IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 20, 2021, accepted August 21, 2021, date of publication August 24, 2021, date of current version September 1, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3107608*

# Intelligent Symmetric Cryptography With Chaotic Map and Quantum Based Key Generator for Medical Images Infosecurity

**CHIA-HUNG LIN[1], JIAN-XING WU[1], PI-YUN CHEN[1], HSIANG-YUEH LAI[1], CHIEN-MING LI[2], CHAO-LIN KUO[3], AND NENG-SHENG PAI[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
[3]Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung 80543, Taiwan

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

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

**ABSTRACT** Medical images can be constructed in two-dimensional (2D) or three-dimensional (3D) view imaging to be applied in disease detection and diagnosis inside the body, such as cancer/tumor, heart, or lung-related diseases. These images may contain patients' privacy information and clinical diagnosis records. Hence, these images need to ensure authorization demands among hospitals, medical service organizations, or physicians in a picture archiving and communication system. This study presents an intelligent symmetric cryptography with a chaotic map and quantum-based key generator (KG) for medical image encryption and decryption. Overall scheme processes include (1) random cipher code generation, (2) training gray relational analysis (GRA)-based encryptor and decryptor, and (3) decrypted image evaluation. The hybrid chaotic map and quantum-based KG are used to increase the chaotic complexity and unpredictable levels to produce cipher codes for changing pixel values (substitution method) in a 2D image by 256 key-space cipher codes. The first and second GRA models are used to train the cipher codes to achieve an encryptor and a decryptor, respectively. Through the methodology validation using a chest X-ray database, the structural similarity index measurement is employed to evaluate the decryption quality between the plain image and decrypted image. The encrypted images show a visual uncorrelation with the plain images, and experimental results indicate higher confidences against the passive eavesdropper.

**INDEX TERMS** Medical image, picture archiving and communication system, chaotic map and quantum-based key generator, gray relational analysis, structural similarity index measurement.

## I. INTRODUCTION

Digital medical images are widely used multimedia or video data for human diagnostic and treatment applications in digital health, including X-ray radiography, ultrasonography/elastography, endoscopy, photoacoustic imaging, and magnetic resonance imaging. Medical images can help physicians promote accurate diagnoses and make appropriate treatment decisions for achieving the accuracy level in digital health. In medical imaging purposes, X-ray and ultrasound are first-line examination techniques used to identify pathological changes in human organs, such as lung-related diseases and possible types of cancers. X-ray images constitute the largest percentage in medical images. Digital Imaging and Communication in Medicine (DICOM) [1] is a standard to exchange medical images and their information in the hospital's picture archiving and communication system (PACS), which is used in querying, storing, printing, and transmitting information in imaging. Therefore, digital images can be generated by different medical devices and can also be integrated into the PACS [2], [3]. Each DICOM file contains patient profiles (privacy information and clinical diagnosis records), origin site, and image attribute (pixel size) [4]. These digital images can be archived in an image database or shared among hospitals, medical service organizations, or physicians. In addition, telemedicine and e-health can

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

transmit these medical messages via wireless communication for applications in remote diagnosis [5]. However, in open space / public communication channels (wireless / wired communication), medical images may be stolen or tampered by passive hacker and active hacker attacks. To ensure data confidentiality, data integrity, and data availability for information communication, this study proposes an intelligent symmetric cryptography for the infosecurity of digital medical images in a PACS.

In recent years, some studies [6]–[14] have been developed for medical signal and image cryptographic applications using chaotic maps, including sine/cosine-power maps, circle maps, tent maps, and logistic maps. Chaos-based pseudorandom numbers are generated by a one-dimensional (1D) chaotic map or a multi-dimensional (2D or 3D) chaotic system with the initial condition and control parameters in specific chaotic ranges, which have promising randomness properties and security levels. With a bifurcation diagram, the Lyapunov exponent (LE) function can be used to find the adequate ranges. In the literature [9], [10], [12], to promote the randomness property, the *sine-/cosine-power* chaotic map (SPCM / CPCM) and *logistic* map have been combined to increase the randomness, non-periodicity, and complexity levels for applications in chaotic encryption and pseudorandom number generators. Image encryption techniques include: (1) the permutation method or rearranging numerical or pixel positions and (2) substitution method or changing numerical or pixel values [14]–[20], which have secret keys in the symmetric cryptography protocol against active hacker or passive hacker attacks. Both methods use different cryptography models for static and dynamic images (gray-scale images or color images) or optics communication. The permutation method uses chaotic sequences or matrix transformation to change the positions of pixel values from plain images, such as chaotic map, chaotification system, and Arnold transformation (AT). The permutation method has promising performance to recover decrypted images with slight loss. The multi-dimensional chaotic system can generate pseudorandom key sequences to change pixel positions and values for ensuring communication security. However, multi-dimensional chaotic schemes increase computational complexity and prolong computational time. In addition, statistical analysis without changing the pixel values, such as the use of the AT method with fixed secret keys, can threaten the security level. In the substitution strategy, traditional methods, such as shift cipher, affine cipher, exclusive (XOR), Hill cipher, Playfair cipher, and hash function methods, may be easily broken by brute force or statistical attack. Hence, they can combine a multi-round cryptography protocol to improve security level [13]. The substitution method can also use chaotic sequences to change the pixel values of plain images. Compared with the permutation strategy, the substitution method has higher security level, however its encryption effect is weaker [21].

Using a single 1D chaotic map to encrypt images causes small key space and low security level. In some models, perturbed chaotic maps with noise sources can also increase the complexity levels and chaotic ranges. However, the additional noise source has drawbacks in the computational cost and constrained cycle length [22], [23]. In addition, the chaotic map system can be implemented in a continuous chaotic system (CCS) or a discrete chaotic system (DCS). The *CCS* is modeled using ordinary differential equations and is simulated on an analog circuit to deal with analog input signals. However, its technique is not suitable in the cryptographic purposes and is unstable. The *DCS* can easily be implemented using difference equations and iteration computations and can be widely used in wireless and computer communication. However, the dynamical degradation and short length of chaotic trajectories are major concerns in pseudorandom number generations [9], [24], [25]. Hence, in this study, a hybrid of 1D *SPCM/CPCM* and 1D logistic map is used to enhance the chaotic complexity and expand large chaotic ranges for increasing the key space for selecting pseudorandom keys. Hence, a 256-long key space is designed to randomly select from the specific chaotic sequences.

In quantum measurement, quantum indeterminacy can be estimated by a probability distribution, which is uniquely determined by system states. Quantum mechanics can be used to calculate the probability distribution, such as projection-valued measurement and Hilbert space formulation [26]. A single photon with polarization directions, i.e., $0°$, $+90°$, $+45°$, and $-45°$, can be encoded in non-orthogonal quantum states, which cannot be easily read or copied by an eavesdropper [27], [28] in a transmission channel. Moreover, the eavesdropper cannot gain partial information from the quantum-based encrypted messages. Quantum coding has been applied in public key cryptography and has an advantage in the secure distribution of random key information against passive eavesdropper. Hence, a quantum-based key generator (KG) is designed by suing the Bell state measurement. With the quantum superposition principle, the normalized linear combination of two states is used to produce quantum pseudorandom numbers [29]–[32] for setting unpredictable cipher codes.

With the combined chaotic map and quantum-based KG, pseudorandom numbers are produced [32]–[34], and non-repeat and non-order 256 cipher codes are randomly selected as the key-space of size 256. These cipher codes can be used to train an image encryptor and an image decryptor using two gray relational analysis (GRA) models [35]–[37] as two pairs of training data: (1) the ordered sequence numbers (OSNs) (0–255) referring to the non-OSNs for image encryptions and (2) the non-OSNs referring to the OSNs (0–255) for image decryptions. In this study, the *GRA*-based multilayer model consisting of an input layer, a comparison layer, a radial Bayesian network (RBN), and an output layer was used to establish a nonlinear mapping scheme to change the medical images' pixel values (substitution method) in the image encryption and decryption processes, which can modify the pixel values in an entire image by 256 key-space cipher codes. For a regular cipher code update,

*GRA* can rapidly retrain new cipher codes and overcome the shortcoming of permutation or substitution methods with fixed secret keys. Through a methodology validation with the Nation Institutes of Health (NIH) Clinical Center (USA) X-ray database [38], [39], for 100 chest X-ray images, the structural similarity index measurement (SSIM) [40-42] was used to evaluate the decrypted performances of the proposed intelligent symmetric cryptographic method. Experimental results indicate that with $SSIM \geq 0.95$, we can obtain reliable and lossless decrypted medical images that can be used for further lung disease diagnostic applications. In addition, encrypted images may suffer hacker attacks and slightly differ from the image. Hence, the differential analysis with hacker attacks can be evaluated by the number of pixel changing rate (NPCR) and unified averaged changed intensity (UACI) [1], [43], [44], which are used to test the number of changing pixels and number of averaged changed intensities between the decrypted and plain images. Differential analysis without hacker attacks can also be evaluated using the index of information entropy (IE) [21], [44].

The remainder of this article is organized as follows: Section II describes the methodology, including the *SPCM*, quantum-based KG, *GRA*-based encryptor and decryptor, and decryption quality evaluation. Section III describes the experimental setup, experimental tests with the NIH chest X-ray database, and performance comparison with traditional cryptographic methods. Section IV concludes the study.

## II. METHODOLOGY

### A. SINE-POWER CHAOTIC MAP (SPCM)

For random data substitution and permutation in a 1D signal and a 2D image, we can use the chaotic map to generate a 1D bifurcation and spatiotemporal diagram, as shown in Figure 1(a), for randomly selecting chaotic sequences on the specific interval, such as *sine-/cosine- power maps*, *circle maps*, *tent maps*, and *logistic maps* [6]–[13]. Its bifurcation points and chaotic trajectories can be controlled by the appropriate initial condition and control parameters. However, the above chaotic maps have simple chaotic behaviors, chaotic trajectories, and frail chaotic intervals [6]–[13]. Hence, in this study, we combined the logistic map and sine map to establish a complex chaotic map, hereafter referred as the SPCM, for producing a non-periodic chaotic sequence as follows:

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

where $r$ is a control parameter; $c_0$ is the initial condition, i.e., $c_0 \in (0, 1)$; and $n_c$ is the sequence length, i.e., $n = 0, 1, 2, 3, \ldots, n_c$. The *SPCM* with control parameters can produce the non-periodic chaotic sequence, $c_n$, from $r = 0.0$ to $r = 4.0$ on the specific amplitude $[-0.5, +0.5]$, as shown in Figure 1(a). Combining the logistic and sine-power map can increase the difficulty levels against passive attacks (eavesdroppers) [22]–[23] in a secure communication system. The *SPCM* has a positive LE for control parameters, i.e., $r \in [1.0, 4.0]$, as shown in Figure 1(b). The LE has the maximum value in the control parameter, $r = 3.3510$, and also shows chaotic behaviors on the specific amplitude $[-0.5, +0.5]$ with the control parameters from values 3.3510 to 4.0000, as shown by the blue dash-line region in Figure 1(a).

