



Article

Multilayer Convolutional Processing Network Based Cryptography Mechanism for Digital Images Infosecurity

Chia-Hung Lin ^{1,*}, Chia-Hung Wen ¹, Hsiang-Yueh Lai ¹, Ping-Tzan Huang ², Pi-Yun Chen ¹, Chien-Ming Li ³ and Neng-Sheng Pai ^{1,*}

¹ Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City 41170, Taiwan

² Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung City 80543, Taiwan

³ Division of Infectious Diseases, Department of Medicine, Chi Mei Medical Center, Tainan City 710, Taiwan

* Correspondence: eechl53@gmail.com (C.-H.L.); pai@ncut.edu.tw (N.-S.P.)

Abstract: Digital images can be easily shared or stored using different imaging devices, storage tools, and computer networks or wireless communication systems. However, these digital images, such as headshots or medical images, may contain private information. Hence, to protect the confidentiality, reliability, and availability of digital images on online processing applications, it is crucial to increase the infosecurity of these images. Therefore, an authorization encryption scheme should ensure a high security level of digital images. The present study aimed to establish a multilayer convolutional processing network (MCPN)-based cryptography mechanism for performing two-round image encryption and decryption processes. In the MCPN layer, two-dimensional (2D) spatial convolutional operations were used to extract the image features and perform scramble operations from grayscale to gray gradient values for the first-image encryption and second-image decryption processes, respectively. In the MCPN weighted network, a sine-power chaotic map (SPCM)-based key generator was used to dynamically produce the non-ordered pseudorandom numbers to set the network-weighted values as secret keys in a sufficiently large key space. It performs the second and first encryption processes using the diffusion method, modifying the image pixel values. Children's headshots and medical images were used to evaluate the security level by comparing the plain and cipher images using the information entropy, number of pixel change rate, and unified averaged changed intensity indices. Moreover, the plain and decrypted images were compared to verify the decrypted image quality using the structural similarity index measurement and peak signal-to-noise ratio.

Keywords: multilayer convolutional processing network (MCPN); spatial convolutional operation; sine-power chaotic map (SPCM); diffusion method



Citation: Lin, C.-H.; Wen, C.-H.; Lai, H.-Y.; Huang, P.-T.; Chen, P.-Y.; Li, C.-M.; Pai, N.-S. Multilayer Convolutional Processing Network Based Cryptography Mechanism for Digital Images Infosecurity. *Processes* **2023**, *11*, 1476. <https://doi.org/10.3390/pr11051476>

Academic Editor: Olympia Roeva

Received: 21 February 2023

Revised: 5 May 2023

Accepted: 10 May 2023

Published: 12 May 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Digital images contain several types of information which represent original images in a set of pixel numbers and can be processed and stored using digital computer and storage devices in multimedia files, such as static images, audio, and video. These files can be widely shared and transmitted through computer networks or wireless communication networks (internet) to the desired destinations. These visual data are visible and accessible to specific users, catering to telemedicine, video-conference, video-on-demand, monitoring in a cloud computing intelligent transportation system (ITS), and medical images in an internet of medical things (IoMT) system [1–4]. However, these digital images may be easily duplicated or modified by their unauthorized distribution and illegal copying. Thus, ensuring digital image infosecurity, including data confidentiality, data integrity, and data availability, is a crucial task in open public communication channels so as to protect them from unauthorized individuals. For example, the users of mobile-phone digital cameras may protect their private pictures such as their headshots on online image-processing

applications [5,6], ensuring image privacy on these applications. The cloud computing ITS acquires and processes images from various motorway sectors for car navigation, traffic-signal control, number-plate recognition, and speed-monitoring applications; thus, it requires a security protocol to protect the drivers' private information, including license-plate numbers, location, and driving habits [1,7]. In addition, an IoMT system [2,3,8] allows for secure communication between the computer network and different medical devices to collect patients' information using smart sensors or medical imaging equipment and, subsequently, analyzes it using artificial intelligence-based interpretation methods [2,8–10]. However, the IoMT is currently facing security and privacy concerns, such as medical record and image thefts or ransomware attacks in the healthcare sector [11]. Hence, the primary concern of online image-processing websites is to improve protection technologies to circumvent possible attacks. The goal of the proposed image encryption method is to apply a cryptography mechanism for restricting unauthorized users and protecting private information from theft, modification, or loss.

The cryptography scheme utilizes an encryption method to secure information by concealing the digital image contents. When encrypted, an image is only accessible to the specific authorized users using the secret keys, including asymmetric and symmetric cryptography methods. To protect security and privacy for digital images, previous studies [12–21] have designed the symmetric cryptography scheme to perform permutation, substitution, or shift operations for the encryption and decryption tasks, such as the permutation method (PM), the diffusion method (DM), or the combination of both methods, which have been used for digital signals and images encryption processes. In the PM-based encryption algorithms, the Arnold map and one-dimensional (1D) and multi-dimensional chaotic maps [12–17,19,22–24] are well-known cryptography schemes to support symmetrical encryption processes. The Arnold map, as a scrambling operator, uses the Arnold transform [12–15,25] to produce pseudorandom sequence numbers to rearrange the image pixel matrix, which randomly permutes the image pixel positions for producing a shuffled image; moreover, its inverse transform is used to decrypt the cipher image. Its chaotic permutation is produced by line mapping while also controlling two positive-integer parameters as secret keys or extending the control parameters to enlarge the secret key space [14–16]. However, the encryption processes are performed by the same keys and cannot affect the frequency of image pixel values. Hence, this method can be easily broken by statistical attacks (with frequency counting or statistical analysis) or brute force attacks.

In the DM-based encryption algorithms, the 1D and multi-dimensional chaotic maps are used to produce the pseudorandom sequence numbers as secret keys, replacing the image pixel values without rearranging their pixel positions. Their cryptography scheme's secret keys are generated by using the chaotic map functions, as the so-called chaotic key generator (CKG), for image encryption, such as the logistic, sine, cosine, circle, tent, and Chebyshev maps [3,14,17,22,26,27]. Moreover, their scrambling operator can produce oscillation and chaotic behaviors by setting an initial condition and adjusting the control parameters in the specific range with the iteration computations. To increase the chaotic-complexity levels, from three-dimensional (3D) to five-dimensional (5D) chaotic maps, such as Euler equations and Hamiltonian conservative chaotic systems [2,18,28,29], are also used to establish a multi-dimensional scrambling operator, which can produce hyperchaotic behaviors, allowing pseudorandom numbers to exhibit probability and fractional-dimension distribution in random-number seed space. These chaotic operators can perform both PM- and DM-based methods to change the image pixel positions and image pixel values in digital color-scale (red, green, and blue) or grayscale images. However, the CKG-based cryptography mechanism is sensitive to the initial conditions and control parameters, and also selects secret keys in a fixed range of the random-number seed. Hence, the CKG needs to enlarge the secret key space to defend against different attacks.

Additionally, deep-learning (DL)-based network models, such as the convolutional neural network (CNN) [2,18], DL-based image encryption and decryption network (DeepEDN),

and conditional generative adversarial network models, have been used to encrypt and decrypt digital images, and owing to their complex structure and the large key space, they exhibit excellent potential for digital image infosecurity. Traditional DL-based models have promising capabilities to perform the feature extraction and classification tasks, such as face recognition and disease or cancer diagnosis [17,19,27,29–32], which use multi convolutional and pooling computations with multi convolutional windows to extract a hierarchy of feature patterns from incoming images [31–33]. Hence, their multilayer model can perform scrambling operations to produce shuffled images, which are different from the plain images, for also defending against statistical and differential attacks. Hence, the DL-based method, an image-to-image transformation technique which uses multi convolutional operations, can also be used to realize the cryptography mechanism and is sensitive to change in secret keys [2].

Therefore, based on the DM-based method, we intend to establish a multilayer convolutional operation-based cryptography mechanism, consisting of two convolutional layers and a weighted network (WN) to perform image encryption and decryption processes, as seen in Figure 1. In the two convolutional layers, the two fractional-order convolutional windows (FOCWs) are used to perform two-dimensional (2D) spatial convolutional operations in order to scramble pixel values from grayscale values to gray gradient values. The FOCW-based operator with the adjustable fractional-order parameters ($\in [0, 1]$) are used to scramble image pixel values using a 3×3 sliding window (sliding stride = 1) [29,34] over the plane image in the horizontal and vertical directions, which allows for the combination of the convolutional weight calculations and scrambled pixel values. The FOCW-based window also has a rotation-invariant ability [33,35] (rotating the angle 45° clockwise in eight directions from 0° to 315°) and can capture the same feature pattern in a 2D image. Before any cipher image transmission, the authorized person can reset the weighted values of FOCWs by adjusting the fractional-order parameter, and the connecting weighted values in the WN are produced by using the sine-power chaotic map (SPCM)-based key generator [17]. Thus, two-round convolutional operations are used to perform the first encryption process. In the WN, the SPCM-based key generator [17,26] generates the non-ordered pseudorandom numbers to set the connecting weighted values of the network, as a large number of secret keys are used to enhance the security level for the second encryption process. Hence, the cipher images are obtained through image-to-image transformation; moreover, the inverse processes, with the WN and two-round convolutional operations, are used to decrypt the cipher image. Through experimental validation with children's headshots (Facial Expression Image Database) [36] and medical images (self-created hand X-ray images and National Institutes of Health (NIH) chest X-ray database), the security level is evaluated by using the information entropy (IE), the number of pixel changing rate (NPCR), and the unified averaged changed intensity (UACI) for the image encryption process [2,15,17,18,27,37]; the structural similarity index measurement (SSIM) and peak signal-to-noise ratio (PSNR) [15,38,39] are used to evaluate the quality of the decrypted image for the decryption process.

The remainder of this article is organized as follows: Section 2 describes the methodology, including the MCPN design, differential (security level) evaluation, and decrypted-image quality evaluation. Section 3 describes the experimental setup, digital image encryption and decryption tests, and performance evaluation using the NPCR, UACI, IE, SSIM, and PSNR indices. Section 4 concludes the paper.

