Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 9576184, 9 pages
https://doi.org/10.1155/2022/9576184

*Research Article*

# Image Recognition and Encryption Algorithm Based on Artificial Neural Network and Multidimensional Chaotic Sequence

**Luoyin Feng**[1] **and Xin Chen**[2]

[1]*School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China*
[2]*School of Software and Microelectronics, Peking University, 24th Jinyuan Road, Daxing Industrial District, Beijing 102600, China*

Correspondence should be addressed to Luoyin Feng; fengluoyin@stumail.neu.edu.cn

Received 9 June 2022; Revised 4 July 2022; Accepted 8 July 2022; Published 5 August 2022

Academic Editor: D. Plewczynski

With the continuous development of Internet technology and technological innovation, image recognition technologies such as face unlocking and face brushing payment have gradually entered daily life. However, it can not be ignored that these technologies not only bring us great convenience but also face great risks. The biological characteristics of a face image are unique, and it will be difficult to modify once it is leaked. If the image information stored in the cloud is leaked because it cannot be properly kept, users have no privacy. The encryption and recognition of face image can effectively solve this problem. Aiming at this, high-dimensional chaos Henon Map and one-dimensional chaos Logistic Map are used to generate a key to complete the encryption of the image in the transformation domain, and the capacity and complexity of the key are further enhanced. Then, combined with BP neural network to achieve face image recognition. Finally, the robustness of the proposed algorithm is verified and analyzed by conventional attacks, geometric attacks, and occlusion attacks.

## 1. Introduction

With the continuous development and progress of Internet technology, information security and privacy protection have attracted more and more attention [1–7]. The development of scientific and technological revolution has promoted the advent of the Internet era, and computer intelligent image recognition technology is becoming more and more mature [8–11]. Face recognition, which is an important field in image recognition, is a biometric technology for identity recognition based on facial features [5, 12, 13]. It is a research hotspot of artificial intelligence and computer vision. It is widely used in the fields of access control system, financial payment, public security, and so on. The process of traditional authentication methods such as ID card, password, and signature is cumbersome. When users forget to carry relevant certificates or forget the password, it will bring a series of unnecessary troubles, and these methods are easy to be tampered with and forged. Compared with other biometric recognition methods such as iris recognition and fingerprint recognition, the advantage of face recognition is noncontact and nonmandatory. Users do not need to contact the device directly. The recognized face image information is actively obtained by the device, and the recognition process is more friendly. At present, most of the research on face recognition is based on the plaintext domain, and there is little research on encrypted face recognition. In order to effectively protect face image data, it is of great significance to study encrypted face image recognition.

Discrete wavelet transform (DWT) [14, 15] has better spatial-frequency domain decomposition characteristics than other frequency-domain transforms, but its antiattack ability is poor. For this reason, we study an encrypted face recognition algorithm based on a neural network [16] and DWT-Discrete Cosine Transform (DWT-DCT) transform [17] and propose an image recognition and encryption algorithm based on an artificial neural network and multidimensional chaotic sequence.

## 2. Encryption Method

The encryption process of the encrypted face image recognition algorithm based on neural network and DWT-DCT transformation is shown in Figure 1.

The detailed encryption steps are as follows:

(1) Use wavelet transform to decompose the face image $f(i, j)$ with a two-layer wavelet, and obtain 4 sub-band matrices [LL, HL, LH, HH];

$$[LL, HL, LH, HH] = DW\ T2(f(i, j)). \tag{1}$$

(2) Perform DCT transformation on the four sub-band matrices, respectively, to obtain sub-band frequency domain coefficient matrices: LL1, HL1, LH1, and HH1;

$$\begin{aligned} \mathrm{LL1} &= \mathrm{DCT2}(\mathrm{LL}),\\ \mathrm{HL1} &= \mathrm{DCT2}(\mathrm{HL}),\\ \mathrm{LH1} &= \mathrm{DCT2}(\mathrm{LH}),\\ \mathrm{HH1} &= \mathrm{DCT2}(\mathrm{HH}). \end{aligned} \tag{2}$$