With the control parameters, $1 < r < 4$, and initial condition, $c_0 = 0$, the estimated values of *LE* can be used to observe the adequate interval of control parameters, as

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

$$r_t = r_{t-1} + \Delta r, \quad \Delta r = 0.0010, t = 1, 2, 3, \ldots, n_r \quad (3)$$

where $r_0$ is the initial control parameter ($r_0 = 1.0000$), $n_r$ is the number of control parameters ($n_r = 3001$), and $n_c$ is the number of sequence length ($n_c = 2.8 \times 10^4$). The blue dash-line region shows the high random sequence in the specific amplitude and frequency. The maximum estimated value of the $LE = +1.6383$ dB can be used to validate the chaotic phenomenon and the adequate interval of control parameter [3.3510, 4.0000], as shown in Figure 1(b).

### B. QUANTUM BASED KEY GENERATOR

Quantum cryptography protocol is a technique of secure communication based on quantum mechanical properties [32] to perform symmetric cryptographic tasks, such as quantum key distribution for infosecurity problems. This protocol is also called the BB84 protocol (Charles H. Bennett and Gilles Brassard, 1984) [33]–[34], which is described using photon polarization states to encode transmission messages, as shown in Figure 2(a). Any two pairs of conjugate states can be used for phase-encoded states in optical fiber-based communication and encoding messages in non-orthogonal states. The BB84 protocol uses two pairs of states, where each pair conjugates to the other pairs and two states conjugate to the other pair. The usual polarization state pairs are the rectilinear basis of vertical (+90°) and horizontal (0°) and the diagonal basis of +45° and −45° (as shown in Figure 2(a)).

Any two bases are conjugate to each other, and the rectilinear and diagonal bases can be encoded in binary codes, where a value of "1" is encoded in the rectilinear basis as a vertical polarization state (+90°) and in the diagonal basis as a −45° state and a value of "0" is encoded

in a horizontal polarization state (0°) and in a + 45° state, as shown in Figure 2(a). In a quantum measurement, we can make an eigenstate with the probability of a qubit having a value of "0" and the probability of a qubit having a value of "1", as

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{subject to } \alpha^2 + \beta^2 = 1 \quad (4)$$

where $\alpha^2$ is the probability of a qubit having a value of "0" and $\beta^2$ is the probability of a qubit having a value of "1." The measuring qubit can also be transformed into binary values for quantum secret applications.

In this study, with the Bell state measurements [29], we can transfer the *SPCM*'s chaotic pseudorandom numbers, $c'_n$, into the Einstein–Podolsky–Rosen (*EPR*) pair by the entangled two-qubit states, $|0\rangle$ and $|1\rangle$ [30], [31], as the

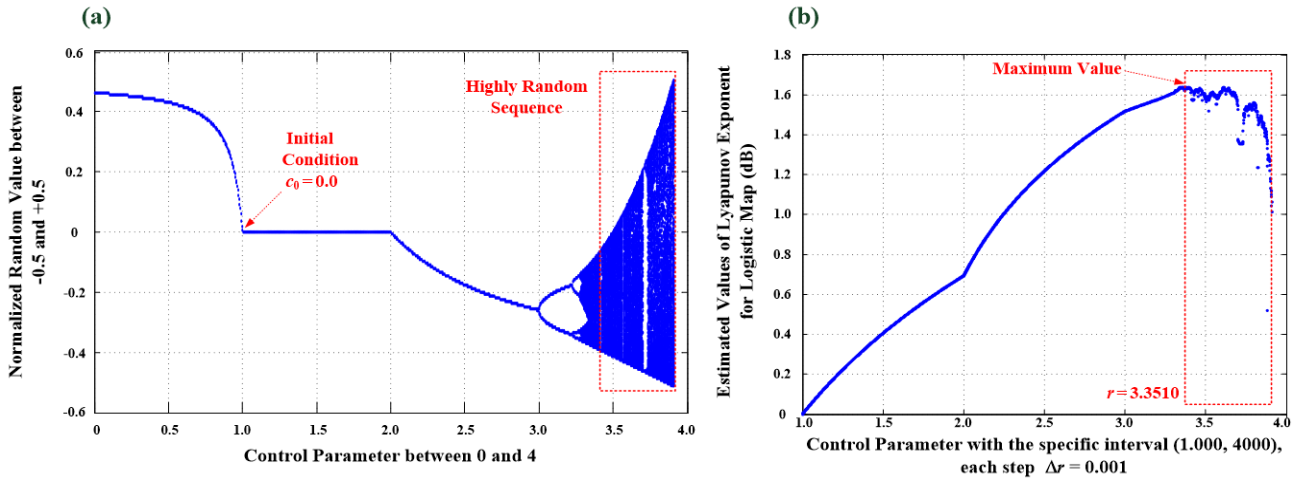


**FIGURE 1.** Sine-power chaotic map. (a) 1D bifurcation and spatiotemporal diagram with control parameters between 0.0 and 4.0, (b) Sine-power-based chaotic trajectories over 2.8 $\times 10^4$ iteration numbers.

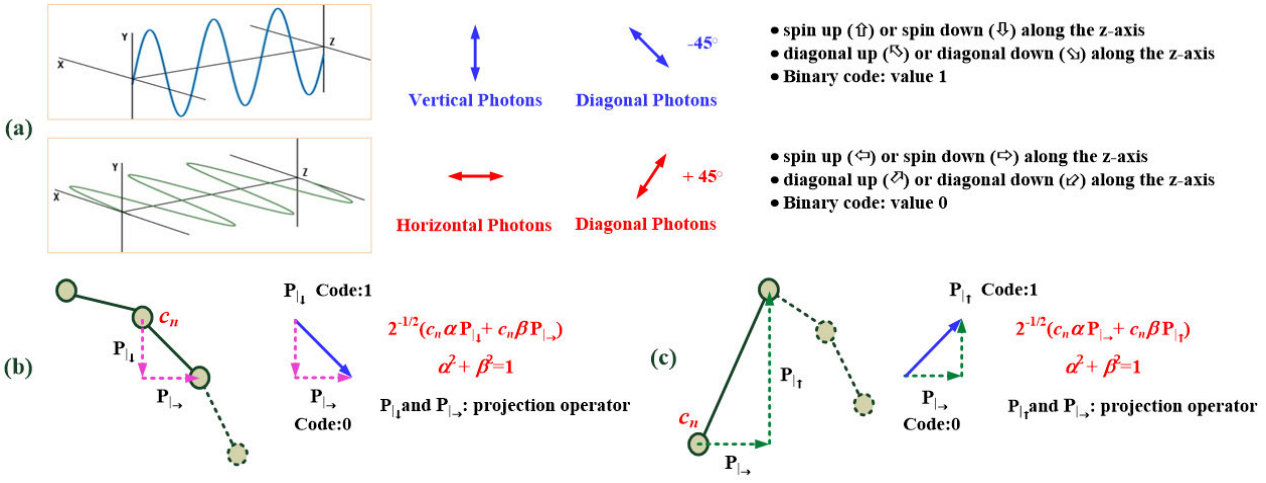


**FIGURE 2.** Quantum cryptography protocol. (a) Photons sent for the quantum transmission, (b) Bell states with entangled two-qubit states.

general form of Bell state

$$c_n' = \text{mod}(floor(255 \cdot |2c_n|), 256) \quad (5)$$

$$|\Phi\rangle_n = 2^{-1/2}(c_n{'}\alpha^2|0\rangle + c_n{'}\beta^2|1\rangle),$$
$$\text{subject to } \alpha^2 + \beta^2 = 1, \quad n = 0, 1, 2, 3, \ldots, n_c \quad (6)$$

where function *floor*(•) is the operator to round the value to the nearest integer number [45]; mod(•) function is the modulo operation [46]; $\alpha^2 = \beta^2 = 0.50$ in this study; value of "1" states that the probability of 50% of them are $P_{|\uparrow}$, $P_{|\downarrow}$, $P_{|\nwarrow}$, or $P_{|\swarrow}$; and the other 50% are $P_{|\leftarrow}$, $P_{|\rightarrow}$, $P_{|\nearrow}$, or $P_{|\swarrow}$, such as the Bell states "$2^{-1/2}(c_n\alpha^2 P_{|\rightarrow} + c_n\beta^2 P_{|\downarrow})$" and "$2^{-1/2}(c_n\alpha^2 P_{|\rightarrow} + c_n\beta^2 P_{|\uparrow})$" in Figure 2(b). With the control parameters between 0.0 and 4.0, *SPCM* can produce chaotic pseudorandom numbers, as shown in Figure 3(a). The Bell states can form an orthonormal bases in a two-qubit space using Equation (6), as shown in State #1 and State #2 in Figure 3(b). Hence, we can produce the quantum pseudorandom numbers, $C_n$, as

$$C_n = floor(255\,|\Phi\rangle_n\,/\,\max(|\Phi\rangle_n)), \quad n = 0, 1, 2, \ldots, n_c \quad (7)$$

where $\max(|\Phi\rangle_n) = 255$. Hence, *SPCM* and the quantum-based KG can be implemented as randomly generating the pseudorandom numbers, as shown in the pseudorandom numbers versus the OSNs in Figure 3(b). Hence, the *KG* can produce the non-OSNs (non-repeating) to set the cipher codes for encryption and decryption processes, which are defined as follows:

- cipher codes for encrypted keys (EKs): $OSN = [0, 1, 2, 3, \ldots, 255]$ refers to $EK = [C_1, C_2, C_3, \ldots, C_{256}]$, where *EK* is a non-OSN,
- cipher codes for decrypted keys (DKs): $DK = [C_1, C_2, C_3, \ldots, C_{256}]$ refers to $OSN = [0, 1, 2, 3, \ldots, 255]$.

Two pairs of cipher codes, (*OSN*, *EK*) and (*DK*, *OSN*), are used to set the symmetric secret keys for medical image infosecurity.

### C. GREY RELATIONAL ANALYSIS BASED ENCRYPTOR AND DECRYPTOR

Two pairs of cipher codes can be set for a regular secret key update by an authenticated sender and an authenticated receiver duration communication authentication, which are used to train the *GRA*-based encryptor and decryptor, as shown in Figure 4. For two *GRA*s, each one consists of an input layer, a comparison layer, a *RBN*, and an output layer and is used to design an encryptor and a decryptor. The number of comparators and Gaussian functions (GFs) are determined by the dimension of the cipher code vector; thus, 256 nodes are set in the *RBN*. Each *GRA* is a nonlinear regression model to map the nonlinear relationship between *OSN* and *EK* for image encryption or between *DK* and *OSN* for image decryption, respectively, where *EK* and *DK* are non-OSNs.

