27], [38].

In performance evaluations, the encryption security level and decryption quality are evaluated using evaluation metrics, such as the number of pixel change rate (NPCR) and unified average change intensity (UACI) [28], [29], respectively. In addition, the structural similarity index measurement (SSIM) and peak signal-to-noise ratio (PSNR) were used to evaluate the decrypted image quality. For evaluating the classifier performance, the classifier produces a confusion matrix, which has four indexes for evaluating the classification capability, namely true positive (TP), true negative (TN), false positive (FP), and false negative (FN) [22], [23], [24], [25], [26], [27], [38]. These indexes can be used to calculate the evaluation metrics of accuracy (%), precision (%), recall (%), and F1 score (%) to validate the classifier and its feasibility for medical purposes or clinical applications.

II. METHODOLOGY

A. DIGITAL DATA ENCRYPTOR AND DECRYPTOR DESIGN

According to the computer security report of the National Institute of Standards and Technology [39], the data confidentiality provided by information systems should be ensured to prevent the unauthorized third person from accessing the data, protect the data from tampering, and ensure reliable data access. The encryption process is employed to transform the data into an unreadable form, as the so-called cipher text, and can only be recovered using the decryption process with a specific secret key. Even if encrypted data are obtained by hackers, the information is meaningless without the secret key. Symmetric encryption algorithms include classical cryptography, modern cryptography, and intelligent encryption algorithms [28], [29], [40], [41], [42]. In modern cryptography, the algorithms combine different encryption processes having key spaces with lengths of 56, 64, 128, or 256 bits, increasing the computational complexity. In advanced cryptography, the AI- based encryption algorithms are performed in two steps:

Step#1) Random-number seeds are generated using the transformation functions, such as Fourier transform, wavelet transform, high-dimensional chaos systems, 1D chaotic maps, or optics-based encryption algorithms [20], [28], [29], [40], [41], [42]. However, high-dimensional chaotic systems are computationally intensive and time- and resource-consuming. The 1D chaotic maps, such as the sine-power, cosine-power, circle, tent, and logistic maps [20], [28], [29], [42] can easily generate random-number seeds (randomly distributed and unordered sequence data in a chaotic range) with the specific initial condition and the specific ranges of system control parameters. The encryption and decryption keys are selected from these random-number seeds. Hence, for generating the lower regularity level of random-number seeds, we employ two-round key generator to produce the random numbers; and then the authorized persons can select a 256 key-space secret keys from theses random numbers by using the proposed key generator, which can be used to set the symmetric encryption and decryption key before any biosignal and image transmission.

Step#2) DL- or ML-based algorithms are employed to train the encryptor and decryptor [20], [28], [29], [42], [43], [44]. The main motivation for such algorithms is to increase the complexity level for all the cryptography protocols. The permutation method (PM) and substitution method (SM) were applied for encryption of digital signals and images [20], [28], [29], [42], [43], [44], [45], [46], [47]. The PM was used to spatially rearrange the data positions without changing their values. However, only changing the pixel positions to scramble the data could result in weak security, allowing hacker attacks, such as statistical and brute-force attacks. In the SM, the numerical values are changed according to the secret keys used, and then the data content is altered at their original positions. However, because of the limited precision of floating-point computations, some differences may be observed in the data contents in the encryption and decryption processes. Nevertheless, these differences may be minimal and visually imperceptible between the plain and decrypted data. Both of the above methods can improve the data security level, retain the data quantity, and preserve the data format.

In this study, the SM-based cryptography method was used to design the data encryptor and data decryptor by using a combining 1D SPCM and quantum-based key generator [28], [29], [42]. Based on quantum mechanics, the Bell inequality [35], [36], [37] is used to estimate the probability distribution, such as projection-valued measurement and Hilbert space formulation [48]. Photon propagations have possible polarization directions, such as 0°, +90°, +45°, and −45°, as seen in Figure 2, which can be encoded in non-orthogonal quantum states [49]. In the specific range of chaotic perturbation trajectories, given two photons, A and B, the spin probability formula is as follows [28]:

- entanglement states:

$$|\Phi^{\pm}\rangle_{AB} = 2^{-1/2}(\alpha^2 P|_{\downarrow} \pm \beta^2 P|_{\rightarrow}) \tag{1}$$

or

$$|\Phi^{\pm}\rangle_{AB} = 2^{-1/2}(\alpha^2 P|_{\uparrow} \pm \beta^2 P|_{\rightarrow}) \tag{2}$$

- constraint condition: $\alpha^2 + \beta^2 = 1$.

where α^2 is the probability of a qubit with the value of "1". and β^2 is the probability of a qubit with the value of "0". Photons, A and B, possess the usual polarization state pairs, such as those in terms of the rectilinear basis: vertical, 90°, and horizontal, 0°; and the diagonal basis: ±45°, as seen in Figure 2 [28]. The rectilinear (90°) and diagonal (−45°) bases can be encoded using the value of "1"; and the rectilinear "0°" and diagonal "+45°" can be encoded using the value of "0" for the 1D chaotic perturbation trajectories.

For random-number seed generation, in the first round, the 1D chaotic map is used to generate a series of pseudo-random sequences form the bifurcation map, as seen in Figure 3(a); and then Bell inequality in (1) and (2) transfers

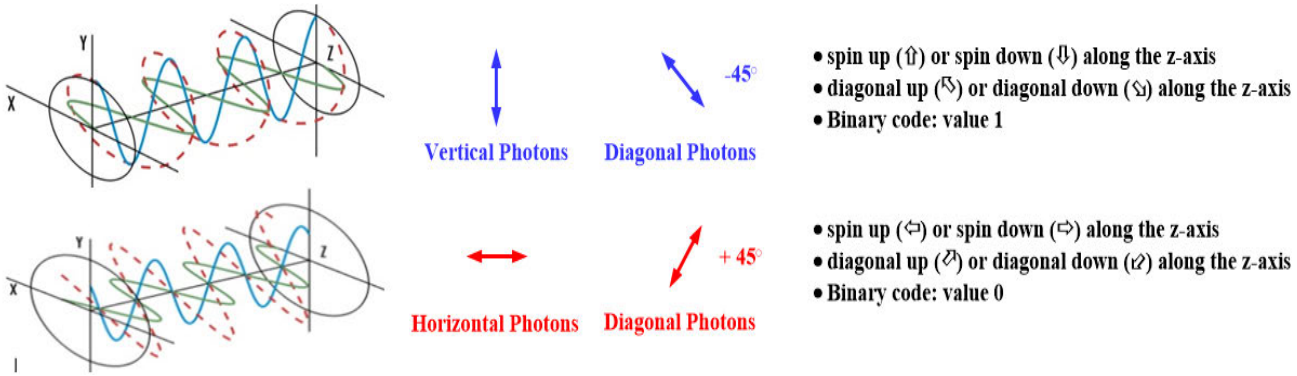

FIGURE 2. Possible particle spin directions during photon propagation and binary coding for each direction.

the pseudorandom numbers in the second round. The formula for two-round random number generation is expressed as follows:

- first-round random-number generator: the generation function is the SPCM [28], [29]

$$c_{n+1} = \sin^2(\sqrt{|c_n|}) + 2(1-r)|c_n|(1-2|c_n|) \quad (3)$$

$$c'_n = \mathrm{mod}(floor(255 \cdot |2c_n|), 256) \quad (4)$$

where c_n is the 1D random sequence data; c_0 is the initial condition, with $c_0 \in (0, 1)$; and r is the control parameter. Equation (3) can produce the nonperiodic chaotic sequence with $c_0 = 0.0$ and $r = 0.0$–4.0, as shown in Figure 3(a) by using the chaotic sequence with an amplitude within ±0.50. In Equation (4), operator $mod(\bullet)$ is the modulo operation; and operator $floor(\bullet)$ is the floor operation. Hence, after generating random sequences, the unrepeated and unordered random numbers can be selected from value 0 to 255.

- Second-round random-number generator: the binary coding in Figure 2 is used in conjunction with (1) and (2) to express the state of the random number distribution, and the formula can be expressed as

$$|\Phi\rangle_{\mathrm{n}} = 2^{-1/2} \begin{cases} (c'_n\alpha^2 P|_{\downarrow} + c'_n\beta^2 P|_{\rightarrow}) \\ (c'_n\alpha^2 P|_{\rightarrow} + c'_n\beta^2 P|_{\uparrow}), \end{cases} \quad (5)$$

$$\text{constraint condition: } \alpha^2 + \beta^2 = 1, \quad n = 0, 1, 2, \ldots, n_{\mathrm{c}} \quad (6)$$

where $\alpha^2 = \beta^2 = 0.50$. In addition, a probability of approximately 50% was assigned to the states coded "1", including $P_{|\uparrow}$, $P_{|\downarrow}$, $P_{|\swarrow}$, and $P_{|\searrow}$, and the remaining states coded "0" for $P_{|\leftarrow}$, $P_{|\rightarrow}$, $P_{|\nearrow}$, and $P_{|\swarrow}$ have the same probability of approximately 50%, as shown in Figure 2. Thus, the possible states in the 1D chaotic map may be "$2^{-1/2}(c_n\alpha^2\ P_{|\downarrow} + c_n\beta^2\ P_{|\rightarrow})$" and "$2^{-1/2}(c_n\alpha^2\ P_{|\rightarrow} + c_n\beta^2\ P_{|\uparrow})$" [28]. In (5), the probability of each superposition state as specific ranges between value "0" and value "1". The probabilities of random distribution are converted into random numbers from 0 to 255, as follows:

$$C_{\mathrm{n}} = floor(255\,|\Phi\rangle_n\ /\ \max(|\Phi\rangle_n)) \quad (7)$$

where $\max(|\Phi\rangle_n) = 255$. Thus, Eq. (3)–(7) are used to generate random numbers in two-round processes, as shown in Figure 3(a). They were then used to select the unrepeated and unordered numbers for setting secret keys for encryption and decryption processes in biosignals and medical images.

- Encryptor and decryptor design: Figure 3(b) shows the encryptor and decryptor, wherein two GRNN-based network models are employed to learn the 256-bit length of secret keys for the symmetric cryptography protocol [20], [28], [42].

In the encryption and decryption processes, two pairs of secret keys can be selected by authorized persons (clinicians or specific users) for setting the "symmetric secret keys"; then, two pairs of secret keys are used to train the encryptor and decryptor; the algorithm is described as follows:

(*1*) encryption key: $W^I = [w_{k1}]^T = [k - 1/255]^T$ and

$$W^I = [w_{k1}]^T = [c_k/255]^T \quad (8)$$

where $k = 1, 2, \ldots, K$, $K = 256$(key space); and c_k represents the 256 unrepeated and the unordered numbers which are selected from the two-round key generator.