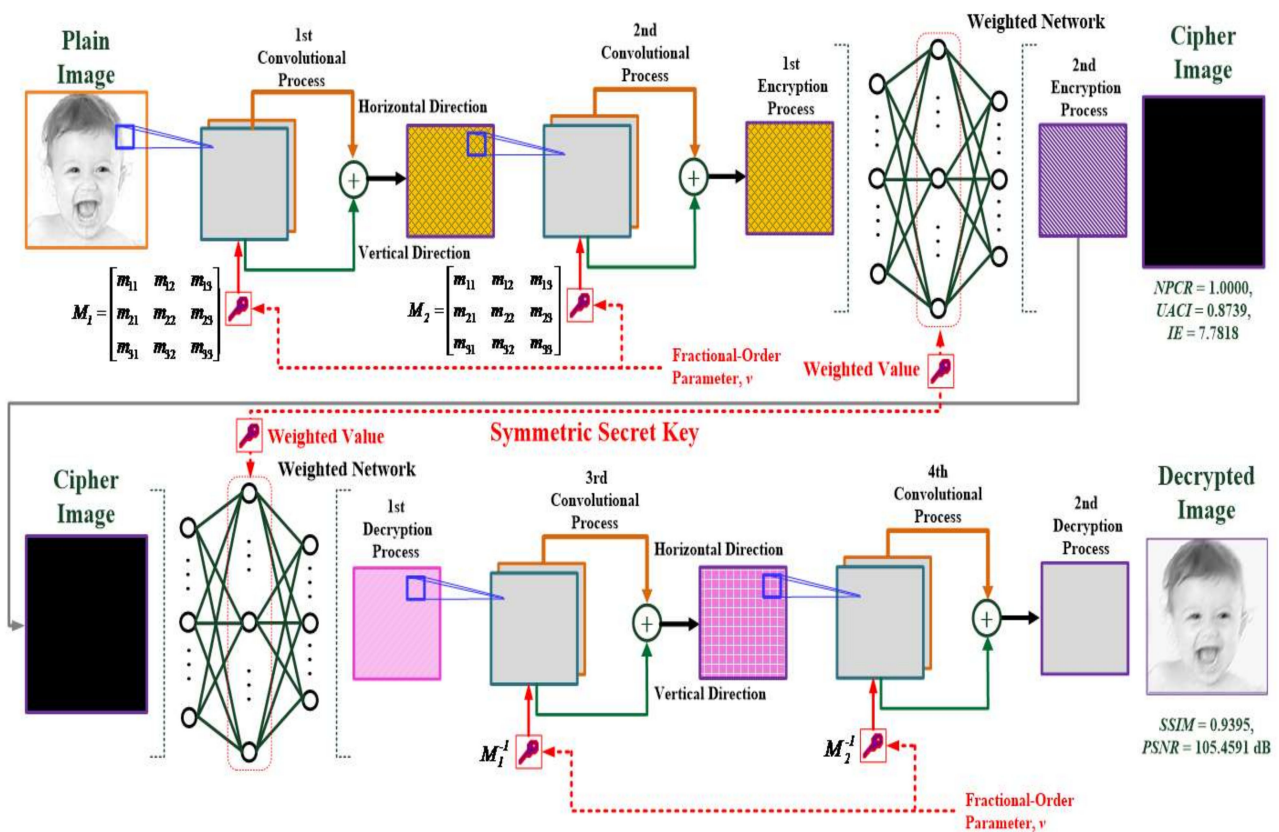


Figure 1. Structure of multilayer convolutional processing network (with two-round convolutional processes)-based cryptography mechanism for image infosecurity.

2. Methodology

2.1. First-Image Encryption Using Fractional-Order Convolutional Processes

A conventional CNN typically contains convolutional, pooling, and fully-connected layers [2,31,33], with more than one convolutional layer for extracting feature maps, enabling the recognition of these features in the images. The pooling layer receives the specific features from a convolutional layer and compresses them using the maximum or average pooling processes. The fully-connected layer is employed to acquire the reduced feature maps for prediction, object recognition, or classification applications. In the CNN, the convolutional process is employed to constantly extract and compress the image features. Herein, it functioned to control the scrambling operations in the image encryption process against the active hacker attacks. Thus, the fractional-order convolutional process [29,30] is used to perform the 2D spatial convolutional operations in both the x horizontal and y vertical directions, which compute the gray gradient of a plain image, I_0 ($I_{xy} = I_0$), and can be expressed as follows [29,30]:

$$ECI_{xy}^c = C^c(I_{xy}, M, v), \quad c = 1, 2, \dots \quad (1)$$

$$M_x = \begin{bmatrix} c_0 & c_1 & c_2 \\ c_1 & c_1 & 0 \\ c_2 & 0 & c_2 \end{bmatrix}, \quad M_y = M_x^T, \quad \text{subject to } \det(M_x) \neq 0 \text{ and } \det(M_y) \neq 0 \quad (2)$$

Elements in matrix M_x and M_y [29,30]:

$$c_n = \frac{\Gamma(n - v)}{(n)! \Gamma(-v)}, \quad n = 0, 1, 2, \dots, \quad \text{subject to } \sum_{n=0}^{\infty} c_n \neq 0 \quad (3)$$

where $C^{(\bullet)}$ is the fractional-order convolutional operator at the c th-round convolutional operation; $I_{xy} \in [0, 255]$ is the grayscale pixel value at location (x, y) in a 2D image, where $N \times M$ is the size of the image, $x = 1, 2, 3, \dots, N$, and $y = 1, 2, 3, \dots, M$; ECl_{xy}^c is the convolution result by the matrix multiplication operation at location (x, y) ; v is the fractional-order parameter, $v \in [0, 1]$; M_x and M_y are the FOCWs, which are derived from the Grünwald–Letnikov (G-L) derivative in fractional calculus [30,31], and are used to perform the convolutional operations both in the horizontal and vertical directions, respectively. In this study, we select the 3×3 convolutional window, as seen in Equations (2) and (3).

Hence, three parameters, c_0 , c_1 , and c_2 , were used to set the elements of the FOCW in the x and y directions. As seen in Figure 1, we defaulted the two-round convolutional operations (two convolution layers) with two 3×3 FOCWs, padding and passing an $N \times M$ matrix through two convolutional windows. The 2D convolutional process can be performed using a window, M_x , in the x direction and subsequent convolution using a window, M_y , in the y direction, which can transform the grayscale values to gray gradient values and also serves as a filter for edge detection and feature extraction. Hence, after each 2D spatial convolutional process, the result of the convolutional operation can be represented in a normalized value as follows [34]:

$$ECl_{xy}^c \cong \frac{|ECl_x^c| + |ECl_y^c|}{255}, \quad c = 1, 2, \dots \quad (4)$$

where ECl_x^c and ECl_y^c are the convolutional values in both the x and y directions for the first encryption processes, respectively. Equation (4) shows the values from the grayscale values $[0, 255]$ to the normalized values $[0, 2]$. After the multi-round convolutional processes ($c = 2$ for two-round operation in this study), the first encrypted image could be obtained. This DM-based method with the fractional-order convolutional operation is a flexibility-encryption mechanism by controlling the fractional-order parameters for enhancing the security level.

2.2. Second-Image Encryption Using the Weighted Network

As seen in Figure 1, the first WN maps the ECl_{xy} to the second encrypted image, EI_{xy} , using the connecting network-weighted values. These connecting weighted values function as secret keys, which are used to construct both the encryption and decryption networks for the second encryption process and first decryption process, respectively, with the number of parameters for each network being $N \times M$. The network-weighted values are obtained using the SPCM-based key generator [17,26] to set the secret keys (SKs) as follows:

$$c_{h+1} = \sin^2(\sqrt{|c_h|}) + 2(1-r)|c_h|(1-2|c_h|), \quad h = 0, 1, 2, \dots, N_c \quad (5)$$

where r is the control parameter, c_0 is the initial condition, as $0 < c_0 < 1$, and $N_c = N \times M$ is the number of SKs, as key space for the second encryption. We can compute the unsigned non-ordered integer numbers, $sk_{xy}, sk_{xy} \in [1, 255]$, using the following equation [16,18]:

$$sk_{xy} = \text{mod}(\text{round}(255 \cdot |2c_h|), 255), \quad h = 0, 1, 2, \dots, N_c \quad (6)$$

where $\text{round}(\bullet)$ is the operator to return the nearest integer number, and $\text{mod}(\bullet)$ is the modulo operator. Hence, the pseudorandom numbers, sk_x , can be used to set the SKs at location (x, y) . Further, the second encryption process can be calculated as follows:

$$EI_{xy} = ECl_{xy} \cdot sk_{xy} \quad (7)$$

where $I_1 = EI_{xy}$ is the cipher image transmitted from a data-emitter end to a data-receiver end via a computer network (IEEE 802.3 standard or IEEE 802.15 standard [16,40]).

2.3. First-Image Decryption Using the Weighted Network

As seen in Figure 1, the second WN uses the symmetric SK to decrypt the cipher image using the following equation:

$$DI_{xy} = ECI_{xy} \cdot \frac{1}{sk_{xy}}, \text{ subject to } sk_{xy} \neq 0 \quad (8)$$

where DI_{xy} is the first decrypted image. In the proposed second encryption and first decryption processes, the key space contains $N \times M$ SKs, ensuring that the encryptor's key space is sufficiently large and sensitive to the SKs, which are randomly distributed between values of 1 and 255. Thus, these multi-SKs can be dynamically readjusted at any time by using the SPCM-based key generator [17,26] to prevent the active hacker attacks.

2.4. Second-Image Decryption Using Fractional-Order Convolutional Processes

In the second decryption process, we used the 2D spatial convolutional operations to decrypt the DI_{xy} with the inverse matrix, M^{-1} , which can be expressed as follows:

$$DCI_{xy}^c = C^c(DI_{xy}, M^{-1}, v), c = 1, 2, \dots \quad (9)$$

$$M_x^{-1} = \text{inv} \left(\begin{bmatrix} c_0 & c_1 & c_2 \\ c_1 & c_1 & 0 \\ c_2 & 0 & c_2 \end{bmatrix} \right), M_y^{-1} = (M_x^{-1})^T, \text{ subject to } \det(M_x^{-1}) \neq 0 \text{ and } \det(M_y^{-1}) \neq 0 \quad (10)$$

where $\text{inv}^c(\bullet)$ is the inverse matrix operator. Hence, after the two-round convolutional operations, the cipher image can be recovered by using Equations (9) and (10), and the final result of the convolutional operation can be represented as follows:

$$DCI_{xy}^c \cong \frac{|DCI_x^c| + |DCI_y^c|}{255}, c = 1, 2, \dots \quad (11)$$

where DCI_x^c and DCI_y^c are the convolutional values in both the x direction and y direction for the decryption processes, respectively.

