IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 3, 2020, accepted September 28, 2020, date of publication October 1, 2020, date of current version October 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3028077

Two-Round Symmetric Cryptography for Medical Image Infosecurity Against-Hacker Attacks in a Picture Archiving and Communication System

JIAN-XING WU[1], (Member, IEEE), NENG-SHENG PAI[1], YU-CHI PU[2], PI-YUN CHEN[1], CHIA-HUNG LIN[1,3], CHAO-LIN KUO[2], (Member, IEEE), AND CHIH-HSIEN LI[1]

[1]Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung 41170, Taiwan
[2]Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung 80543, Taiwan
[3]Artificial Intelligence Application Research Center, National Chin-Yi University of Technology, Taichung 41170, 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 Hospital Research Ethics Committee and the Institutional Review Board (IRB), Taipei Veterans General Hospital, Taipei, under Contract V103C-059; and in part by the Ministry of Science and Technology, Taiwan, during August 1, 2019–July 31, 2021, 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.

ABSTRACT Digitalizing medical images, such as images in ultrasonography or mammography, or magnetic resonance imaging, can be applied for telemedicine applications in telediagnosis and telesurgery, and can be stored in a cloud database via computer networking transmission or wireless communications. Besides, these images contain the patient privacy information. Thus, their reliability and availability should be protected to ensure medical image infosecurity in public channels or open spaces. Medical images can also be hacked by unauthorized people. Therefore, in the picture archiving and communication system (PACS), this study proposes against-hacker attacks with two-round symmetric cryptography models for medical image infosecurity. Hash transformation with multi secret keys is performed to change the pixel values and produce dynamic errors for the two-round encryption processes. In image decryption, two-round decryption processes are employed to estimate the possible hacker attacks at the routing path and to determine the decryption key parameter by using an optimization-based controller. For a case study of mammographic images consisting of 50 benign tumors and 50 malignant tumors, the peak signal-to-noise ratio (PSNR) is employed to evaluate the decryption quality between the plain and decrypted images.

INDEX TERMS Symmetric cryptography, hacker attack, hash transformation, optimization-based controller, peak signal-to-noise ratio.

I. INTRODUCTION

Network security attacks are unauthorized actions used to crack private and corporate resources, data, and applications, which intercept the transit of information to modify, steal, and copy the content of messages, such as plain words, plain texts, and plain images. These security attacks are divided into two—active and passive, resulting in security threats and attacks in computer network communication, as shown by the red dashed line in Figure 1. With the digitalized data transmission via wired or wireless in public spaces, these attacks can be launched at the network layer. For example, in 2018, a large-scale security attack occurred in Singapore; the health information system was hacked, resulting in the theft of medical data of 50 million patients. Hackers broke into the health database in a deliberate, targeted, and well-planned attack [1]. In the same year, in Taiwan, the Health Bureau public health information system was also hacked. These events were the most serious data breach incidents in recent years. Ensuring that these digital data will not be stolen, tampered with, damaged, nor lost after transfer by unauthorized people has become a major concern in computer network communication, especially with regard to medical images.

Digital medical imaging is a non-invasive technique to create two-dimensional (2D) or (three-dimensional) 3D scans

The associate editor coordinating the review of this manuscript and approving it for publication was Easter Selvan Suviseshamuthu.

for visually representing the internal aspects of the human body for clinical analysis, medical intervention, and treatment applications, such as indicating internal structures of human organs and tissues, medical images can be produced by various physical devices, including ultrasonography, X-ray mammographic images/radiography, computed tomography (CT), magnetic resonance imaging (MRI), thermography, photography, and so on, and be used to establish a database of anatomy and physiology to identify abnormalities. Such technique is also required for archiving, telemedicine, and emergency applications in telesurgery and telediagnosis [2]. Hence, remote diagnosis is becoming increasingly popular for the evaluation and treatment of patients without requiring in-person visits; it transmits biosignals and medical images at a distance with computer networking or wireless transmission in web-based picture archiving and communication system (PACS) [3]–[7]. In the mobile emergency medical care system, a set of body sensors is performed to collect a patient's health status, which is transmitted to the doctors or emergency staff in public communication channels. The chaotic maps based on authentication and key agreement mechanisms with the Diffie–Hellman key (DHK) exchange have been designed to protect patients' electronic medical data in wireless body area networks [8]. However, the DHK algorithm needs large computational time and high computing power for digital image cryptography with large data [7]. This method is suitable for exchanging only a few messages, such as digital signatures and authentication in real-time applications. In addition, radio frequency identification (RFID) technique is also used for healthcare applications, such as patient monitoring and drug administration in the telecare medicine information system (TMIS) [9]. RFID tag authentication protocol with the hash operation and synchronized secret key can ensure patient privacy in TMIS. These technologies include the follow-up visits, chronic condition management, medication management, and specialist consultation. Given that patient data will be transmitted via electronic communication, providers will select technology solutions that employ data encryption to protect patient privacy and data. Digital medical images in PACS will have a higher degree of security compared to other digital images, including the X-ray, CT, and MRI films. Hence, digital medical image encryption has certain confidentiality, integrity, and availability for information communication with enhanced security.

Medical image security via internet communication, multimedia systems, and telemedicine has attracted increasing research attention [4]. Various image encryption algorithms with permutation and diffusion methods or mixed permutation and diffusion have been proposed for medical images [7], [10]–[18], including (1) change in pixel values and (2) change in pixel positions. The permutation method can change the position of image pixels without altering pixel values, such as those in chaotic Cat maps, chaotic logistic maps, and chaotic Hopfield neural networks [4], [10]–[12]. In diffusion methods, the pixel values are modified or substituted in the whole image using the transformation function or combining the substitution and transposition methods, such as shift cipher, exclusive (XOR), circular S-box, and hash function methods, to improve the security [12]–[17]. Mixed permutation- substitution methods are used to change pixel positions and pixel values with respect to the secret key in dependent dynamic blocks; these dynamic blocks undergo key- dependent diffusion and substitution processes [12], [18], [19]. However, these secret keys, as control parameters used in the permutation and substitution methods, are fixed in the whole symmetric image encryption processes, which will favor the hacker attacks. In addition, the encrypted and decrypted images are obtained with a symmetric key, which gives the original image. In the symmetric key cryptography, the data or bits of streaming data are changed by a definite pattern with adding a secret key, which is known to a sender and a receiver, as shown in the same key for encryption and decryption in Figure 1. Symmetric key modes use the identical cryptographic keys for encrypted plain image and decrypted cipher image between the data emitter and receiver ends; they can be employed to maintain private information communication. However, this condition is one of the major drawbacks of symmetric cryptography.

Hence, for the unique characteristics of the medical images, more-round permutation and substitution processes can ensure the confidentiality of digital images and make the distribution of pixel values to have a uniform distribution in histogram analysis of encrypted images. Some studies [20], [21] have proposed encryption schemes by combining the more-round permutation and substitution processes and chaotic key generator (CKG) function to ensure both gray and color image security. The CKG functions, including sine map, circle map, tent map, and logistic map functions, are employed to produce the secret key, which is used to generate any length of random numbers in the specific ranges (256-bit length block). Two random values can be generated using these CKG functions and then selected to mix the row and column positions for a permutation table. But, state variables for different chaotic map functions need the special determined initial conditions and control parameters [21], [22]. The control parameters are used to set the dynamics of the chaotic map in both amplitude and frequency. These CKG functions are required to determine the suitable initial conditions and control parameters to generate chaotic signals with smooth bifurcation. Moreover, chaotic selection based encryption algorithm has not against the active hacker attacks.

In this study, based on symmetric cryptography against active attacks, as seen in Figure 2, a diffusion method with hash transformation functions was carried out to change the pixel values of X-ray medical images, such as cipher image H hash weighting values, and secret key B, and then produce the dynamic error E. The hash transformation function [17], [23]–[26] was implemented to convert graphic data (any image) into sequence data by mixing the hash weighting values and multisecret keys in an X-ray image.

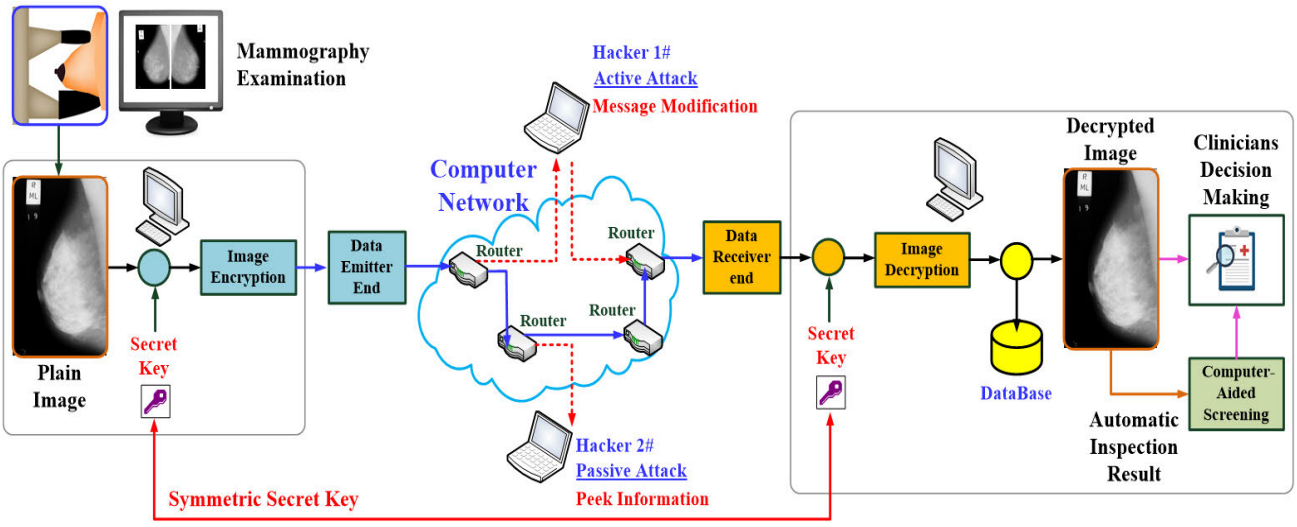

FIGURE 1. Architecture of medical image infosecurity in picture archiving and communication system (PACS).