(*2*) decryption key: $W^2 = [w_{k1}, w_{k2}]^T = [c_k/255, 1]^T$ and

$$W^2 = [w_{k1}, w_{k2}]^T = [k - 1/255, 1]^T \quad (9)$$

Two paired secret keys (W^1, W^2) can rapidly be used to determine the GRNN structure, which has 1 node in input layer, 256 nodes in pattern layer, 2 nodes in summation layer, and 1 node in output layer, as shown in Figure 3(b).

(*3*)The GRNN-based model has already been proposed in previous studies [20], [28], [42] to adjust the optimal network parameters for training the encryptor and decryptor. The Gaussian function is employed as the activation function in pattern layer, as follows:

- encryptor: $G_k = \exp[-\sum_{k=1}^{K} \frac{(x_i - w_{ki})^2}{2\sigma_k^2}]$,

$$i = 1, 2, 3, \ldots, 256 \quad (10)$$

- decryptor: $G_k = \exp[-\sum_{k=1}^{K} \frac{(c_i - w_{ki})^2}{2\sigma_k^2}]$,

$$i = 1, 2, 3, \ldots, 256 \quad (11)$$

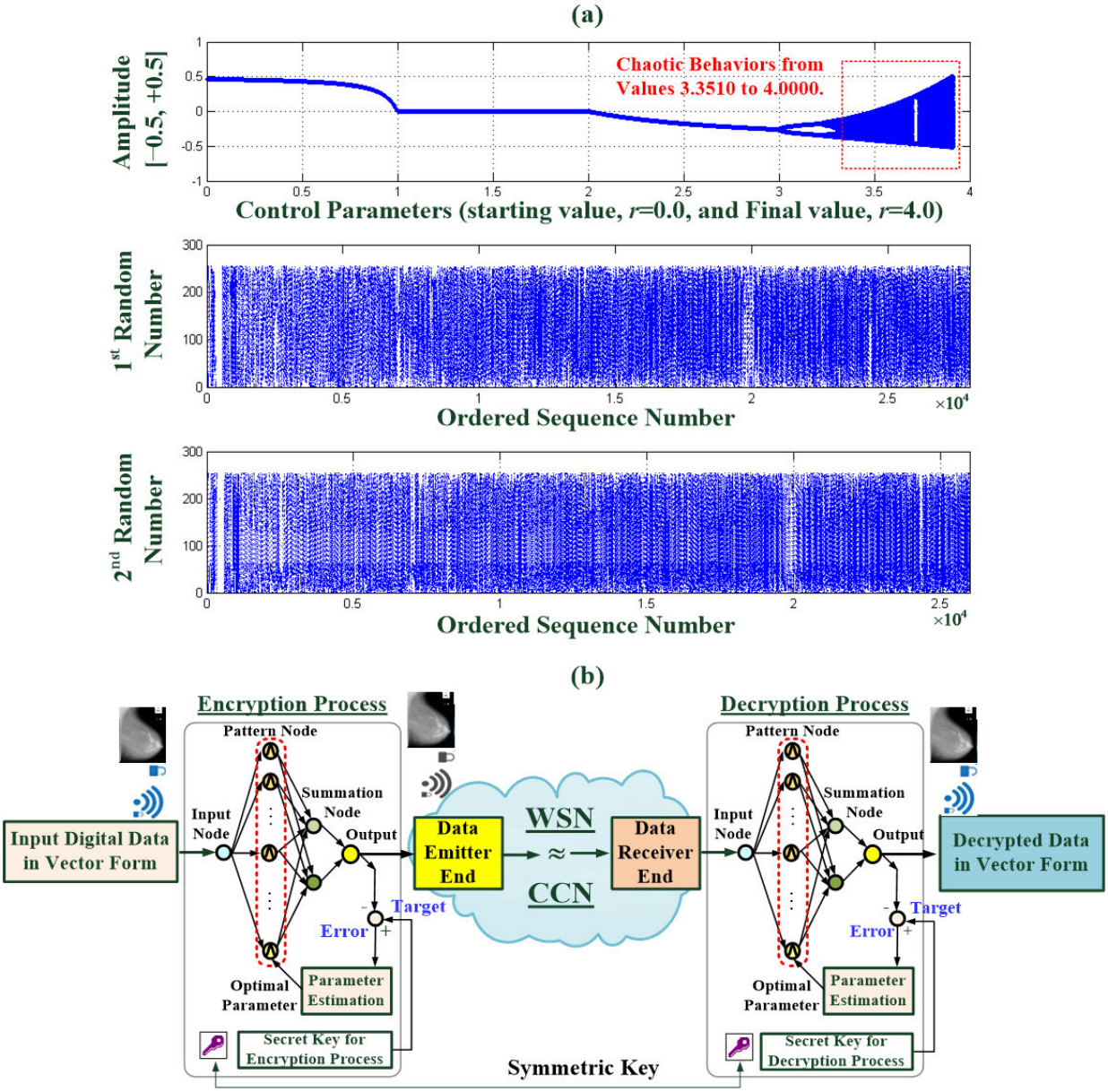

FIGURE 3. Random-number seeds and GRNN-based encryptor and decryptor. (a) Random-number seeds generated from the two-round key generator. (b) GRNN-based encryptor and decryptor.

where the network parameter is $\sigma = \sigma_1 = \sigma_2 = \ldots = \sigma_K$, which can be adjusted by optimization algorithms, such as gradient descent and particle swarm optimization (PSO) algorithms [20], [28], [29], [42], [50], [51]. In this study, the PSO is used to adjust the optimal network parameter, σ.

The GRNN-based model is superior to conventional backpropagation neural networks (BPNN), which does not require adjusting entire network parameters in the fully connected layer, and then reduce the higher computational load. Thus, before digital data are transmitted through communication networks, the newly generated symmetric keys can be set by authorized persons, and then they are fed to rapidly determine the connected weights of the encryptor and decryptor, respectively. The PSO algorithm can be employed to quickly refine the optimal parameter σ without extensively adjusting the network parameters, facilitating establishment of optimal cryptography scheme.

B. CLASSIFIER DESIGN FOR DIAGNOSIS APPLICATION

The DL-based models, including TTCNN (Transferable Texture Convolutional Neural Network), Grad-CAM Gradient-Weighted Class Activation Mapping) CNN, DNN (Deep Neural Network), FCN (Fully Convolutional Network), Attention Dense-Unet, and Dense-Unet [22], [23], [24], [25], [26], [27], [38], have been applied in digital image and signal classification) tasks. These models comprise multiple layers,

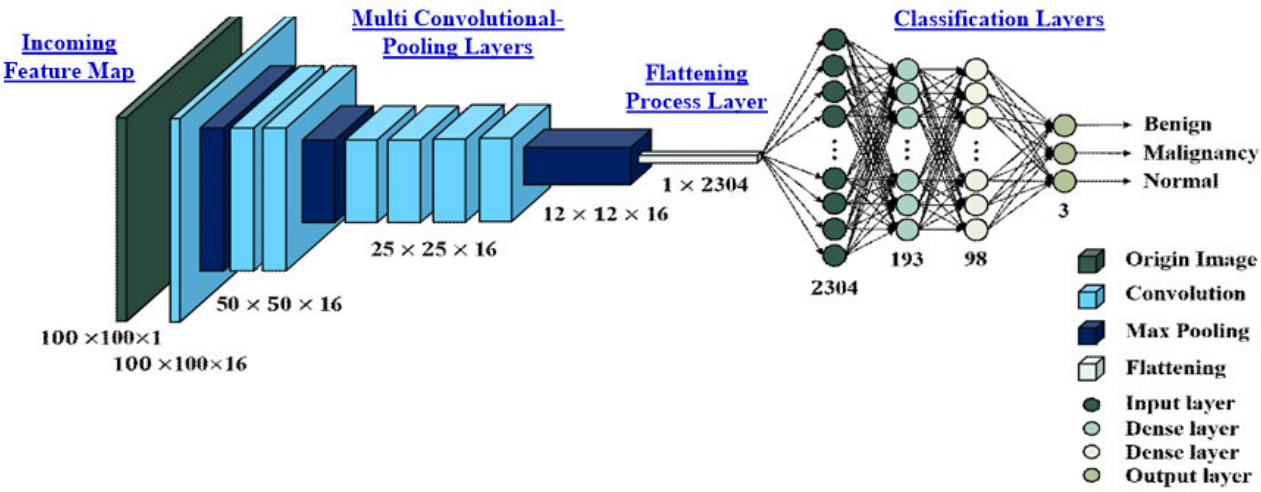

FIGURE 4. Architecture of cascaded CNN-based classifier, including multiple convolutional layers, multi pooling layers, a flattening layer, and a fully connected layer.

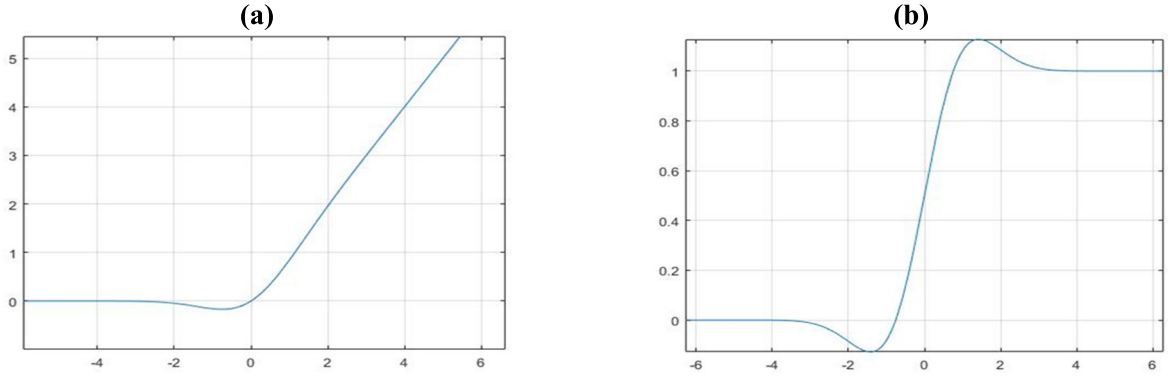

FIGURE 5. Activation functions. (a) ReLU activation function; (b) GeLU activation function.

such as convolutional layer, pooling layer, flattening layer, and classification layer (fully connected layer), as shown in Figure 4. This model can automatically extract and learn key-feature patterns from input signals or images. The classification layer performs classification, image segmentation, or regression prediction. The aforementioned CNN models have also been applied for medical images, such as mammography images in automatic breast cancer diagnosis and classification, breast density estimation, breast lesion segmentation, and rapid detection of breast lesions [22], [23], [24], [25], [26], [27], [38].

However, the number and type of convolutional layers and kernel convolutional windows (with different combinations of weights) may affect the depth of feature patterns, such as edges, textures, and shapes. In this study, the designed classifier has a cascaded CNN structure, as seen in Figure 4. A series of convolutional and pooling layers (convolutional–pooling layer) with sixteen 3×3 kernel windows and sixteen 2×2 Max-pooling windows are used for automatic feature extraction. The BPNN was then employed for mammography images classification, and its fully connected topology is 2,304 × 193 × 98 × 3, including an input layer (2,304 nodes), two dense layers (with 193 and 98 nodes individually), and an output layer (3 nodes) for mammography images classification as normal (Nor), benign (B), or malignant (M).