Feed two pairs of training data, i.e., (*OSN*, *EK*) and (*DK*, *OSN*). These training data are used to establish the *RBN* computational network, and *GRA* uses the similarity measurement between a reference sequence (input data), $\Phi_0$, and the comparative sequences (training data), $\Phi_c = [\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_k, \ldots, \varphi_K]$, $k = 1, 2, 3, \ldots, K$, which are used to set the weighted values, $W^1$, in comparators, $com_k$, and the weighted values in RBN output connecting network, $W^2$, respectively, as [13]

- for image encryption : $W^1 = [w_{k1}]^T = [k-1]^T$ (8)
- for image decryption : $W^I = [w_{k1}]^T = [C_k]^T$ (9)

where $k = 1, 2, 3, \ldots, K$, $K$ is the number of training data, and $K = 256$ in this study. Then, the weighted values, $W^2 = [w_{kj}], j = 1, 2$ is set as the RBN output connecting network, as [13]

- for image encryption : $W^2 = [\, w_{k1},\ \ w_{k2}\,]^T = [C_k, 1]^T$ (10)
- for image decryption : $W^2 = [\, w_{k1},\ \ w_{k2}\,]^T = [k-1, 1]^T$ (11)

The output of each comparator, $com_k$, is computed by the *Euclidean distance* (ED) operation (as shown in Figure 4), as [35]

$$ED : \mathrm{ED}_k = (\Delta d_k)^2, \Delta d_k = (\Phi_0 - \varphi_k)/K \quad (12)$$

$$Variance : \sigma^2 = \sum_{k=1}^{K} \mathrm{ED_k} \quad (13)$$

where the standard deviation, $\sigma$, is estimated by *ED*. Then, each output of *GF* is computed by [35]

$$g_k = \xi \exp(-\frac{1}{2}(\frac{ED_k}{\sigma})^2) \quad (14)$$

Hence, *GRA* uses Equation (14) to measure the level of similarity degree with the $ED_k$. Parameter $\xi$ is the recognition coefficient (RC), $\xi \in (0, 5)$, which is used to make the difference between an input data and $K$ training data more distinguishable. The output of *GF*, $g_k$, is inversely proportional to $ED_k$, and $0 \le g_k \le \xi$. Parameter *RC*, $\xi = 5$, is chosen in this study [35]. For image encryption and decryption applications, in the output layer, the final output of *GRA* is

$$\mathrm{Y}_m = 255(\sum_{k=1}^{K} w_{k1} g_k \Big/ \sum_{k=1}^{K} w_{k2} g_k), \quad m = 1, 2 \quad (15)$$

where $m = 1$ for the encryptor's output and $m = 2$ for the decryptor's output. The plain image is $\Phi_{01} = [\varphi_{01,1,1}, \varphi_{01,1,2}, \ldots, \varphi_{01,1,N} | \varphi_{01,2,1}, \varphi_{01,2,2}, \ldots, \varphi_{01,2,N} | \ldots | \varphi_{01,N,1}, \varphi_{01,N,2}, \ldots, \varphi_{01,N,N}]$ for the image encryption; the cipher image is $\Phi_{02} = [\varphi_{02,1,1}, \varphi_{02,1,2}, \ldots, \varphi_{02,1,N} | \varphi_{02,2,1}, \varphi_{02,2,2}, \ldots, \varphi_{02,2,N} | \ldots | \varphi_{02,N,1}, \varphi_{02,N,2}, \ldots, \varphi_{02,N,N}]$ for the image decryption. $\Phi_{01}$ and $\Phi_{02}$ were fed to the encryptor and decryptor for performing the encryption or decryption tasks, respectively. Each medical image is an $N \times N$ pixel image ($N$ = 1,024 in this study). Image $Y_1 = [y_{1,1,1}, y_{1,1,2}, \ldots, y_{1,1,N} | y_{1,2,1}, y_{1,2,2}, \ldots, y_{1,2,N} | \ldots | y_{1,N,1}, y_{1,N,2}, \ldots, y_{1,N,N}]$ is the encrypted image; $Y_2 = [y_{2,1,1}, y_{2,1,2}, \ldots, y_{2,1,N} | y_{2,2,1}, y_{2,2,2}, \ldots, y_{2,2,N} | \ldots | y_{2,N,1}, y_{2,N,2}, \ldots, y_{2,N,N}]$ is the decrypted image.

### D. EVALUATION OF THE DECRYPTION PERFORMANCE

After obtaining the decrypted image, $Y_2$, the *SSIM* index was used to measure the perceived quality between the plain image, $\Phi_{01}$, and decrypted image, $Y_2$, with size $N \times N$. The pixel values of $\Phi_{01}$ and $Y_2$ are non-negative data. The *SSIM* index used the comparison measurements with three terms, i.e., luminance (L), contrast (C), and structure (S) [40-41]:

$$\mathrm{L}(\Phi_{01},\mathrm{Y}_2) = \frac{2\mu_{\Phi_{01}}\mu_{Y_2} + d_1}{\mu_{\Phi_{01}}^2 + \mu_{Y_2}^2 + d_1},$$
$$\mathrm{C}(\Phi_{01},\mathrm{Y}_2) = \frac{2\sigma_{\Phi_{01}}\sigma_{Y_2} + d_2}{\sigma_{\Phi_{01}}^2 + \sigma_{Y_2}^2 + d_2}, \quad (16)$$

and

$$\mathrm{S}(\Phi_{01},\mathrm{Y}_2) = \frac{\sigma_{\Phi_{01}Y_2} + d_3}{\sigma_{\Phi_{01}}\sigma_{Y_2} + d_3}$$
$$d_1 = (0.01l)^2,\ d_2 = (0.03l)^2,\ \text{and}\ d_3 = \frac{1}{2}d_2 \quad (17)$$

$$SSIM(\Phi_{01}, Y_2) = L(\Phi_{01}, Y_2)^{\alpha} C(\Phi_{01}, Y_2)^{\beta} S(\Phi_{01}, Y_2)^{\gamma} \quad (18)$$

where $\mu_{\Phi 01}$ is the local mean value of the plain image $\Phi_{01}$; $\mu_{Y2}$ is the local mean value of the decrypted image $Y_2$; $\sigma_{\Phi 01}$ is the standard deviation of the plain image $\Phi_{01}$; $\sigma_{Y2}$ is the standard deviation of the decrypted image $Y_2$; and $\sigma_{\Phi 01 Y2}$ is the cross-covariance of images $\Phi_{01}$ and $Y_2$; parameter $l$ is the dynamic range of the pixel values ($l$ is the maximum value in an image, that is, 255 for an 8-bit grayscale image); parameters 0.01 and 0.03 are small constant parameters. Thus, $d_1, d_2$, and $d_3$ are also small constants; the values of parameters $\alpha$,