Then, the decrypted image, I_2 , can be computed by

$$I_2 \cong \frac{255 \cdot DCI_{xy}^c}{\max(DCI_{xy}^c)} \quad (12)$$

where operator $\max(\bullet)$ is the function for finding the maximum value in DCI_{xy}^c ($c = 2$ in this study).

2.5. Differential Evaluation between the Plain and Cipher Images

In general analysis, the graph of a histogram analysis is preliminary to evaluate the robustness of the image-cryptography mechanism, which indicates frequency distributions in grayscale pixel values within an image [15,18], as seen in the number of pixels distribution and the correlation analysis in Figure 2, respectively, where the green color represents the plain image, the blue color represents the cipher image and plain image versus cipher image, and the red color represents the plain image versus the decrypted image. Hence, we used a 227×227 -sized ($N = 227$, $M = 227$, and $N_c = 51,529$ grayscale pixels for key space) digital image (resolution of 96×96 dots per inch and 24 bits per pixel (colored image)) to perform the encryption process and demonstrate the frequency distributions among the plain, cipher, and decrypted images. The plain and decrypted images exhibit the right-skewed distributions, whereas the histogram plot of the cipher image is uniform and nearly flat (plateau distribution), and exhibits significantly different behavior of the cipher image compared to the plain image as regards offering a secure encryption process. This also indicates that the proposed encryption model can change the distribution relationship

in pixel values between the plain and cipher images for the statistical attack (frequency counting analysis). Additionally, for correlation analysis with the linear regression method, a good cipher image exhibits low adjacent correlation between the plain and cipher images, as evidenced by the adjacent location $(x + 1, y)$ versus the location (x, y) in Figure 2, where the correlation coefficient (CC) of the plain image versus the cipher image is 0.1022 (blue coloring plot) and that of the plain image versus the decrypted image is 0.8126 (red coloring plot). The adjacent pixels in the cipher image exhibit extremely low correlation at $CC = 0.0284$ (blue coloring plot).

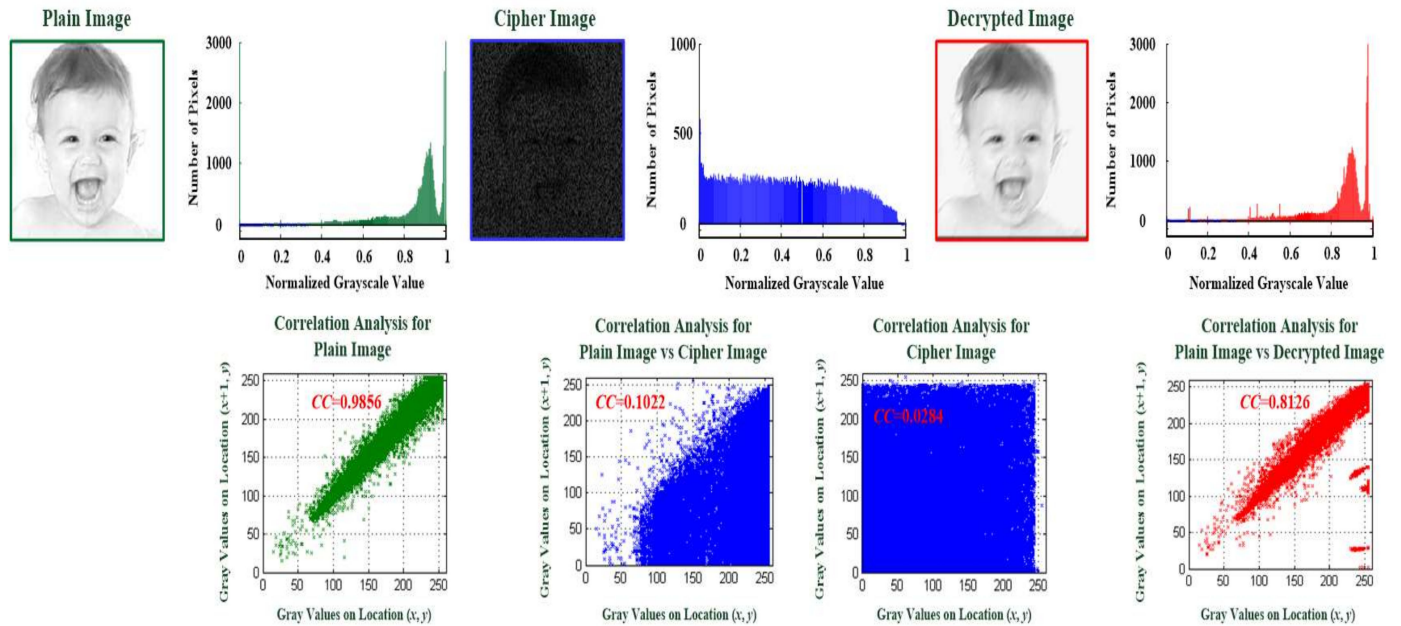


Figure 2. Histogram and correlation analyses for image-cryptography mechanism (image encryption and decryption processes).

The IE is also an index to evaluate the level of randomness distribution in a cipher image [17,24,37,41]. The complexity and chaotic encryption processes can increase the *IE* level. For an 8-bit encrypted image, the ideal *IE* level is 8.00, as the larger the *IE*, the more confusing the information in the cipher image is. The *IE* index can be defined as follows [17,24,37,41]:

$$IE(q) = \sum_{j=0}^{Q-1} P(q_j) \log_2\left(\frac{1}{P(q_j)}\right), \sum_{j=1}^Q P(q_j) = 1, j = 0, 1, 2, \dots, Q - 1 \quad (13)$$

where Q is the total number of grayscale pixels, j is the grayscale pixel value ($Q = 2^8 = 256$ in this study) in a cipher image, q_j is the j th grayscale value, and $P(q_j)$ is the emergence probability of q_j . The *IE* value indicates that the same *SKs* can generate different diffusion images for different images. To evaluate the security level, the NPCR and UACI [2,15,17,18,27,37,42] are used to quantify the confidentiality between the plain image, I_0 , and the cipher image, I_1 , as follows:

$$NPCR = \frac{\sum_{x=1,y=1}^{N,M} D(x,y)}{N \times M} \times 100\% \quad (14)$$

$$D(x,y) = \begin{cases} 0, & \text{if } I_0(x,y) = I_1(x,y) \\ 1, & \text{if } I_0(x,y) \neq I_1(x,y) \end{cases} \quad (15)$$

$$UACI = \frac{\sum_{x=1, y=1}^{N, M} |I_0(x, y) - I_1(x, y)|}{N \times M} \times 100\% \quad (16)$$

where I_0 and I_1 represent the size of the $N \times M$ images; $x = 1, 2, 3, \dots; N$ and $y = 1, 2, 3, \dots, M$; and $I_0(x, y)$ and $I_1(x, y)$ are the grayscale pixel values of plain and encrypted images, respectively. The *NPCR* index indicates the pixel change rate in a plain image after the encryption process, and the *UACI* index indicates the degree, which is used to measure the pixel differences between the plain and cipher images. For an ideal condition, the values of *NPCR* = 99.59% and *UACI* = 33.46% [37] yield the best performance for encryption processing.

2.6. Decrypted Image Quality Evaluation and Similarity Level Calculation between the Plain and Decrypted Images

After the image decryption process, the *SSIM* index is used to measure the recovery quality of a decrypted image and the similarity level between the plain image, I_0 , and the decrypted image, I_2 . The *SSIM* uses three comparison measurements, the luminance (L), contrast (C), and structure (S) [15,38,39]:

$$L(I_0, I_2) = \frac{2\mu_{I_2}\mu_{I_0} + d_1}{\mu_{I_2}^2 + \mu_{I_0}^2 + d_1}, C(I_0, I_2) = \frac{2\sigma_{I_2}\sigma_{I_0} + d_2}{\sigma_{I_2}^2 + \sigma_{I_0}^2 + d_2}, \text{ and } S(I_0, I_2) = \frac{\sigma_{I_2 I_0} + d_3}{\sigma_{I_2}\sigma_{I_0} + d_3} \quad (17)$$

$$d_1 = (0.01l)^2, d_2 = (0.03l)^2, \text{ and } d_3 = \frac{1}{2}d_2 \quad (18)$$

$$SSIM(I_0, I_2) = L(I_0, I_2)^\alpha C(I_0, I_2)^\beta S(I_0, I_2)^\gamma \quad (19)$$

where μ_{I_2} and μ_{I_0} represent the mean values of the decrypted and plain images (I_2 and I_0), respectively; σ_{I_2} and σ_{I_0} are the standard deviations of the plain and decrypted images, respectively; $\sigma_{I_2 I_0}$ is the covariance of images, I_2 and I_0 ; parameter, l , is the dynamic range of the pixel values (l is the maximum value in an image, that is, 255 for an 8-bit grayscale image); d_1 and d_2 are constants used to maintain the stability; parameters, 0.01 and 0.03 [15,17,39], are small constants; and the values of parameters, α , β , and γ , are set to 1. Hence, the *SSIM* offers a quantitative indication for evaluating the recovery quality and can be represented as follows [15,38,39]:

$$SSIM(I_2, I_0) = \frac{(2\mu_{I_2}\mu_{I_0} + d_1)(2\sigma_{I_2 I_0} + d_2)}{(\mu_{I_2}^2 + \mu_{I_0}^2 + d_1)(\sigma_{I_2}^2 + \sigma_{I_0}^2 + d_2)}, SSIM(I_2, I_0) \in [0, 1], SSIM(I_2, I_0) \geq 0.95 \quad (20)$$

The value of *SSIM* lies between 0 and 1. A value closer to 1 or greater than 0.95 indicates higher similarity (good recovery quality) between the plain and decrypted images, whereas a value of 0 indicates the absence of structural similarity. This index is also a human perception of recovery quality. The larger the *SSIM* value, the smaller the loss, which means that the proposed decryptor exhibits a good recovery quality without any active hacker attack.