(3) The chaotic sequence is generated by the Henon map and Logistic map, respectively, and the chaotic sequence is binarized to obtain the binarized matrix $H(i, j)$ and $L(i, j)$;

(4) XOR the binary matrix to obtain the encrypted binary matrix $S'(i, j)$;

$$S'(i, j) = H(i, j) \otimes L(i, j). \tag{3}$$

(5) Set the 0 element in $\mathrm{S}'(\mathrm{i}, \mathrm{j})$ to -1, and construct the encrypted binary matrix $\mathrm{S}(\mathrm{i}, \mathrm{j})$ according to the size of the image;

(6) Do point multiplication with the encrypted binary matrix $\mathrm{S}(\mathrm{i}, \mathrm{j})$ and the sub-band frequency domain coefficient matrix LL1, HL1, LH1, and HH1 to complete the face image encryption in the frequency domain;

$$\begin{aligned} ELL &= S(i, j) \cdot^{*} LL1,\\ EHL &= S(i, j) \cdot^{*} HL1,\\ ELH &= S(i, j) \cdot^{*} LH1,\\ EHH &= S(i, j) \cdot^{*} HH1. \end{aligned} \tag{4}$$

(7) Then, carry out IDCT transformation on ELL, EHL, ELH, and EHH to get the encrypted sub-band matrix ELL1, EHL1, ELH1, and EHH1;

$$\begin{aligned} ELL1 &= I\ DC\ T2(ELL),\\ EHL1 &= I\ DC\ T2(EHL),\\ ELH1 &= I\ DC\ T2(ELH),\\ EHH1 &= I\ DC\ T2(EHH). \end{aligned} \tag{5}$$

(8) Finally, perform IDWT transformation on the encrypted sub-band matrix to obtain the encrypted face image $\mathrm{E}(\mathrm{i}, \mathrm{j})$;

$$E(i, j) = I\ DW\ T2(ELL1, EHL1, ELH1, EHH1), \tag{6}$$

*2.1. Encryption Effect.* The images before and after encryption by Logistic Map [18–20] and Henon Map [21–23] are shown in Figure 2. It can be seen from the image effects before and after encryption that the encrypted image has a good encryption effect, which can effectively protect image data under the condition that the key is not leaked.

*2.2. Sensitivity Analysis.* During the experiment, the parameter values of Henon mapping are selected as follows, $a = l.5$, $b = 0.323$, $X_0 = 0.76235607$, $Y_0 = 0.2236674091$, the growth parameter of Logistic mapping is 4, and the initial value $X_0 = 0.122$. Taking the first expressive face of the first person in the ORL face database as the test object to test the sensitivity. Due to the limited computational precision of the computer, there will be some data loss in the encryption and decryption of the frequency domain transform, and the image decrypted by the correct key will be slightly different from the original image, but overall the same.

It can be seen from the decrypted images that even if a slight change in the key cannot decrypt the image correctly, causing the decryption to fail, indicating that the encryption method is highly sensitive.

*2.3. Correlation Analysis.* Correlation analysis is also a kind of data analysis attacks. Generally, the correlation between adjacent pixel values of any plaintext image is strong, whether in the horizontal direction, vertical direction, or diagonal direction. If the encryption effect is good, the correlation between adjacent pixel values in these three directions is relatively weak. The calculation formula of the correlation coefficient between adjacent pixels is

$$C = \frac{\sum_{n=1}^{N} (x(n) - \overline{x})(y(n) - \overline{y})}{\sqrt{\sum_{n=1}^{N} (x(n) - \overline{x})^2 \sum_{n=1}^{N} (y(n) - \overline{y})^2}}, \tag{7}$$

where $N$ represents the logarithm of randomly selected adjacent pixels, $x(n)$ and $y(n)$ are pixel values of randomly selected adjacent pixel pairs.