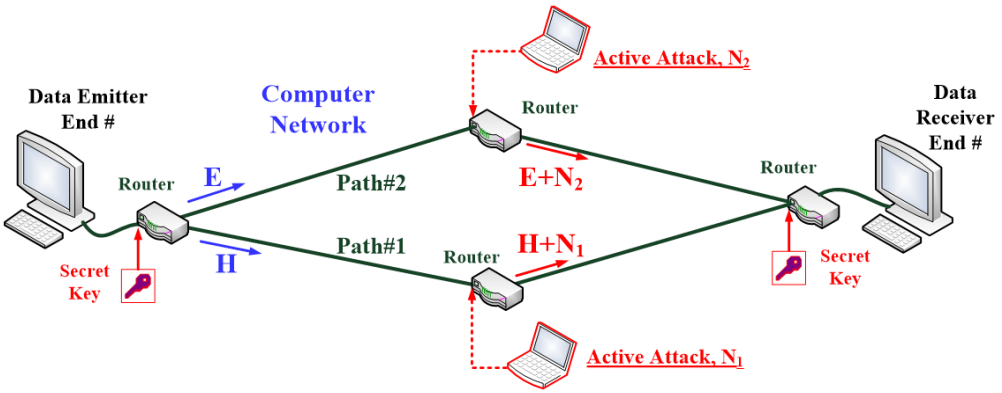

FIGURE 2. Computer Network Communication with active attacks in a small scale PACS.

A sinusoidal linear chirp signal with the sine and cosine of the phase in radians [27], [28] was carried out to generate a multisecret security key, which embeds an encryption in the whole image for 24- or 30-bit color images. Via the computer/telecommunication network, the sequence data of H and E were converted into binary values, and the fragmentation process [29] segmented the sequence data and transmits the cipher data (encrypted image) with the packet sender. At the data receiver end, after converting binary values to decimal ones and combining these fragments in fragmented order, the optimization algorithm-based controller, known as the particle swarm optimization (PSO) algorithm [30]–[32], was used to search the hash weighting parameter to minimize the decryption objective function by iterative computations, which can recover the plain image with a slight loss. In addition, for example, in a small scale picture archiving and communication system (PACS) as presented in Figure 2, any hacker attack, N_1 or N_2, may occur at any routing Path#1 or Path#2. The proposed method provided against manner to estimate the hacker attacks, N_1 or N_2, in routing path and could decrypt the cipher image with two-round decrypted processes. The proposed method provides a secure manner of producing cipher images (H and E), which can also be decrypted with against-hacker attacks in a lossless manner. For 100 mammographic images, including those of case studies on benign and malignant tumors, the peak signal-to-noise ratio (PSNR) [33]–[35] was used to evaluate the two-round decrypted performance of the proposed symmetric cryptographic methods; the experimental results indicate that the recoverable image is reliable and lossless for further diagnostic applications and decision making.

The remainder of this article is organized as follows. Section II describes the methodology, including computer network communication, two-round medical image encryption and decryption, modeling establishment against active attack, and optimization-based controller with *PSO* algorithm for image decryption. Section III describes the medical X-ray image collection, experimental results, and comparison with the other optimization algorithm-based controller. Section IV concludes the paper.

II. METHODOLOGY

A. COMPUTER NETWORK COMMUNICATION

A computer network is a group of computers connected to each other and can communicate and share data and messages, as seen a small scale PACS in Figure 2. A communication packet is a formation unit of data carried by a packet-switched network. This packet is a digital data transmission unit in computer networking and telecommunication. Each packet consists of control information and user data (payload). The control information, including source and destination addresses, sequencing information, and error detection codes, is set in packet headers and trailers, with payload data in between. For digital data transmission from the emitter end to the receiver end, packetized frame provides a sender to transmit the sequence data of H and E via the computer networking or telecommunication at Path#1 and Path#2. At the data emitter end, the sequence data of H and E are first converted to binary values, and fragmentation [29] is performed to segment the sequence data H and E into several smaller fragments, such as a data packet. Data packets can be transmitted along more than one path to the destination across a computer network. In a network (IEEE 802.3 standard [29], [30]), a router forwards data packets from one router to another through the networks. Packetized communication increases the reliability and speed at which digital data can travel across the computer network. At the data receiver end, after converting binary values to decimal ones, defragmentation process is used to put back data packets together in the correct order to reassemble its original sequence data.

During data transmission, security attacks, including passive or active attacks, may intercept the connection and modify the transit of information. Attackers can intercept the transferred information to modify or alter it as active attacks. Active attacks may attempt to modify the information or create a false message at routing Path#1 or Path#2, as seen in Figure 2. The prevention of these attacks is difficult. Hence, this study intends to propose a smart symmetric cryptography against-hacker attacks for medical image infosecurity.

B. TWO-ROUND MEDICAL IMAGE ENCRYPTION AND DECRYPTION

For an $n \times m$ size (in pixels) medical image as a plain image, hash transformation [17], [23]–[26] was used to access the image encryption. Its transformation function consists of a weighting parameter "a" and a matrix of secret key B. At the data emitter end, the hash transformation function was used to transfer the plain image I to the cipher image H in the first-round processing:

$$H = a\mathrm{I} + B = W + B \tag{1}$$

$$B = \begin{bmatrix} \Delta_{11} & \Delta_{12} & \cdots & \Delta_{1m} \\ \Delta_{21} & \Delta_{22} & \cdots & \Delta_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{n1} & \Delta_{n2} & \cdots & \Delta_{nm} \end{bmatrix} \tag{2}$$

where matrix B is the secret key. The number of secret keys was determined by the size of medical image, $n \times m$, and each element as secret key "$\Delta_{nm} = b_{nm}(\sin(\omega_{nm}) + \cos(\omega_{nm}))$," in matrix B can be set using the "chirp function":

$$\omega_{nm} = 2\pi(c_{nm}i^2 + f_0 i) \tag{3}$$

where b_{nm} and c_{nm} are any constant values, $i = 1, 2, 3, .., n$ are $i = 1, 2, 3, \ldots m$ for sinusoid and cosine functions, respectively, and parameter f_0, is the initial frequency, which can be set by authorized people. The human flicker fusion threshold is usually between 60 and 90 Hz. Thus, $f_0 = 60$ Hz was selected due to the human flicker fusion threshold was between 60 and 90 Hz [25].

We can set the multisecret keys in matrix B using Equations (2) and (3) in the key generation phase, with $b_{nm} = 255(2^8 - 1)$ and $f_0 = 60$, where b_{nm} and f_0 are the amplitude and starting frequency of chirp function, respectively; the varying parameters c_{nm}, $c_{nm} \in [1, 9]$. The multisecret keys can be set and certified by authorized people at the data emitter and receiver ends. Then, a dynamic error matrix E can be computed with the plain image, I, and secret key, B, which is subtracted from the cipher image H in second-round process [25], [26]:

$$E = H + B - I \tag{4}$$

For example, given a mammographic image, as seen in

Figure 3, hash transformation with multisecret keys was used to change the pixel values. The results of image encryption are shown in Figure 3 as the two cipher images H and E. As presented in Figure 2, hacker attacks as active attacks will change the content of transmitted messages at Path #1 or Path #2. Suppose that unknown data N are a random active attack at any path at any time that can be divided into two conditions:

- ***Active attack N_1 at routing Path#1*:** The cipher image H will be mixed with N_1, as represented by hacked cipher image H'. The modified cipher images can be observed in Figure 3(a):

$$H' = aI + B + N_1 \tag{5}$$

active attack:

$$N_1 = a_{nm}rand(\sin(c_{nm}f_0\pi i) + \cos(c_{nm}f_0\pi i)) \tag{6}$$

where a_{nm} and c_{nm} are any constant values, and $rand \in [0, 1]$ is the randomization parameter. At the data receiver end, we can perform the image decryption with the secret key, B, and the cipher images H' and E can be decrypted as follows:

$$I' = \frac{H' - B}{a_{opt1}} \quad \text{and } I' = \frac{E - 2B}{(a_{opt1} - 1)}$$
$$\Rightarrow \frac{H' - B}{a_{opt1}} - \frac{E - 2B}{(a_{opt1} - 1)} = 0 \tag{7}$$

Based on optimization algorithms, Equation (7) was used to determine the optimal weighting parameter a_{opt1}, which