In addition, the *PSNR* is an index to quantify the recovery quality level in image decryption [18,43], which measures the image distortion level by using the mean squared error (*MSE*) between the plain and decrypted images as follows:

$$MSE = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M [I_2(i, j) - I_0(i, j)]^2 \quad (21)$$

$$PSNR(dB) = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (22)$$

where $I_0(x, y)$ and $I_2(x, y)$ represent the plain and decrypted images, respectively, and MAX_I is the maximum pixel value in image I_2 , where each point is represented by 8 bits, and the maximum value may be 255. The *PSNR* is a nonnegative index, which is used to evaluate

the difference between the plain and decrypted images. This index has a smaller value for evaluating the encrypted image and performs better; the larger the index value, the smaller the distortion after the decryption process.

3. Experimental Results and Discussion

For the validated proposed *MCPN*-based cryptography mechanism, in experimental tests, the digital images were collected from headshots of 100 children (facial expression image database [36]) and 10 medical images (hand X-ray images, self-created), as seen in Figures 3 and 4, respectively. Each digital image in joint photographic experts group (JPEG) format was digitized to a resolution of 96×96 dots per inch and 24 bits per pixel, with each image sized 227×227 pixels ($N = 227$, $M = 227$, and $N_c = 51,529$ represents KS), where the row numbers were $x = 1, 2, 3, \dots, 227$, and the column numbers were $y = 1, 2, 3, \dots, 227$. The proposed *MCPN*-based cryptography mechanism was designed on a tablet PC (Intel® Xeon®, CPU E5-2620, v4, 2.1 GHz and 64 GB of RAM) using MATLAB 9.0 version software (MathWorks, Natick, MA, USA), with a graphics processing unit (GPU: NVIDIA Quadro P620, 64-bit Windows 10.0 operating system) used to process digital images. Herein, we used a 2D FOCW with the fractional-order parameters $v \in [0, 1]$ (using Equation (3)) [29,30] to perform the first encryption process; for example, the fractional-order parameter $v = 0.02$ was set, and then the FOCW and its inverse FOCW in both the horizontal and vertical directions were represented as follows:

$$M_x = M_y^T = \begin{bmatrix} 1.0000 & -0.0200 & -0.0098 \\ -0.0200 & -0.0200 & 0 \\ -0.0098 & 0 & -0.0098 \end{bmatrix} \text{ and } M_x^{-1} = (M_y^T)^{-1} = \begin{bmatrix} 0.9711 & -0.9711 & -0.9711 \\ -0.9711 & -49.0289 & 0.9711 \\ -0.9711 & 0.9711 & -101.0698 \end{bmatrix}$$

In the WN, the *SPCM*-based key generator was used to produce the pseudorandom numbers with the initial condition $c_{h=0} = 0.0$ and control parameter $r \in [3.3510, 4.0000]$ [17], and, further, 51,529 non-ordered pseudorandom numbers could be selected to set the *SKs* for image encryption and decryption using Equations (5) and (6), as seen in Figure 5a,b, respectively. Table 1 shows the related formula and parameters for setting *MCPN*-based encryption mechanism. Finally, through experimental tests using children's headshots and medical images (hand X-ray and chest X-ray images), the difference between the plain and cipher images, as the so-called "security level", could be evaluated by *IE*, *NPCR*, and *UACI* indexes after the encryption process; and the *SSIM* and *PSNR* (dB) indexes were used to evaluate the "quality of decrypted images" after the decryption process, as seen in the flowchart in Figure 6, including secret keys generation, image encryptor and decryptor establishment, image encryption and decryption processes, and security level and decrypted image quality evaluations, respectively.

In experimental tests, the digital images, including children's headshots and medical images, were used to validate the proposed *MCPN*-based cryptography mechanism. From 100 children's headshots, we randomly selected five images, as seen in Figure 7; the correlation analysis showed the relationships of two horizontally adjacent grayscale pixel values (location $(x + 1, y)$ versus location (x, y)) for the plain images and cipher images (green and blue coloring plots) and the plain images versus decrypted images (red coloring plots), respectively. For example, as seen in the headshot in the first row in Figure 6, after encryption processing with the linear regression method, the *CC* was 0.0129 in the cipher image, which was extremely small, and small relationships were observed between the adjacent grayscale pixel values. It was challenging to restructure the relationship between the cipher and plain images. Hence, the proposed encryption mechanism was able to effectively shuffle the plain images against frequency counting, statistical, and entropy hacker attacks. For differential evaluation, the *IE*, *NPCR*, and *UACI* indices could also be used to evaluate the security levels for image encryption between the plain and cipher images.



Figure 3. Children’s headshots (Facial Expression Image Database [36]).



Figure 4. Medical images (hand X-ray images, self-created).

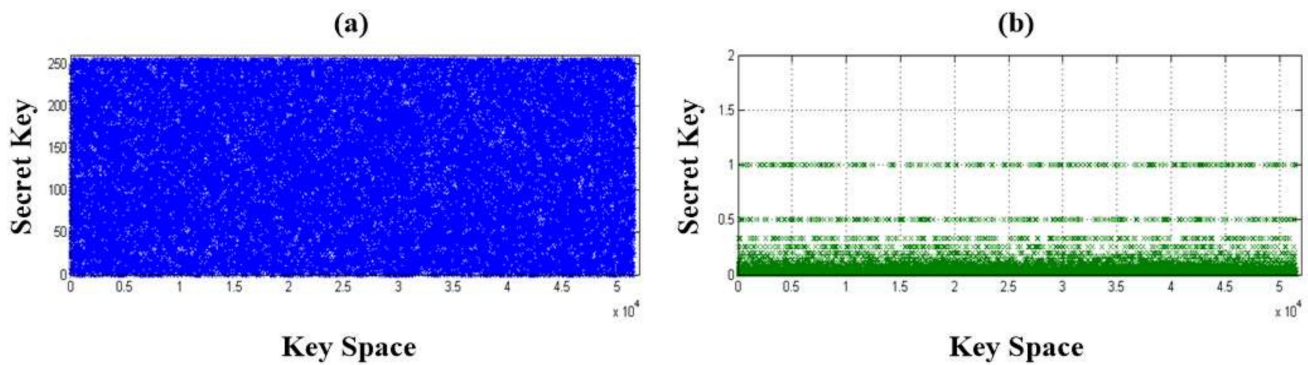


Figure 5. Secret keys (SKs) in key space. SKs for image (a) encryption and (b) decryption.

Table 1. Related formula and parameters for setting MCPN-based encryption mechanism.

Task	Method	Parameter Assignment
First Image Encryption	<p>Two-round 2D spatial convolutional operations (two convolution layers) in the x and y directions [29,30]</p> $ECI_{xy}^c = C^c(I_{xy}, M, v), c = 1, 2$ $M_x = \begin{bmatrix} c_0 & c_1 & c_2 \\ c_1 & c_1 & 0 \\ c_2 & 0 & c_2 \end{bmatrix}, M_y = M_x^T c_0 = 1,$ $c_1 = -v, c_2 = \frac{v^2 - v}{2}, v \in [0, 1].$ <p>The results of the convolutional operations are normalized by using Equation (4).</p> $ECI_{xy}^c \cong \frac{ ECI_x^c + ECI_y^c }{255}$	<p>The fractional-order parameter, v, is set by the authorized persons, $v \in [0, 1]$.</p>
Second Image Encryption	<p>The 2nd image encryption is performed by using $EI_{xy} = ECI_{xy} \cdot sk_{xy}$</p>	<p>The secret keys, sk_{xy}, are produced by SPCM based key generator [17].</p>
First Image Decryption	<p>The 1st image decryption is performed by using $DI_{xy} = ECI_{xy} \cdot \frac{1}{sk_{xy}}$, subject to $sk_{xy} \neq 0$.</p>	$c_{h+1} = \sin^2(\sqrt{ c_h }) + 2(1-r) c_h (1-2 c_h),$ $c_{h=0} = 0.0, r \in [3.3510, 4.0000].$ $sk_{xy} = \text{mod}(\text{round}(255 \cdot 2c_h), 255)$
Second Image Decryption	<p>Two-round 2D spatial convolutional operations in the x and y directions.</p> $DCI_{xy}^c = C^c(DI_{xy}, M^{-1}, v), c = 1, 2$ $M_x^{-1} = inv \left(\begin{bmatrix} c_0 & c_1 & c_2 \\ c_1 & c_1 & 0 \\ c_2 & 0 & c_2 \end{bmatrix} \right), M_y^{-1} = (M_x^{-1})^T,$ <p>subject to $\det(M_x^{-1}) \neq 0$ and $\det(M_y^{-1}) \neq 0$.</p> <p>The decrypted image is computed by $DCI_{xy}^c \cong \frac{ DCI_x^c + DCI_y^c }{255}, I_2 \cong \frac{255 \cdot DCI_{xy}^c}{\max(DCI_{xy}^c)}$</p>	<p>The fractional-order parameter, v, is set by the authorized persons, $v \in [0, 1]$.</p>

As seen in Table 2, Equations (13)–(16) were used to compute the values of the IE , $NPCR$, and $UACI$ indices; for example, for the headshot (No. 1) in first row in Figure 6, the $NPCR\% = 100.00\%$ and $UACI\% = 80.24\%$ were obtained to estimate the number of changing grayscale pixels and the number of averaged changed intensity, respectively; the IE index was used to quantify the randomness, disorder, and unavailable information using the probability, and it exhibited higher values and better performance for image encryption. As seen in Table 2, their IE values were greater than 7.5000 (very close to 8 [43]). Hence, the proposed encryption mechanism could produce random SKs to protect the digital images, and the promising quality of random number generation could contribute to the higher security value of the secret key. Additionally, with Equations (17)–(20), the $SSIM$ index, as a value range of 0–1, was used to measure the similarity level between the decrypted and

plain images. Their average value was greater than 0.9000, which indicated that the cipher images had been effectively recovered after the decryption process; otherwise, the similarity level of the cipher images was extremely low. The *PSNR* index (average value = 105.2928 dB) exhibited a higher value and also indicated that the proposed cryptography mechanism could meet the criteria for image recovery. Therefore, for five of the children’s headshots, the proposed *MCPN*-based cryptography mechanism could effectively resist differential attacks (with an average *IE* of 7.7564, average *NPCR* of 100.00%, and average *UACI* of 75.19%). The proposed cryptography mechanism took an average CPU time of 0.065 s and 0.107 s to perform the image encryption and decryption tasks, respectively.

