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

1Jian-Xing Wu, 1Neng-Sheng Pai, 3Yu-Chi Pu, 1,2Pi-Yun Chen, 3Chao-Lin Kuo, 1Chih-Hsien Li

1Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, 41170, Taiwan. E-mail: jian0218@gmail.com, pai@ncut.edu.tw, chenby@ncut.edu.tw, eechl53@gmail.com, li1556255@gmail.com
2Artificial Intelligence Application Research Center, National Chin-Yi University of Technology, Taichung City, 41170, Taiwan. E-mail: eechl53@gmail.com
3Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung City, 80543, Taiwan. E-mail: elkuo@nkust.edu.tw, ycpu@nkust.edu.tw

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 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. 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.

1. 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 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 a crop 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. 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 \( \alpha \) and a matrix of secret key \( B \). At the data emitter end, the hash transformation function has been accepted for publication in a future issue of this journal, but has not been fully edited.
Figure 3. Procedure of two-round processes of image encryption (secret key parameters: $b_{nm}=255$, $f_0=60$, and $c_{nm}=2$)

was used to transfer the plain image $I$ to the cipher image $H$ in the first-round processing:

$$H = aI + B = W + B$$  \hspace{1cm} (1)

where $B$ 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”:

$$\omega_{nm} = 2\pi c_{nm} i^2 + f_0 i$$  \hspace{1cm} (3)

where $b_{nm}$ and $c_{nm}$ are any constant values, 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 $c_{nm}$, $c_{mn} \in [1, 9]$. 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]:

$$E = H + B - I$$  \hspace{1cm} (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):

$$N_1 = a_{nm} rand(c_{nm} f_0 \pi n + \cos(c_{nm} f_0 \pi n))$$  \hspace{1cm} (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:

$$I' = H' - B$$

and

$$I' = E - 2B$$

$$\Rightarrow H' - B = E - 2B$$

$$\Rightarrow a_{opt} = \frac{E - 2B}{a_{opt} - 1} \equiv 0$$  \hspace{1cm} (7)

Based on optimization algorithms, Equation (7) was used to determine the optimal weighting parameter $a_{opt}$, which can minimize the objective function $T_1(a = a_{opt})$ in the
following form:

\[
T_r(a_{opt}) = \min \left[ \frac{H' - B - E - 2B}{a_{opt} - (a_{opt} - 1)} \right]
\]

(8)

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

\[
MSE_2 = E[T_r(a_{opt})]^2 \leq \varepsilon = 10^{-2}
\]

(9)

where parameter \(\varepsilon\) is the prespecified tolerance error. The optimization-based controller can be used to tune the optimal weighting parameter \(a_{opt}\) and to minimize the \(MSE_2\) in the first-round image decryption process. With Equation (7), the active attack \(N_1\) can be estimated as follows:

\[
\frac{H' - B - N_1}{a_{opt}} - \frac{E - 2B}{(a_{opt} - 1)} = 0
\]

\[
\Rightarrow N_1 = (H' - B) - \frac{a_{opt}}{a_{opt} - 1}(E - 2B)
\]

(10)

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

\[
T_2(a_{opt}) = \min \left[ \frac{H' - B - N_1 - E - 2B}{a_{opt} - 1} \right]
\]

(11)

\[
MSE_2 = E[T_2(a_{opt})]^2 \leq \varepsilon = 10^{-2}
\]

(12)

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

\[
I' = \frac{H' - B - N_1}{a_{opt}} \quad \text{or} \quad I' = \frac{E - 2B}{(a_{opt} - 1)}
\]

(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):

\[
E = H + B - I + N_2
\]

(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]:

\[
I' = \frac{H - B}{a_{opt}} \quad \text{and} \quad I' = \frac{E' - 2B}{a_{opt} - 1}
\]

\[
\Rightarrow \frac{H - B}{a_{opt}} - \frac{E' - 2B}{(a_{opt} - 1)} = 0
\]

(15)

Based on optimization algorithms, Equation (15) is used to determine the optimal weighting parameter \(a_{opt}\), which can minimize the objective function \(T_1'(a = a_{opt})\) in the following form:

\[
T_1'(a_{opt}) = \min \left[ \frac{H - B - E' - 2B}{a_{opt} - 1} \right]
\]

(16)

\[
MSE_1' = E[T_1'(a_{opt})]^2 \leq \varepsilon = 10^{-2}
\]

(17)

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

\[
\frac{H - B}{a_{opt}} - \frac{E' - 2B - N_2}{a_{opt} - 1} = 0
\]

(18)

\[
\Rightarrow N_2 = (E - 2B) - \frac{a_{opt} - 1}{a_{opt}}(H - B)
\]

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 \(a_1(p)\) be the current center position of the pth 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 \([a_{1p}, a_{2p}, a_{3p}, \ldots, a_{Gp}]\) and \([\Delta a_{1p}, \Delta a_{2p}, \Delta a_{3p}, \ldots, \Delta a_{Gp}]\), respectively. The particle agent velocity \(\Delta a_i(p+1)\) is computed with acceleration factors using Equations (12) and (13).