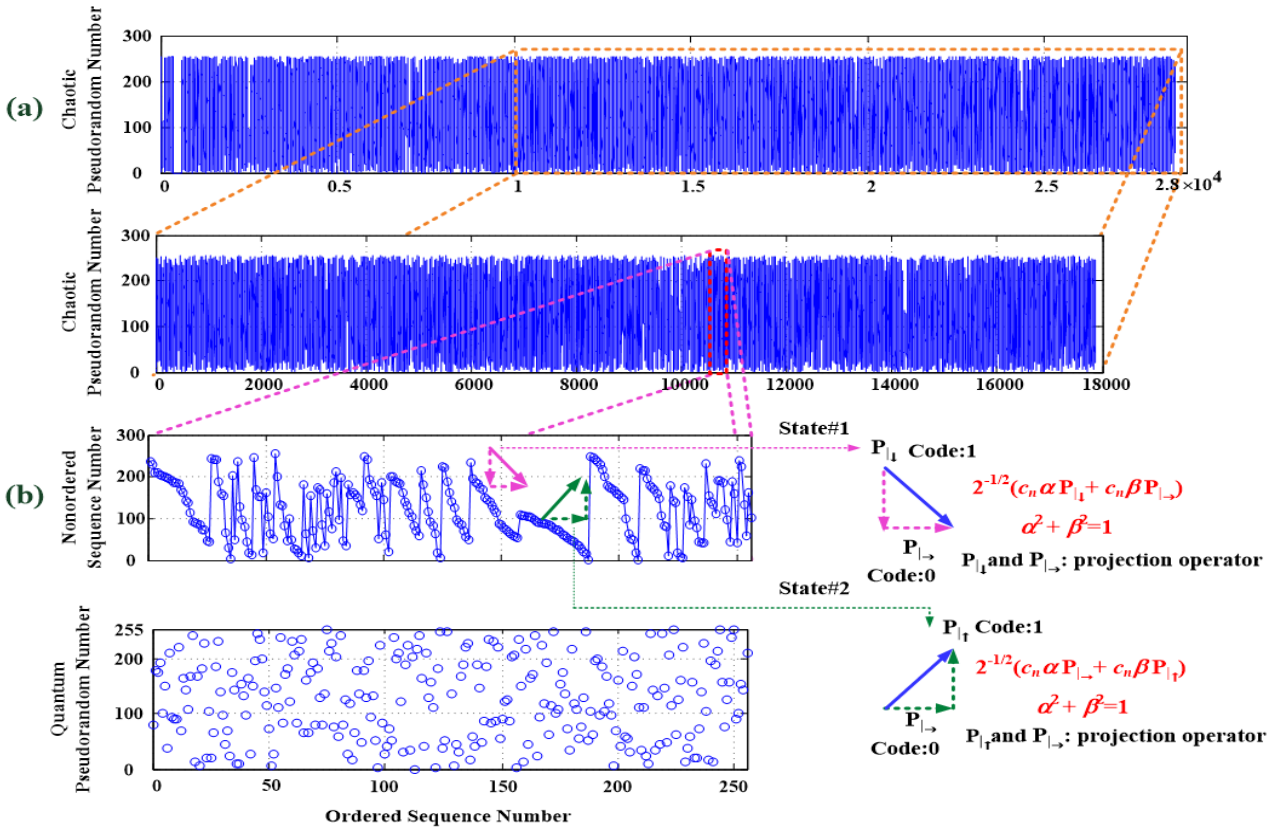


**FIGURE 3.** *SPCM* and quantum-based non-OSNs. (a) Chaotic pseudorandom numbers, (b) Quantum pseudorandom numbers.

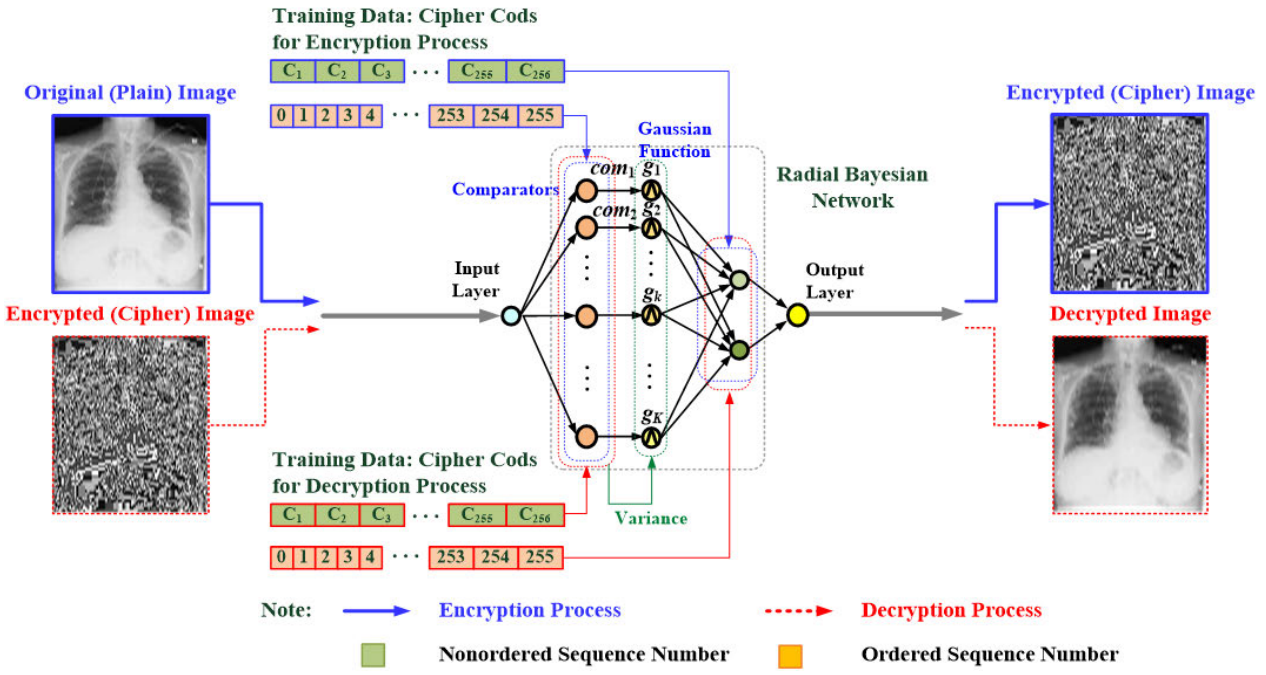


**FIGURE 4.** Structure of the GRA-based image encryptor and image decryptor.

$\beta$, and $\gamma$ are set to 1 [42]. Hence, we can represent the *SSIM* index for recovery quality evaluation, as follows:

$$SSIM(\Phi_{01}, Y_2) = \frac{(2\mu_{\Phi_{01}}\mu_{Y_2} + d_1)(2\sigma_{\Phi_{01}Y_2} + d_2)}{(\mu^2_{\Phi_{01}} + \mu^2_{Y_2} + d_1)(\sigma^2_{\Phi_{01}} + \sigma^2_{Y_2} + d_2)},$$

$$SSIM(\Phi_{01}, Y_2) \in [0,1], \quad SSIM(\Phi_{01}, Y_2) \geq 0.95 \tag{19}$$

where $SSIM \in [0, 1]$. A value close to 1.00 or greater than 0.95 indicates a structural similarity between plain images and a decrypted image, whereas a value of 0.00 indicates

the absence of structural similarity, satisfying (1) symmetry: $SSIM(\Phi_{01}, Y_2) = SSIM(Y_2, \Phi_{01})$; (2) boundedness: $SSIM(\Phi_{01}, Y_2) \leq 1.00$; (3) unique maximum: $SSIM(\Phi_{01}, Y_2) = 1.00$, if and only if $\Phi_{01} = Y_2$ [42]. The larger the *SSIM* value, the smaller the loss, which means that the proposed decryptor has a good recovery quality without noise interferences nor any active attack, whereas $SSIM(\Phi_{01}, Y_2) \geq 0.95$. Hence, the *SSIM* indicates a quantitative index for evaluating the recovery quality.

### E. DIFFERENTIAL ANALYSIS BETWEEN PLAIN IMAGE AND DECRYPTED IMAGE WITH/WITHOUT HACKER ATTACKS

#### 1) INFORMATION ENTROPY (IE)

Information entropy (IE) is an index that measures the distribution of gray values in an image. For an image with 256 ($2^8$) gray-scale levels, if the distribution of gray values is more uniform, the *IE* index is greater and approaches 8. This index is defined as follows [1], [21], [44]:

$$\mathrm{IE}(q) = \sum_{j=1}^{Q} P(q_j) \log_2(\frac{1}{P(q_j)}), \quad \sum_{j=1}^{Q} P(q_j) = 1 \tag{20}$$

where $Q$ is the total number of gray scales ($Q = 256$ in this study), $q_j$ is the $j$th gray values, and $P(q_j)$ is the emergence probability of $q_j$. For an ideal random level of encrypted image, the *IE* index is 8. An effective encryptor will make the *IE* index approach 8 for an encrypted image without hacker attacks. Hence, the uniform distribution of gray values makes statistical attacks difficult [21], [47].

#### 2) NPCR AND UACI INDEXES

When a hacker attack makes a minor or major change in encrypted pixels, *NPCR* and *UACI* are the indexes used to measure the performance and efficiency against differential hacker attacks. These indexes can be defined as follows [1], [43], [44]:

$$\mathrm{NPCR} = \frac{\sum_{x=1}^{N}\sum_{y=1}^{N} D(x,y)}{NN} \times 100\%, \tag{21}$$

$$D(x,y) = \begin{cases} 0, & if\ \Phi_{01}(x,y) = Y_2(x,y) \\ 1, & if\ \Phi_{01}(x,y) \neq Y_2(x,y) \end{cases} \tag{22}$$

$$\mathrm{UACI} = \frac{\sum_{x=1}^{N}\sum_{y=1}^{N} |\Phi_{01}(x,y) - Y_2(x,y)|}{255 \times NN} \times 100\% \tag{23}$$

where $N \times N$ is the dimension of an image, $x = 1, 2, 3, \ldots, N$ and $y = 1, 2, 3, \ldots, N$ for the height and width of the image, respectively; $\Phi_{01}(x, y)$ and $Y_2(x, y)$ denote the pixel gray values of a plain and a decrypted image on the location $(x, y)$, respectively. High values of the *NPCR* and *UACI* indexes indicate that the images have active hacker attacks.

## III. EXPERIMENTAL RESULTS

### A. EXPERIMENTAL SETUP

In this study, the chest X-ray images (frontal view image) were collected from the NIH X-ray database [38], [39]. These images were available through the NIH download website, which included a freely available annotated medical image database for patient care. The associated chest X-ray images were accumulated and stored in the hospital's PACS. The images were in Portable Network Graphics format. We can apply these X-ray images in clinical research and efforts in image understanding, digital image processing, and computer-aided diagnosis (CAD) applications. Patients with the mined eight disease image labels or with multi-labels could be used to establish deep/machine learning for enhancing the precision of CAD and infosecurity systems. Hence, for the eight pathology classes, as shown in Figure 5, the 100 frontal view images, which included 20 images for normal condition (Nor) and 80 images related to lung diseases (pleural effusion (Eff), emphysema (Em), pneumonia (P), pneumothorax (Pt), inflammation (In), fibrosis (F), and mass (M)/nodule (N)), were used to evaluate and validate the proposed chaotic map and quantum-based cryptography protocol. Each X-ray image was digitized to a resolution of 96×96 dots per inch and 24 bits per pixel (colored image), and each one was a 1,024 ×1,024 pixel image (1,048,576 pixels), where the row numbers were $p = 1, 2, 3, \ldots, 1{,}024$, and the column numbers were $q = 1, 2, 3, \ldots, 1{,}024$. The proposed intelligent symmetric image cryptography was designed on a tablet PC (Intel®Xeon®, CPU E5-2620, v4, 2.1 GHz and 64 GB of RAM) using MATLAB version 9.0 software (1994–2021, The MathWorks, Inc., Natick, MA, USA) and was also used with a graphics processing unit (NVIDIA Quadro P620, 64-bit Windows 10.0 operating system), which can speed up the encrypted and DK generations, image encryption and decryption processes, and recovery quality evaluation, as shown in the flowchart in Figure 6.

### B. PARAMETERS SETTING FOR KEY GENERATOR

Before medical image sharing or transmission, the authorized persons at the data emitter (Alice) end data receiver (Bob) can set the cryptography protocol with the symmetric encrypted and DKs. The proposed *SPCM* and quantum-based KG can rapidly produce more random numbers, which were selected to set the 256 key-space cipher codes for image encryption and decryption. In the *SPCM*-based generator, we can randomly generate the non-periodic sequence data using the hybrid of 1D *sine-power* and *logistic* chaotic map with the initial condition $c_0 = 0.0$ and control parameter $r \in [3.3510, 4.0000]$. As shown in Figure 1(b), the bifurcation point was at approximately 3.0000, and the chaotic trajectories were controlled by the control parameters. The *LE* index indicating the positive maximum value of 1.6383 dB at point 3.3510 was used to validate the chaotic behaviors in this specific interval, which could be