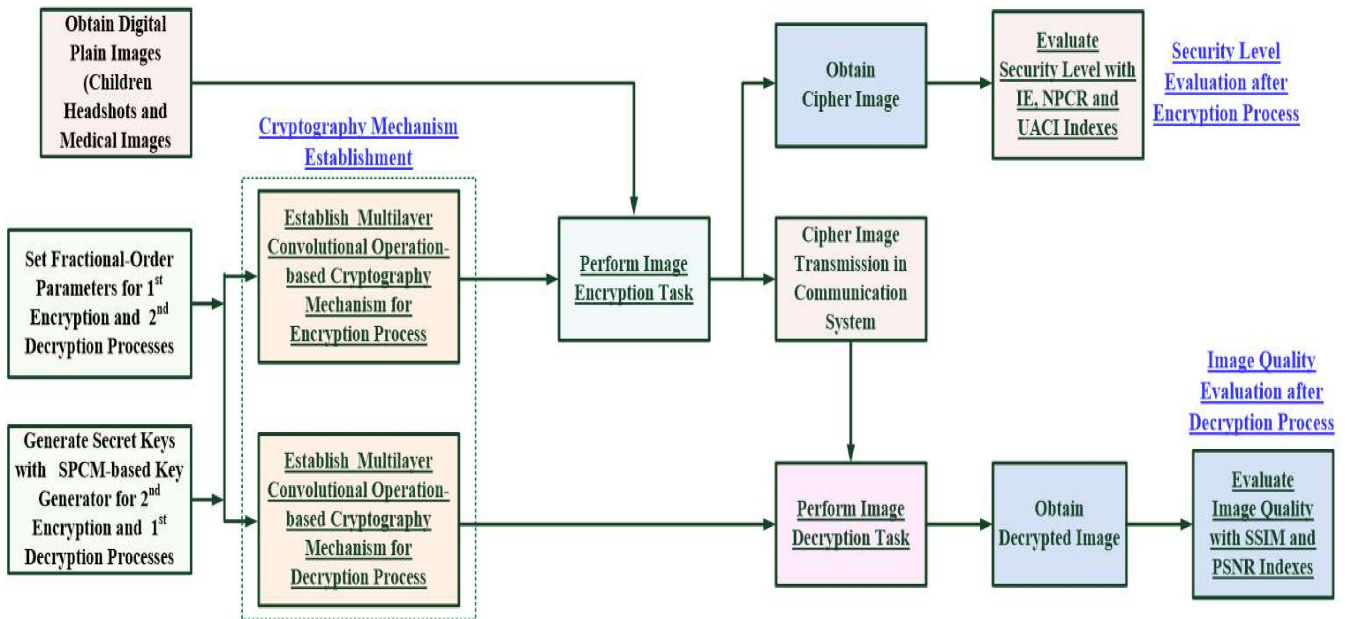


Figure 6. Flowchart of multilayer convolutional processing network-based cryptography mechanism for digital image encryption and decryption processes.

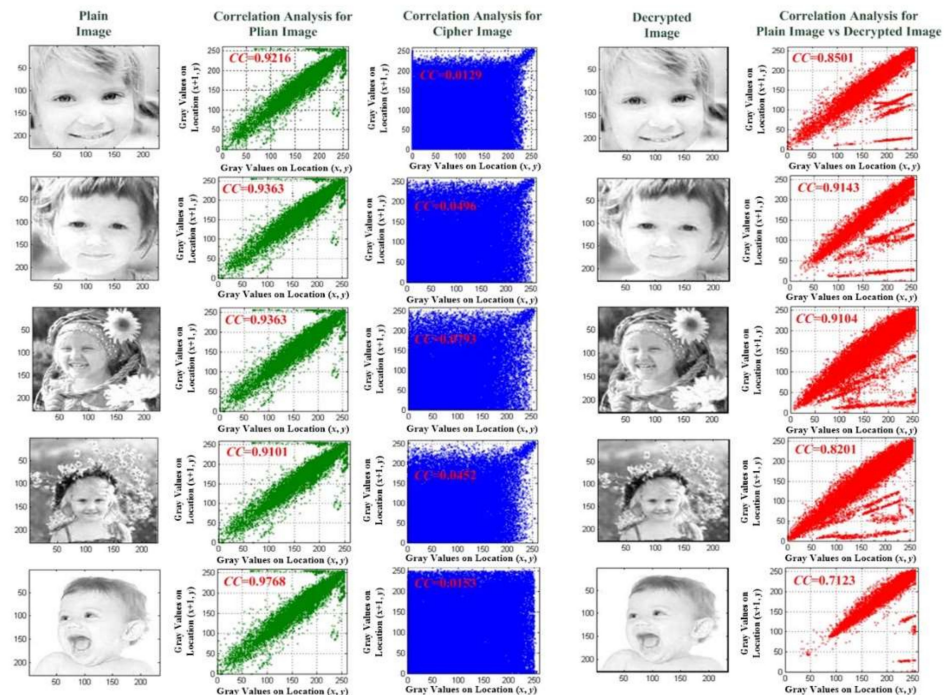





Figure 7. Five children’s headshots for experimental tests.

Table 2. Experimental results for differential evaluation and decrypted-image quality evaluation.

Digital Image	NO.	Security Level Evaluation			Decrypted Image Quality Evaluation	
		<i>IE</i>	<i>NPCR%</i>	<i>UACI%</i>	<i>SSIM</i>	<i>PSNR (dB)</i>
	1	7.7936	100.00	80.24	0.9406	105.2513
	2	7.7864	100.00	75.45	0.9371	105.2513
	3	7.6396	100.00	65.33	0.8715	105.2513
	4	7.6338	100.00	67.24	0.8946	105.2513
	5	7.9286	100.00	87.72	0.9405	105.4591
	1	6.8112	100.00	34.60	0.9162	105.2704
	2	6.9452	100.00	37.86	0.9066	105.4208
	3	6.5357	100.00	28.29	0.9194	105.2513
	4	6.7082	100.00	32.02	0.9025	105.2513
	1	7.2054	100.00	45.11	0.9279	104.4977
	2	7.7354	100.00	60.87	0.9244	104.4977
	3	7.7686	100.00	60.87	0.9244	104.4977
	4	7.6144	100.00	58.66	0.9492	104.5395
	5	7.3966	100.00	46.17	0.9392	104.5205
	6	6.9366	100.00	39.54	0.9264	104.4977

For the medical images, the hand X-ray images were low-radiation exposure images, which are used to detect fractures, bone tumors, degenerative bone conditions, and osteomyelitis [44,45]. As evident from the four hand X-ray images in Figure 8, the hand X-rays were used to determine the bone age of children so as to circumvent the problem of impaired growth in children. Hence, they also contained patients' private information and thus required protection. In Figure 8, in the plain images and decrypted images, the correlation between the adjacent pixels was extremely high (average $CC = 0.9125$, as seen in the blue and purple coloring plots); in contrast, the correlation between the adjacent pixels of the cipher image was extremely low (average $CC = 0.1058$, as seen in the green coloring plots). For the four randomly selected hand X-rays, an average IE , $NPCR$, and $UACI$ of 6.7500, 100.00%, and 33.19%, respectively, were obtained to evaluate the encryption performance, and an average $SSIM$ and $PSNR$ of 0.9112 and 105.2985 dB, respectively, indicated the decryption performance for the quality evaluation of decrypted images. For these decrypted images, they exhibited sufficient quality to evaluate the bone age using DL-based computer-aided diagnosis methods [44,45].

Furthermore, six chest X-ray (CXR) images were selected from the Nation Institutes of Health Chest X-ray Database (Nation Institutes of Health, Clinical Center, Bethesda, MD, USA) [46–48] for validating the proposed cryptography mechanism (Table 2). Six images were labeled as representing normal condition, pneumonia, fibrosis, pleural effusion, emphysema, and pneumothorax, respectively, and each image in portable network graphics (PNG) format was digitized to a resolution of 96×96 dots per inch and 24 bits per pixel (colored image), and was a 1024×1024 -pixel image. They were resized from 1024×1024 pixels to 227×227 pixels in JPEG format. As seen from the results of the correlation and histogram analyses in Figure 9, the linear regression method showed a low correlation in the cipher image, being $CC = 0.9063$ for the plain image in Figure 9a and $CC = 0.1338$ for the cipher image in Figure 9c, respectively; the histograms were significantly different for the cipher and plain images (Figure 9b,d). The average $NPCR$, $UACI$, and IE of 100.00%, 51.87%, and 7.4428, respectively, could be obtained to indicate the significant potential of the proposed method for CXR image encryption. In the decryption process, the

average *SSIM* and *PSNR* of 0.9319 and 104.5048 dB, respectively, were obtained to measure the recovery quality of the decrypted images, offering promising recovery quality for the existing medical imaging examinations of cardiopulmonary diseases and lung cancers. The experimental results of the six selected CXR images are shown in Table 2. Additionally, with a standard digital image (512 × 512 pixels in tagged image file format, 96 × 96 dots per inch and 24 bits per pixel) from the University of Southern California-Signal and Image Processing Institute (USC-SIPI) Image Dataset [48,49], Figure 10 indicates the satisfactory encryption performance of the proposed method using correlation and histogram analyses. With 100 children’s headshots [36], 10 hand X-rays, 20 CXR images [46,47,50], and 10 standard images [49], Table 3 shows the experimental results for the image encryption and decryption evaluations. The experimental results validated the performance of the proposed cryptography mechanism and its encryption and decryption abilities. In Table 4 is shown comparison of different cryptography mechanisms for digital image encryption.