$$\begin{aligned} \overline{x} &= \frac{1}{N} \sum_{n=1}^{N} x(n)\\ \overline{y} &= \frac{1}{N} \sum_{n=1}^{N} (n) \end{aligned} \tag{8}$$

In order to more clearly see the difference between encrypted image and plaintext image, plaintext image Einstein will be used as a test image to test the correlation coefficient of encrypted image and plaintext image in three directions. Figure 3, respectively, shows the correlation distribution Figure 4 of plaintext image and Figure 5ciphertext image in horizontal, vertical, and diagonal directions.

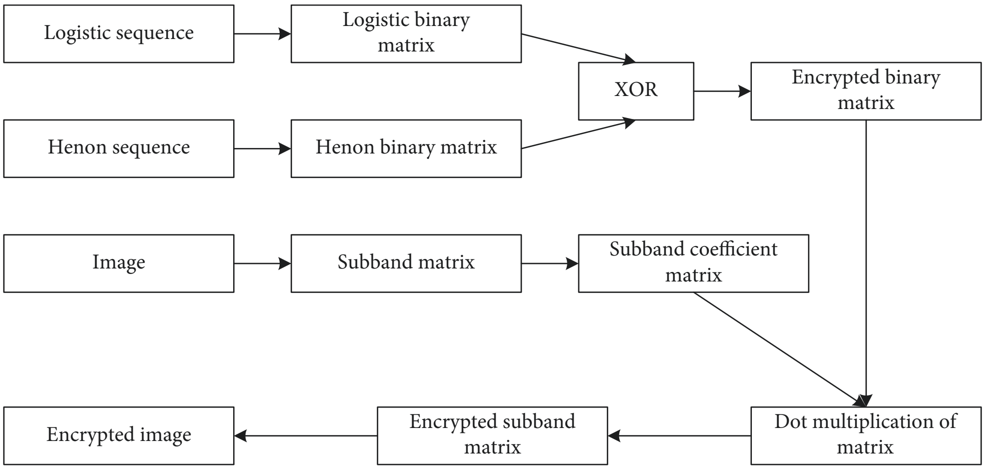


Figure 1: The encryption process of the encrypted face image recognition algorithm.

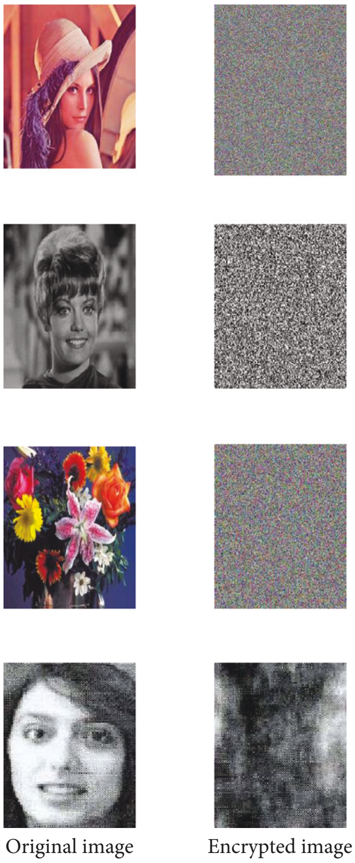


Figure 2: The Original Images and corresponding encrypted images.

Through the test of multiple images, the test values of the correlation coefficient between the plaintext image and the corresponding ciphertext image in three directions show that the value of the correlation coefficient of the ciphertext image in three directions is close to 1, while the value of the correlation coefficient of the ciphertext image in the corresponding direction is close to 0, and some even show a negative correlation. Therefore, the plaintext image eliminates the correlation between adjacent pixel values under the action of the encryption algorithm, so that the attacker cannot obtain directly valuable information.

## 3. Algorithm Flow

The specific flow of the proposed image recognition and encryption algorithm based on an artificial neural network and multidimensional chaotic sequence is shown in Figure 6.