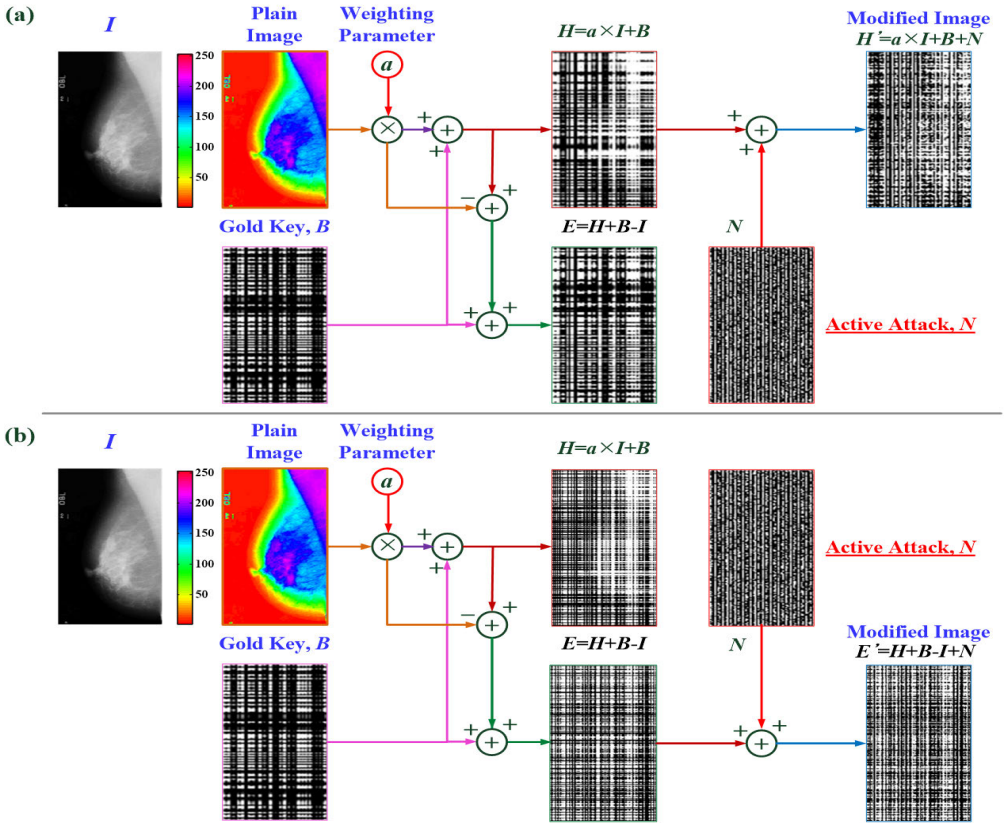

FIGURE 3. Procedure of two-round processes of image encryption (secret key parameters: $b_{nm} = 255$, $f_0 = 60$, and $c_{nm} = 2$).

can minimize the objective function $T_1(a = a_{opt1})$ in the following form:

$$T_1(a_{opt1}) = \min[\frac{H' - B}{a_{opt1}} - \frac{E - 2B}{(a_{opt1} - 1)}] \tag{8}$$

where the restricted conditions are $a_{opt1} \neq 0$ and $a_{opt1} \neq 1$. The mean squared error (MSE) function was computed as follows:

$$MSE_1 = E[T_1(a_{opt1})]^2 \leq \varepsilon = 10^{-2} \tag{9}$$

where parameter ε is the prespecified tolerance error. The optimization-based controller can be used to tune the optimal weighting parameter a_{opt1} and to minimize the MSE_1 in the first-round image decryption process. With Equation (7), the active attack N_1 can be estimated as follows:

$$\frac{H' - B - N_1}{a_{opt1}} - \frac{E - 2B}{(a_{opt1} - 1)} = 0$$
$$\Rightarrow N_1 = (H' - B) - (\frac{a_{opt1}}{a_{opt1} - 1})(E - 2B) \tag{10}$$

Given the estimated attack N_1 at Path#1, we can continuously search for the optimal weighting parameter a_{opt2} to minimize the objective function $T_2(a = a_{opt2})$ in the second-round image decryption process in the following form:

$$T_2(a_{opt2}) = \min[\frac{H' - B - N_1}{a_{opt2}} - \frac{E - 2B}{(a_{opt2} - 1)}] \tag{11}$$

$$MSE_2 = E[T_2(a_{opt2})]^2 \leq \varepsilon = 10^{-2} \tag{12}$$

where the restricted conditions are $a_{opt2} \neq 0$ and $a_{opt2} \neq 1$. Hence, at Path#1, the decrypted medical image I' can be obtained by using Equation (13):

$$I' = \frac{H' - B - N_1}{a_{opt2}} \quad \text{or } I' = \frac{E - 2B}{(a_{opt2} - 1)} \tag{13}$$

- ***Active attack N_2 at routing Path#2*:** The cipher image E will be mixed with N_2 as hacked cipher image E'; the cipher images can be observed in Figure 3(b):

$$E' = H + B - I + N_2 \tag{14}$$

where active attack N_2 can be produced using Equation (6). Hence, we can perform image decryption with the secret key B, and cipher images H and E' can be decrypted as follows [25], [26]:

$$I' = \frac{H - B}{a_{opt3}} \quad \text{and } I' = \frac{E' - 2B}{(a_{opt3} - 1)}$$
$$\Rightarrow \frac{H - B}{a_{opt3}} - \frac{E' - 2B}{(a_{opt3} - 1)} = 0 \tag{15}$$

Based on optimization algorithms, Equation (15) is used to determine the optimal weighting parameter a_{opt3}, which

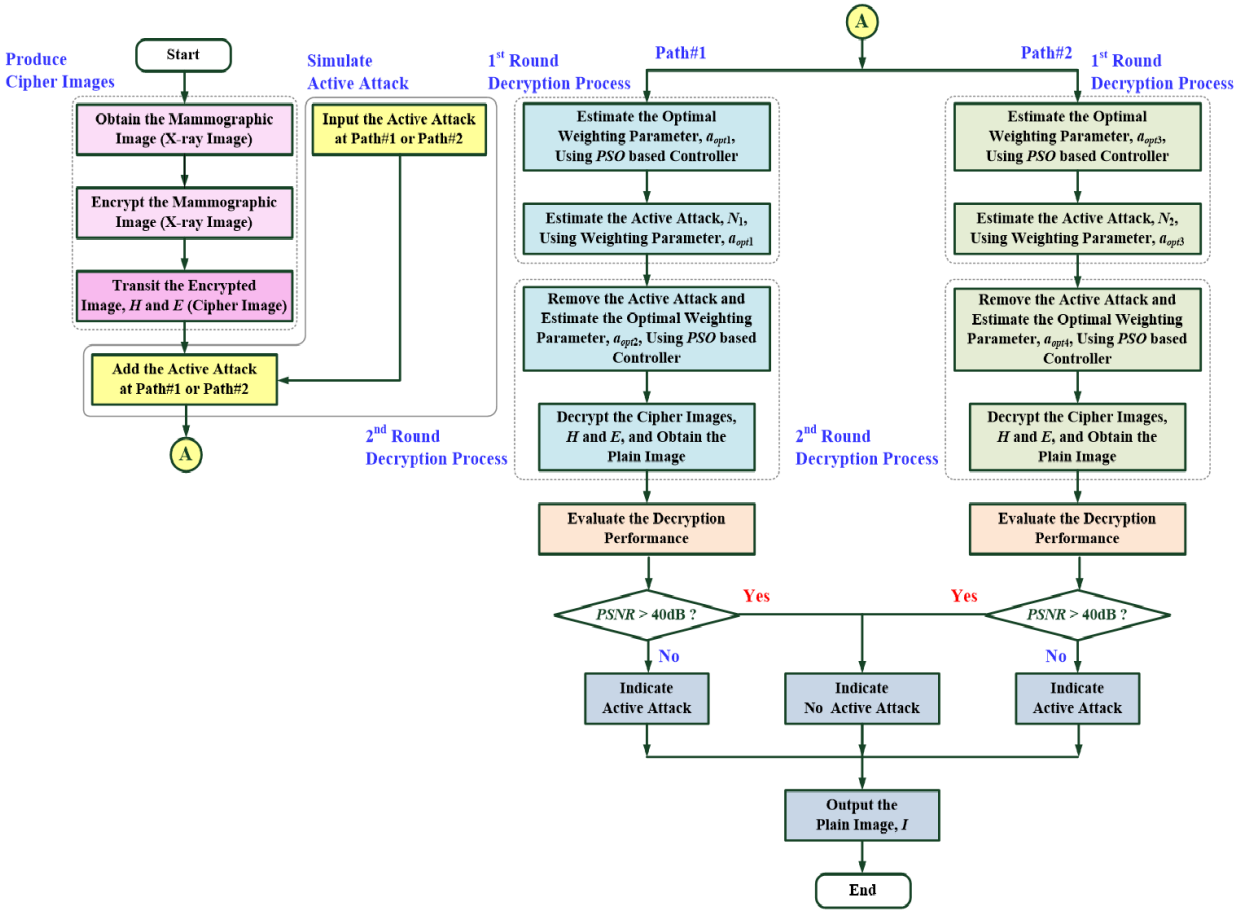

FIGURE 4. Flowchart of medical image two-round encryption and decryption against-hacker attacks.