During training CNN-based classifier, the outputs of rectified linear unit (ReLU) activation functions (as seen in Figure 5(a)) in neurons may gradually decrease or become value 0, resulting in no longer be updated the network parameters. Hence, the Gaussian error linear unit (GeLU) activation function is used instead of ReLU, as seen in Figure 5(b). The GeLU function can prevent its gradient does not reach value 0, mitigating the problem of gradient vanishing [38], [52], [53], and also increasing the convergence speed and reducing the training time. The dense networks in the classification layer are typically arranged in ascending or descending powers of two or base on the number of input data and output classes. In this study, two dense networks are chosen with 193 and 98 neurons, respectively. A dropout layer is inserted in between them and set to 0.1; that is, 10% of the neurons are randomly deactivated to overcome the overfitting problem during training stage.

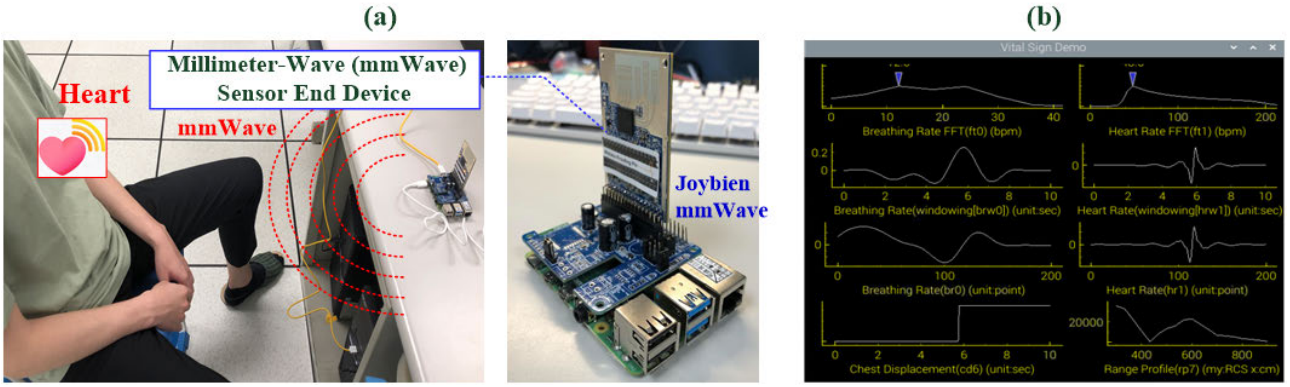

FIGURE 6. Doppler radar mm-Wave sensing firmware. (a) Short distance (<1.0 m) and contactless measurements, (b) Human machine interface for HR and RR data display.

A back-propagation algorithm is employed to adjust the connected weighted parameters and bias parameters. The loss function (LF), as categorical cross- entropy is used and can be represented as follows [38], [54], [55]:

$$L = \frac{-1}{N} \sum_{k=1}^{K} \sum_{m=1}^{M} y_{km} \log(p_{km}) \tag{12}$$

where K represents the number of training datasets: k =1, 2, 3, …, K; Mrepresents the number of classes: m =1, 2, 3, …, M; and y_{km} is the output of kth training dataset in mth class. The three classes (M =3) are coded in a binary value "0" or value "1", as follows: B [1, 0, 0], M [0, 1, 0], and Nor [1, 0, 0]. p_{km} is the predicted probability that kth training dataset is in class m; parameter $p_{km} \in [1, 0]$ and $p_{max} = \max(p_{km})$ is the maximum probability for identifying the possible class. The ADAM (Adaptive Moment Estimation) optimizer [38], [56], [57] is used to adjust the connected weighted parameters and bias parameters by iteration computations to minimize the LF until the LF value reaches the specific threshold value.

The TensorFlow Inception V3 platform (Keras, open-source software library, Google Brain Team, 2015) is used to design the ML and DL models in Python or Language C++ [21], [57], which is easy to use, modular, and extensible to design various models, such as multilayer perceptron, CNN, and recurrent neural network, hence, facilitating to design ML or DL models for applications in signals or images classification. In addition, the designed model can be performed with a graphics processing unit (GPU, NVIDIA GeForce RTX 2,080 Ti, 1,755 MHz, 11 GB GDDR6) to speed up the overall processes [57]. The breast lesion classification model is trained using a dataset comprised mammography images from the Mammographic Image Analysis Society (MIAS) database (United Kingdom National Breast Screening Program) [58]. An automatic breast lesion inference system is thus developed that can rapidly generate classifier models with improved execution efficiency.

C. CONTACTLESS PHYSIOLOGICAL SIGNAL SENSING

The Joybien mmWave (76-77 GHz: 14 db and 77-81 GHz: 15 dB), as seen in Figure 6, is a Doppler radar mm-Wave sensing firmware with FMCW control [59], including Radar mm-Wave Sensor, Raspberry Pi-Hat Board (ARM® Cortex®-R4F-Based Radio Control System), and Python software, which can be applied for VSD applications. This mm-Wave sensing firmware can perform contactless and short-range measurements (<1.0 m), and the subject does not need to wear any sensors, as seen in Figure 6(a). The sensing vital signs can be used to estimate HR and RR and determine whether human subjects are within a normal range, which is 48–120 (beats/min) for HR and 6–30 (breaths/min) for RR. Such sensors can be applied to enable the early detection of life-threatening conditions, such as respiratory difficulties, chronic obstructive pulmonary disease, and adult respiratory distress syndrome. For this contactless sensing method, the mm-Wave sensing firmware can be used for contactless continuous patients monitoring.

A digital filter can be applied to measured raw data to remove unwanted high- or low-frequency components. Then, the measured heartbeat and respiratory signals are transformed into the frequency spectrum by using the FFT (fast Fourier transform) method, which is used to estimate the HR and RR from the characteristic frequency (f_c) in the frequency-domain parameters, as follows: HR=60×f_{c1}(beats/min) and RR=60×f_{c2}(breaths/min), where f_{c1} and f_{c2} represent the characteristic frequencies of the heartbeat and respiratory signals, respectively. For example, if the characteristic frequency f_{c1} is 0.9 Hz, as seen in Figure 7(a), the HR can be estimated as approximately 54 beats/min; similarly, the characteristic frequency f_{c2} is 0.3 Hz, as shown in Figure 7(b), the RR can also be estimated as approximately 18 breaths/min. In adults, the normal range of resting HR is 60–70 beats/min, and the normal range of RR is 12–20 breaths/min. These estimated values may increase during subject activity. The measured signals can also be used to continuously monitor patients with chronic diseases, cardiovascular disorders, or special applications, such as

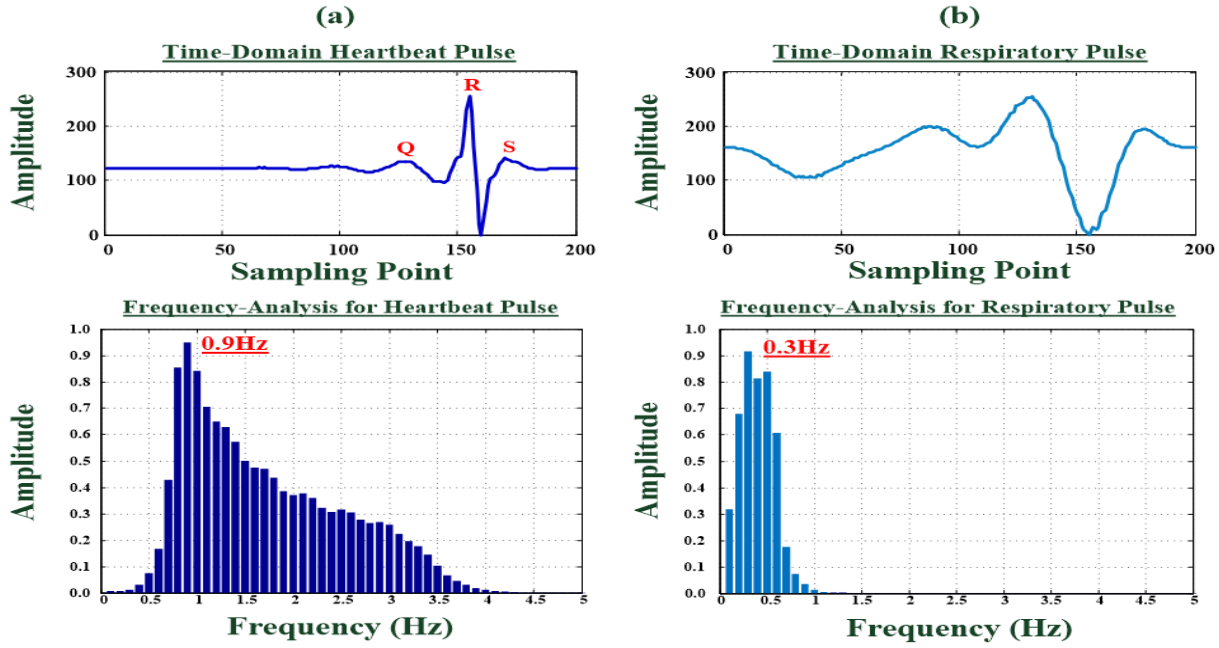

FIGURE 7. Characteristic frequencies of heartbeat and respiratory signals. (a) Heartbeat signals, (b) respiratory signals.

burns, COVID-19, and adult respiratory distress syndrome. In addition, the heartbeat and respiratory signals are required for ensuring the patients' privacy.

D. MAMMOGRAPHY IMAGE COLLECTION AND CLASSIFICATION

Currently, various mammography image databases are available for public use, including Suspicious Regions on Mammograms from Palermo Polyclinic, which is manually annotated by expert radiologists; Digital Database of Screening Mammography (DDSM) from hospitals and medical universities; Curated Breast Imaging Subset of DDSM as a modified and standardized version of DDSM, and MIAS image databases [22], [23], [24], [25], [26], [27], [38]. In this study, the MIAS database is selected for classifier training and testing. The biomarker has been made by expert radiologists, which includes the image size, image category, background tissue, class of abnormality, and severity of abnormality. The 4,320×2,600 pixels mammography images (vertical and horizontal resolutions of 600 dpi and depth of 24 bits) [58] were selected. The database has a total of 156 images of both left and right breasts from 78 female subjects. Among these images, 62 indicate breast-lesion images (either M or B classes), and 94 are nontumor images. For the proposed human–machine interface (HMI), biomarker information was used to bound the specific ROI, and screenshots of the feature patterns were obtained manually for the 156 images, yielding 422 tumor screenshots and 578 nontumor screenshots (a total of 1,000 images). These screenshots can be randomly selected for the training datasets at the learning stage; the remaining images comprise testing datasets at the recalling stage.