The detailed identification steps are as follows:

(1) Encrypt the image in the DWT-DCT transform domain for the original image database

(2) Using the PCA algorithm to extract the characteristics of the encrypted image of the training sample and obtain the projection matrix $T$

(3) The dimension reduction matrix $D$ is obtained by projecting the training sample $X$ through the projection matrix $T$

(4) Use the dimensionality reduction matrix $D$ as the input of the neural network to create and train the neural network

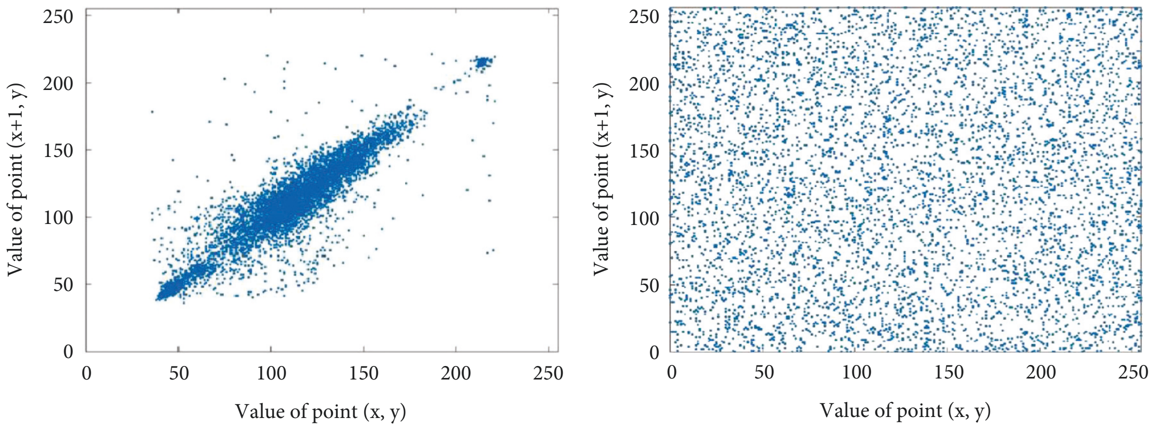
(5) Use the proposed encryption method to encrypt the face to be tested to obtain the encrypted image $E_1$

(6) Project the encrypted image $E_1$ through the projection matrix $T$ to obtain the dimension-reduced face matrix $E_2$

(7) Input the dimensionality reduction face matrix $E_2$ into the trained neural network to complete the recognition of the face to be tested

## 4. Experiment

*4.1. Recognition Rate.* In constructing the BP neural network [24–26], the input of the BP neural network is also different with different energy selected, and the recognition rate of the encryption algorithm will be different. During the experiment, the influence of the energy coefficient on the recognition rate of the neural network was analyzed by changing the size of the energy coefficient. The recognition rates of



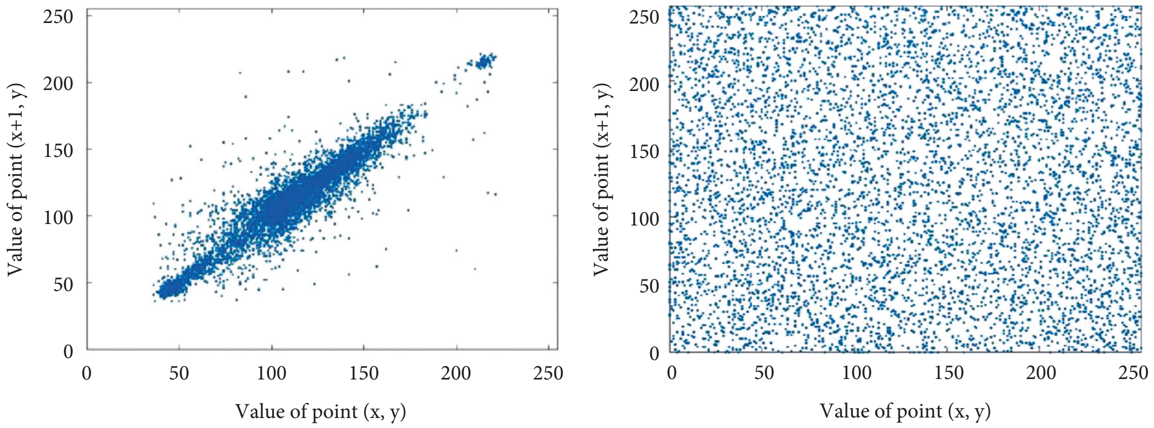
Correlation distribution of plaintext image