**Velocity component:**

\[
\Delta a_i(p+1) = [\Delta a_i(p) + c_1 \cdot rand(\Delta a_i(p), a_i(p)) + c_2 \cdot rand(\Delta a_i(p-1), a_i(p))] \quad \text{(22)}
\]

**Adaptive acceleration factors:**

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

where \(a_i\) is the global best in the particle population; \(a_i\) 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 \(rand_i \in (0, 1)\) and \(rand_i \in (0, 1)\); 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]; \(a_1, b_1, a_2, b_2\) 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 \(a_i\) around the search space. By monotonously decreasing the parameters \(c_1\) and \(c_2\), the search region will gradually approach the global best solution \(a_i\) 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 $a_i(p+1)$ using Equation (24).

**Center position**:

$$a_i(p+1) = a_i(p) + \Delta a_i(p+1)$$  \hspace{1cm} (24)

If the maximum number of iterations $p_{\text{max}}$ 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 $a_{\text{opt}}$ 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 $I'$:

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

$$PSNR(I, I') = 10 \cdot \log_{10} \left( \frac{\text{MAX}_I^2}{\text{MSE}_I} \right) = 20 \cdot \log_{10} \left( \frac{\text{MAX}_I}{\sqrt{\text{MSE}_I}} \right)$$  \hspace{1cm} (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$_E = \text{max}(I')$, 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:

$$\text{Index} = \begin{cases} 1, & 0 < \text{PSNR} \leq 40\text{dB} \\ 0, & \text{PSNR} > 40\text{dB} \end{cases}$$  \hspace{1cm} (27)

If $\text{Index}$ is “1,” then, the signal of active attack means that the decrypted image has a promising quality (0 < $\text{PSNR}$ ≤ 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. $\text{Index}$ 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.

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.

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 \( n = 1, 2, ..., 250; m = 1, 2, ..., 380; 95,000 \) 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 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 (NITM, 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 chip function with the fixed parameters \( b_{\text{max}} = 255, f_0 = 60, \) and \( c_{\text{max}} = 6 \) 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:

- **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) 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 decryption deciphered the cipher images \( H - N_1 \) and \( E \) to the plain image \( \Gamma \) using Equations (10) to (12). For the cipher images \( H - N_1 \) and \( E \) and at specific convergence condition, the PSO-based controller performed ≤ 25 iteration computations and used a mean CPU execution time of \( < 6.1058 \) s to search the optimal weighting parameter \( a_{\text{opt}} = 4.2678 \), as shown in Figure 5(f).

The given weighting parameter \( a_{\text{opt}} = 4.2678 \), the decrypted image \( \Gamma \) could be recovered by using Equation (13). The index \( \text{PSNR} = 35.7512 \) dB and \( \text{PSNR} = 38.4258 \) dB were obtained, which were less than the 40 dB needed to recover

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

| Totals         | 34   | 31  | 35  | 100  | 100  |

Note: B: Benign Tumor; M: Malignant Tumor

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
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 $H$ by using Equations (18). Then, the decrypted image $I$ was obtained from the cipher images $E - N_2$ (Figure 6(f)) using Equations (19) to (21).

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

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 $H$.
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.

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.
The grayscale image was encrypted and decrypted using the Arnold transformation (AT) [44, 45] had been performed and used as a block cipher for the grayscale images. The AT method was also applied for image encryption and decryption [44, 45]; it could change the layout of grayscale images, with PSNR = 41.1902 dB and PSNR = 34.9270 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 grayscale images, with PSNR = 41.1902 dB and PSNR = 34.9270 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 grayscale images, with PSNR = 41.1902 dB and PSNR = 34.9270 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.
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

| Abbreviations                  | Description                                                                 |
|-------------------------------|-----------------------------------------------------------------------------|
| 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                                    |

### Acknowledgment

The enrolled data was approved by the hospital research ethics committee and the Institutional Review Board (IRB), under contract number: V103C-059#, Taipei Veterans General Hospital, Taipei City. This work was supported by the Ministry of Science and Technology, Taiwan, under contract number: MOST 108-2218-E-167-00-MY2, MOST 108-2221-E-167-005-MY2, and MOST 109-2635-E-167 -001, duration: August 1, 2019 – July 31, 2021.