The K-fold cross-validation method was used to validate the classifier. In this study, the tenfold cross- validation was selected, and for each testing fold, the training datasets were divided into normal (Nor) and abnormal (M & B) feature patterns and randomly split into training and testing datasets with a 50: 50 ratio. Four evaluation metrics were used to evaluate the classifier performance, namely precision (%), recall (%), F1 score, and accuracy (%) [22], [23], [24], [25], [26], [27], [38].

E. PERFORMANCE EVALUATION

1) ENCRYPTION AND DECRYPTION PERFORMANCE EVALUATION

The encryption security level and decrypted image quality are evaluated by using three evaluation metrics: NPCR, UACI, and SSIM. An cryptography system is highly sensitive to subtle variations in the secret keys. The sensitivity can be quantitatively evaluated by NPCR and UACI with equations (13) and (14), respectively [28], [29], [60].

$$NPCR = \frac{\sum_{i=1,j=1}^{N,M} D(i,j)}{N \times M} \times 100\%,$$
$$D(i,j) = \begin{cases} 0, & if\ C_0(i,j) = C_1(i,j) \\ 1, & if\ C_0(i,j) \neq C_1(i,j), \end{cases} \quad (13)$$

$$UACI = \frac{\sum_{i=1,j=1}^{N,M} |C_0(i,j) - C_1(i,j)|}{N \times M} \times 100\% \quad (14)$$

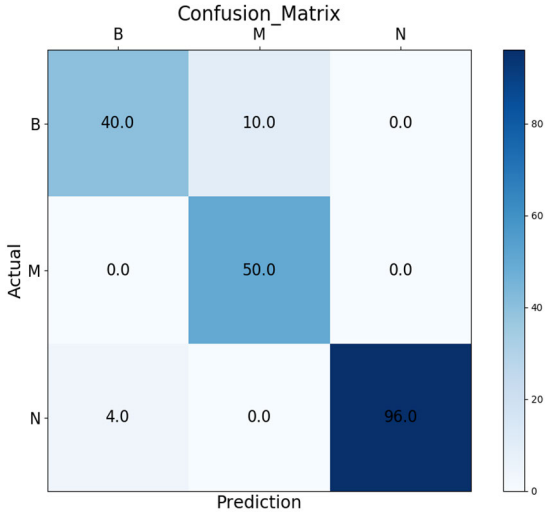

FIGURE 8. Confusion Matrix for the Nor, B, and M classes.

where $N \times M$ is the image size, C_0 is the plaintext; $C_0(i, j)$ is a plaintext value; C_1 is the cyphertext; and $C_1(i, j)$ is a corresponding cyphertext value. Higher NPCR and lower UACI indicate higher encryption performance and higher cyphertext sensitivity to key changes. The NPCR and UACI metrics can be used to evaluate the security level of the encryption process [60], and the SSIM indicates the image quality after decryption process. A higher SSIM indicates greater similarity between the plaintext and the decrypted data [28], [29]. An SSIM index>0.95 or near 1.00 indicates that minor difference occurred in the encryption and decryption processes.

2) CLASSIFIER PERFORMANCE EVALUATION

The confusion matrix for the classifier is presented in Figure 8. The confusion matrix is used to calculate precision (%), recall (%), F1 score, and accuracy (%) as follows [22], [23], [24], [25], [26], [27], [38]:

$$\bullet\ \text{Recall}(\%) = \left(\frac{TP}{TP + FN}\right) \times 100\%, \tag{15}$$

$$\bullet\ \text{Precision}(\%) = \left(\frac{TP}{TP + FP}\right) \times 100\%, \tag{16}$$

$$\bullet\ \text{Accuracy}(\%) = \left(\frac{TP + TN}{TP + FN + TN + FP}\right) \times 100\%, \tag{17}$$

$$\bullet\ \text{F1 Score} = \frac{2TP}{2TP + FP + FN}. \tag{18}$$

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed AI-assisted system was designed to ensure the information security level and facilitate in the rapid screening for breast lesions. Clinically, this system could help clinicians transmit physiological signals and medical images through communication networks while ensuring the confidentiality of patients' personal and medical information for further provided VSD and related medical purposes. After the encryption and decryption processes, for screening breast lesions, clinicians or radiologists could manually or automatically input mammography images containing tumors to the AI-assisted diagnosis system; this could help in the identification of potential breast lesions, thereby helping clinicians or radiologists rapidly classify images as normal or abnormal. The LabVIEW 2019 Software (NI^{TM}) was used to integrate the encryption, decryption, and classification algorithms, and an HMI was designed to display heartbeat signals, respiratory signals, HR, and RR, as shown in Figures 6(b). In addition, mammography images were obtained from the MIAS database, and the results of the encryption and decryption processes and image classification (Nor, B, or M) were displayed through the HMI, as shown in Figure 9. These testing procedures are described in detail as follows.

A. PHYSIOLOGICAL SIGNAL ENCRYPTION AND DECRYPTION TEST

A radar mm-Wave sensing firmware (Joybien mmWave) [59] was used for short-range and contactless VSD in a laboratory setting. The subject was a male-aged approximately 22 years old. The subject underwent at least 10 resting VSD tests; approximately 1 min of heartbeat and respiratory signals was recorded per test. Figure 10(a) and 10(d) present raw data of heartbeat and respiratory recordings, respectively, of approximately 10s in data length (plain signals). Encryption and decryption keys were generated using the proposed two-round key generator. Two GRNN-based models were used to train the encryptor and decryptor, respectively, and the plain signals, including heartbeat and respiratory signals, were fed into the encryptor, obtaining the cipher signals, as seen in Figures 10(b) and 10(e), respectively. The heartbeat signal encryption for NPCR and UACI evaluations were 99.50% and 33.42%, respectively; the corresponding values for respiratory signals were 94.20% and 30.85%, respectively. These values were close to the ideal values of NPCR= 99.59% and UACI=33.46% [60]. The decrypted signals as seen in Figures 10(c) and 10(f), were then obtained for heartbeat and respiratory signals, respectively. In addition, we evaluated the pixel value correlations between the decrypted and plain signals and between the cipher and plain signals, as shown through the correlation analysis in Figures 10(g) and 10(h), respectively.

As shown, the cipher and plain signals display low correlation, but the decrypted and plain signals had high correlation coefficients of 0.9943 and 0.9942 for the heartbeat and respiratory signals, respectively. After the decryption process, the R-R interval and HR could be estimated from the decrypted heartbeat signals in time domain, as seen in Figure 11(a), which closely resembled the plain signals. The average HR can be estimated from decrypted signal as 75.38 beats/min, and the R-R interval was approximately 0.796 seconds, as seen in Figure 11(b). For the 10 measurements, the average HR was 78.26±10.25 beats/min, and the average RR was 17.96 ± 4.56 breaths/min, as seen in Table 1

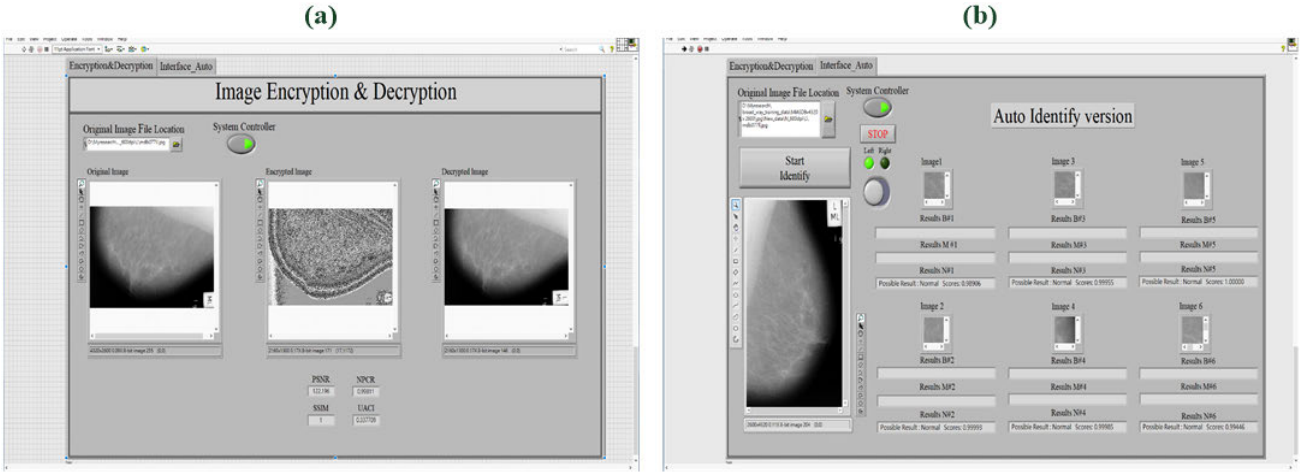

FIGURE 9. Human machine interface (HMI). (a) HMI for image encryption and decryption processes, (b) HMI for breast lesions screening.

TABLE 1. The average HR and average RR estimation for 10 static measurements of heartbeat and respiratory signals.

Measurement	1	2	3	4	5	6	7	8	9	10	Average
HR (beats/min)	102.42	80.61	96.09	50.61	64.73	96.83	79.41	84.85	69.91	67.50	79.29 ± 15.56
RR (breaths/min)	19.86	16.84	20.38	17.12	14.99	17.67	18.30	13.65	16.20	24.64	17.97 ± 2.95

B. MEDICAL IMAGE ENCRYPTION AND DECRYPTION TESTING AND ANALYSIS

In the medical-image encryption and decryption tests, mammography images were examined. Specifically, we randomly selected 100 Nor, 50 B-tumor, and 50 M-tumor images to test the proposed image encryptor and decryptor. To ensure patient's privacy, the NPCR and UACI were used to evaluate the security level of encrypted images and also to validate the encryption algorithms. As observed through the Nor, M-tumor, and B-tumor images in Figure 12(a), the correlation analysis was used to preliminarily evaluate the correlations between the pixel values of the decrypted and plain images and between the pixel values of the encrypted (cipher) and plain images. These are displayed as gray values on location $(x+1, y)$ versus gray values on location (x, y), as shown by the correlation analysis in Figures 12(b). Furthermore, Figure 12(c) shows the correlation analysis for the encrypted and decrypted images with the Riemann– Lebesgue-based key generator and ML-based intelligent encryption scheme [20]. The experimental results of the encrypted images indicated no significant correlation between the pixel values of the encrypted and plain images. In addition, the pixel values of the neighboring encrypted image showed lower correlation with the plain image's pixel values and a uniform distribution. Compared with the encryption algorithm in [20], the proposed method shows promising results for image encryption and decryption. The correlation coefficient (CC) between the encrypted image and plain image approached zero, as shown in Table 2. After decrypted the images, the pixel values of the neighboring decrypted image demonstrated extremely higher correlation with the pixel values of plain image. The distribution was linear, and the average CC was 0.9659, as shown in Table 2. The preliminary validation with the correlation analysis indicated that the proposed encryption algorithm possesses favorable ability to produce confused images for frequency counting attacks and statistical attacks.