(a)

Correlation distribution of ciphertext image

(b)

Figure 3: The correlation distribution of plaintext image (a) and ciphertext image (b) in a horizontal direction.



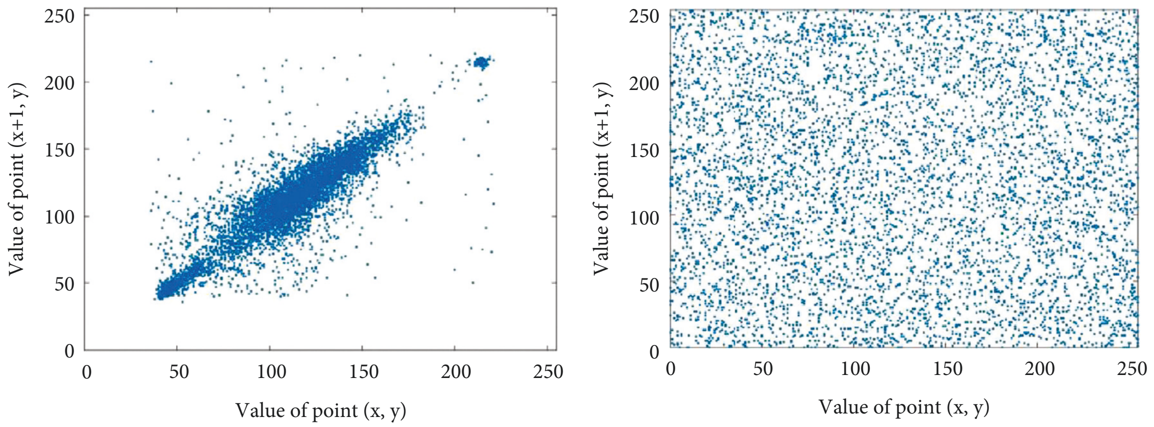
Correlation distribution of plaintext image

(a)

Correlation distribution of ciphertext image

(b)

Figure 4: The correlation distribution of plaintext image (a) and ciphertext image (b) in a vertical direction.



Correlation distribution of plaintext image

(a)

Correlation distribution of ciphertext image

(b)

Figure 5: The correlation distribution of plaintext image (a) and ciphertext image (b) in a diagonal direction.