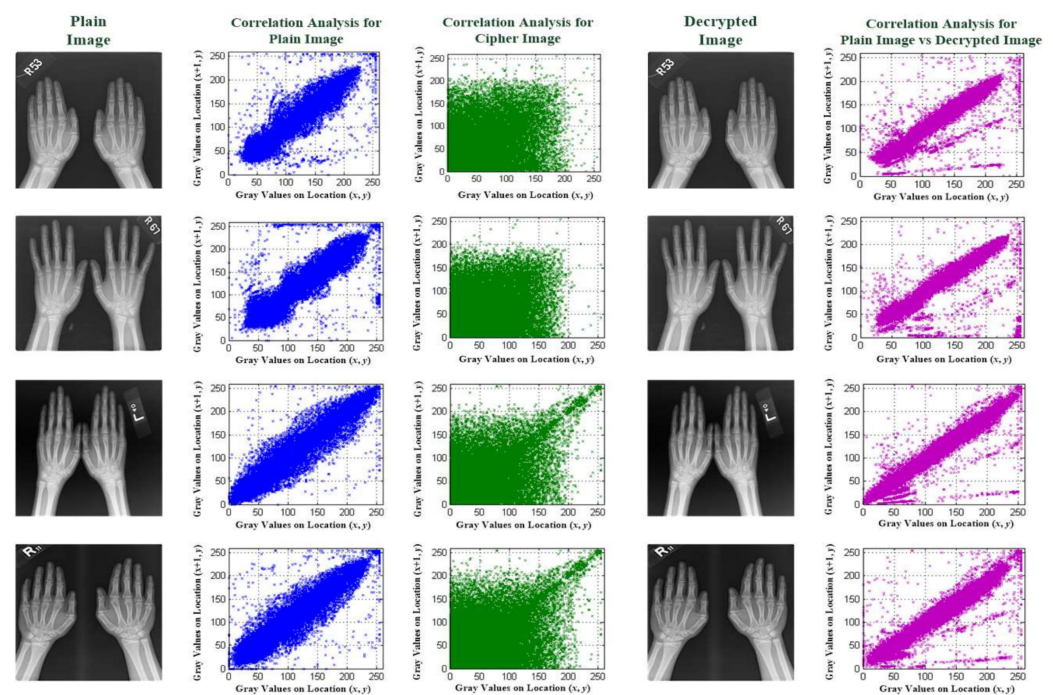


Figure 8. Four hand X-ray images for experimental tests.

Table 3. Experimental results for encryption and decryption evaluations using *IE*, *NPCR*, *UACI*, *SSIM*, and *PSNR*.

Image Type	Security Level (Differential) Evaluation			Decrypted Image Quality Evaluation	
	Average <i>IE</i>	Average <i>NPCR</i> %	Average <i>UACI</i> %	Average <i>SSIM</i>	Average <i>PSNR</i> (dB)
100 Children’s Headshots [36]	7.7900 ± 0.1553	99.99 ± 0.02	78.01 ± 9.27	0.9400 ± 0.0124	105.2532 ± 0.0083
10 Hand X-ray Images	6.7292 ± 0.1507	100.00 ± 0.00	32.88 ± 3.96	0.9039 ± 0.0127	104.6487 ± 0.8096
20 CXR Images [46,50]	7.4491 ± 0.2984	99.69 ± 0.69	56.01 ± 11.37	0.9363 ± 0.0092	104.5053 ± 0.0152
10 Standard Images [49]	7.4692 ± 0.1930	99.89 ± 0.02	53.88 ± 8.85	0.9013 ± 0.0012	112.3162 ± 0.0015

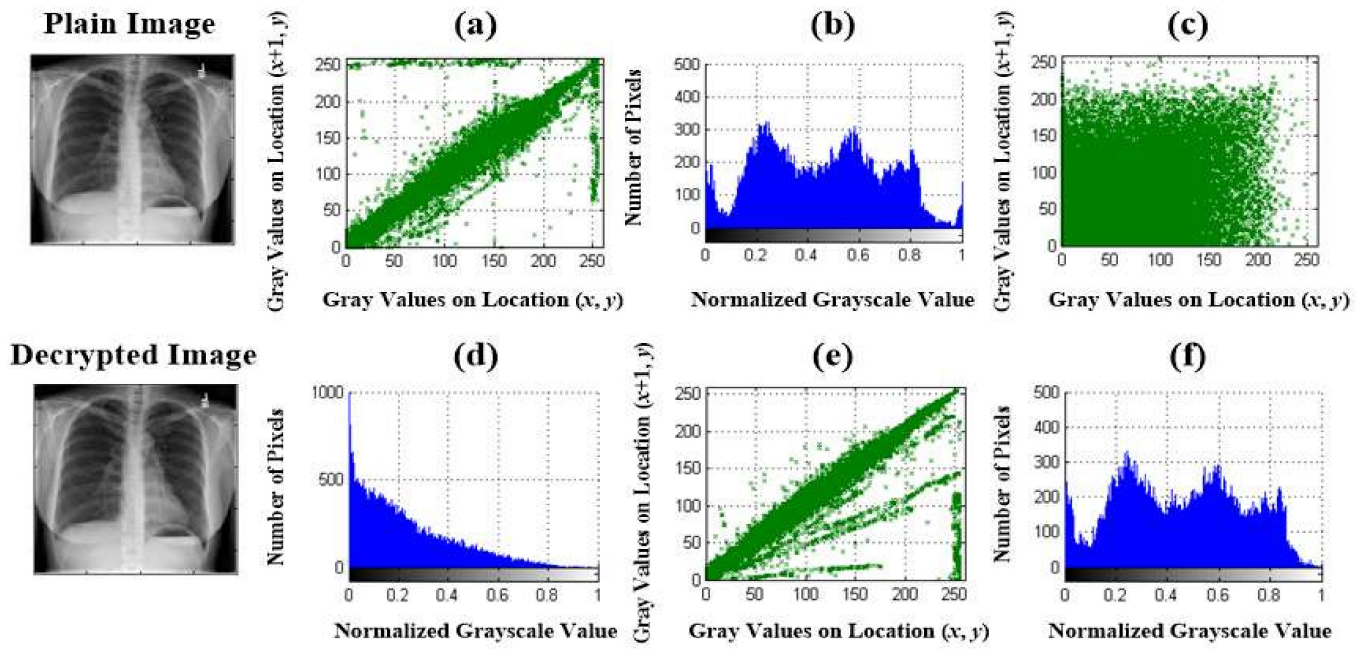


Figure 9. Correlation analysis and histogram analysis for chest X-ray images. (a,c,e) Correlation analysis for plain image, cipher image, and decrypted versus plain image, respectively; (b,d,f) histogram analysis for plain, cipher, and decrypted images, respectively.

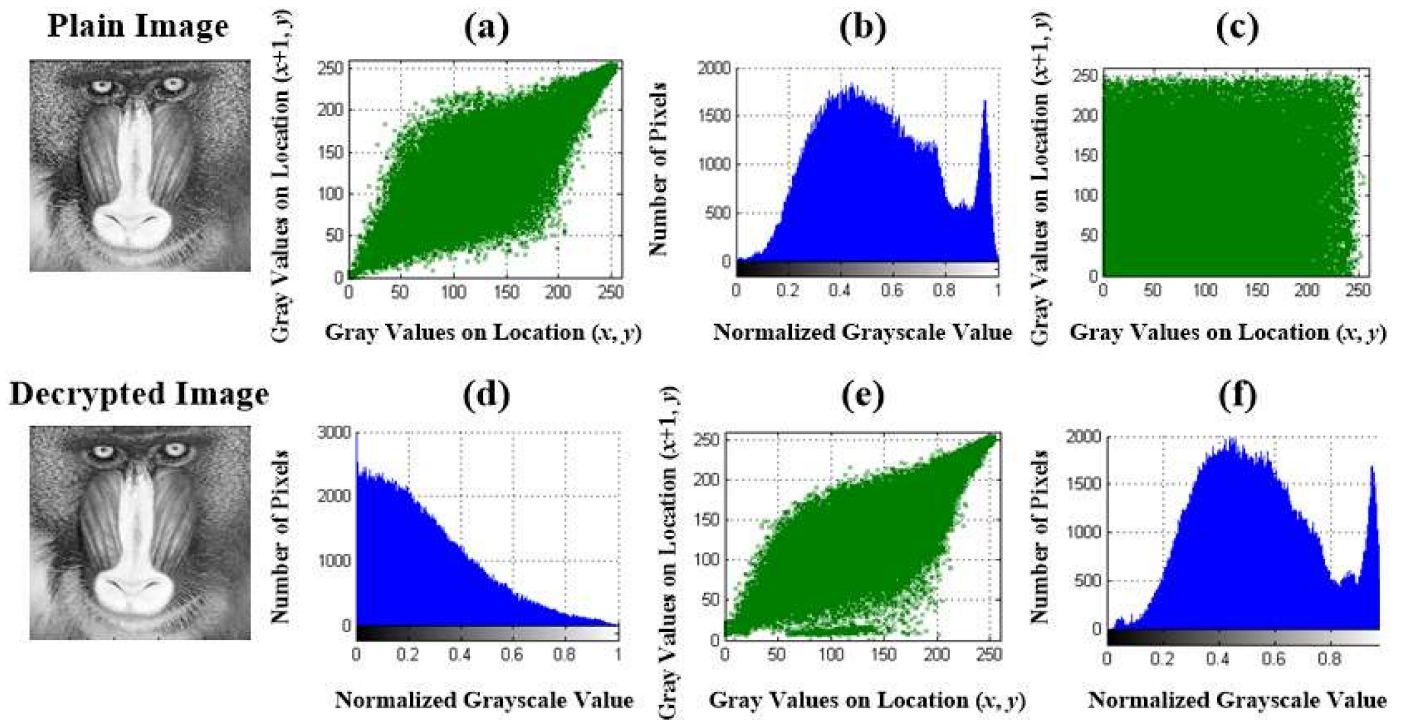


Figure 10. Correlation and histogram analyses for standard images. (a,c,e) Correlation analysis for plain image, cipher image, and decrypted versus plain image, respectively; (b,d,f) histogram analysis for plain, cipher, and decrypted images, respectively.

Table 4. Comparison of different cryptography mechanisms for digital image encryption.