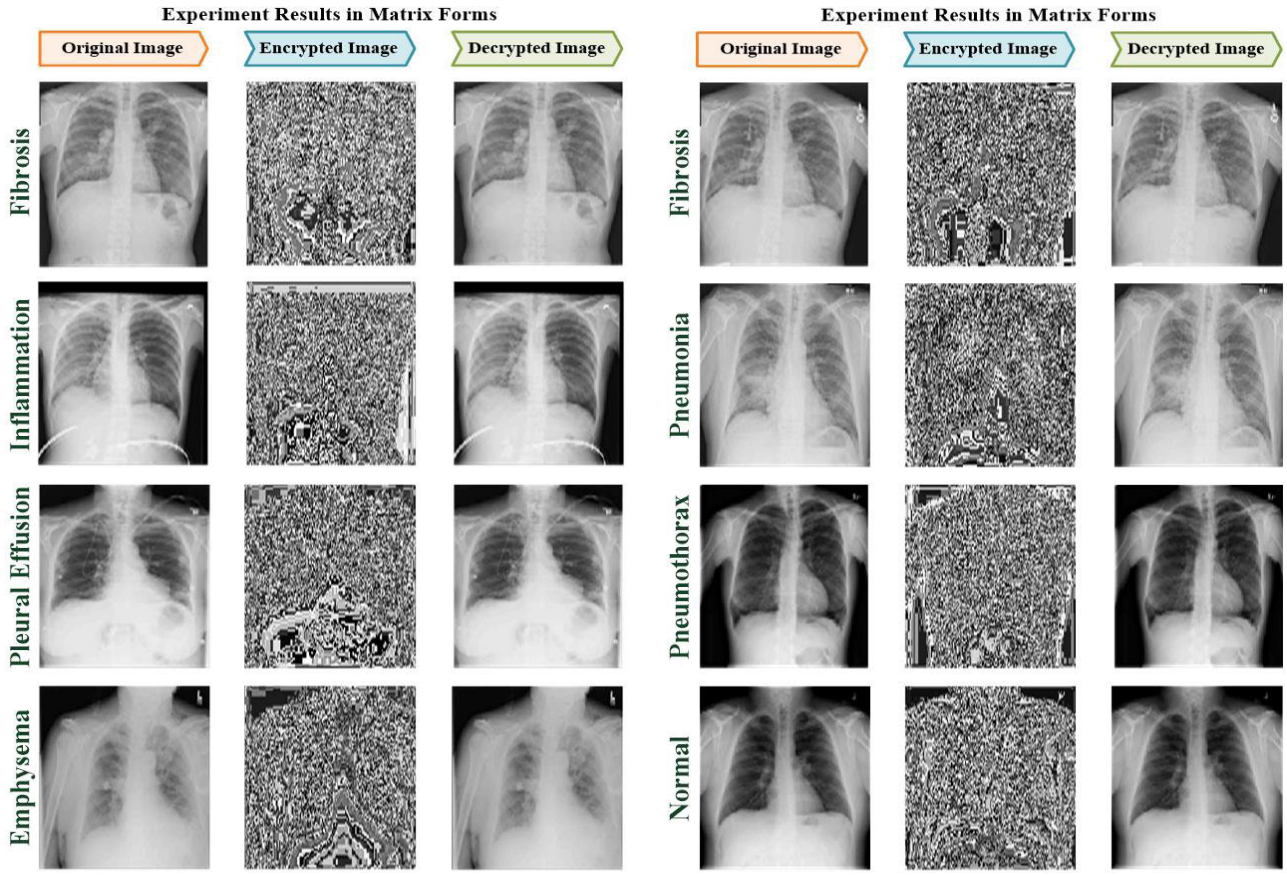


**FIGURE 5.** Plain frontal view of the X-ray images, encrypted images, and decrypted images for the normal condition and different lung-related diseases, including fibrosis (F), inflammation (In), pneumonia (P), pleural effusion (Eff), pneumothorax (Pt), and emphysema (Em), and normal condition (Nor).

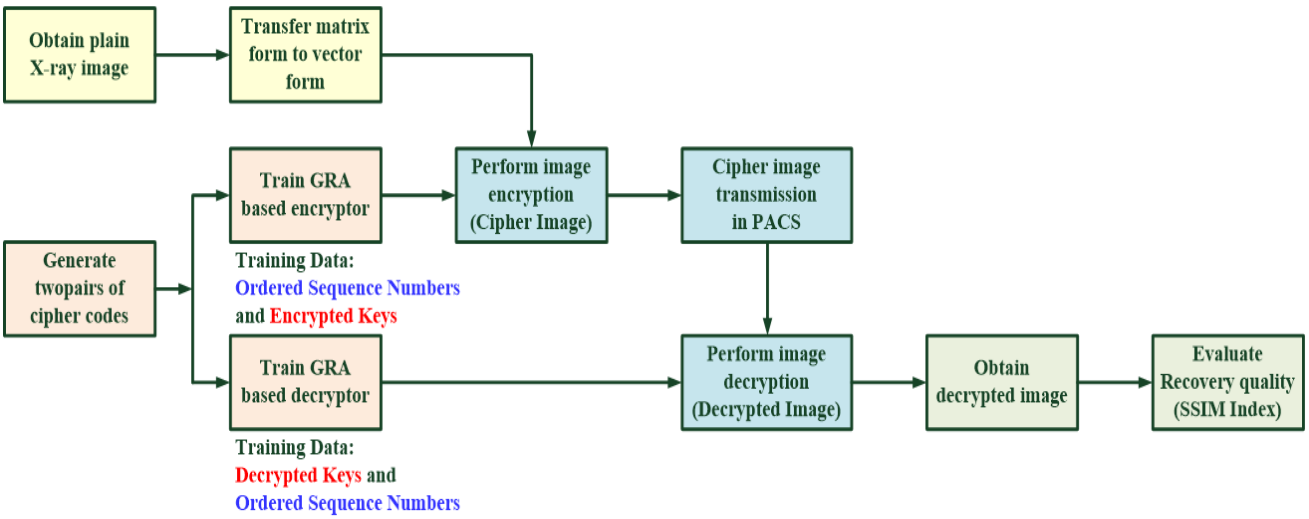


**FIGURE 6.** Flowchart of the chest X-ray image encryption and image decryption processes.

used to select the non-ordered and non-repeated 256 numbers from the highly random sequence data for setting the cipher codes. Table 1 shows the comparison results of LE values between the proposed chaotic map (Logistic map+SPCM) and traditional chaotic maps. The LE value of the proposed chaotic map was larger than those of traditional chaotic maps. Larger LE values correspond to more evident chaotic behavior [21].

**TABLE 1. Comparison results of LE values between the proposed chaotic map (Logistic map + SPCM) and traditional chaotic maps.**

| Chaotic Map | Logistic Map | SPCM | Logistic Map + SPCM |
|---|---|---|---|
| LE Value (dB) | 1.5523 dB | 1.3843 dB | 1.6383 dB |

Then, the quantum-based generator can produce the random numbers using the terms of Bell states "$2^{-1/2}(c_n\alpha^2 P_{|\rightarrow} + c_n\beta^2 P_{|\downarrow})$" and "$2^{-1/2}(c_n\alpha^2 P_{|\rightarrow} + c_n\beta^2 P_{|\downarrow})$", as shown in Equations (5) to (7). With the source of the chaotic sequence data (as shown in Figure 3(a)), the quantum-based generator can rapidly produce the random numbers and increase the complexity levels and chaotic ranges. Hence, in an electronic communication, for transmitting medical images, a computer network or telecommunication system can use the proposed symmetric cryptography protocol to share/exchange digital data or messages between the data emitter end data receiver. As shown in the 10 rounds of cipher codes in Figure 7, 10 pairs of cipher codes (*OSN*, *ED*/*DK*) can be produced for a regular symmetric encryption and DK update duration communication authentication.

### C. IMAGE ENCRYPTOR AND DECRYPTOR TRAINING

Authorized persons used the proposed KG to generate the two pairs of cipher codes: (1) for image encryption, the ordered sequence, $OSN = [0, 1, 2, \ldots, 255]$ referring to the non-ordered sequence, $EK = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$; (2) for image decryption, $DK = [ck_1, ck_2, ck_3, \ldots, ck_{256}]$ referring to *OSN*. For two pairs of cipher codes, we can rapidly establish an image encryptor and an image decryptor, which both consisted of 1 input node, 256 comparators, 256 *GF*s, 2 summation nodes, and 1 output node. In the RBN, the RC, $\xi$, was set as constant value 5, which was used to make the difference between an input pixel value and an encrypted number and an encrypted number and a decrypted number more distinguishable. The standard deviations of *GF*s can be estimated using Equations (12) and (13), which can be self-tuned by the *ED* between the input pixel values and 256 cipher codes. Figures 8(a) and 8(b) show the mean standard deviations of the image encryptor and image decryptor for different pathology classes, which can automatically determine the network connecting the topology and parameters for image encryption and decryption processes without iteration computations. In addition, the image encryptor and image decryptor can automatically produce new standard deviations without any optimization method to tune the optimal parameters.

For this adaptive scheme with 100 frontal view X-ray images, the proposed *GRA*-based encryptor and decryptor can encrypt the plain X-ray images (frontal view) and recover the decrypted images without the active hacker attacks, respectively. For all chest X-ray images, the mean *SSIM* index $= 1.0000 \geq 0.9500$ was obtained to evaluate the quality of decrypted medical images for the pathology classes of lung-related diseases. In addition, the mean *PSNR* index $= 68.1308$ dB $\geq 30.0000$dB (peak signal-to-noise ratio [13]) was obtained to evaluate the image recovery quality. A small loss, represented by a large *SSIM* index, means that the proposed decryptor had a good recovery quality without the active attacker attacks, as shown in Figure 9. Hence, the decrypted images had higher possibility to be interpretable for diagnostic applications in lung-related diseases. Each encryption and decryption process took approximately $<$ 3s CPU execution time. In addition, as shown in Figures 9(a) and 9(b), the *SSIM* and *PSNR* indexes decreases indicated the medical images with the active attacks, transformation errors, or transmission noises. While the received image was visually unreco-gnizable, the data receiver could exclude the received cipher images and again request a new transmission of the cipher images.

In addition, Figure 10(a) shows the correlation of two horizontally adjacent pixels in plain images and its encrypted images for different pathology classes (including P, Eff, F, and Nor). The average correlation coefficients (CCs) were 0.9158 and 0.006679 (with the linear regression method [48], [49]), respectively, for different pathology classes, as listed in Table 2. The average CC was very small (close to zero). The relationships between a plain image and its encrypted image might be difficult to establish, indicating that the proposed encryptor could effectively destroy the relativity between the plain image and the encrypted image against statistical attacks. We could also obtain the average *IE* index $= 7.5538$ (256 gray-scale levels) to measure the randomness distribution level [21], [47] for validating the effective encryptor for nine pathology classes, as shown in Table 2. For key sensitivity analysis, with sight changes in decrypted keys, as incorrect key $=$ original cipher code $+1$) [1], we could use the incorrect decrypted keys to evaluate the sensitivity of the proposed decryptor in decryption, including P, Eff, F, and Nor. As displayed in Figure 10(b), with the incorrect keys , the decrypted images were different from the plain images, indicating that the proposed scheme was highly sensitive to the slightest changes in secret keys.