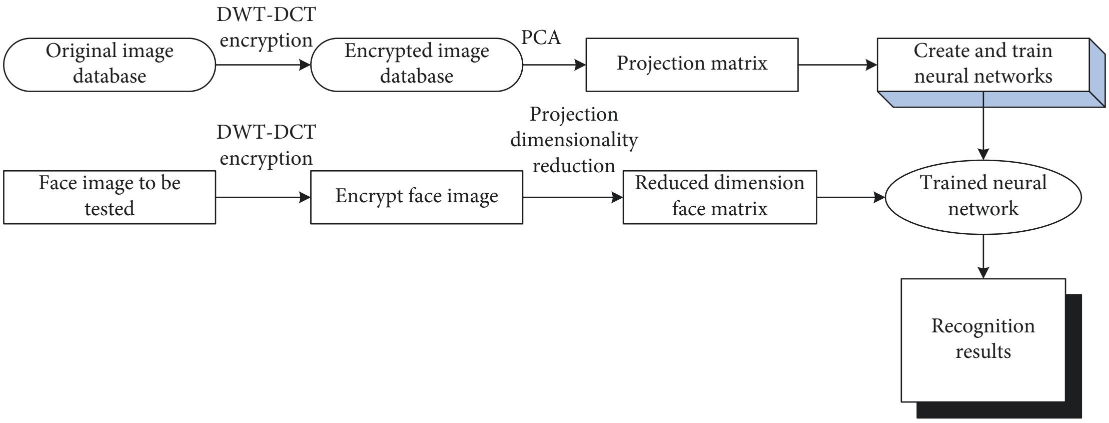


Figure 6: The specific flow of the proposed image recognition and encryption algorithm.

encrypted face recognition algorithms based on neural network and DWT-DCT transform under different energy coefficient conditions are shown in Table 1. Table 1 shows that when the selected energy coefficient is 75, the recognition rate of the encryption algorithm at this time is 63.5%. When the energy coefficient chosen increases gradually, the recognition rate of the encryption algorithm will also increase accordingly. When the energy coefficient goes 85%, the eigenvectors corresponding to the first 48 largest eigenvalues are selected, the projection matrix is $10315 * 48$, the input after dimension reduction is $200 * 48$, and the recognition rate of the encryption algorithm goes to the maximum value of 82%. Then, as the energy coefficient increases, the recognition rate of the encryption algorithm will decrease correspondingly. It can be seen that the more significant the selected energy coefficient, the better, and the more retained eigenvectors, the better. Only by selecting appropriate energy coefficients and eigenvectors can the performance of the encryption algorithm be optimal.

In the simulation experiment, the face image of the first person in the ORL face database is selected as the test image to test the robustness of the encrypted face recognition algorithm based on neural network and DWT-DCT transformation. Before the experiment, 50 people in the ORL face database were marked as serial numbers 1–50. The face images to be tested were subjected to conventional attacks, geometric attacks, lighting attacks, occlusion attacks, and others. The robustness of the encryption algorithm is evaluated by testing whether the image to be tested can still be accurately recognized after being attacked.

### 4.2. Conventional Attack

*4.2.1. Gaussian Noise.* During the experiment, the function imnoise() of Matlab is used to add Gaussian noise to the image to be tested. The data obtained from the experiment are shown in Table 2.

Observing the data in Table 2, it can be concluded that when the Gaussian noise attack intensity increases from 5% to 25%, the PSNR value of the image drops from 12.86 to 8.21. At this time, the image is quite blurred and difficult to see visually.

Table 1: Image recognition rate of encryption algorithm under different energy coefficients.

| Energy coefficients (%) | 75 | 80 | 85 | 90 | 95 |
|---|---|---|---|---|---|
| Eigenvectors (number) | 24 | 32 | 48 | 71 | 114 |
| Recognition rate (%) | 63.5 | 74.5 | 82 | 80.5 | 78.7 |

Table 2: The experiment data after Gaussian noise attack.

| Noise intensity (%) | 5 | 10 | 15 | 20 | 25 |
|---|---|---|---|---|---|
| PSNR (dB) | 12.86 | 10.11 | 9.24 | 8.77 | 8.21 |
| Identification number | 1 | 1 | 1 | 1 | 1 |

However, the proposed encryption algorithm can always accurately identify the person whose serial number is 1, indicating that this chapter's encryption algorithm has good antiattack ability against Gaussian noise attacks.

*4.2.2. JPEG Compression.* A JPEG compression experiment was performed on the face image to be tested, and the compression quality was used to describe the degree of image compression. The smaller the compression quality, the higher the compression degree of the image, and the worse the image quality. The purpose of image compression is achieved by selectively removing high-frequency redundant parts.

The data obtained in the experiment after the JPEG compression attack are shown in Table 3.