As shown in Table 2, the encrypted images display NPCR and UACI values close to the ideal values. The average NPCR value (99.65%) was favorable in that it approached 100.00% (ideal value = 99.71%). Furthermore, the average UACI value (34.99%) is also close to the ideal value (33.40%) [60]. The proposed method demonstrated favorable performance for the encrypted Nor, B-tumor, and M-tumor images. The experimental results indicate that

C. AI-ASSISTED DIAGNOSIS CLASSIFIER TRAINING AND TESTING

This study designed a cascaded CNN architecture torealize AI-assisted diagnosis classifiers and its relevant design parameters were depicted in Figure 13. The CNN architecture consisted of convolutional layers, pooling layers, flattening process layers, and a fully connected network. Each convolutional layer contained 16 3×3 kernel windows for convolutional operations to enhance and extract the image features or objects. Each pooling layer had 16 2×2 Max-pooling windows for extracted the key feature parameters. The fully connected network in classification layer had an

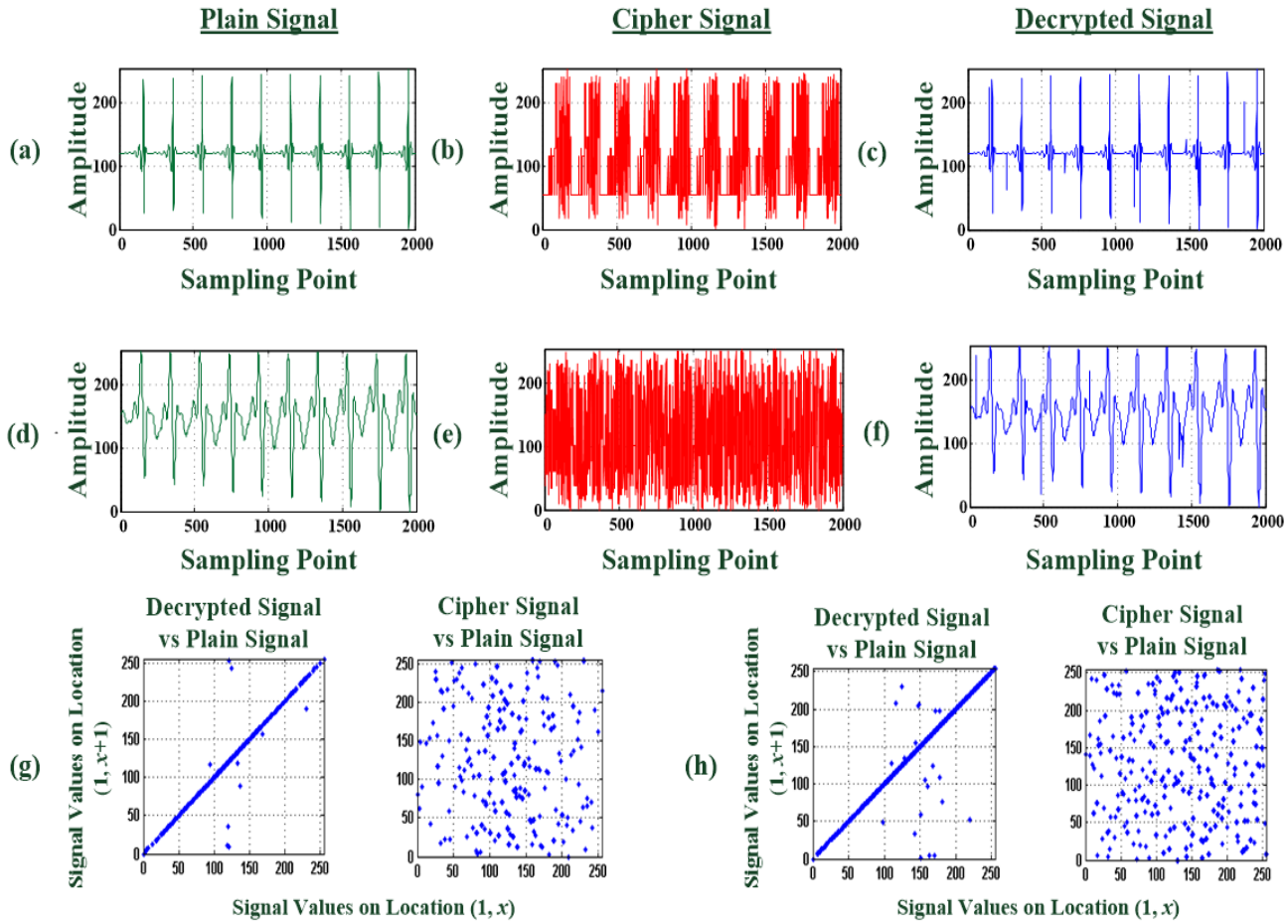

FIGURE 10. Plain signals, cipher signals, decrypted signals, and correlation analysis for heartbeat and respiratory signals. (a) and (d) Plain signals for heartbeat and respiratory signals, (b) and (e) Cipher signals for heartbeat and respiratory signals, (c) and (f) Decrypted signals for heartbeat and respiratory signals, (g) and (h) correlation analysis for decrypted signal versus plain signal and cipher signal versus plain signal.

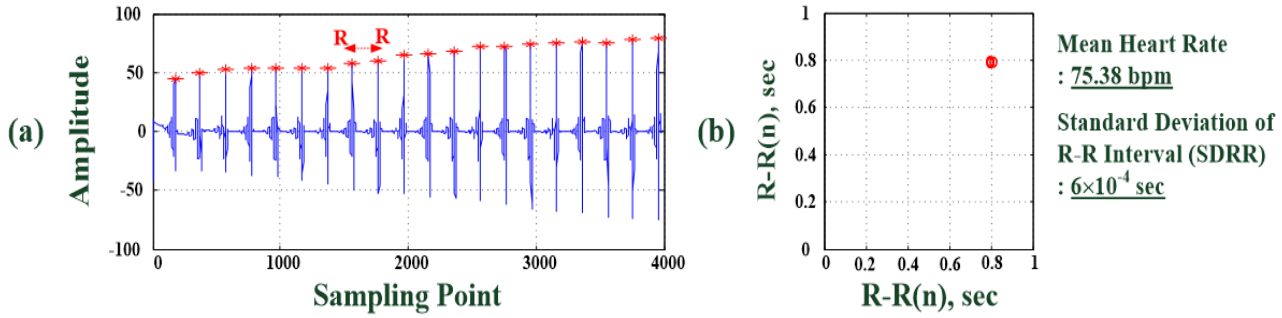

FIGURE 11. Raw data of heartbeat signals and heart rhythm analysis. (a) Heartbeat signals in time domain, (b) R-R interval heart rhythm analysis.

input layer, multiple hidden layers, and an output layer. The hidden layers involved GeLU activation functions (as seen in Figure 5(b)), and the output layer involved the softmax activation functions. A cross-entropy LF was employed to evaluate the classifier's training performances. The learning rate was set as 0.001, and the number of training iterations was set as 1,000 iteration numbers. An iteration computational method was employed to adjust the classifier's network parameters. Figure 14 showed the training history curves of 1,000 iteration computations for accuracy saturation History curves and convergence history curves, respectively. Followed the increases in the iteration numbers, the classifier's output accuracy gradually increased, and the LF value gradually decreases to the specific tolerance errors. In this study, an accuracy of 93% was obtained in the training stage after approximately 200 training iterations.

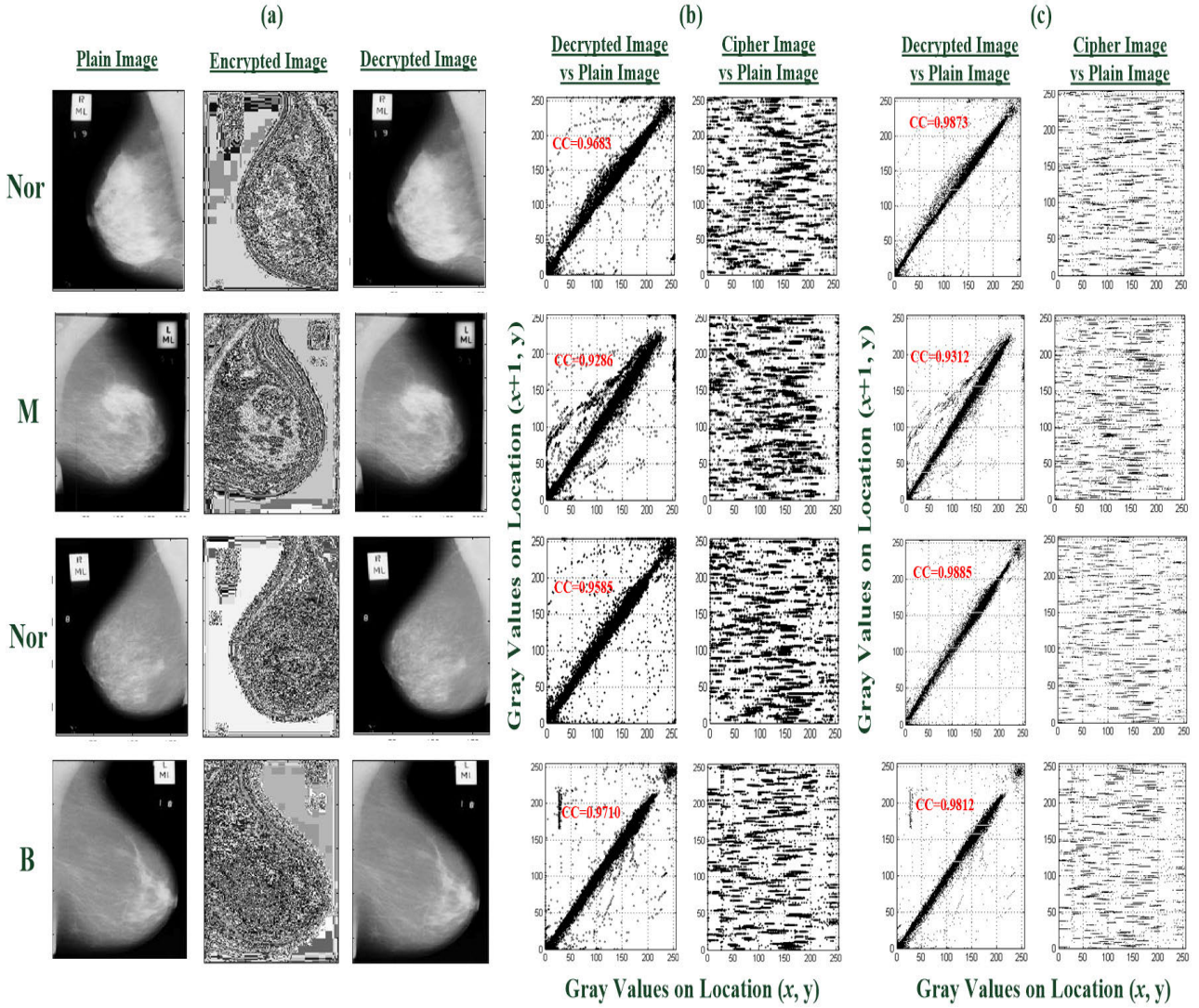

FIGURE 12. Correlation analysis for the encrypted and decrypted images for Nor, B-tumor, and M-tumor classes. (a) Nor, B-tumor, and M-tumor classes for plain images, encrypted images, and decrypted images. (b) Correlation analysis for encrypted and decrypted images by using the proposed method. (c) Correlation analysis for encrypted and decrypted images with the Riemann–Lebesgue-based key generator and ML-based intelligent encryption scheme.