Table 2 lists the average *NPCR* and *UACI* with minor active hacker attacks. The index *NPCR* concentrated on pixel changes in differential attacks, and the index *UACI* focused on the average differences between the plain and decrypted images, which were computed using Equations (21)–(23). The averages of 71.71% and 20.57% (a larger value is better) indicate the ability to resist against minor differential attacks. Equations (21)–(23) were also used to compute the indexes of *NPCR* and *UACI* with the plain and encrypted images. Hence, the higher average *NPCR* of 99.45% and average *UACI* of 31.92% (larger-the-better) could be obtained from experimental results to validate whether or not the pixel gray values of the plain images were completely scrambled by the proposed encryptor. No relationship was also found between

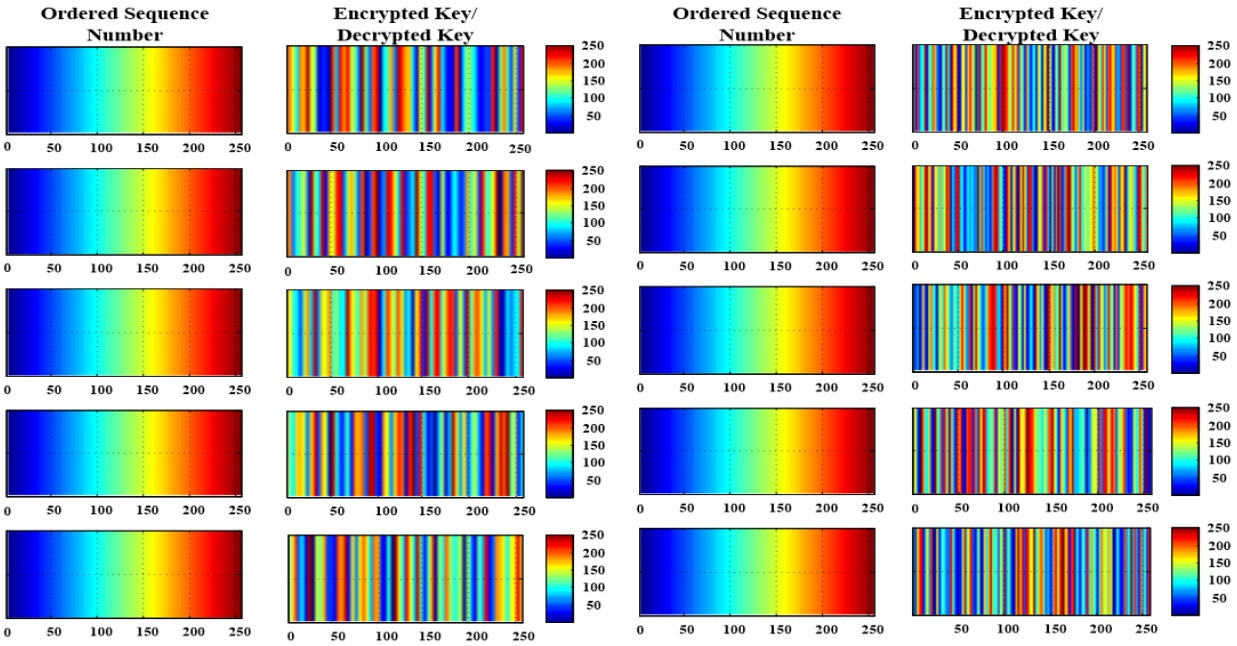


**FIGURE 7.** Ten rounds of cipher codes produced for the symmetric encryption and DK update.

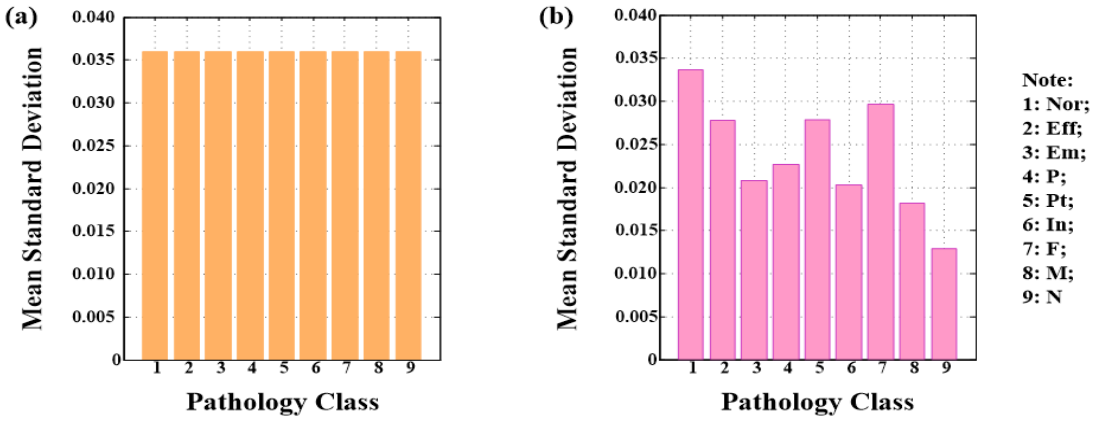


**FIGURE 8.** Image encryptor and decryptor parameter settings for different pathology classes. (a) Mean standard deviations of the image encryptor for different pathology classes. (b) Mean standard deviations of the image decryptor for different pathology classes.

the plain and encrypted images. An average CC of 0.0019 (with the linear regression method [48, 49]) was obtained, validating that the proposed encryptor could destroy the relativity effectively. Experimental results of different pathology classes are shown in Table 3.

### *D. COMPARISON WITH THE TRADITIONAL METHOD (GRNN)*

In this study, two general regression neural networks (GRNN) were also used to establish an image encryptor and an image decryptor, which both consisted of 1 node in the input layer, 256 nodes in the pattern layer, 2 nodes in the summation layer, and 1 node in the output layer. In the pattern layer, an optimization method, such as particle swarm optimization (PSO) search algorithm [13], [18], [50], was used to adjust the smoothing parameters in the pattern layer using the iteration computations. The proposed KG was also used to produce a pair of cipher codes for image encryption and image decryption. For the two pairs of cipher codes (as shown in Figure 7), using the iterative computations, the near-optimal smoothing parameters (0.0019 for the image encryptor and 0.0015 for the image decryptor) could be obtained and be guaranteed to minimize the mean squared error for reaching the convergent condition. Through at least 10 experimental tests, we could suggest to assign the PSO's parameters, such as particle population size $= 20$, convergent condition $\leq 10^{-2}$, and a maximum iteration number $= 20$ for searching the optimal parameters. Each iteration computation process

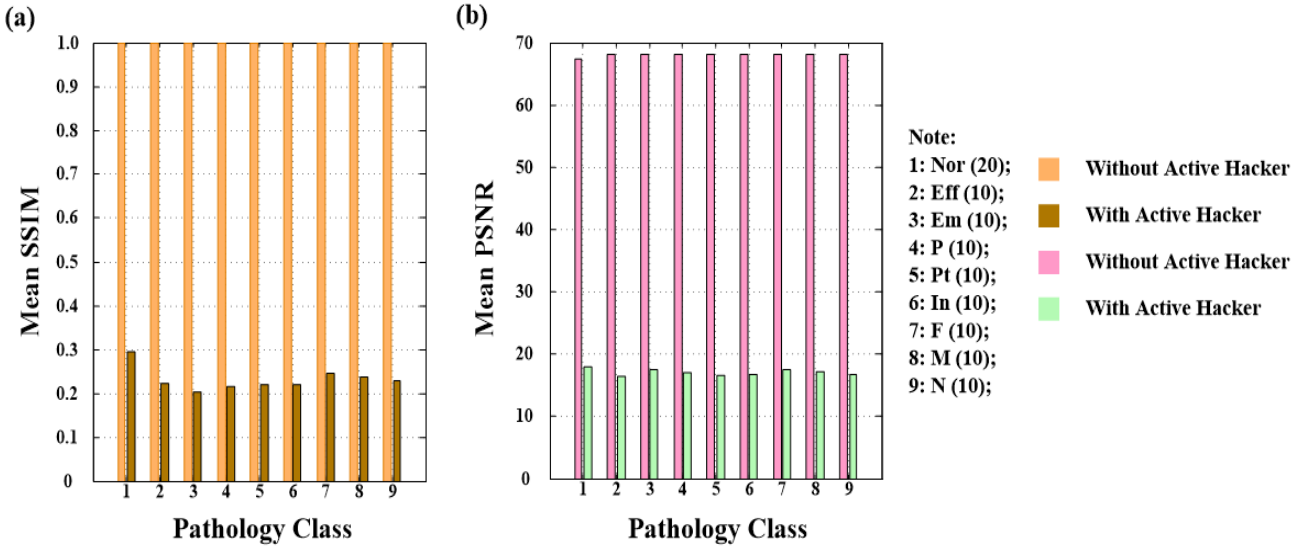


**FIGURE 9.** Experimental results for the *GRA*-based encryptor and decryptor. (a) Mean SSIM index for the image decryption without and with active hacker attacks. (b) Mean PSNR index for the image decryption without and with active hacker attacks.

**TABLE 2.** Comparisons of *NCPR*, *UACI*, *IE* and *CC* indexes with / without active hacker attacks for different pathology classes.

| Pathology Class | With Active Hacker Attack | | Without Active Hacker Attack | | | | |
|---|---|---|---|---|---|---|---|
| | *NPCR* (%) | *UACI* (%) | *NPCR* (%) | *UACI* (%) | *IE Index* | *Correlation Coefficient* (*CC*) | |
| | | | | | | *Plain Image* | *Encrypted Image* |
| Nor | 71.23 | 19.08 | 0.00 | .0.00 | 7.7754 | 0.9835 | 0.019300 |
| Eff | 72.23 | 21.05 | 0.00 | 0.00 | 7.6256 | 0.9516 | 0.000010 |
| Em | 70.81 | 19.94 | 0.00 | 0.00 | 7.1618 | 0.9083 | 0.000001 |
| P | 72.37 | 22.71 | 0.00 | 0.00 | 7.6592 | 0.9019 | 0.016300 |
| Pt | 71.56 | 22.63 | 0.00 | 0.00 | 7.7969 | 0.9185 | 0.001700 |
| In | 70.75 | 20.27 | 0.00 | 0.00 | 7.7203 | 0.9053 | 0.003300 |
| F | 70.70 | 20.81 | 0.00 | 0.00 | 7.5727 | 0.9046 | 0.005500 |
| M | 74.86 | 17.42 | 0.00 | 0.00 | 7.2034 | 0.8846 | 0.013700 |
| N | 70.89 | 21.19 | 0.00 | 0.00 | 7.4693 | 0.8835 | 0.000300 |
| Average | 71.71 | 20.57 | 0.00 | 0.00 | 7.5538 | 0.9158 | 0.006679 |

**TABLE 3.** Comparisons of *NCPR*, *UACI* and *CC* indexes for different pathology classes between plain images and encrypted images.

| Pathology Class | *NPCR* (%) | *UACI* (%) | *Correlation Coefficient* (CC) |
|---|---|---|---|
| Nor | 99.62 | 30.94 | 0.0004 |
| Eff | 99.12 | 38.60 | 0.0028 |
| Em | 98.22 | 31.05 | 0.0012 |
| P | 99.46 | 34.15 | 0.0007 |
| Pt | 100.00 | 34.79 | 0.0028 |
| In | 99.44 | 30.53 | 0.0002 |
| F | 100.00 | 28.88 | 0.0016 |
| M | 99.91 | 26.50 | 0.0033 |
| N | 99.26 | 31.81 | 0.0038 |
| Average | 99.45 | 31.92 | 0.0019 |

required $<10$ iterations and a CPU execution time of $<10$ s to achieve the convergent condition. For the same 100 chest X-ray images, the experimental results for the *GRNN*-based encryptor and decryptor are shown in Figure 11. Without active hacker attacks, the mean *SSIM* index $= 1.0000$ and mean *PSNR* index $= 104.4977$ dB were obtained to evaluate the quality of decrypted medical images; their values decayed, which implied serious active hacker attacks.