### Reference

[1] BBC News Services, Singapore personal data hack hits 1.5m, health authority says, 2019, available: https://www.bbc.com/news/world-asia-44900507.

[2] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux, “A joint encryption/watermarking system for verifying the reliability of medical images,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, 2012, pp. 891-899.

[3] K. Shankar, Secure image transmission in wireless sensor network applications, *Lecture Notes in Electrical Engineering*, vol. 564, Springer Nature, Switzerland, 2019.

[4] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic Cat maps,” *Chaos Solit. Fract.*, vol. 21, 2004, pp. 749-761.

[5] Scott A. Allison, Clifford F. Sweet, Douglas P. Beall, Thomas E. Lewis, and Thomas Monroe, “Department of defense picture archiving and communication system acceptance testing: results and identification of problem components,” *J. Digit. Imaging*, vol. 18, no. 3, 2005, pp. 203–208.

[6] Nakintorn Patanachai, Bunyarit Uyyanonvara, Chanjira

---

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

| Method               | With Active Attack | Without Active Attack |
|----------------------|--------------------|-----------------------|
| Proposed Method      | -10.78             | 10.53                 |
| CSCS                 | -10.84             | 10.65                 |
| AT                   | -10.83             | 10.64                 |

The enrolled data was approved by the hospital research ethics committee and the Institutional Review Board (IRB), under contract number: V103C-059#, Taipei Veterans General Hospital, Taipei City. This work was supported by the Ministry of Science and Technology, Taiwan, under contract number: MOST 108-2218-E-167-00-MY2, MOST 108-2221-E-167-005-MY2, and MOST 109-2635-E-167 -001, duration: August 1, 2019 – July 31, 2021.

### Reference

[1] BBC News Services, Singapore personal data hack hits 1.5m, health authority says, 2019, available: https://www.bbc.com/news/world-asia-44900507.

[2] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux, “A joint encryption/watermarking system for verifying the reliability of medical images,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, 2012, pp. 891-899.

[3] K. Shankar, Secure image transmission in wireless sensor network applications, *Lecture Notes in Electrical Engineering*, vol. 564, Springer Nature, Switzerland, 2019.

[4] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic Cat maps,” *Chaos Solit. Fract.*, vol. 21, 2004, pp. 749-761.

[5] Scott A. Allison, Clifford F. Sweet, Douglas P. Beall, Thomas E. Lewis, and Thomas Monroe, “Department of defense picture archiving and communication system acceptance testing: results and identification of problem components,” *J. Digit. Imaging*, vol. 18, no. 3, 2005, pp. 203–208.

[6] Nakintorn Patanachai, Bunyarit Uyyanonvara, Chanjira
Sinhthanyothin, Wichit Tharamon, Palakon Sompot, and Kritkamol Muandet, “PACS (Picture Archiving Communication System) for dentistry,” 2008 5th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Krabi, Thailand, 2008.

[7] Winnol San-Urn and Nathorn Chuayphan, “A lossless physical-layer encryption scheme in medical picture archiving and communication systems using highly-robust chaotic signals,” The 2014 Biomedical Engineering International Conference, Fukuoka, Japan, 2014.

[8] Chun-Ta Li, Cheng-Chi Lee, and Chi-Yao Weng, “A secure could-assisted wireless body area network in mobile emergency medical care system,” Journal of Medical Systems, vol. 40, no. 117, 2016, DOI: 10.1186/s10065-016-0474-0.

[9] Chun-Ta Li, Chi-Yao Weng, and Cheng-Chi Lee, “A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system,” Journal of Medical Systems, vol. 39, no. 77, 2015, DOI https://doi.org/10.1007/s10065-015-0260-0.

[10] Y. Huang and X. S. Yang, “Hyperchaos and bifurcation in a new class of four-dimensional Hopfield neural network,” Neurocomputing, vol. 69, 2006, vol. 1787-1795.

[11] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, “Applications of tripled chaotic maps in cryptography,” Chaos Solit. Fract., vol. 40, 2009, pp. 505-519.

[12] Nooshin Bigdeli, Yousef Farid, and Karim Afshar, “A robust hybrid method for image encryption based on Hopfield neural network,” Computers and Electrical Engineering, vol. 38, 2012, pp. 356-369.

[13] Amitava Nag, Jyoti Prakash Singh, Sabrani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, and Partha Pratim Sarkar, “Image encryption using affine transform and XOR operation,” Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, Thuckafay, India, 2011.