Observing at Table 3, it can be seen that when the compression quality is 5, the PSNR value of the image is 22.34, the image has become quite blurred and difficult to identify, but the encryption algorithm can still accurately identify the face image with serial number 1. When the compression quality increases gradually, the PSNR value of the image will increase progressively, and the degree of distortion will become lower and lower. When the compression quality is 25, the PSNR value at this time is 29.75. The proposed encryption algorithm recognizes the encrypted face image as the person whose serial number is 1 in the ORL face database. To sum up, the proposed image recognition and encryption algorithm based on an artificial

Table 3: The experiment data after JPEG compression attack.

| Compression quality (%) | 5 | 10 | 15 | 20 | 25 |
|---|---|---|---|---|---|
| PSNR (dB) | 22.34 | 25.56 | 27.88 | 29.42 | 29.75 |
| Identification number | 1 | 1 | 1 | 1 | 1 |

Table 4: The experiment data with median filter.

| Parameter | | [3 × 3] | | | [5 × 5] | | | [7 × 7] | |
|---|---|---|---|---|---|---|---|---|---|
| Frequency | 1 | 5 | 10 | 1 | 5 | 10 | 1 | 5 | 10 |
| PSNR (dB) | 31.44 | 29.71 | 29.03 | 28.66 | 24.32 | 24.01 | 26.55 | 22.34 | 20.76 |
| Identification number | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

neural network and multidimensional chaotic sequence has good resistance to JPEG attacks.

*4.2.3. Median Filter.* Median filtering is a nonlinear processing technology that reorders the gray values in the field according to their size. It selects the median value of the ordered sequence as the output pixel value, which can overcome the blurring of image details caused by linear average filtering. The filter window size is [7 × 7], and the face image with 10 times of filtering is tested, and the specific experimental data obtained in the experiment are shown in Table 4.

Observing Table 4, it can be seen that as the number of filters or the filter window increases, the PSNR value of the image will decrease, and the proposed encryption algorithm can always accurately identify the face image with serial number 1. The encryption algorithm has an excellent antiattack ability to median filter.

### *4.3. Geometric Attack*

*4.3.1. Translation Attack.* Under the condition of translation attack, the image is moved up and down, left and right, and the antitranslation attack ability of the encryption algorithm is tested by changing the percentage coefficient of translation. The experimental data obtained by horizontal left shift and horizontal right shift are shown in Table 5.

Observing Table 5, it can be seen that before the horizontal left shift percentage goes 32%, the encryption algorithm can accurately identify the face with serial number 1. When the left shift percentage is 32%, it has suffered a considerable strength attack. The PSNR value of the image is 8.25, the encryption algorithm cannot accurately recognize the face, and it will be mistakenly identified as the person whose serial number is 20. The horizontal right shift can be accurately recognized until the horizontal right shift percentage goes 10%. When the right shift percentage goes 10%, the PSNR is 13.11 at this time, and the encryption algorithm will incorrectly identify the face image for the person whose serial number is 15 in the ORL face database. It is not difficult to see that the ability of the proposed algorithm to resist a horizontal left shift attack is obviously better than that of a horizontal right shift attack.

Table 5: The experiment data with horizontal attack.

| | Horizontal left | | | | Horizontal right | | | |
|---|---|---|---|---|---|---|---|---|
| Move percentage (%) | 30 | 31 | 32 | 33 | 8 | 9 | 10 | 11 |
| PSNR (dB) | 8.57 | 8.34 | 8.25 | 8.13 | 14.44 | 13.36 | 13.11 | 12.52 |
| Identification number | 1 | 1 | 20 | 20 | 1 | 1 | 15 | 15 |

The experimental data obtained by moving the face image to be tested vertically up and down are shown in Table 6.

Observing the data in Table 6, it can be seen that the encryption algorithm has almost the same resistance to vertical upward and vertical downward attacks. When the vertical upward movement percentage is less than 7%, it can accurately identify the person with serial number 1. When the moving percentage reaches 7%, the encryption algorithm will incorrectly identify the person with serial number 19. When the percentage of vertical downward movement goes 6%, the PSNR value of the image will be 16.35, and it will be mistakenly identified as the person with the serial number 17. It can be seen that the encrypted face recognition algorithm has the same resistance to vertical up and vertical down.