For a cross-sectional view of $512 \times 512$ pixel computed tomography (CT) images in an 8-bit Joint Photographic

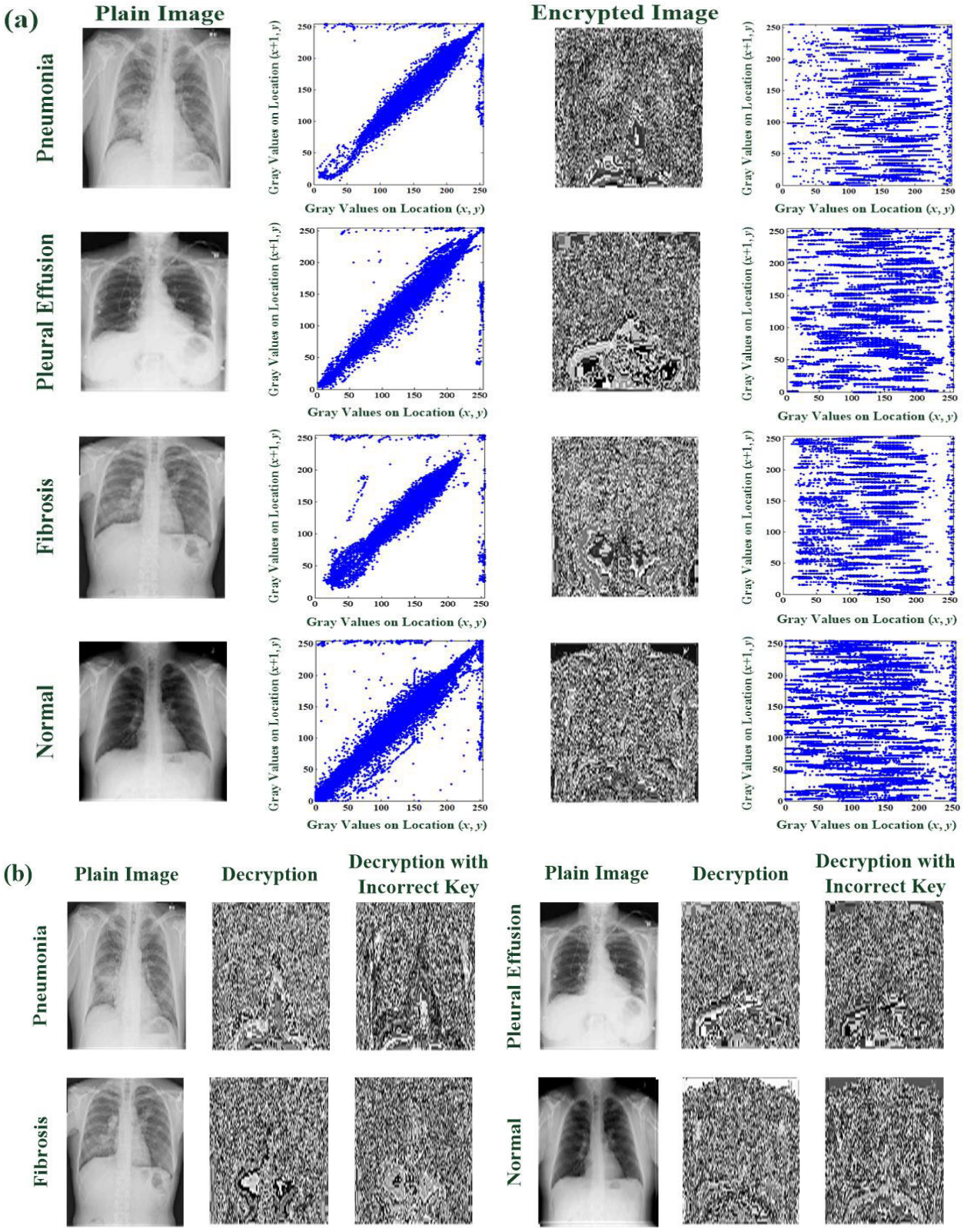


**FIGURE 10.** Results of correlation analysis and key sensitivity analysis. (a) Correlation analysis for two horizontally adjacent pixels in plain images and encrypted images, including pneumonia (P), pleural effusion (Eff), fibrosis (F), and normal condition (Nor), (b) Decryption with correct key and incorrect key for key sensitivity analysis.

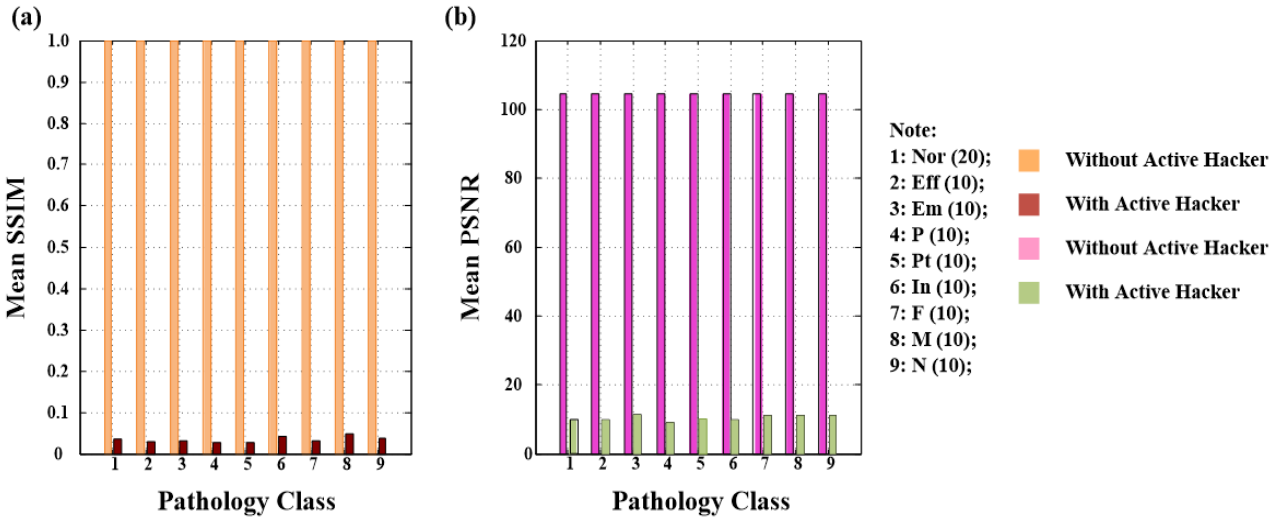


**FIGURE 11.** Experimental results for the *GRNN*-based encryptor and decryptor. (a) Mean SSIM index for the image decryption without and with active hacker attacks. (b) Mean PSNR index for the image decryption without and with active hacker attacks.

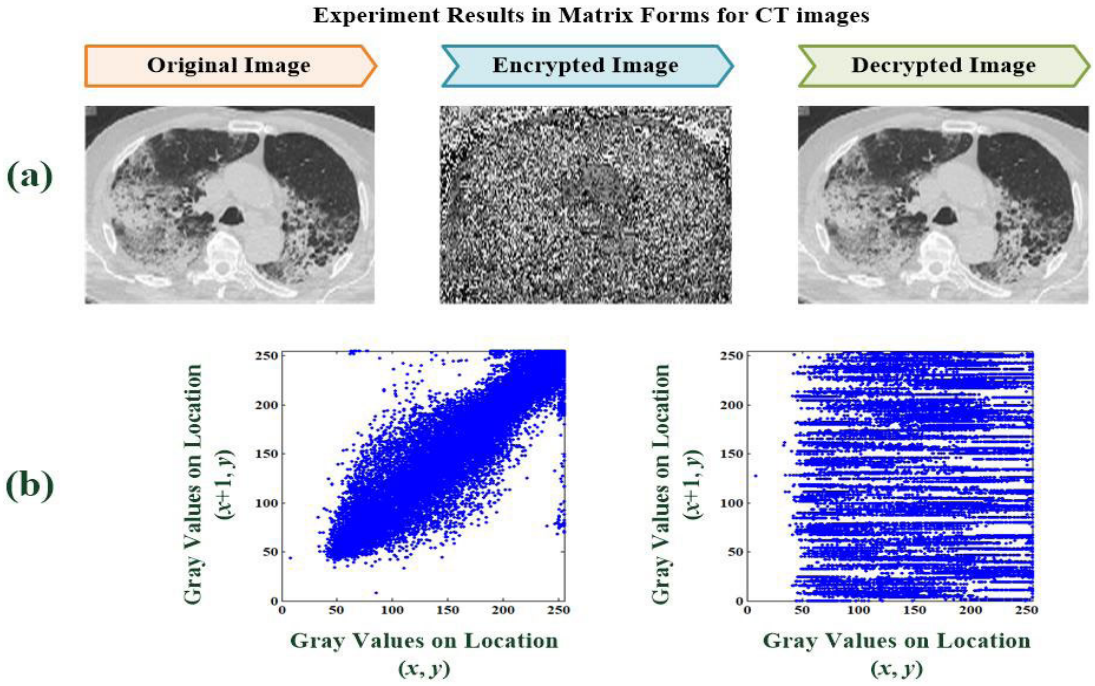


**FIGURE 12.** (a) Plain CT image, encrypted CT image, and decrypted CT image (cross-sectional view) for a novel COVID-19 patient, (b) Correlation analysis for CT image.

Group file format, as shown in Figure 12(a), the proposed image encryptor and image decryptor could also offer promising results in CT image encryption and decryption; the *SSIM* index (= 1.0000) and *PSNR* index (= 68.1308 dB) also had higher critical values to evaluate the image recovery quality, and Figure 12(b) shows the correlation analysis in a plain CT image and its encrypted image. The CCs were 0.8994 and 0.0002 in the plain image and its encrypted image, respectively. In addition, no relationship was found between the plain CT image and its encrypted image. In addition, an *IE* index = 7.5353 could be obtained to measure the randomness level, and its value was very close to 8.0000 for validating the effective encryptor for CT image encryption against statistical attacks and eavesdropper [47]. With a minor active attack in CT image, the *NPCR* and *UACI* indexes were 71.65% and 21.38%, indicating that the proposed encryptor and decryptor had a promising ability against active hacker attacks. In addition, the *NPCR* and *UACI* indexes were 96.84%

and 33.14%, respectively, between the plain and encrypted images, and the relationship between them was difficult to establish. Hence, the decrypted image had promising confidences for lung disease diagnosis (novel COVID-19 patient). Hence, the proposed methods can extend their applications in ultrasonography / elastography, endoscopy, photoacoustic imaging, and magnetic resonance imaging. In addition, in contrast to the *GRNN*-based method, the proposed *GRA*-based method had a straightforward mathematical scheme (using Equations (12) to (15)) to process numerical computations without optimization algorithms and iteration computations, which could reduce the CPU execution time and computational resources to search the optimal the optimal parameters and also obtained promising results for medical image infosecurity in the X-ray images and CT images.