[14] Narasimhan Arul, Pragath and Rengarajan Amirtharajan, “Image encryption: an information security perceptive,” Journal of Artificial Intelligence, vol. 7, no. 3, 2014, pp. 123-135.

[15] Shrija Somaraj and Mohammed Ali Hussain, “Securing medical images by image encryption using key image,” International Journal of Computer Applications, vol. 104, no. 3, 2014, pp. 30-35.

[16] Anurag Singh and Namrata Dhanda, “DIP using image encryption and XOR operation affine transform,” IOSR Journal of Computer Engineering, vol. 17, no. 2, 2015, pp. 7-15.

[17] Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mizraukachi, and Mohammad Reza Mosavi, “A novel image encryption based on hash function with only two-round diffusion process,” Multimedia Systems, vol. 20, no. 1, 2014, pp. 45-64.

[18] Narendra Meshram, Vinod Partidar, and Krishan K. Sud, “Diffusion-substitution based gray image encryption scheme,” Digital Signal Processing, vol. 23, 2013, pp. 894-901.

[19] Aliqueza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumaram, “Comments on the security of “Diffusion-substitution based gray image encryption scheme,” Digital Signal Processing, vol. 32, 2014, pp. 34-36.

[20] Zahir Muhammad, Ziad Muhammad, and Fatih Ozkaynak, “Security problems of chaotic image encryption algorithm based on crytanalysis driven design technique,” IEEE Access, vol. 7, 2019, pp. 99945-99954.

[21] Zahir Muhammad, Ziad Muhammad, and Fatih Ozkaynak, “An image encryption algorithm based on chaotic selection of robust cryptographic primitives,” IEEE Access, vol. 8, 2020, pp. 56581-56589.

[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] Peiya Li and Kwok-Tung Lo, “A content-adaptive joint image compression and encryption scheme,” IEEE Transactions on Multimedia, vol. 20, no. 8, 2018, pp. 1960-1972.

[24] Xuncai Zhang, Zheng Zhou, and Ying Niu, “An image encryption based on the Cauchy distribution and dynamic DNA encoding,” IEEE Photonics Journal, vol. 10, no. 4, 2018, pp. 1-14.

[25] Pi-Yun Chen, Jian-Xing Wu, Chien-Ming Li, Chao-Lin Kuo, Neng-Sheng Pai, and Cha-Hung 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, 2020, pp. 61340 – 61354.

[26] Pi-Yun Chen, Jian-Xing Wu, Chien-Ming Li, Chao-Lin Kuo, Neng-Sheng Pai, and Cha-Hung Lin, “Symmetric cryptography with shift 2-int,” Hash transformation, optimization-based controller for medical image infosecurity: case study in mammographic image,” IEEE Photonics Journal, vol. 12, no. 3, 2020, pp. 1-16.

[27] Yanis Mehdil Benane, Denis Bujoreanu, Christian Cachard, Barbara Nicolas, and Olivier Basset, “An enhanced chirp modulated golyay code for ultrasound diverging wave compounding,” 2018 26th European Signal Processing Conference, Rome, Italy, 2018, pp. 81-85.

[28] Che-Chou Shen and Chien-Hsiang Lin, “Chirp-encoded excitation for dual-frequency ultrasound tissue harmonic imaging,” IEEE Trans UltraSon TransFer Freq Control, vol. 59, no. 11, 2012, pp. 2420-2430.

[29] IEEE 802 LANMAN Standards Committee, 2019, available: http://grouper.ieee.org/groups/802/.

[30] M. A. Mohamed, F. W. Zaki and A. M. El-Mohandes, “Novel fast encryption algorithms for multimedia transmission over mobile WimMax Networks,” IJCSI International of Computer Science Issue, vol. 6, no. 3, 2012, pp. 60-67.

[31] Tsuzu-Hseng Li, Chih-Yin Liu, Ping-Huan Kuo, Nien-Chu Fang, Cheng-Hui Li, Ching-Wen Cheng, Ching-Ting Hsieh, Li-Fan Wu, Jie-Jong Liang, and Chih-Yen Chen, “A three-dimensional adaptive PSO-based packing algorithm for an IOT-based automated e-fulfillment packing system,” IEEE Access, vol. 5, 2017, pp. 9188-9205.

[32] Chung-Dann Kan, Wei-Ling Chen, Chia-Hung Lin, Jieh-Neng Wang, Pong-Jeu Lu, Ming-Yao Chan, and Jui-Te Wu, “Customized hand-held pulsevalved conduit reconstruction for children and adult patients using meta-learning based intelligent model,” IEEE Access, vol. 6, 2018, pp. 21381-21396.