Literature	Image Database	Method	Promising Result
[2]	Image Database from U.S. National Library of Medicine, Department of Health and Human Services in the USA and Shenzhen No. 3 People’s Hospital in China [47].	Deep-Learning-based Image Encryption and Decryption Network (DeepEDN) with Backpropagation Algorithm	Average $IE = 7.96$, Average $SSIM = 0.014$ for Encryption, Average $SSIM = 0.913$ for Decryption, Average $PSNR = 36.35$ dB
[16]	Standard 512×512 Pixels Images from SIPI Database [48] (Boats, Bridge, Baboon, Sailboat, Airplane, Peppers)	Cascading 1D Logistic-Chebyshev and 1D Logistic-Sine Maps.	Average $IE = 7.9995$ (Global), Average $NPCR = 99.62\%$, Average $UACI = 33.47\%$, and Average $PSNR = 8.2123$ dB for Image Encryption
[17]	NIH CXR Image Database (100 PA CXR Images) [46,50]	Chaotic Map and Quantum based Key Generator + GRA based Image Encryptor and Decryptor	Average $IE = 7.55$, Average $NPCR = 99.45\%$, and Average $UACI = 31.92\%$ for Image Encryption,
[18]	Standard 256 Grayscale Images (Pepper, Butterfly, Architecture, Boat)	Logistic Map + 5D Conservative Hyper-Chaotic System + CNN	Average $IE = 7.9983$, Average $NPCR = 99.61\%$, Average $UACI = 33.45\%$, Average $MSE = 8,315.6$, and Average $PSNR = 8.6125$ dB for Image Encryption;
[26]	USC-SIPI Image Dataset [49], including 256×256 , 512×512 , and 1024×1024 Pixels Images (Miscellaneous Database)	2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map	Average ISE (Local Shannon Entropy) = 7.9020 , Average $NPCR = 99.6096\%$, Average $UACI = 33.4629\%$ for Image Encryption;
[51]	PEIR (Pathology Education Informational Resource) Digital Library Image Database [51] (Medical Images)	Logistic Map based Key Generator + Perceptron Neural Network based Encryption System	Average $PSNR=4.82$ dB, Average $IE = 7.98$, Average $NPCR = 99.88\%$, Average $UACI = 24.54\%$ for Image Encryption,
Proposed Method	100 Children’s Headshots [36] 10 Hand X-ray Images (self created) NIH CXR Image Database (20 CXR Images) [46,50] USC-SIPI Image Dataset [49] (10 Standard Images)	MCPN based Cryptography Mechanism (2D Spatial Fractional-Order Convolutional Operations + SPCM based Key Generator) [17,27,29,30]	As seen Experimental Results in Table 3

As is evident from the literature in Table 4 [2,16–18,26,51], DeepEDN [2], chaotic map-based key generator [16,26], and chaotic map-based key generator + neural network-based encryption systems [17,18,52] have been implemented for digital image encryption and decryption processes. For example, a previous study [16] used cascaded 1D logistic-Chebyshev and 1D logistic-sine maps to permute the plain image and substitute the permuted image, respectively. With the standard 512×512 pixel-images from SIPI Database (boats, bridge, baboon, sailboat, airplane, and peppers) [48], the experimental results, having an average $IE = 7.9995$ (Global), average $NPCR = 99.62\%$, average $UACI = 33.47\%$, and average $PSNR = 8.2123$ dB, showed the effectiveness of the cascading chaotic map-based cryptosystem for image encryption. Moreover, in a previous report [18], the 5D conservative hyperchaotic system was used to establish a multi-dimensional key generator with a strong pseudorandomness scheme to produce pseudorandom numbers for a large key space, and, further, the CNN was used to generate the chaotic pointer to control the scrambling operations for image encryption. With 256 standard grayscale images (pepper, butterfly, architecture, and boat), an average IE , $NPCR$, $UACI$, MSE , and $PSNR$ of 7.9983, 99.61%, 33.45%, 8,315.6, and 8.6125 dB, respectively, were obtained to validate the feasibility of

the cryptography mechanism in the digital encryption channel. Dridi et al. [52] used the combined cryptography mechanism as a “logistic map-based key generator + perceptron neural network (PNN)” to generate cipher images with sufficiently large key space ($>2^{100}$) to resist brute-force attacks. With medical images from the Pathology Education Informational Resource digital library image database [53], average *PSNR*, *IE*, *NPCR*, and *UACI* values of 4.82 dB, 7.98, 99.88%, and 24.54%, respectively, showed that the PNN with chaotic map could enhance the cryptography technique for statistical and differential attacks. Ding et al. [2] and Lin et al. [17] demonstrated promising results for image encryption in medical images using the DL-based cryptography mechanism [46,50]. Through the experimental tests utilizing the standard image database [37,46,47,49], the proposed cryptography mechanism indicated the following advantages for digital image encryption:

- The FOCW was a flexible encryptor to perform the first-image encryption and second-image decryption processes, which could control the scrambling operations by adjusting the multiscale fractional-order parameters.
- The SPCM-based key generator was used to produce the non-ordered pseudorandom numbers as *SKs* to perform second-image encryption and first-image decryption processes in the WN.
- The proposed cryptography mechanism presented a simple structure to scramble image pixel values using two-round 2D spatial convolutional operations and diffusion processes.
- Using the children’s headshots [36], medical image database [46,50], and standard digital image database [49], the security level (differential evaluation) could be verified using the *IE*, *NPCR*, and *UACI* indices.
- The decrypted image quality could be evaluated using the *SSIM* and *PSNR* indices.

4. Conclusions

In this study, an MCPN-based cryptography mechanism was proposed to ensure online digital image infosecurity in a computer network, an ITS, an IoT, or an IoMT system [53–55]. The proposed MCPN consisted of two 2D spatial convolutional layers and a WN to perform the image encryption and decryption processes. In the two convolutional layers, two FOCW-based operators were used to scramble image pixel values for the purpose of, first, encrypting the plain image and, second, in WN, to produce the cipher image, the SPCM-based key generator produced the non-ordered pseudorandom numbers as *SKs*. With 100 children’s headshots and 10 hand X-rays, the *IE*, *NPCR*%, and *UACI*% indices were used to validate the security level of the proposed cryptography mechanism against statistical and differential attacks. For image decryption processes, the reciprocal numbers in WN and 2D spatial convolutional operations with a FOCW inverse matrix were used to decrypt the cipher images. The *SSIM* and *PSNR*, used to reevaluate the recovery quality, indicated a satisfactory decryption performance. Hence, the proposed MCPN-based cryptography mechanism offers promising capabilities to protect the data confidentiality, data recoverability, and data availability of digital images. In future works, we can combine the artificial intelligence (AI)-based classifiers for online applications in face recognition or disease and cancer diagnosis (lung cancer, cardiopulmonary-related diseases, or bone tumors) to extend its applications in the ITS, IoT, and IoMT systems, and continually integrate new secure communication techniques, such as blockchain or discrete fractional fourier transform methods, to enhance the security level in the physical layer for data transmission and sensing or imaging data fusion between heterogeneous devices.

Author Contributions: Conceptualization: C.-H.L., N.-S.P. and C.-M.L.; Analysis and Materials: C.-H.L., H.-Y.L., P.-T.H. and P.-Y.C.; Data Analysis: C.-H.W., P.-T.H. and H.-Y.L.; Writing—Original Draft Preparation: C.-H.L. and N.-S.P.; Writing—Review and Editing: C.-H.L.; Supervision: C.-H.L. and C.-M.L.; Funding Acquisition: C.-H.L. and P.-Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Science and Technology Council (NSTC), Taiwan, under contract number: MOST 111-2221-E-167-034, duration: 1 August 2022–31 July 2023.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and the protocol was approved by the Ethics Committee of Show Chwan Memorial Hospital, Changhua, Taiwan; Protocol Number: SCM_H_IRB No: 1110404; duration: 1 April 2022–31 March 2023.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

MCPN	Multilayer Convolutional Processing Network
2D	Two-Dimensional
1D	One-Dimensional
SPCM	Sine-Power Chaotic Map
ITS	Intelligent Transportation System
IoMT	Internet of Medical Things
PM	Permutation Method
DM	Diffusion Method
CKG	Chaotic Key Generator
3D	Three-Dimensional
5D	Five-Dimensional
DL	Deep-Learning
CNN	Convolutional Neural Network
WN	Weighted Network
FOCW	Fractional-Order Convolutional Window
NIH	National Institutes of Health
IE	Information Entropy
NPCR	Number of Pixel Change Rate
UACI	Unified Averaged Changed Intensity
SSIM	Structural Similarity Index Measurement
PSNR	Peak Signal-to-Noise Ratio
SK	Secret Key
ECl_x^c and ECl_y^c	Convolutional Values in both x and y Directions
CC	Correlation Coefficient
MSE	Mean Squared Error
CXR	Chest X-ray
JPEG	Joint Photographic Experts Group
PNG	Portable Network Graphics
USC-SIPI	University of Southern California-Signal and Image Processing Institute
DeepEDN	Deep-Learning-based Image Encryption and Decryption Network
PEIR	Pathology Education Informational Resource
PNN	Perceptron Neural Network

References

- Lidkea, V.M.; Muresan, R.; Al-Dweik, A. Convolutional neural network framework for encrypted image classification in cloud-based ITS. *IEEE Open J. Intell. Transp. Syst.* **2020**, *1*, 35–50. [[CrossRef](#)]
- Ding, Y.; Wu, G.; Chen, D.; Zhang, N.; Gong, L.; Cao, M.; Qin, Z. DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet Things J.* **2021**, *8*, 1504–1518. [[CrossRef](#)]
- Wimol, S.U.; Chuayphan, N. A Lossless physical-layer encryption scheme in medical picture archiving and communication systems using highly-robust chaotic signals. In Proceedings of the 7th 2014 Biomedical Engineering International Conference, Fukuoka, Japan, 26–28 November 2014; pp. 1–5.
- Han, Q.; Zhao, W.; Zhai, A.; Wang, Z.; Wang, D. Optical encryption using uncorrelated characteristics of dynamic scattering media and spatially random sampling of a plaintext. *Opt. Express* **2020**, *28*, 36432–36444. [[CrossRef](#)] [[PubMed](#)]