## IV. CONCLUSION

In this study, a *GRA*-based encryptor and decryptor were established for application in medical image infosecurity in a small-scale PACS. The *SPCM* and quantum-based KG can increase the chaotic complexity level and produce more random numbers for setting encrypted and decrypted cipher codes. Two *GRA*-based multilayer networks were used to train the encryptor and decryptor. Through the selected 100 chest X-ray images from the NIH database, without active hacker attacks, a visual uncorrelation occurred between the plain images and encrypted images; the mean $SSIM = 1.0000$ and mean $PSNR = 68.1308$dB were used to evaluate the recovery quality between the plain image and decrypted image. The overall process required a mean CPU execution time of $<3$ s to complete the image encryption and image decryption. In addition, experimental results of security analysis revealed that the proposed encryptor and decryptor had promising encryption and decryption performances using *NCPR*, *UACI*, and *IE*, and the correlation analysis was sensitive to the secret keys. In contrast to the *GRNN*-based encryptor and decryptor, the proposed method does not require the following: (1) *PSO* algorithm's parameter assignment for training an encryptor and a decryptor; (2) network optimal parameter tuning in training or retraining processes; (3) *PSO* algorithm's parameter and GRNN's parameter storage; and (4) iteration computations. The statistical method is used to rapidly estimate the standard deviation of *GF*s in the *RBN* by the current training data without complexity iteration computations. Hence, the proposed method can speed up the encryption and decryption processes with an adaptive scheme. Its adaptive scheme has straightforward mathematical operations and statistical parameter estimation to perform the retrained operation with feeding new pairs of cipher codes at each regular encrypted and DK update. The *SPCM* and quantum-based KG can also enhance the confidentiality, recoverability, and availability of medical image infosecurity in the PACS for sharing/ exchanging digital data among hospitals, medical service organizations, or physicians. The method can also be applied to commonly used clinical medical images.

## ABBREVIATIONS

| | |
|---|---|
| DICOM | Digital Imaging and Communication in Medicine. |
| PACS | Picture Archiving and Communication System. |
| LE | Lyapunov Exponent. |
| SPCM | Sine Power Chaotic Map. |
| CPCM | Cosine Power Chaotic Map. |
| KG | Key Generator. |
| CCS | Continuous Chaotic System. |
| DCS | Discrete Chaotic System. |
| OSN | Ordered Sequence Numbers. |
| GRA | Gray Relational Analysis. |
| RBN | Radial Bayesian Network. |
| NIH | Nation Institutes of Health. |
| SSIM | Structural Similarity Index Measurement. |
| NPCR | Number of Pixel Changing Rate. |
| UACI | Unified Averaged Changed Intensity. |
| IE | Information Entropy. |
| EPR | Einstein–Podolsky–Rosen. |
| EK | Encrypted Key. |
| DK | Decrypted Key. |
| GF | Gaussian Function. |
| ED | Euclidean Distance. |
| CAD | Computer-Aided Diagnosis. |
| PSNR | Peak Signal-to-Noise Ratio. |
| CC | Correlation Coefficient. |
| GRNN | General Regression Neural Networks. |
| PSO | Particle Swarm Optimization. |
| CT | Computed Tomography. |

## REFERENCES


[1] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images," *Informat. Med. Unlocked*, vol. 20, Jan. 2020, Art. no. 100396.

[2] 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.

[3] M. Hosseini and E. B. Dixon, "Syntactic interoperability and the role of standards," in *Health Information Exchange: Navigating and Managing a Network of Health Information Systems*. Amsterdam, The Netherlands: Elsevier, 2016, pp. 123–136.

[4] I. D. McLean and J. Martensen, *Specialized Imaging, Clinical Imaging*, 3rd ed. Amsterdam, The Netherlands: Elsevier, 2014, p. 4478.

[5] Y. Zhou, K. Panetta, and S. Agaian, "A lossless encryption method for medical images using edge maps," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Sep. 2009, pp. 3707–3710.

[6] A. Kanso, "Self-shrinking chaotic stream ciphers," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 822–836, Feb. 2011.

[7] 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, Dec. 2014.

[8] 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.

[9] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, 2017.

[10] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.

[11] C. Li, K. Qian, S. He, H. Li, and W. Feng, "Dynamics and optimization control of a robust chaotic map," *IEEE Access*, vol. 7, pp. 160072–160081, 2019.
[12] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Digital cosine chaotic map for cryptographic applications," *IEEE Access*, vol. 7, pp. 150609–150622, 2019.
[13] 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.
[14] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," *IEEE Trans. Signal Process.*, vol. 68, pp. 1937–1949, 2020.
[15] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion–substitution based gray image encryption scheme," *Digit. Signal Process.*, vol. 23, no. 3, pp. 894–901, May 2013.
[16] 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, 2014.
[17] 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.
[18] 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.
[19] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing," *Signal Process.*, vol. 183, Jun. 2021, Art. no. 107998.
[20] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dyn.*, vol. 104, no. 1, pp. 807–825, Mar. 2021.
[21] Q. Zhang, L. Guo, and X. P. Wei, "Image encryption using DNA addition combining with chaotic maps," *Math. Comput. Model.*, vol. 52, nos. 11–12, pp. 2028–2035, Dec. 2010.
[22] L. Shu-Bo, S. Jing, X. Zheng-Quan, and L. Jin-Shuo, "Digital chaotic sequence generator based on coupled chaotic systems," *Chin. Phys. B*, vol. 18, no. 12, p. 5219, 2009.
[23] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.
[24] Y. Deng, H. Hu, N. Xiong, W. Xiong, and L. Liu, "A general hybrid model for chaos robust synchronization and degradation reduction," *Inf. Sci.*, vol. 305, pp. 146–164, Jun. 2015.
[25] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, and J. Harkin, "Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation," *Int. J. Bifurcation Chaos*, vol. 27, no. 3, Mar. 2017, Art. no. 1750033.
[26] V. Braginski, F. Khalili, and K. Thorne, *Quantum Measurements*. Cambridge, U.K.: Cambridge Univ. Press, 1992, doi: 10.1017/CBO9780511622748.
[27] T. Sui, D. Marelli, X. Sun, and K. You, "A networked state estimation approach immune to passive eavesdropper," in *Proc. Chin. Control Conf. (CCC)*, Jul. 2019, pp. 8867–8869.
[28] 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.
[29] D. Sych and G. Leuchs, "A complete basis of generalized Bell state," *New J. Phys.*, vol. 11, pp. 1–9, Jan. 2009.
[30] S. Braunstein, A. Mann, and M. Revzen, "Maximum violation of Bell inequalities for mixed states," *Phys. Rev. Lett.*, vol. 68, no. 22, pp. 3259–3261, 1992.
[31] V. Vedral, *Introduction to Quantum Information Science*. London, U.K.: Oxford Univ. Press, 2006.
[32] S. V. Kartalopoulos, "Chaotic quantum cryptography," in *Proc. 4th Int. Conf. Inf. Assurance Secur.*, Sep. 2008, pp. 338–342.
[33] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, vol. 175. New York, NY, USA, Dec. 1984, pp. 1–8.
[34] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Mar. 2014.
[35] C.-H. Lin, "Assessment of bilateral photoplethysmography for lower limb peripheral vascular occlusive disease using color relation analysis classifier," *Comput. Methods Programs Biomed.*, vol. 103, no. 3, pp. 121–131, Sep. 2011.
[36] Y. Cenglin, "Application of gray relational analysis method in comprehensive evaluation on the customer satisfaction of automobile 4S enterprises," *Phys. Procedia*, vol. 33, pp. 1184–1189, Jan. 2012.
[37] K. S. Prakash, P. M. Gopal, and S. Karthik, "Multi-objective optimization using Taguchi based grey relational analysis in turning of Rock dust reinforced Aluminum MMC," *Measurement*, vol. 157, pp. 1–13, Jun. 2020.
[38] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and M. R. Summers, "ChestX-ray8: Hospital-scale chest X-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jul. 2017, pp. 2097–2106.
[39] (2019). *Nation Institutes of Health (NIH), Clinical Center, Images are Ailable Via Box*. [Online]. Available: https://Nihcc.app.box.com/v/ChestXray-NIHCC
[40] (2021). *Syntax: SSIM*. The MathWorks, Inc. [Online]. Available: https:/www.mathworks.com/help/images/ref/ssim.html
[41] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[42] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multiscale structural similarity for image quality assessment," in *Proc. 37th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2003, pp. 1398–1402.
[43] S. A. Banu and R. Amirtharajan, "Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach," *Multimedia Tools Appl.*, vol. 79, no. 39, pp. 28807–28824, 2020.
[44] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Med. Biol. Eng. Comput.*, vol. 59, no. 3, pp. 589–605, Mar. 2021.
[45] (2021). *Syntax: Floor*. [Online]. Available: https://www.mathworks.com/help/matlab/ref/floor.html
[46] (2021). *Syntax: Mod*. [Online]. Available: https://www.mathworks.com/help/matlab/ref/mod.html
[47] R. Sivaraman, S. Rajagoplalan, J. B. B. Rayappan, and R. Amirtharajan, "Ring oscillator as confusion-diffusion agent: A complete TRNG drove image security," *IET Image Process.*, vol. 14, no. 13, pp. 2987–2997, Nov. 2020.
[48] C. Tofallis, "Least squares percentage regression," *J. Modern Appl. Stat. Methods*, vol. 7, no. 2, pp. 526–534, Nov. 2008.
[49] (2021). *Syntax: Linear Regression*. [Online]. Available: https://www.mathworks.com/help/matlab/data_analysis/linear-regression.html
[50] T.-H. 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.

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

He was a Professor with the Department of Electrical Engineering, Kao Yuan University, Kaohsiung, from 2004 to 2017. He has been 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, Taiwan, 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 the National Cheng Kung University, Tainan, in 2014.

He was a Postdoctoral Research Fellow at X-ray and IR Imaging Group, National Synchrotron Radiation Research Center, Hsinchu, Taiwan, from 2014 to 2017. He was also a Postdoctoral Research Fellow with the Department of Niche Biomedical LLC, California NanoSystems Institute, UCLA, Los Angeles, USA, from 2017 to 2018. He has been an Assistant Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan, since 2019. His research interests include artificial intelligence applications in electrical engineering and biomedical engineering, biomedical signal processing, medical ultrasound, 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 has been the Chief with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan, since 2019, where she is currently an Associate Professor with the Department of Electrical Engineering. Her current research interests include neural network computing and its applications, fuzzy systems, and advanced control systems.

**HSIANG-YUEH LAI** received the Ph.D. degree from the Department of Engineering and System Science, National Tsing Hua University, Hsinchu, Taiwan, in 2010.

She is currently an Associate Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan. Her current research interests include intelligent systems, embedded systems, and solid-state electronic devices.

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

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

**CHAO-LIN KUO** 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, in 2006.

He was an Associate Professor with the Institute of Maritime Information and Technology, National Kaohsiung Marine University, Kaohsiung, Taiwan, from 2011 to 2017. He has been a Professor with the Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung, since 2017, where he has been the Chief, 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.

**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, where he was the Chairman of the department (from 2004 to 2007) and the Computer Center (from 2013 to 2017). His current research interests include fuzzy systems, artificial intelligence, imagine processing, advanced control systems, and microprocessor systems.