can minimize the objective function $T_1'(a = a_{opt3})$ in the following form:

$$T_1'(a_{opt3}) = \min[\frac{H-B}{a_{opt3}} - \frac{E'-2B}{(a_{opt3}-1)}] \quad (16)$$

$$MSE_1' = E[T_1'(a_{opt3})]^2 \le \varepsilon = 10^{-2} \quad (17)$$

where the restricted conditions are $a_{opt3} \neq 0$ and $a_{opt3} \neq 1$. The optimization-based controller was used to minimize the MSE_1' in the first-round image decryption to determine the optimal weighting parameter a_{opt3}. With Equation (15), the active attack N_2 can be estimated as follows:

$$\frac{H-B}{a_{opt3}} - \frac{E'-2B-N_2}{(a_{opt3}-1)} = 0$$

$$\Rightarrow N_2 = (E'-2B) - (\frac{a_{opt3}-1}{a_{opt3}})(H-B) \quad (18)$$

Given the estimated attack N_2 at Path#2, we can search for the optimal weighting parameter a_{opt4} to minimize the objective function $T_2'(a = a_{opt4})$ in the second-round decryption process:

$$T_2'(a_{opt4}) = \min[\frac{H-B}{a_{opt4}} - \frac{E'-2B-N_2}{(a_{opt4}-1)}] \quad (19)$$

$$MSE_2' = E[T_2'(a_{opt4})]^2 \le \varepsilon = 10^{-2} \quad (20)$$

where the restricted conditions are $a_{opt4} \neq 0$ and $a_{opt4} \neq 1$. At Path#2, the decrypted medical image I' can be obtained by using Equation (21):

$$I' = \frac{H-B}{a_{opt4}} \quad \text{or } I' = \frac{E'-2B-N_2}{(a_{opt4}-1)} \quad (21)$$

C. OPTIMIZATION-BASED CONTROLLER WITH PSO ALGORITHM

In this study, the optimization-based controller with the *PSO* algorithm [31]–[33] was used to tune the optimal weighting parameter and to minimize the objective function. As shown in the flowchart of two-round image decryption process in Figure 4, the *PSO*-based controller for image decrypted procedure was summarized:

- ***Searching for the optimal weighting parameter a_{opt}***

Let $a_g(p)$ be the current center position of the gth particle agent at the pth search stage, and agent $g = 1, 2, 3, \ldots, G$, where G is the particle population size. Each particle agent is encoded with the center position and velocity components, which are represented by a G-dimensional vector as $a^p = [a_1^p, a_2^p, a_3^p, \ldots, a_g^p, \ldots, a_G^p]$ and $\Delta a^p = [\Delta a_1^p, \Delta a_2^p, \Delta a_3^p, \ldots, \Delta a_g^p, \ldots, \Delta a_G^p]$, respectively. The

particle agent velocity $\Delta a_g(p+1)$ is computed with acceleration factors using Equations (12) and (13).

Velocity component:

$$\Delta a_g(p+1) = [\Delta a_g(p) + c_1 rand_1(abest_g - a_g(p)) + c_2 rand_2(abest - a_g(p))] \quad (22)$$

Adaptive acceleration factors:

$$c_1 = (b_1 - a_1)\frac{p}{p_{\max}} + a_1, \quad c_2 = (b_2 - a_2)\frac{p}{p_{\max}} + a_2 \quad (23)$$

where *abest* is the global best in the particle population; $abest_g$ is the individual best at pth search stage; $p = 1, 2, 3, \ldots, p_{max}$, p_{max} is the maximum iteration number; the parameters include $rand_1 \in (0, 1)$ and $rand_2 \in (0, 1)$; parameters c_1 and c_2 are the time-varying acceleration factors considered as "cognitive component c_1" from 2.5 to 0.5 (representing the individuality coefficient) and "social component c_2" from 0.5 to 2.5 (representing the group coefficient), respectively [31]–[33]; a_1, b_1, a_2, and b_2 are constant values.

When the value of cognitive component c_1 is high, the search region will expand at each search stage. Multiple particle agents are allowed to determine the individual best solution $abest_g$ around the search space. By monotonously decreasing the parameters c_1 and c_2, the search region will gradually approach the global best solution *abest* during fine tuning at the end of the search stage. The term $p/p_{\max}$ is also used to control the acceleration parameters c_1 and c_2, which pull each particle agent toward the best solution and then update the particle agent's center position $a_g(p+1)$ using Equation (24).

$$\textit{Center position}: \quad a_g(p+1) = a_g(p) + \Delta a_g(p+1) \quad (24)$$

If the maximum number of iterations p_{max} is achieved, or the objective function *MSE* (Equations, (9), (12), (17), and (20)) is less than the specified tolerance error $\varepsilon = 10^{-2}$, then the *PSO* iterative computations are terminated. When the optimal weighting parameter a_{opt} is obtained, then the decrypted medical image *I'* can be obtained using Equation (13) or (21).

- ***Evaluation of the decryption performance***

After medical image encryption and decryption processes, the *PSNR* [34]–[36] was used to measure the distortion between the plain medical image *I* and decrypted image *I'*:

$$MSE_I(I, I') = \frac{1}{nm}\sum_{i=1}^{n}\sum_{j=1}^{m}[I(i,j) - I'(i,j)]^2 \quad (25)$$

$$PSNR(I, I') = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE_I}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE_I}}\right) \quad (26)$$

where *I* is the medical image as plain image; *I'* is the decrypted medical image from cipher image to plain image that can be obtained by using Equations (13) and (21); MAX_I is the maximum pixel values in image *I'*; $MAX_I = \max(I')$, where each point is represented by 8- or 10-bit depth images, and the maximum value is 255 or 1023. Index *PSNR* (in dB) specifies as a nonnegative value obtained via the MSE_I; it indicates the differences between the images before image encryption and after image decryption. When the *PSNR* is high, then images *I* and *I'* are similar. If index MSE_I has a small value, it will be better. The index *PSNR* is an approach to human perception of recovery quality. The larger the *PSNR* value (dB), the smaller the loss is, and the image could not be observed with the naked eyes. Through experiments, the mean *PSNR* value obtained without active attacks is greater between about 40 and 80 dB. In our study, the threshold value can be set to evaluate the decryption performance:

$$Index^* = \begin{cases} 1, & 0 < PSNR \le 40dB \\ 0, & PSNR > 40dB \end{cases} \quad (27)$$

If *Index** is "1," then, the signal of active attack means that the decrypted image has a promising quality ($0 < PSNR \le 40$ dB). This finding reflects the recovery of the plain image from the cipher image with the active attack N_1 or N_2. Otherwise, we can obtain good quality to recover plain images at higher than 40 dB. *Index** with a value of "0" implies the lack of specific active attacks.

III. EXPERIMENTAL RESULTS AND DISCUSSION

A. MAMMOGRAPHIC IMAGE COLLECTION

In this study, mammographic images were collected from 322 films from the Mammographic Image Analysis Society (MIAS, United Kingdom National Breast Screening Program) Digital Mammogram Database [37- 38], including 204 normal breast X-ray images and 118 abnormalities (benign and malignant tumors) in breast X-ray images. Digitization was performed on a Joyce–Loebl scanning microdensitometer (SCANDIG-3, at the Royal Marsden Hospital) at a spatial resolution of 50 μm square pixel edge with a linear response in the optical density range of 0.0 to 3.2 at 8 bits per pixel. The 50 μm pixel edge was a compromise between scanning durations, image resolutions, and file sizes [38]. Clinical information, such as image size, image category, background tissue, class of abnormality, and severity of abnormality (benign or malignant tumor), were inputted into the database for further computer vision research, as seen in Table 1. The image categories were confirmed and agreed upon by expert radiologists (biomarker). Breast X-ray images, including 50 malignant and 50 benign tumor images, were selected from MIAS Digital Mammogram Database and converted into Tagged Image File format.

Each image was digitized to a resolution of 96 × 96 dots per inch, which produced 24 bits per pixel (colored image), and was incorporated into a 250 × 380 pixel image ($n = 1, 2, \ldots, 250$; $m = 1, 2, \ldots, 380$; 95,000 pixels), as presented in the right lateral views in Figures 5(a) and 6(a). The proposed two-round symmetric cryptographic method was designed on a tablet PC (Intel® Xeon®, CPU

TABLE 1. MIAS (United Kingdom) digital mammogram database for experimental tests [37], [38].