[33] Tsung-Lung Yang, Chia-Hung Lin, Wei-Ling Chen, Hsin-Yu Lin, Chen-San Su, and Chih-Kuang Liang, “Hash transformation and machine learning-based decision-making classifier improved the accuracy rate of automated Parkinson’s disease screening,” IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 28, no. 1, 2020, pp. 72-82.

[34] Hiba Chougrad, Hamid Zouaki, and Omar Alhayebne, “Deep convolutional neural networks for breast cancer screening,” Computer Methods and Programs in Biomedicine, vol. 157, 2018, pp. 19-30.

[35] Salar Zahed, Charlie Obimbo, Tarfa Hamed and Robert Dony, “Improving the security of the medical images,” International Journal of Advanced Computer Science and Applications, vol. 4, no. 9, 2013, pp.137-146, 2013.

[36] Manel Dridi, Mohamed Ali Hajjaji, Belgacem Bouallegue, and Abdellatif Mtibaa, “Cryptography of medical images based on a combination between chaotic and neural network,” IET Image Processing, vol. 10, no. 11, 2016, pp. 830-839.

[37] Mammographic Image Analysis Society (MIAS) database v1.21, 2018 5th International Conference on Image Processing, Communications, Computing and Networking Technologies, Goa, India, 2011.

[38] Ahmed G. Radwan, Sherif H. AbdEIHaleem, and Salwa K. Abd-El-Hafiz, “Methods and Programs in Biomedicine, vol. 157,” Experim. Medica., International Congress Series 1069, 1994, pp. 375-378.

[39] Ahmed G Radwan, Sherif H. AbdEIHaleem, and Salwa K. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: a review,” Journal of Advanced Research, vol. 7, no. 2, 2016, pp. 193-208.

[40] Akram Belazi, Ahmed A. Abd El-Atif, and Safya Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,” Signal Processing, vol. 128, 2016, pp. 155-170.

[41] C. K. Huang and H. H. Nien, “Multi chaotic systems based pixel encryption scheme,” IEEE Access, vol. 7, 2019, pp. 99945-99953.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3028077, IEEE Access
Jian-Xing Wu was born in 1985. He received the B.S. degree in Electrical Engineering from the Southern Taiwan University of Science and Technology, Tainan, Taiwan, in 2007, the M. S. degree in Electrical Engineering from the Southern Taiwan University of Science and Technology, Tainan city, Taiwan, in 2009 and the Ph.D. degree in Biomedical Engineering from National Cheng Kung University, Tainan city, Taiwan, in 2014. He is a postdoctoral research fellow of X-ray and IR Imaging Group, National Synchrotron Radiation Research Center, Hsinchu City, Taiwan, from 2014 to 2017 years. He is also a postdoctoral research fellow of Department of Niche Biomedical LLC, California NanoSystems Institute at UCLA, Los Angeles, USA, from 2017 to 2018 years. Currently, he is an assistant professor of Department of Electrical Engineering, National Chia-Yi University of Technology, Taichung City, Taiwan, which has been since 2019.

His research interests include artificial intelligence applications in electrical engineering and biomedical engineering, biomedical signal processing, medical ultrasound, and medical device design, X-ray microscopy.

Chia-Hung Lin was born in 1974, Kaohsiung City, Taiwan. He received the B.S. degree in Electrical Engineering from the Tatung Institute of Technology, Taipei City, Taiwan, in 1998, the M.S. degree in Electrical Engineering from the National Sun Yat-Sen University, Kaohsiung City, Taiwan, in 2000, and the Ph.D. degree in Electrical Engineering from National Sun Yat-Sen University in 2004. He is a professor of Department of Electrical Engineering, Kao-Yuan University, Kaohsiung City, Taiwan, from 2004 to 2017 years. Currently, he is a professor of Department of Electrical Engineering and a researcher of Artificial Intelligence Application Research Center, National Chia-Yi University of Technology, Taichung City, Taiwan, where has been since 2018.

His research interests include neural network computing and its applications, fuzzy systems, and advanced control systems.
Kaohsiung University of Science and Technology, Kaohsiung City, Taiwan, where he has been since 2017. He is also the chief of Department of Maritime Information and Technology, where he has been since 2018.

His current research interests include artificial intelligence applications in electrical engineering and ocean engineering, intelligent control systems, fuzzy systems, and embedded systems and its applications.

Chih-Hsien Li is pursuing his B.S. degree in the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan, where he has been since 2017.

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