TABLE 2. Experimental Results of the performance evaluation of the proposed encryptor and decryptor.

Image Class	Security Level (Differential) Evaluation			Decrypted Image Quality Evaluation		
	Average *CC*	Average *NPCR* (%)	Average *UACI* (%)	Average *CC*	Average *SSIM* (≥ 0.95)	Average *PSNR* (dB) (≥ 30 dB)
B (50)	0.0022	99.74	34.27	0.9810	1.00	122.22
M (50)	0.0023	99.69	35.58	0.9534	1.00	122.13
Nor (100)	0.0022	99.46	35.17	0.9686	1.00	122.07
Nor (100) + M (50)	0.0021	99.72	34.93	0.9634	1.00	122.18
Average	0.0022	99.65	34.99	0.9666	1.00	122.15

The convergence history curve revealed that the LF value converged toward 0.1413 as the number of iterations increased. A smaller LF value indicated more accurate predictions by the classifier training. The entire training process of the classifier took 237.36 s of CPU time. At each fold validation, the classifier was trained with random selected 200 training datasets and was tested with random selected 200 untrained datasets (untrained feature patterns), respectively. Figure 8 showed the classifier's output confusion matrix, for example, of the 50 B-tumor images,

TABLE 3. Evaluation metrics results of the proposed classifier on classifying the various classes (B, M, and Nor).

Index / Class	Accuracy (%)	Precision (%)	Recall (%)	Negative Predictive Value, NPV (%)	F1 Score (%)	Prevalence (%)
B (50)	93.00	90.00	95.74	96.00	92.78	47.00
M (50)						
Nor (100)						

Note: (1) $NPV = (\frac{TN}{TN+FN}) \times 100\%$; (2) $Prevalence = (\frac{TP+FN}{TP+FP+TN+FN}) \times 100\%$

TABLE 4. Results comparison of the different classifiers for breast lesion detection.

Model (Image) / Index	Average Accuracy (%)	Average LF Value	Average Precision (%)	Average Recall (%)
ResNet50 [61] (Mammography)	92.93	0.2864	89.83	79.98
VGG19 [62] (Mammography)	92.93	0.3680	85.60	65.86
MobileNet-V3 [63] (Breast Cancer Histology Images)	92.59	0.2662	93.08	65.44
Custom CNN [64] (Mammography)	93.62	0.2017	92.00	80.25
Proposed Model [38, 67] (Mammography)	93.00	0.1413	94.00	93.00