Image Category	Background Tissue and Severity of Abnormality			Totals	
	Fatty	Fatty-Glandular	Dense Breast		
Calcifications	B: 2 M: 4	B: 2 M: 4	B: 3 M: 5	B: 7 M: 13	20
Circumscribed Masses	B: 2 M: 2	B: 2 M: 2	B: 3 M: 0	B: 7 M: 4	11
Spiculated Masses	B: 2 M: 4	B: 2 M: 3	B: 6 M: 2	B: 10 M: 9	19
Architectural Distortions	B: 4 M: 2	B: 2 M: 4	B: 4 M: 4	B: 10 M: 10	20
Asymmetries	B: 2 M: 2	B: 3 M: 2	B: 3 M: 3	B: 8 M: 7	15
Miscellaneous	B: 4 M: 4	B: 3 M: 2	B: 1 M: 1	B: 8 M: 7	15
Totals	34	31	35	100	100

Note: B: Benign Tumor; M: Malignant Tumor

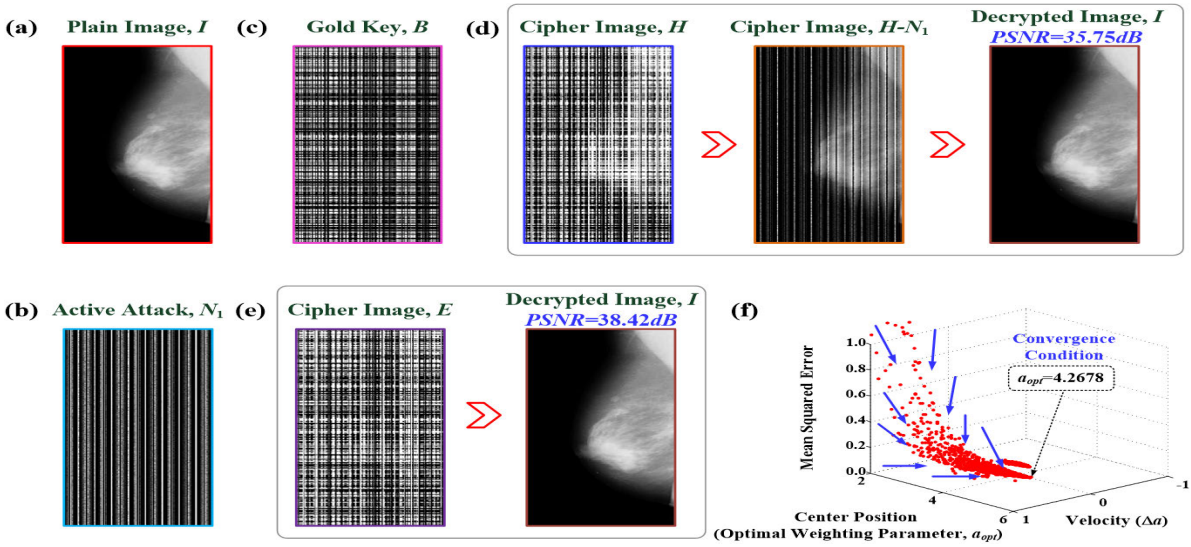

FIGURE 5. Experimental results for active attack at Path#1. (a) Plain image, (b) active attack, (c) gold key, (d) decrypted image from cipher image *H*, (e) decrypted image from cipher image *E*, and (f) MSE versus each agent's center positions and velocities.

E5-2620, v4, 2.1 GHz and 64 GB of RAM; GPU: NVIDIA Quadro P620, 64-bits Windows 10.0 operating system) using a high-level graphical programming language in the LabVIEW programming software and MATLAB software (NI^{TM}, Austin, Texas, USA). The MIAS Digital Mammogram Database was used to validate the proposed algorithms. The experimental procedure included the (1) production of cipher image H using the hash transformation with a secret gold key B and computation of the dynamic error E; (2) simulation of active attacks N_1 or N_2 at routing Path#1 and Path#2; (3) estimation of the active attack using the first round of optimization-based controller with the *PSO* algorithm; (4) decryption of the cipher images using the second round of optimization-based controller with *PSO* algorithm; (5) evaluation of the image decryption performance using the *PSNR* index. For available digital mammographic images, the proposed cryptography method could validate the good performance and robustness, as shown in detail below.

B. EXPERIMENTAL RESULTS OF MEDICAL IMAGE ENCRYPTION AND DECRYPTION

In medical image encryption, the pixels of each X-ray image were represented using 8 bits per sample (24/3), and we could set the multisecret gold keys in matrix B using the chirp function with the fixed parameters $b_{nm} = 255$, $f_0 = 60$, and $c_{nm} = 6$ for overall X-ray image encryption and decryption experiments, as shown in Figures 5(c) and 6(c). These symmetric multisecret gold keys could be dynamically generated at any time in both data emitter end and data receiver end by authorized individuals. Therefore, identical gold key B could be set for both encryption of the plain image and decryption of the cipher image. Then, as shown in Figure 2, we could simulate any active attack N_1 or N_2 at routing Path#1 (Figure 5(b)) and Path#2 (Figure 6(b)), which could be randomly produced using Equation (6). We used two experimental results for active attacks as shown below:

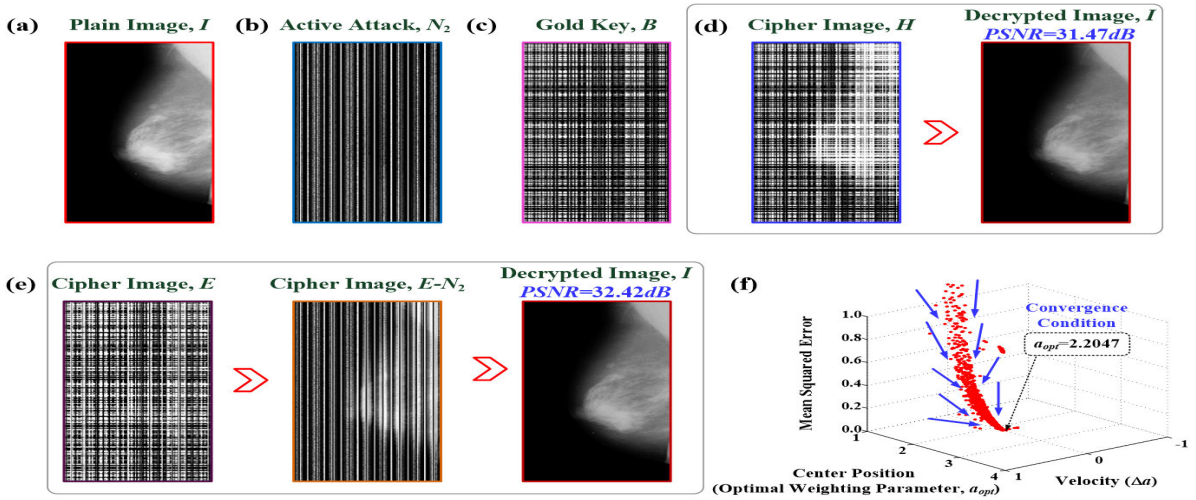

FIGURE 6. Experimental results for active attack at Path#2. (a) Plain image, (b) active attack, (c) gold key, (d) decrypted image from cipher image *H*, (e) decrypted image from cipher image *E*, and (f) MSE versus each agent's center positions and velocities.

TABLE 2. Experimental results of medical image decryption for against hacker attack.

Active Attack	At Routing Path#1		At Routing Pat #2	
Image Category	Malignant Tumor (right lateral view)	Benign Tumor (right lateral view)	Malignant Tumor (right lateral view)	Benign Tumor (right lateral view)
Active Attack Estimation	$H' = aI + B + N_1$ (5) $\frac{H' - B - N_1}{a_{opt1}} - \frac{E - 2B}{(a_{opt1} - 1)} = 0$ Active Attack: $N_1 = (H' - B) - (\frac{a_{opt1}}{a_{opt1} - 1})(E - 2B)$ (10)		$E' = H + B - I + N_2$ (14) $\frac{H - B}{a_{opt3}} - \frac{E' - 2B - N_2}{(a_{opt3} - 1)} = 0$ Active Attack: $N_2 = (E' - 2B) - (\frac{a_{opt3} - 1}{a_{opt3}})(H - B)$ (18)	
Image Decryption	$I' = \frac{H' - B - N_1}{a_{opt2}}$, $I' = \frac{E - 2B}{(a_{opt2} - 1)}$ (13)		$I' = \frac{H - B}{a_{opt4}}$, $I' = \frac{E' - 2B - N_2}{(a_{opt4} - 1)}$ (21)	
Security Parameter	Multi Secret Keys: $\Delta_{nm} = b_{nm}(\sin(\omega_{nm}) + \cos(\omega_{nm}))$, $\omega_{nm} = 2\pi(c_{nm} i^2 + f_0 i)$, $i = 1, 2, 3, \ldots, n$ and $i = 1, 2, 3, \ldots, m$ for sin(•) and cos(•) functions; Weighting Parameter: $a \in \mathrm{R}^+$ ($a \geq 2$) $b_{nm} = 255$, $c_{nm} \in \mathrm{R}^+$ ($c_{nm} \neq 0$), $f_0 = 60 \sim 90$ Parameters, $b_{nm} = 255$, $c_{nm} = 6$, and $f_0 = 60$ were selected in this study.			
Objective Function	1st Round: $T_1(a_{opt1}) = \min[\frac{H' - B}{a_{opt1}} - \frac{E - 2B}{(a_{opt1} - 1)}]$ 2nd Round: $T_2(a_{opt2}) = \min[\frac{H' - B - N_1}{a_{opt2}} - \frac{E - 2B}{(a_{opt2} - 1)}]$		1st Round: $T_1'(a_{opt3}) = \min[\frac{H - B}{a_{opt3}} - \frac{E' - 2B}{(a_{opt3} - 1)}]$ 2nd Round: $T_2'(a_{opt4}) = \min[\frac{H - B}{a_{opt4}} - \frac{E' - 2B - N_2}{(a_{opt4} - 1)}]$	
Optimization Algorithm	Two-round *PSO* Algorithm based Controller		Two-round *PSO* Algorithm based Controller	
Iteration Computation	≤25	≤25	≤25	≤25
Mean CPU Execution Time (s)	48.3185 ± 2.5389	47.2282 ± 1.5870	51.6756 ± 8.1684	48.1639 ± 4.9284
Mean Desired Weighting Parameter	3.2262 ± 0.0749	3.3673 ± 0.1809	2.3487 ± 0.2056	2.8976 ± 0.5443
Mean *PSNR* (dB)	39.2297 ± 12.5917	33.5519 ± 5.1280	22.0576 ± 15.7000.	23.8195 ± 9.9017.