5. Otair, M.A. Chapter 21: Security in digital images: From information hiding perspective. In *Handbook of Research on Threat Detection and Countermeasures in Network Security*; IGI Global Book Series, Advances in Information Security; IGI Global Book Series: Hershey, PA, USA, 2014; pp. 381–394.
6. Liu, F.; Wang, Y.; Wang, F.-C.; Zhang, Y.-Z.; Lin, J. Intelligent and secure content-based image retrieval for mobile users. *IEEE Access* **2019**, *7*, 119209–119222. [[CrossRef](#)]
7. Chou, D.C. Cloud computing: A value creation model. *Comput. Stand. Interfaces* **2015**, *38*, 72–77. [[CrossRef](#)]
8. Srivastava, J.; Routray, S.; Ahmad, S.; Waris, M.M. Internet of medical things (IoMT)-based smart healthcare system: Trends and progress. *Comput. Intell. Neurosci.* **2022**, *2022*, 7218113. [[CrossRef](#)] [[PubMed](#)]
9. Javaid, A.; Niyaz, Q.; Sun, W.; Alam, M. A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, New York, NY, USA, 3–5 December 2015; Volume 3, pp. 1–6.
10. Spone, N.; Ngoc, T.N.; Phai, V.D.; Shi, Q. A deep learning approach to network intrusion detection. *IEEE Trans. Emerg. Top. Comput. Intell.* **2018**, *2*, 41–50.
11. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of medical things security assessment framework. *Internet Things* **2019**, *8*, 100123. [[CrossRef](#)]
12. Ge, R.; Yang, G.; Wu, J.; Chen, Y.; Coatriehux, G.; Luo, L. A novel chaos-based symmetric image encryption using bit-pair level process. *IEEE Access* **2019**, *7*, 99470–99480. [[CrossRef](#)]
13. Wang, J.; Li, J.; Di, X.; Zhou, J.; Man, Z. Image encryption algorithm based on bit-level permutation and dynamic overlap diffusion. *IEEE Access* **2020**, *8*, 160004–160024. [[CrossRef](#)]
14. Huang, L.; Cai, S.; Xiao, M.; Xiong, X. A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion. *Entropy* **2018**, *20*, 535. [[CrossRef](#)]
15. Kang, X.; Luo, X.; Zhang, X.; Jiang, J. Homogenized chebyshev-Arnold map and its application to color image encryption. *IEEE Access* **2019**, *7*, 114459–114471. [[CrossRef](#)]
16. Alanezi, A.; Abd-El-Atty, B.; Kolivand, H.; El-Latif, A.A.A.; El-Rahiem, B.A.; Sankar, S.; Khalifa, H.S. Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environmen. *Secur. Commun. Netw.* **2021**, *2021*, 6615512. [[CrossRef](#)]
17. Lin, C.-H.; Wu, J.-X.; Chen, P.-Y.; Lai, H.-Y.; Li, C.-M.; Kuo, C.-L.; Pai, N.-S. Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity. *IEEE Access* **2021**, *9*, 118624–118639. [[CrossRef](#)]
18. Man, Z.; Li, J.; Di, X.; Sheng, Y.; Liu, Z. Double image encryption algorithm based on neural network and chaos. *Chaos Solitons Fractals* **2021**, *152*, 111318. [[CrossRef](#)]
19. Rehman, M.U.; Shafique, A.; Ghadi, Y.Y.; Boulila, W.; Jan, S.U.; Gadekallu, T.R.; Driss, M.; Ahmad, J. A novel chaos-based privacy-preserving deep learning model for cancer diagnosis. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 4322–4377. [[CrossRef](#)]
20. Upadhyay, D.; Gaikwad, N.; Zaman, M.; Sampalli, S. Investigating the avalanche effect of various cryptographically secure Hash functions and Hash-based applications. *IEEE Access* **2022**, *10*, 112472–112486. [[CrossRef](#)]
21. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* **2020**, *8*, 21091–21116. [[CrossRef](#)]
22. Das, S.; Gautam, A.; Thokchom, S.; Balabantaray, B.K. Batch image encryption and compression using chaotic map infused autoencoder network. In Proceedings of the IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Prayagraj, India, 2–4 December 2022; pp. 1–6.
23. Niu, Z.; Zheng, M.; Zhang, Y.; Wang, T. A new asymmetrical encryption algorithm based on semitensor compressed sensing in WBANs. *IEEE Internet Things J.* **2020**, *7*, 734–750. [[CrossRef](#)]
24. Benlashram, A.; Al-Ghamdi, M.; AlTalhi, R.; Laabidi, K. A novel approach of image encryption using pixel shuffling and 3D chaotic map. *J. Phys. Conf. Ser.* **2020**, *1447*, 012009. [[CrossRef](#)]
25. Jithin, K.C.; Sankar, S. Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. *J. Inf. Secur. Appl.* **2020**, *50*, 102428. [[CrossRef](#)]
26. Zhu, H.; Zhao, Y.; Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **2019**, *7*, 14081–14098. [[CrossRef](#)]
27. Lin, C.-H.; Wu, J.-X.; Pai, N.-S.; Chen, P.-Y.; Li, C.-M.; Pai, C.C. Intelligent physiological signal infosecurity: Case study in photoplethysmography (PPG) signal. *IET Signal Process.* **2022**, *16*, 267–280. [[CrossRef](#)]
28. Dong, E.; Yuan, M.; Du, S.; Chen, Z. A new class of hamiltonian conservative chaotic systems with multistability and design of pseudo-random number generator. *Appl. Math. Model* **2019**, *73*, 40–71. [[CrossRef](#)]
29. Pu, Y.-F.; Zhou, J.-L.; Yuan, X. Fractional differential mask: A fractional differential-based approach for multiscale texture enhancement. *IEEE Trans. Image Process.* **2010**, *19*, 491–511. [[PubMed](#)]
30. Wu, J.-X.; Chen, P.-Y.; Li, C.-M.; Kuo, Y.-C.; Pai, N.-S.; Lin, C.-H. Multilayer fractional-order machine vision classifier for rapid typical lung diseases screening on digital chest X-ray images. *IEEE Access* **2020**, *8*, 105886–105902. [[CrossRef](#)]
31. He, R.; Wu, X.; Sun, Z.; Tan, T. Wasserstein CNN: Learning invariant features for NIR-VIS face recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **2019**, *41*, 1761–1773. [[CrossRef](#)] [[PubMed](#)]
32. Chen, P.-Y.; Zhang, X.-H.; Wu, J.-X.; Pai, C.C.; Hsu, J.-C.; Lin, C.-H.; Pai, N.-S. Automatic breast tumor screening of mammographic images with optimal convolutional neural network. *Appl. Sci.* **2022**, *12*, 4079. [[CrossRef](#)]

33. Hong, T.-P.; Hu, M.-J.; Yin, T.-K.; Wang, S.-L. A multi-scale convolutional neural network for rotation-invariant recognition. *Electronics* **2022**, *11*, 661. [CrossRef]
34. Qi, G. Modelings and mechanism analysis underlying both the 4d euler equations and hamiltonian conservative chaotic systems. *Nonlinear Dyn.* **2019**, *95*, 2063–2077. [CrossRef]
35. Fang, G.; Ba, S.; Gu, Y.; Lin, Z.; Hou, Y.; Qin, C.; Zhou, C.; Xu, J.; Dai, Y.; Song, J.; et al. Automatic classification of galaxy morphology: A rotationally-invariant supervised machine-learning method based on the unsupervised machine-learning data set. *Astron. J.* **2013**, *165*, 35. [CrossRef]
36. Facial Expression Image Database. Available online: <https://www.mac69.com/material/50309.html> (accessed on 21 January 2023).
37. Wu, Y.; Noonan, J.P.; Aghaian, S. NPCR and UACI randomness tests for image encryption. *J. Sel. Areas Telecommun.* **2012**, *1*, 31–38.
38. Syntax: Ssim, 1994–2023, The MathWorks, Inc. Available online: <https://www.mathworks.com/help/images/ref/ssim.html> (accessed on 21 January 2023).
39. Chen, Y.H. Application of Symmetric Encryption/Decryption: Taking a Chest X-ray Medical Image as an Example. Ph.D. Thesis, Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, Taiwan, 2020.
40. *IEEE 802.15.1-2005-Part 15.1*; Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). IEEE Standards Association: Piscataway, NJ, USA, 2011.
41. Banu, S.A.; Murthy, B.K.; Balasubramanian, V.; Fathima, S.; Amirtharajan, R. An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Med. Biol. Eng. Comput.* **2021**, *59*, 589–605.
42. Zhou, J.; Li, J.; Di, X. A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. *IEEE Access* **2020**, *8*, 122210–122228. [CrossRef]
43. Yu, J.; Guo, S.; Song, X.; Xie, Y.; Wang, E. Image parallel encryption technology based on sequence generator and chaotic measurement matrix. *Entropy* **2020**, *22*, 76. [CrossRef]
44. Li, S.; Liu, B.; Li, S.; Zhu, X.; Yan, Y.; Zhan, D. A deep learning-based computer-aided diagnosis method of X-ray images for bone age assessment. *Complex Intell. Syst.* **2022**, *8*, 1929–1939. [CrossRef]
45. Spampinato, C.; Palazzo, S.; Giordano, D.; Aldinucci, M.; Leonardi, R. Deep learning for automated skeletal bone age assessment in X-ray images. *Med. Image Anal.* **2017**, *36*, 41–51. [CrossRef]
46. Nation Institutes of Health, NIH Clinical Center Provides One of the Largest Publicly Available Chest X-ray Datasets to Scientific Community. 2017. Available online: <https://www.nih.gov/news-events/news-releases/nih-clinical-center-provides-one-largest-publicly-available-chest-x-ray-datasets-scientific-community> (accessed on 18 December 2017).
47. Jaeger, S.; Candemir, S.; Antani, S.; Wang, Y.X.J.; Lu, P.X.; Thoma, G. Two public chest X-ray datasets for computer-aided screening of pulmonary diseases. *Quant. Imag. Med. Surg.* **2014**, *4*, 475–477.
48. Signal and Image Processing Institute Database. 2023. Available online: <http://sipi.usc.edu/database/database.php?volume=miscTheUSC-SIPI> (accessed on 26 January 2023).
49. Image Database. 2023. Available online: <https://sipi.usc.edu/database/> (accessed on 26 January 2023).
50. Nation Institutes of Health (NIH), Clinical Center, Images are Available via Box. 2019. Available online: <https://Nihcc.app.box.com/v/ChestXray-NIHCC> (accessed on 15 December 2022).
51. Pathology Education Informational Resource Digital Library. 2023. Available online: <https://peir.path.uab.edu/library/index.php/?category/2> (accessed on 29 January 2023).
52. Dridi, M.; Hajjaji, M.A.; Bouallegue, B.; Mtibaa, A. Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Process.* **2016**, *10*, 830–839. [CrossRef]
53. Dwivedi, R.; Mehrotra, D.; Chandrac, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofac. Res.* **2022**, *12*, 302–318. [CrossRef]
54. Wen, H.; Tang, J.; Wu, J.; Song, H.; Wu, T.; Wu, B.; Ho, P.-H.; Lv, S.-C.; Sun, L.-M. A Cross-layer Secure Communication Model Based on Discrete Fractional Fourier Transform (DFRFT). *IEEE Trans. Emerg. Top. Comput.* **2015**, *3*, 119–126. [CrossRef]
55. Hsiao, S.-J.; Sung, W.-T. Enhancing cybersecurity using blockchain technology based on IoT data fusion. *IEEE Internet Things J.* **2023**, *10*, 486–498. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.