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 100, 100, 16)      160
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 50, 50, 16)        0
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 50, 50, 16)        2320
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 50, 50, 16)        2320
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 25, 25, 16)        0
_________________________________________________________________
conv2d_3 (Conv2D)            (None, 25, 25, 16)        2320
_________________________________________________________________
conv2d_4 (Conv2D)            (None, 25, 25, 16)        2320
_________________________________________________________________
conv2d_5 (Conv2D)            (None, 25, 25, 16)        2320
_________________________________________________________________
conv2d_6 (Conv2D)            (None, 25, 25, 16)        2320
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 12, 12, 16)        0
_________________________________________________________________
flatten (Flatten)            (None, 2304)              0
_________________________________________________________________
dense (Dense)                (None, 193)               444865
_________________________________________________________________
dense_1 (Dense)              (None, 98)                19012
_________________________________________________________________
dropout (Dropout)            (None, 98)                0
_________________________________________________________________
dense_2 (Dense)              (None, 3)                 297
=================================================================
Total params: 478,254
Trainable params: 478,254
Non-trainable params: 0
```

FIGURE 13. AI-assisted diagnosis classifier design.

40 were accurately classified as B class, whereas 10 were classified as M class, and all 50 M-tumor images were accurately classified, including TP=90 and FP=10. Of the 100 Nor images, 96 were accurately classified as Nor class (TN=96), and 4 were misclassified as B class (FN=4). The evaluation metrics for the classifier's performance in classifying the three classes were shown in Table 3.The F1 Score (%) for identifying B, M, and Nor images exceeded 90%, and both the precision (%) and recall (%) values were greater than 80%. The proposed classifier reached the accuracy of 95.74% in TP prediction (as the so-called positive predictive value) for identified the B and M classes. The negative predictive value (NPV) reached 96% for the TN prediction. The prevalence rate of the randomly selected testing datasets was 47.00%. Based on the validation results, the proposed classifier demonstrated promising results for breast lesions evaluation metrics.

DL-based classifiers have been widely applied in mammography and histology image classifications, such as ResNet50 (deep residual network with 50 layers) [61], VGG19 (CNN with 19 layers, Visual Geometry Group) [62], MobileNet-V3 [63], and Custom CNN [64]. In the case of medical purposes for automatic breast lesion detection, the four classifiers [61], [62], [63], [64] depicted in Table 4 could be used to realize various models based on the TensorFlow Inception V3 platform (Keras). For example, the architecture of ResNet50 had five convolutional layers (conv#1–conv#5) and an output layer. The convolutional layers from conv#1 to conv#5 involved 1, 9, 12, 18, and 9 layers of convolutional operations, respectively, in 3×3 convolutional kernel windows. The output layer consisted of pooling processing, a fully connected network, and softmax output. The models of ResNet family include ResNet-18, ResNet-34, ResNet-101, and ResNet-152, and these have been applied to computer-vision applications in image

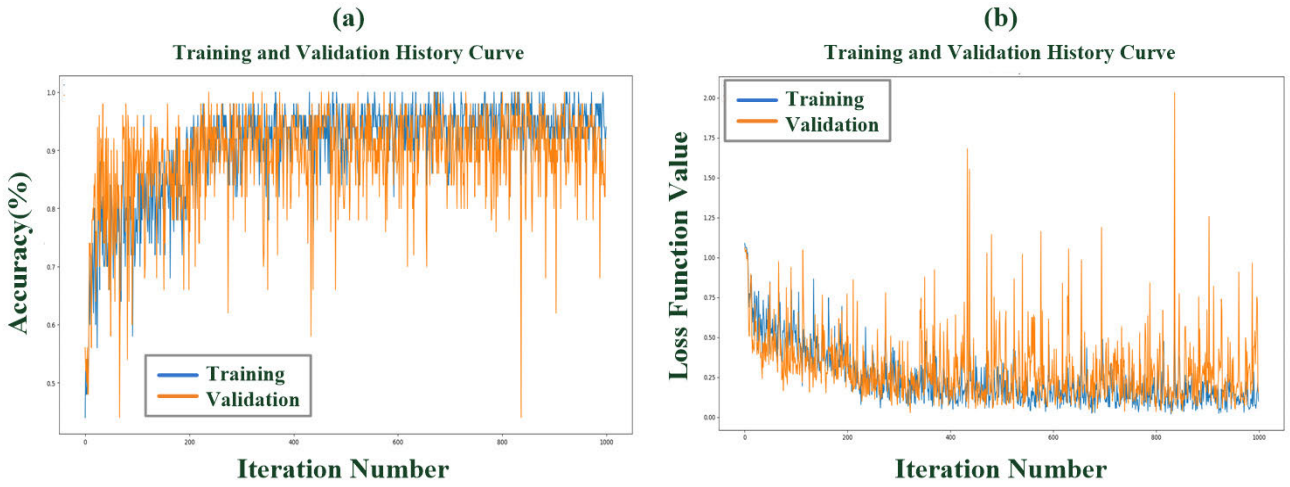

FIGURE 14. Training and validation history curves for CNN-based classifier training. (a) Accuracy versus iteration number, (b) Loss Function value versus iteration number.

classification, image segmentation, and object detection. Such models could overcome the vanishing gradient problem in training such deep neural networks by using the skip connections or residual blocks [54], [65], [66], [67]. Skip connections can create shortcut paths for an input to a weight layer is directly added to the output of a later weight layer, which allowed the classifier to directly learn the residuals or the differences between the desired and current outputs. A residual block comprises identity and residual paths, allowing the block to learn residuals (differences) between the input and desired output. This causes a reduction in computation complexities and the required number of parameters for the classifier model. However, the classifier model's training processes and inference speeds were the major drawback. In addition, a degradation problem was observed with increasing number of layers that resulted in higher training errors throughout the training procedure (average LF value in Table 4; LF = 0.2864 is greater than proposed model's value of 0.1413). Therefore, for the same datasets (MIAS database [58]), LF (as Equation (12)), and maximum iteration number, with the 10-fold cross-validation, at each fold validation, 100 Nor, 50 B-tumor, and 50 M-tumor images were randomly selected to train and test the classifier. For the ResNet50- based classifier, the experimental results for average accuracy (92.93%), average precision (89.93%), and average recall (79.98%) were obtained for the three identified classes, as seen in Table 4 [38], [61], [62], [63], [64], [67].

In practical applications, ResNet models comprise $\geq$ 20 layers to establish a classifier, degrading the learning performance. Hence, VGG19 and VGG16 models were subsequently developed for image classification. VGG19 comprises 16 convolutional layers and 3 fully connected networks, and VGG16 comprises 13 convolutional layers and 3 fully connected networks [62]. These models are simpler than ResNet model. Each layer of VGG model uses 3×3 convolutional kernel windows and 2×2 Max-pooling windows for the convolutional–pooling operations. However, these models require relatively large number of parameters and computational resources. For the same datasets, LF, and maximum iteration number, VGG19 model displayed 92.93% average accuracy, 85.60% average precision, and 65.86% average recall for breast-lesion detection; and the experimental results of MobileNet-V3 and Custom CNN were also shown in Table 4 [67].

This study proposed a small-scale multilayer training model (network architecture in Figure 4), which extracts feature patterns with three convolutional–pooling layers (Figure 13). The training model effectively reduced the dimensionality of the feature patterns (from 100×100 to 25 × 25) and reduced the training load of the classifier task in the classification layer to overcome the overfitting problem using an excessive number of training datasets in the learning stage. The entire learning stage utilized approximately 240 s of CPU time to complete the training and 10-fold cross-validation processes. The experimental results of the proposed classifier show that the model achieved an average accuracy of 93.00%, average precision of 94.00%, and average recall of 93.00%, as seen in Table 4. The recall index (detection rate of TP) and precision index (accuracy of TP prediction) for the detection samples were both higher than 80%. Compared with conventional classifiers [61], [62], [63], [64], the proposed classifier demonstrated comparable and promising results and also favorable detection performance for our intended medical purpose.

IV. CONCLUSION

The 5G communication technology has gradually been applied to the IoMTS for healthcare services, including remote physiological monitoring, telehealth carts, surgical navigation systems, and medical robots. Various wearable devices can be used to sense the patients' physiological

signals and transmit these measurement data to the medical institutions for real-time monitoring and healthcare applications. In this framework, PACS can manage the medical-image/signal storage, process, and transmission, including vital-signs data, X-ray images, CT images, MRI images, and mammography images. These medical data allow for medical-image interpretation and consultation from clinicians and various specialties through the communication system. When these digital data was transmitted over the public communications channel, data confidentiality and integrity should be provided to ensure that unauthorized persons cannot access these data. To address these solutions, in the IoMTS, this study established a system that combined the information security and AI-assisted diagnosis for the encryption, decryption, and detection functions for the bio-signals and medical images. In bio-signals measurement, the short- range and contactless radar mm-Wave sensing firmware was used to detect the heartbeat and respiratory pulsation signals. Then, the biosignals were encrypted before they were transmitted through a wireless communication network; at the data receiving end, the encrypted data were decrypted to estimate the HR and RR by time- domain or frequency-domain analysis

The experimental results indicated that the encrypted heartbeat signals had average security levels of NPCR=99.50% and UACI=33.42%. In addition, the decrypted respiratory pulsation signals showed average security levels of NPCR = 94.20% and UACI= 30.85%. Hence, the decrypted bio-signals were used to estimate the vital signs through frequency-domain analysis, as an average HR of 72.370±0.022 beats/min and an average RR of 17.96± 2.95 breaths/min. The proposed decryption algorithm was validated to be able to yield promising quality of decrypted signals for VSD application. Regarding medical image application, this study used mammography images for encryption and decryption tests. The image encryption process achieved average NPCR=99.65% and average UACI=34.99%. Thus, the values of both evaluation metrics were extremely close to the ideal values for favorable encryption performance in Nor, B-tumor, and M-tumor images. For decrypted images, the proposed classifier showed an average accuracy of 93.00%, average precision of 94.00%, and average recall of 93.00% for three-class classification. Therefore, the proposed secret-key generator, encryptor, decryptor, and image classifier could be integrated into the IoMTS for infosecurity and diagnosis applications. In addition, their application can be extended to X-ray, CT, and MRI images. In addition, to enhance the encryption and decryption performance, a PMs and SMs combination was used for biosignal and image encryption to increase the security level. The proposed methods offer the following advantages:

- Radar mm-Wave sensing devices displayed continuous monitoring functions for contactless, short range, and high sensing sensitivity measurement capability,
- the chaotic map and quantum-based keys could generate randomly unordered and unrepeated sequence seeds for further selecting 256-bit length of secret keys for setting encryption and decryption keys
- proposed encryptor and decryptor were applicable for encryption–decryption processes for biosignals and medical images,
- the design of a small-scale cascaded CNN architecture could effectively reduce the multilayer architecture and requirements of network parameters to expedite classifier training and reduce the detection time,
- the proposed encryption, decryption, and automated diagnosis algorithms could easily be integrated into IoMTS to enhance its security level and improve its diagnosis functions.

INSTITUTIONAL REVIEW BOARD STATEMENT

The enrolled data was also approved by the hospital research ethics committee and the Institutional Review Board (IRB), under protocol number: **SRD-110044**, and contract number:**SCMH_ IRB No: 1101206**, January 04, 2022 – January 03, 2023, Show Chwan Memorial Hospital, Changhua, Taiwan.

ABBREVIATIONS

IoMTS	Internet of Medical Thing System.
PACS	Picture Archiving Communication System.
5G	5th Generation.
CNN	Convolutional Neural Network.
mm-Wave	Millimeter-Wave.
FMCW	Frequency Modulated Continuous Wave.
Nor	Normal (Nor).
B	Benign.
M	Malignancy.
VSD	Vital Signs Detection.
DICOM	Digital Imaging and Communications in Medicine.
CT	Computed Tomography.
MRI	Magnetic Resonance Imaging.
JPEG	Joint Photographic Experts Group.
FDA	Food and Drug Administration.
RSA	Rivest-Shamir-Adleman.
DES	Data Encryption Standard.
AES	Advanced Encryption Standard.
ML	Machine Learning.
DL	Deep Learning.
HR	Heart Rate.
RR	Respiratory Rate.
PPG	Photoplethysmography.
GRNN	General Regression Neural Network.
ROI	Region of Interest.
NPCR	Number of Pixel Change Rate.
UACI	Unified Averaged Changed Intensity.
SSIM	Structural Similarity Index Measurement.
PSNR	Peak Signal-to-Noise Ratio.
PM	Permutation Method.
SM	Substitution Method.

SPCM	Sine-Power Chaotic Map.
BPNN	Back-propagation Neural Network.
SVM	Support Vector Machines.
PSO	Particle Swarm Optimization.
GPU	Graphics Processing Unit.
TTCNN	Transferable Texture Convolutional Neural Network.
Grad-CAM	Gradient-Weighted Class Activation Mapping.
DNN	Deep Neural Network.
FCN	Fully Convolutional Network.
ReLU	Rectified Linear Unit.
GeLU	Gaussian Error Linear Unit.
LF	Loss Function.
ADAM	Adaptive Moment Estimation.
MIAS	Mammographic Image Analysis Society.
DDSM	Digital Database of Screening Mammography.
FFT	Fast Fourier Transform.
HMI	Human Machine Interface.
CC	Correlation Coefficient.
NPV	Negative Predictive Value.
VGG	Visual Geometry Group.
TP	True Positive.
FP	False Positive.
TN	True Negative.
FN	False Negative.

REFERENCES

[1] J. Srivastava, S. Routray, S. Ahmad, and M. M. Waris, "Internet of Medical Things (IoMT)-based smart healthcare system: Trends and progress," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–17, Jul. 2022.

[2] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *J. Oral Biol. Craniofacial Res.*, vol. 12, no. 2, pp. 302–318, Mar. 2022.

[3] 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 Biomed. Eng. Int. Conf.*, Nov. 2014, pp. 1–5.

[4] Y.-W. Ma, J.-L. Chen, and W.-K. Shih, "The survey for next generation mobile networks framework applied to intelligent Internet of Medical," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2021, pp. 267–270.