• ***Simulation of the Active Attack N_1 at Routing Path#1***

Suppose the active attack N_1 at routing Path#1. First, the weighting value W was computed with the weighting parameter $a = 4.0000$. The cipher image H was produced by mixing the weighting value W, multisecret gold key B, and active attack N_1 in whole image using Equations (5)

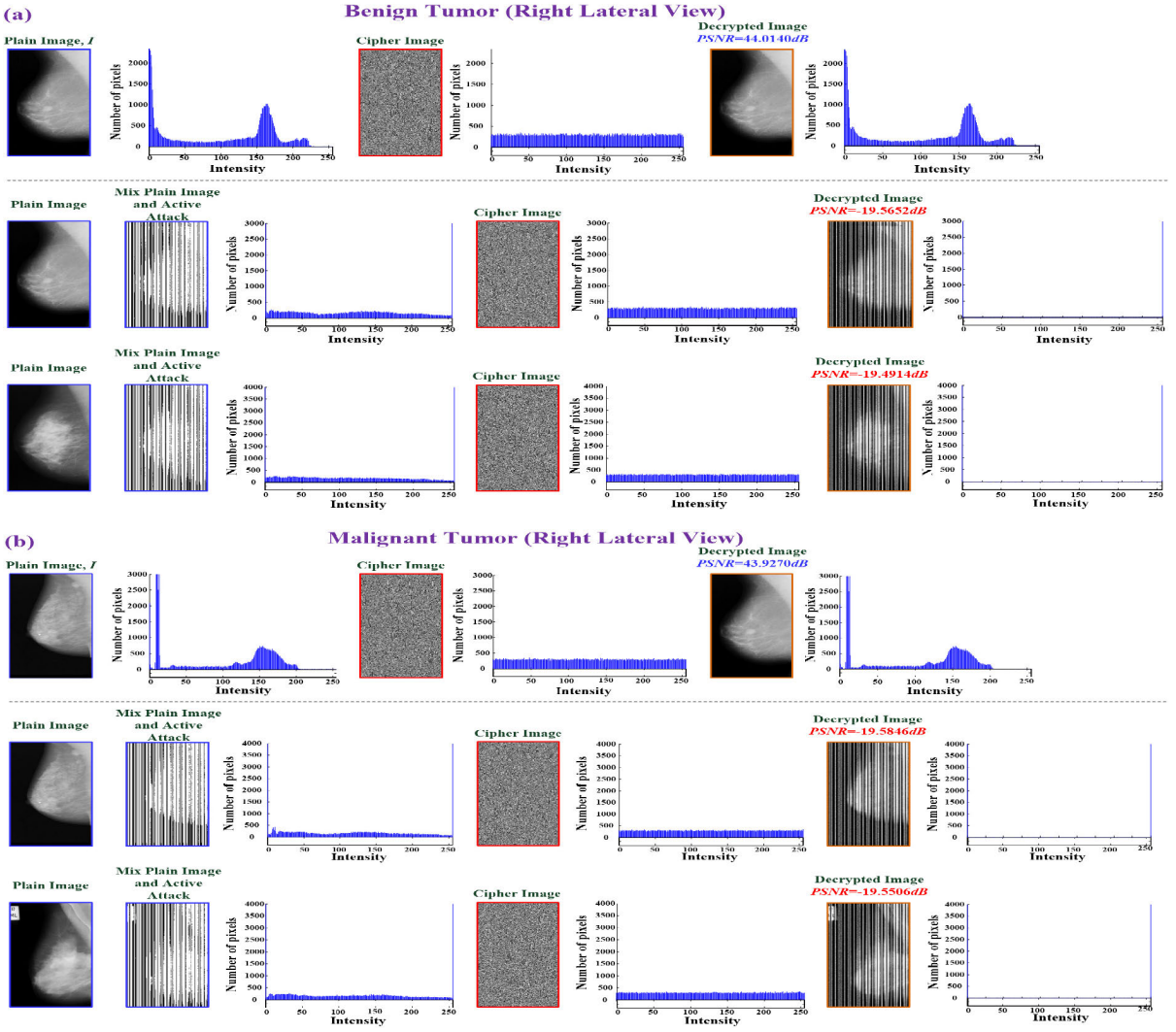

FIGURE 7. Experimental results of X-ray image (right lateral view) encryption and decryption using a CSS with a fuzzy rule-based controller for benign and malignant tumors. (a) Experimental results for benign tumors, including the plain image, cipher image, decrypted image, plain image histogram, shuffling histogram, and decrypted image histogram. (b) Experimental results for malignant tumors, including the plain image, cipher image, decrypted image, plain image histogram, shuffling histogram, and decrypted image histogram.

and (6). Then, the dynamic error, as the cipher image E, can be computed using Equation (4). Figures 5(d) and 5(e) show the cipher images H and E, respectively. In the first-round image decryption process, *PSO*-based controllers are used to estimate the active attack N_1 and to produce the cipher image H - N_1 (Figure 5(d)) using Equations (5) to (9). The second-round process decrypted the cipher images H - N_1 and E to the plain image I' using Equations (10) to (12). For the cipher images H - N_1 and E and at specific convergence condition, the *PSO*-based controller performed $\leq$25 iteration computations and used a mean CPU execution time of <6.1058 s to search the optimal weighting parameter $a_{opt2} = 4.2678$, as shown in Figure 5(f). Given the weighting parameter $a_{opt2} = 4.2678$, the decrypted image I' could be recovered by using Equation (13). The index $PSNR = 35.7512$ dB and $PSNR = 38.4258$ dB were obtained, which were less than the 40 dB needed to recover the encrypted image with the active attack at routing Path#1.

- ***Simulation of the Active Attack N_2 at Routing Path#2***

Suppose the active attack N_2 at routing Path#2. The weighting value W is computed with the weighting parameter, $a = 2.0000$. The cipher image H was produced by mixing the weighting value W and multisecret gold key B, as shown in Figure 6(d). Then, the dynamic error E was computed and then mixed with the active attack N_2 using Equations (6) and (14), as indicated in Figure 6(e). In the first-round decryption process, *PSO*-based controllers were used to estimate the active attack N_2 and to produce the cipher image E - N_2 (Figure 6(e)) using Equations (15) to (17). Second-round process decrypted the cipher images H and E - N_2 to the plain image I' using Equations (18) to (20). For the cipher images H and E - N_2 and at specific convergence

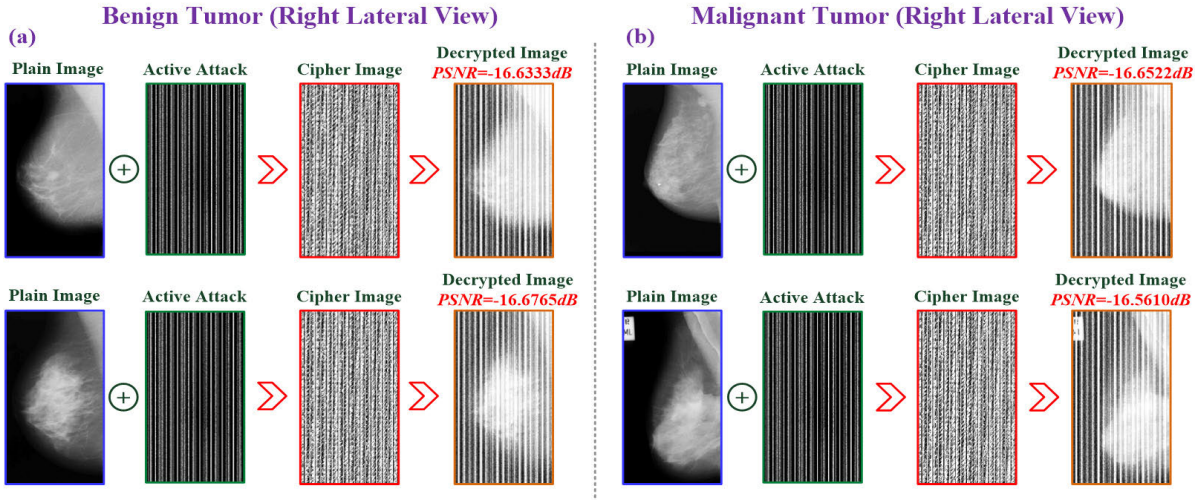

FIGURE 8. Experimental results of X-ray image (right lateral view) encryption and decryption using an AT for benign and malignant tumors. (a) Experimental results for active attack in X-ray images of benign tumor; (b) experimental results for active attack in X-ray images of malignant tumor.

condition, the *PSO*-based controller performed ≤25 iteration computations and required a mean CPU execution time of <5.1012 s to search the optimal weighting parameter $a_{opt4} = 2.2047$ (Figure 6(f)). Given the weighting parameter $a_{opt4} = 2.2047$, the plain image *I'* could be recovered by using Equation (21). The index $PSNR = 31.4711$ dB and $PSNR = 32.4225$ dB were obtained and were less than the needed 40 dB to recover the encrypted image with the active attack at routing Path#2. For the 100 X-ray images, which consisted of 50 benign tumor and 50 malignant tumor images, the mean $PSNR = 33.5057 \pm 14.1559$ dB and $PSNR = 30.3078 \pm 8.4617$ dB were achieved for the recovered the encrypted images with active attack, respectively. The proposed cryptography method required a mean execution time of approximately 48.48889 ± 4.2406 s to complete the image encryption and decryption processes for the X-ray images, as seen in Table 2. Meanwhile, the index was $0 < PSNR < 40$ dB, and the output would indicate the warning sign for the authorized people.

C. COMPARISON WITH THE TRADITIONAL CRYPTOGRAPHIC METHOD

In this research topic, chaotic system, logistic map [36]–[39], chaotic synchronization system (CSS) [43], and Arnold transformation (AT) [44], [45] had been performed with the diffusion and permutation-based image cryptography method design for grayscale image, color image, video, multimedia, or optics communication. These methods shuffled the pixel position and varied the pixel values between the plain and encrypted images. Given the high-security requirement, chaotic systems such as first-, third-, or high-order systems with digital-image schemes had been proposed to produce chaotic sequences, so as to enlarge image gray levels or to generate the pseudorandom keystream for sequence generation and random mixing to ensure communication security. In this study, a Sprott chaotic system, fuzzy rules, and a sliding-mode controller [46], [47] were integrated into a discrete chaotic synchronous cryptographic system (CSCS). The Sprott chaotic system consisted of a master and slave chaotic systems. 49 fuzzy rules are used to control the controller parameters (14 input membership functions and seven output membership functions) [47]. Then, a sliding-mode controller was used to synchronize the trajectories of a master and a slave system with fuzzy rules to control a two-system synchronization. For X-ray images without any active attack, *CSCS* could recover the plain image with a slight loss from cipher images, with $PSNR = 44.0140$ dB and $PSNR = 43.9270$ dB for decrypted images of benign (Figure 7 (a)) and malignant tumors (Figure 7 (b)), respectively. The results for the *CSCS* method show feasibility for image encryption and decryption. This method required a mean execution time of approximately 41.1902 ± 1.2842 s for the X-ray images. However, the *CSCS* could not adequately recover the plain images involving any possible active attack, as presented by index $PSNR < 0.0000$ dB in Figures 7 (a) and (b). The *CSCS* had no capability against any active attack. In addition, *CSCS* using fuzzy rule-based controller requires initial value condition assignments (sensitivity to initial conditions), 3D chaotic maps, *CSS* parameter assignment (three system parameters), fuzzy rules, fuzzy input and output membership function assignment, and controller parameter assignment (four controller parameters) [47]. Hence, this cryptography scheme would increase the computational complexity and incur the high commercialization costs.

The *AT* method was also applied for image encryption and decryption [44], [45]; it could change the layout of gray values by rearranging the coordinate of pixels. The layout was a 2D invertible chaotic map [48]. Thus, the matrix of plain image could be changed into a new matrix, thereby resulting in a scrambled version to achieve better security. This method

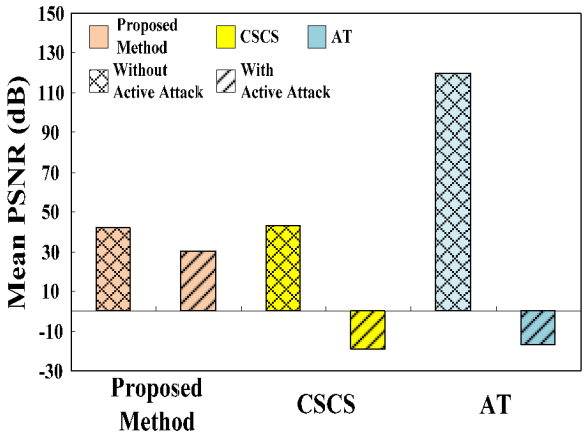

FIGURE 9. Mean *PSNR* (dB) for image decryption with and without active attack in proposed cryptography method, *CSCS* method, and AT method.

only scrambled the pixel positions by iterative computations and was invertible without loss of information. The grayscale values were intact in the whole image. However, the AT parameters were fixed. Thus, the cipher image would be deduced by randomly applying inverse AT several times. The AT method could not recover the plain images involving any possible active attack, as indicated by index $PSNR < 0.0000$ dB in Figures 8 (a) and (b). The AT parameters were fixed for image encryption, which would favor hacker attacks. The AT method had no capability against any active attack either. This method required a mean execution time of approximately 86.6658 ± 2.3230 s for the X-ray images. The index *PSNR* indicated that the image content could not be visually identified by authorized observers for the *CSCS* and *AT* methods. The recoverability capabilities of the *CSCS* and *AT* methods were better than that of the proposed cryptography method, as seen in Figure 9. However, both were ineffective against possible active attacks at routing paths in a computer network. By contrast, the proposed method surpassed the *CSCS* and *AT* methods in terms of computational speed, and it reduced the computational complexity. The proposed method can also recover plain images or prevent any active attack, indicating that the recoverable image is reliable and lossless and can be used for further diagnostic applications, as presented by the mean $PSNR \geq 40$ dB for "without active attack" and $0 < PSNR < 40$ dB for "with active attack" in Figure 9.

IV. CONCLUSION

A two-round symmetric cryptography method against-hacker attack had been proposed for digital X-ray images in this study. The image encryption was carried out in a two-round process by hash transformation with weighting parameters and multisecret keys. Multisecret keys were generated by chirp function. First-round process was used to modify the pixel values by hash transformation and multisecret keys and to produce the dynamic error in the second-round process, thus protecting the encrypted images against passive hackers. A small-scale health information system was established to simulate the computer network communication/telecommunication and active attack at any possible routing path. Two-round decryption process with *PSO*-based controller was used to search the decryption weighting parameter by using iterative computations. In the first-round process, the proposed decrypted models, as depicted by Equations, (5), (10), (14), and (18), were employed to estimate the active attack at routing Path#1 or Path#2. Then, the second-round process was employed to recover the plain image. For 50 malignant and 50 benign tumor images, the proposed cryptography method not only showed promising results to protect the privacy of individual anamnesis images but also recovered the plain image with a slight loss for X-ray image without or with active attack. The proposed method required 48.48889 ± 4.2406 s execution time. The mean *PSNR* were 33.5057 ± 14.1559 and 30.3078 ± 8.4617 dB for measuring the quality of decrypted images that could be validated against active attacks. The index *PSNR* declined in the range of 0 – 40 dB. The output would serve as the warning sign for authorized people and require message retransmission from the data emitter end and data receiver end. Hence, the confidentiality, recoverability, and availability of digital-image infosecurity in clinical applications could be proven for further imaging examination and diagnosis and be applied to medical images, such as those obtained ultrasonography, X-ray, MRI, or computed tomography.

ABBREVIATIONS

PACS	Picture Archiving and Communication System
CT	Computed Tomography
MRI	Magnetic Resonance Imaging
DHK	Diffie-Hellman Key
RFID	Radio Frequency Identification
TMIS	Telecare Medicine Information System
XOR	Exclusive
CKG	Chaotic Key Generator
PSO	Particle Swarm Optimization
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error
MIAS	Mammographic Image Analysis Society
CSS	Chaotic Synchronization System
AT	Arnold Transformation
CSCS	Chaotic Synchronous Cryptographic System

REFERENCES

[1] BBC News Services. (2019). *Singapore Personal Data Hack Hits 1.5m, Health Authority Says*. [Online]. Available: https://www.bbc.com/news/world-asia-44900507

[2] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 5, pp. 891–899, Sep. 2012.