[5] M. M. Kamal, S. Yang, S. H. Kiani, M. R. Anjum, M. Alibakhshikenari, Z. A. Arain, A. A. Jamali, A. Lalbakhsh, and E. Limiti, "Donut-shaped mmWave printed antenna array for 5G technology," *Electronics*, vol. 10, no. 12, p. 1415, Jun. 2021.

[6] *The Working Group for WLAN Standards, Wireless Local Area Networks*, Standard IEEE 802.11TM, 2023. [Online]. Available: https://www.ieee802.org/11/

[7] H. S. Yang, Y. Hou, L. V. Vasovic, P. A. D. Steel, A. Chadburn, S. E. Racine-Brzostek, P. Velu, M. M. Cushing, M. Loda, R. Kaushal, Z. Zhao, and F. Wang, "Routine laboratory blood tests predict SARS-CoV-2 infection using machine learning," *Clin. Chem.*, vol. 66, no. 11, pp. 1396–1404, Nov. 2020.

[8] A. S. Adly, A. S. Adly, and M. S. Adly, "Approaches based on artificial intelligence and the Internet of Intelligent Things to prevent the spread of COVID-19: Scoping review," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, Art. no. e19104.

[9] C.-W. Park et al., "Artificial intelligence in health care: Current applications and issues," *J. Korean Med. Sci.*, vol. 35, no. 42, p. e379, 2020.

[10] S. A. Allison, C. F. Sweet, D. P. Beall, T. E. Lewis, and T. Monroe, "Department of defense picture archiving and communication system acceptance testing: Results and identification of problem components," *J. Digit. Imag.*, vol. 18, no. 3, pp. 203–208, Sep. 2005.

[11] N. H. Strickland, "Current topic: PACS (picture archiving and communication systems): Filmless radiology," *Arch. Disease Childhood*, vol. 83, no. 1, pp. 82–86, Jul. 2000.

[12] (2023). *Since 2018, Ransomware Attacks on Healthcare Organizations Have Cost the World Economy $92BN in Downtime Alone*. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/worldwide-healthcare-ransomware-attacks/

[13] US Food and Drug Administration. (2023). *Cybersecurity*. [Online]. Available: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[14] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," *Artif. Intell. Healthcare*, vol. 2020, pp. 295–336, Jan. 2020.

[15] C.-H. Lin, G.-H. Hu, C.-Y. Chan, and J.-J. Yan, "Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm," *Appl. Sci.*, vol. 11, no. 3, p. 1329, Feb. 2021.

[16] P. Malathi and Devi. S. Suganthi, "Secure data sharing of personal health records in cloud using advanced encryption standard," in *Proc. Int. Conf. Adv. Comput., Commun. Appl. Informat. (ACCAI)*, Chennai, India, Jan. 2022, pp. 1–6.

[17] M. Mahendra and P. S. Prabha, "Classification of security levels to enhance the data sharing transmissions using blowfish algorithm in comparison with data encryption standard," in *Proc. Int. Conf. Sustain. Comput. Data Commun. Syst. (ICSCDS)*, Erode, India, Apr. 2022, pp. 1154–1160.

[18] S. Mukherjee, A. Bose, A. N. Das, J. K. Chandra, and D. Ghosh, "A novel technique to compress photoplethysmogram signal: Improvised with particle swarm optimization and Rivest–Shamir–Adleman algorithm," in *Proc. IEEE Calcutta Conf. (CALCON)*, Kolkata, India, Dec. 2022, pp. 139–144.

[19] Y. V. Lakshmi, K. Naveena, M. Ramya, N. Pravallika, and T. Sindhu, "Medical image encryption using enhanced Rivest Shamir Adleman algorithm," in *Proc. 3rd Int. Conf. Artif. Intell. Smart Energy (ICAIS)*, Coimbatore, India, Feb. 2023, pp. 1–5.

[20] C.-H. Lin, H.-Y. Lai, P.-T. Huang, P.-Y. Chen, N.-S. Pai, and F.-Z. Zhang, "Combining Riemann–Lebesgue based key generator and machine learning based intelligent encryption scheme for IoMT images infosecurity," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 1344–1360, 2024.

[21] M. Abadi et al., "TensorFlow: Large-scale machine learning on heterogeneous distributed systems," 2016, *arXiv:1603.04467*.

[22] S. Maqsood, R. Damasevicius, and R. Maskeliunas, "TTCNN: A breast cancer detection and classification towards computer-aided diagnosis using digital mammography in early stages," *Appl. Sci.*, vol. 12, no. 7, p. 3273, Mar. 2022.

[23] Y. J. Suh, J. Jung, and B.-J. Cho, "Automated breast cancer detection in digital mammograms of various densities via deep learning," *J. Personalized Med.*, vol. 10, no. 4, p. 211, Nov. 2020.

[24] J. Lee and R. M. Nishikawa, "Automated mammographic breast density estimation using a fully convolutional network," *Med. Phys.*, vol. 45, no. 3, pp. 1178–1190, Mar. 2018.

[25] M. AlGhamdi, M. Abdel-Mottaleb, and F. Collado-Mesa, "DU-Net: Convolutional network for the detection of arterial calcifications in mammograms," *IEEE Trans. Med. Imag.*, vol. 39, no. 10, pp. 3240–3249, Oct. 2020.

[26] K.-J. Tsai, M.-C. Chou, H.-M. Li, S.-T. Liu, J.-H. Hsu, W.-C. Yeh, C.-M. Hung, C.-Y. Yeh, and S.-H. Hwang, "A high-performance deep neural network model for BI-RADS classification of screening mammography," *Sensors*, vol. 22, pp. 1–15, Feb. 2022.

[27] S. Boumaraf, X. Liu, C. Ferkous, and X. Ma, "A new computer-aided diagnosis system with modified genetic feature selection for BI-RADS classification of breast masses in mammograms," *BioMed Res. Int.*, vol. 2020, pp. 1–17, May 2020.

[28] C.-H. Lin, J.-X. Wu, P.-Y. Chen, H.-Y. Lai, C.-M. Li, C.-L. Kuo, and N.-S. Pai, "Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity," *IEEE Access*, vol. 9, pp. 118624–118639, 2021.

[29] C. Lin, J. Wu, N. Pai, P. Chen, C. Li, and C. C. Pai, "Intelligent physiological signal infosecurity: Case study in photoplethysmography (PPG) signal," *IET Signal Process.*, vol. 16, no. 3, pp. 267–280, May 2022.

[30] A. Alanezi, B. Abd-El-Atty, H. Kolivand, A. A. A. El-Latif, B. Abd El-Rahiem, S. Sankar, and H. S. Khalifa, "Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment," *Secur. Commun. Netw.*, vol. 2021, pp. 1–17, Feb. 2021.
[31] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, p. 535, Jul. 2018.
[32] X. Kang, X. Luo, X. Zhang, and J. Jiang, "Homogenized chebyshev-arnold map and its application to color image encryption," *IEEE Access*, vol. 7, pp. 114459–114471, 2019.
[33] J. Tang, Z. Zhang, P. Chen, F. Zhang, H. Ni, and Z. Huang, "An image layered scrambling encryption algorithm based on a novel discrete chaotic map," *IET Image Process.*, vol. 17, no. 2, pp. 518–532, Feb. 2023.
[34] D. Vignesh, N. A. A. Fataf, and S. Banerjee, "A novel fractional sine chaotic map and its application to image encryption and watermarking," *Appl. Sci.*, vol. 13, no. 11, p. 6556, May 2023.
[35] D. Sych and G. Leuchs, "A complete basis of generalized Bell state," *New J. Phys.*, vol. 11, Jan. 2009, Art. no. 013006.
[36] S. L. Braunstein, A. Mann, and M. Revzen, "Maximal violation of bell inequalities for mixed states," *Phys. Rev. Lett.*, vol. 68, no. 22, pp. 3259–3261, Jun. 1992.
[37] V. Vedral, *Introduction to Quantum Information Science*. Oxford, U.K.: Oxford Univ. Press, 2006.
[38] F.-Z. Zhang, C.-H. Lin, P.-Y. Chen, N.-S. Pai, C.-M. Su, C.-C. Pai, and H.-W. Ho, "Number of convolution layers and convolution kernel determination and validation for multilayer convolutional neural network: Case study in breast lesion screening of mammographic images," *Processes*, vol. 10, no. 9, p. 1867, Sep. 2022.
[39] (2023). *An Introduction to Computer Security: The NIST Handbook*. [Online]. Available: https://www.nist.gov/publications/introduction-computer-security-nist-handbook
[40] 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, pp. 1–13, Jan. 2014.
[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] C.-H. Lin, J.-X. Wu, P.-Y. Chen, C.-M. Li, N.-S. Pai, and C.-L. Kuo, "Symmetric cryptography with a chaotic map and a multilayer machine learning network for physiological signal infosecurity: Case study in electrocardiogram," *IEEE Access*, vol. 9, pp. 26451–26467, 2021.
[43] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "DeepEDN: A deep-learning-based image encryption and decryption network for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, Feb. 2021.
[44] C.-H. Lin, C.-H. Wen, H.-Y. Lai, P.-T. Huang, P.-Y. Chen, C.-M. Li, and N.-S. Pai, "Multilayer convolutional processing network based cryptography mechanism for digital images infosecurity," *Processes*, vol. 11, no. 5, p. 1476, May 2023.
[45] N. K. Pareek, V. Partidar, and K. K. Sud, "Diffusion-substitution based gray image encryption scheme," *Digit. Signal Process.*, vol. 23, pp. 894–901, May 2013.
[46] 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.
[47] 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.
[48] V. Braginski, F. Khalili, and K. Thorne, *Quantum Measurements*. Cambridge, U.K.: Cambridge Univ. Press, 1992.
[49] S. Cho, G. Chen, and J. P. Coon, "Zero-forcing beamforming for active and passive eavesdropper mitigation in visible light communication systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1495–1505, 2021.
[50] T. 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.
[51] 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.
[52] D.-A. Clevert, T. Unterthiner, and S. Hochreite, "Fast and accurate deep network learning by exponential linear units (ELUs)," in *Proc. 4th Int. Conf. Learn. Represent.*, San Juan, Puerto Rico, 2016, pp. 1–14.
[53] D. Hendrycks and K. Gimpel, "Gaussian error linear units (GELUs)," 2016, *arXiv:1606.08415*.
[54] P.-T. de Boer, D. P. Kroese, S. Mannor, and R. Y. Rubinstein, "A tutorial on the cross-entropy method," *Ann. Oper. Res.*, vol. 134, no. 1, pp. 19–67, Feb. 2005.
[55] Y. Ho and S. Wookey, "The real-world-weight cross-entropy loss function: Modeling the costs of mislabeling," *IEEE Access*, vol. 8, pp. 4806–4813, 2020.
[56] J. Ma and D. Yarats, "Quasi-hyperbolic momentum and Adam for deep learning," in *Proc. ICLR*, 2019, pp. 1–38.
[57] J. Bergstra, O. Breuleux, F. Bastien, P. Lamblin, R. Pascanu, G. Desjardins, J. Turian, D. Warde-Farley, and Y. Bengio, "Theano: A CPU and GPU math compiler in Python," in *Proc. Python Sci. Conf.*, 2010, pp. 1–7.
[58] (2019). *Mammographic Image Analysis Society (MIAS) Database V1.21*. [Online]. Available: https://www.repository.cam.ac.uk/handle/1810/250394
[59] (2023). *Joybien Technologies*. Joybien mmWave. [Online]. Available: https://computer-consultant-1700.business.site/andhttp://www.joybien.com/
[60] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Sel. Areas Telecommun. (JSAT)*, vol. 1, pp. 31–38, Apr. 2012.
[61] W. Islam, M. Jones, R. Faiz, N. Sadeghipour, Y. Qiu, and B. Zheng, "Improving performance of breast lesion classification using a ResNet50 model optimized with a novel attention mechanism," *Tomography*, vol. 8, no. 5, pp. 2411–2425, Sep. 2022.
[62] K. Rautela, D. Kumar, and V. Kumar, "Detection and localization of breast lesion with VGG19 optimized vision transformer," in *Proc. 4th Int. Conf. Artif. Intell. Speech Technol. (AIST)*, Delhi, India, Dec. 2022, pp. 1–4.
[63] J. Huang, L. Mei, M. Long, Y. Liu, W. Sun, X. Li, H. Shen, F. Zhou, X. Ruan, D. Wang, S. Wang, T. Hu, and C. Lei, "BM-net: CNN-based mobilenet-V3 and bilinear structure for breast cancer detection in whole slide images," *Bioengineering*, vol. 9, no. 6, p. 261, Jun. 2022.
[64] R. M. Al-Tam, A. M. Al-Hejri, S. M. Narangale, N. A. Samee, N. F. Mahmoud, M. A. Al-masni, and M. A. Al-antari, "A hybrid workflow of residual convolutional transformer encoder for breast cancer classification using digital X-ray mammograms," *Biomedicines*, vol. 10, no. 11, p. 2971, Nov. 2022.
[65] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Las Vegas, NV, USA, Jun. 2016, pp. 770–778.
[66] M. Shafiq and Z. Gu, "Deep residual learning for image recognition: A survey," *Appl. Sci.*, vol. 12, no. 18, p. 8972, Sep. 2022.
[67] F.-Z. Zhang, "Study on information security and breast lesion screening in an Internet of Medical Thing system: Using mammography as an example," M.S. thesis, Dept. Elect. Eng., Nat. Chin-Yi Univ. Technol., Taichung City, Taiwan, Jul. 2021.

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, where she has been the Chief of the Department of Electrical Engineering, since 2019. Her current research interests include neural network computing and its applications, fuzzy systems, advanced control systems, biosignal and medical image processing and classification, and deep learning/artificial intelligence applications.

YU-CHENG CHENG received the B.S. degree from the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan, in 2022, where is currently pursuing the M.S. degree.

His research interests include SLAM, embedded system application, deep learning, and image processing and classification.

ZI-HENG ZHONG was born in October 2000. He received the B.S. degree in electrical engineering from the National Chin-Yi University of Technology, Taichung City, Taiwan, in June 2023. He is currently pursuing the M.S. degree with the Institute of Artificial Intelligence Cross-Disciplinary Tech, National Taiwan University of Science and Technology.

His research interests include embedded system applications, digital signal and image processing and classification, and deep reinforcement learning/artificial intelligence applications.

FENG-ZHOU ZHANG received the B.S. and M.S. degrees in electrical engineering from the National Chin-Yi University of Technology, Taichung City, Taiwan, in 2021 and 2023, respectively.

His research interests include medical image processing and classification, infosecurity applications, and deep learning/artificial intelligence applications.

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

He is currently a Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung. He was the Chairman of the Department, from 2004 to 2007, and also the Chairman of the Computer Center, 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.

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

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

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 was a Professor with the Department of Electrical Engineering, Kao-Yuan University, Kaohsiung City, from 2004 to 2017. Currently, he is a Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan, where he has been, since 2018. His research interests include neural network computing and its applications in biomedical engineering, smart grid, and infosecurity applications, biomedical signal and image processing, healthcare, hemodynamic analysis, and pattern recognition.