[3] K. Shankar, *Secure Image Transmission in Wireless Sensor Network Applications* (Lecture Notes in Electrical Engineering), vol. 564. Cham, Switzerland: Springer, 2019.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[5] 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.
[6] N. Patanachai, B. Uyyanonvara, C. Sinthanayothin, W. Tharanon, P. Sompot, and K. Muandet, "PACS (Picture archiving communication system) for dentistry," in *Proc. 5th Int. Conf. Elect. Eng./Electron., Comput., Telecommun. Inf. Technol.*, Krabi, Thailand, 2008, pp. 77–80.
[7] W. San-Urn and N. Chuayphan, "A lossless physical- layer encryption scheme in medical picture archiving and communication systems using highly-robust chaotic signals," in *Proc. Biomed. Eng. Int. Conference.*, Fukuoka, Japan, 2014, pp. 1–5.
[8] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *J. Med. Syst.*, vol. 40, no. 5, p. 117, May 2016, doi: 10.1007/s10916-016-0474-9.
[9] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system," *J. Med. Syst.*, vol. 39, no. 8, Aug. 2015, doi: 10.1007/s10916-015-0260-0.
[10] Y. Huang and X.-S. Yang, "Hyperchaos and bifurcation in a new class of four-dimensional hopfield neural networks," *Neurocomputing*, vol. 69, nos. 13–15, pp. 1787–1795, Aug. 2006.
[11] S. Behnia, A. Akhshani, A. Akhavan, and H. Mahmodi, "Applications of tripled chaotic maps in cryptography," *Chaos, Solitons Fractals*, vol. 40, no. 1, pp. 505–519, Apr. 2009.
[12] N. Bigdeli, Y. Farid, and K. Afshar, "A robust hybrid method for image encryption based on hopfield neural network," *Comput. Electr. Eng.*, vol. 38, no. 2, pp. 356–369, Mar. 2012.
[13] A. Nag, J. P. Singh, S. Khan, S. Ghosh, S. Biswas, D. Sarkar, and P. P. Sarkar, "Image encryption using affine transform and XOR operation," *Proc. Int. Conf. Signal Process., Commun., Comput. Netw. Technol.*, Thuckafay, India, 2011, pp. 309–312.
[14] R. Amirtharaj and N. Aarthie, "Image encryption: An information security perceptive," *J. Artif. Intell.*, vol. 7, no. 3, pp. 123–135, Mar. 2014.
[15] S. Madhu and M. Ali Hussain, "Securing medical images by image encryption using key image," *Int. J. Comput. Appl.*, vol. 104, no. 3, pp. 30–34, Oct. 2014.
[16] A. Singh and N. Dhanda, "DIP using image encryption and XOR operation affine transform," *IOSR J. Comput. Eng.*, vol. 17, no. 2, pp. 7–15, 2015.
[17] 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.
[18] K. Narendra Pareek, V. Partidar, and K. Krishan Sud, "Diffusion-substitution based gray image encryption scheme," *Digit. Signal Process.*, vol. 23, pp. 894–901, Oct. 2013.
[19] A. Jolfaei, X.-W. Wu, and V. Muthukkumaramy, "Comments on the security of 'Diffusion–substitution based gray image encryption' scheme," *Digit. Signal Process.*, vol. 32, pp. 34–36, Sep. 2014.
[20] Z. M. Z. Muhammad and F. Ozkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019.
[21] Z. M. Z. Muhammad and F. Ozkaynak, "An image encryption algorithm based on chaotic selection of robust cryptographic primitives," *IEEE Access*, vol. 8, pp. 56581–56589, 2020.
[22] S. H. Strogatz, *Nonlinear Dynamics and Chaos With Applications to Physics* (Biology, Chemistry and Engineering), 2nd ED., New York, NY, USA: Taylor & Francis, 2014.
[23] P. Li and K.-T. Lo, "A content-adaptive joint image compression and encryption scheme," *IEEE Trans. Multimedia*, vol. 20, no. 8, pp. 1960–1972, Aug. 2018.
[24] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic DNA encoding," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 3901014.
[25] P.-Y. Chen, J.-X. Wu, C.-M. Li, C.-L. Kuo, N.-S. Pai, and C.-H. Lin, "Medical image infosecurity using hash transformation and optimization-based controller in a health information system: Case study in breast elastography and X-ray image," *IEEE Access*, vol. 8, pp. 61340–61354, 2020.
[26] P.-Y. Chen, J.-X. Wu, C.-M. Li, C.-L. Kuo, N.-S. Pai, and C.-H. Lin, "Symmetric cryptography with shift 2n-1, Hash transformation, optimization-based controller for medical image infosecurity: Case study in mammographic image," *IEEE Photon. J.*, vol. 12, no. 3, 2020, pp. 1–16.
[27] Y. M. Benane, D. Bujoreanu, C. Cachard, B. Nicolas, and O. Basset, "An enhanced chirp modulated golay code for ultrasound diverging wave compounding," in *Proc. 26th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2018, pp. 81–85.
[28] C.-C. Shen and C.-H. Lin, "Chirp-encoded excitation for dual-frequency ultrasound tissue harmonic imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 59, no. 11, pp. 2420–2430, Nov. 2012.
[29] (2019). *IEEE 802 LAN/MAN Standards Committee*. [Online]. Available: http://grouper.ieee.org/groups/802/
[30] M. A. Mohamed, F. W. Zaki, and A. M. EI-Mohandes, "Novel fast encryption algorithms for multimedia transmission over mobile WimMax Networks," *IJCSI Int. Comput. Sci.*, vol. 6, no. 3, 2012, pp. 60–67.
[31] T.-H.-S. Li, C.-Y. Liu, P.-H. Kuo, N.-C. Fang, C.-H. Li, C.-W. Cheng, C.-Y. Hsieh, L.-F. Wu, J.-J. Liang, and C.-Y. Chen, "A three-dimensional adaptive PSO-based packing algorithm for an IoT-based automated e-Fulfillment packaging system," *IEEE Access*, vol. 5, pp. 9188–9205, 2017.
[32] C.-D. Kan, W.-L. Chen, C.-H. Lin, J.-N. Wang, P.-J. Lu, M.-Y. Chan, and J.-T. Wu, "Customized handmade pulmonary valved conduit reconstruction for children and adult patients using meta-learning based intelligent model," *IEEE Access*, vol. 6, pp. 21381–21396, 2018.
[33] 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.
[34] H. Chougrad, H. Zouaki, and O. Alheyane, "Deep convolutional neural networks for breast cancer screening," *Comput. Methods Prog. Biomed.*, vol. 157, pp. 19–30, Apr. 2018.
[35] A. Mahmood, T. Hamed, C. Obimbo, and R. Dony, "Improving the security of the medical images," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 9, pp. 137–146, 2013.
[36] 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.
[37] (2019). *Mammographic Image Analysis Society (MIAS) Database v1.21*. [Online]. Available: https://www.repository.cam.ac.uk/handle/1810/250394
[38] J. Suckling, J. Parker, D. R. Dance, S. Astley, I. Hutt, C. R. M. Boggis, I. Ricketts, E. Stamatakis, N. Cerneaz, S. L. Kok, P. Taylor, D. Betal, and J. Savage, "The mammographic image analysis society digital mammogram database," *Exerpta Medica., Int. Congr. Series9*, vol. 106, pp. 375–378, Oct. 1994.
[39] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review," *J. Adv. Res.*, vol. 7, no. 2, pp. 193–208, Mar. 2016.
[40] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.
[41] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Opt. Commun.*, vol. 282, no. 11, pp. 2123–2127, Jun. 2009.
[42] L. Zhang, S. Zhu, and S. Tang, "Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 2, pp. 465–475, Mar. 2017.
[43] H.-T. Yau, T.-H. Hung, and C.-C. Hsieh, "Bluetooth based chaos synchronization using particle swarm optimization and its applications to image encryption," *Sensors*, vol. 12, no. 6, pp. 7468–7484, Jun. 2012.
[44] Q. Guo, Z. Liu, and S. Liu, "Color image encryption by using arnold and discrete fractional random transforms in IHS space," *Opt. Lasers Eng.*, vol. 48, no. 12, pp. 1174–1181, Dec. 2010.
[45] M. R. Abuturab, "Color image security system based on discrete hartley transform in gyrator transform domain," *Opt. Lasers Eng.*, vol. 51, no. 3, pp. 317–324, Mar. 2013.
[46] D. I. R. Almeida, J. Alvarez, and J. G. Barajas, "Robust synchronization of Sprott circuit using sliding mode control," *Chaos Solitons Fractals*, vol. 30, 2006, pp. 11–18.
[47] C.-L. Kuo, "Design of an adaptive fuzzy sliding-mode controller for chaos synchronization," *Int. J. Nonlinear Sci. Numer. Simul.*, vol. 8, no. 4, pp. 631–636, Jan. 2007.
[48] S. Bharath, "Data hiding in encrypted images using Arnold transform," *ICTACT J. Image Video Process.*, vol. 7, no. 1, pp. 1339–1344, Aug. 2016.

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

From 2014 to 2017, he was a Postdoctoral Research Fellow with the National Synchrotron Radiation Research Center, X-ray and IR Imaging Group, Hsinchu, Taiwan. From 2017 to 2018, he was a Postdoctoral Research Fellow with the Department of Niche Biomedical LLC, California NanoSystems Institue, UCLA, Los Angeles, CA, USA. Since 2019, he has been an Assistant Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan. 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.

NENG-SHENG PAI received the B.S. and M.S. degrees from the Department of Automatic Control Engineering, Feng Chia University, Taichung, Taiwan, R.O.C., 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.

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

YU-CHI PU received the B.S. degree in mathematics from National Taiwan University, in 1993, the M.S. degree in information science from National Tsing Hua University, in 1995, and the Ph.D. degree in computer and communication from the National Kaohsiung First University of Science and Technology, Taiwan, in 2010.

She joined the Department of Electrical Engineering, Far East University, as a Lecturer, in 2000, where she became an Assistant Professor, in 2008. Since 2013, she has been with the Department of Maritime Information and Technology, National Kaohsiung Marine University, which has been merged into the National Kaohsiung University of Science and Technology. She is currently an Associate Professor with the Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan. Her current research interests include image processing and ocean engineering, multimedia signal processing, and embedded systems and its applications.

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.

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

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

From 2004 to 2017, he was a Professor with the Department of Electrical Engineering, Kao-Yuan University, Kaohsiung. Since 2018, he has been a Researcher with the Artificial Intelligence Application Research Center, National Chin-Yi University of Technology, Taichung, Taiwan. He is currently a Professor with the Department of Electrical Engineering, National Chin-Yi University of Technology. 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.

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

From 2011 to 2017, he was an Associate Professor with the Institute of Maritime Information and Technology, National Kaohsiung Marine University, Kaohsiung, Taiwan. Since 2017, he has been a Professor with the Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung. Since 2018, he has been the Chief of the Department of Maritime Information and Technology. 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.

CHIH-HSIEN LI is currently pursuing the B.S. degree with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan.

His research interests include digital signal processing, embedded system applications, and digital healthcare.