*4.3.2. Rotation Transformation.* In the experiment, the rotation angle change is used as the change parameter, and the face image to be tested is rotated clockwise and anticlockwise to test the antirotation attack ability of the proposed encrypted face image recognition algorithm.

The experimental data obtained after clockwise rotation and anticlockwise rotation are shown in Table 7.

It can be seen from Table 7 that the PSNR value of the image is inversely proportional to the degree of rotation. When the degree of clockwise or anticlockwise rotation increases, the PSNR value of the image will decrease accordingly. When the clockwise rotation goes 13°, the encryption algorithm can be accurately identified. When the rotation degree increases to 13°, the PSNR value is 14.89. The person with serial number 5 will be wrongly identified at this time. For anticlockwise rotation, when the degree of rotation increases to 14°, the encrypted face recognition algorithm will incorrectly identify the person with the serial number 2.

Table 6: The experiment data with vertical attack.

| | Vertical up | | | | Vertical down | | | |
|---|---|---|---|---|---|---|---|---|
| Move percentage (%) | 5 | 6 | 7 | 8 | 4 | 5 | 6 | 7 |
| PSNR (dB) | 14.78 | 14.06 | 13.45 | 13.11 | 18.57 | 17.78 | 16.35 | 16.02 |
| Identification number | 1 | 1 | 19 | 19 | 1 | 1 | 17 | 17 |

Table 7: The experiment data with rotation attack.

| | Clockwise rotation | | | | Anticlockwise rotation | | | |
|---|---|---|---|---|---|---|---|---|
| Degree of rotation (°) | 11 | 12 | 13 | 14 | 12 | 13 | 14 | 15 |
| PSNR (dB) | 15.48 | 15.17 | 14.89 | 14.63 | 15.16 | 14.87 | 14.62 | 14.89 |
| Identification number | 1 | 1 | 5 | 5 | 1 | 1 | 2 | 2 |

Table 8: The experiment data with light intensity.

| Light intensity (%) | −90 | −60 | −30 | 30 | 60 | 90 |
|---|---|---|---|---|---|---|
| PSNR (dB) | 11.35 | 14.87 | 22.13 | 23.41 | 15.67 | 11.81 |
| Identification number | 1 | 1 | 1 | 1 | 1 | 1 |

Table 9: The experiment data with different occlusion.

| Occlusion | Occluded by glasses | | | Occluded by mask | | | Occluded by hat | | |
|---|---|---|---|---|---|---|---|---|---|
| | Small | Middle | Large | Small | Middle | Large | Small | Middle | Large |
| PSNR (dB) | 18.89 | 17.22 | 15.43 | 18.78 | 17.21 | 15.41 | 12.78 | 11.66 | 10.81 |
| Identification number | 1 | 1 | 21 | 1 | 1 | 1 | 25 | 25 | 25 |

It can accurately identify the person with the serial number 1 before that. The proposed encrypted face recognition algorithm has the same resistance to clockwise rotation as anticlockwise rotation.

*4.4. Light Attack.* During the experiment, Photoshop software was used to simulate the lighting conditions to preprocess the image. The antilight attack ability of the encrypted face recognition algorithm was tested by changing the light intensity. The experimental data under different illumination conditions are shown in Table 8.

Observing the data in Table 8, it can be seen that when the intensity of the light attack changes from strong to weak and then strong, the PSNR value of the image will decrease as it increases. In this change process, the encrypted face recognition algorithms proposed in this chapter can be accurately identified as the person whose serial number is 1, which indicates that the encrypted face recognition algorithm based on the network and DWT-DCT transformation has good resistance to light attacks.

*4.5. Occlusion Attack.* In real life, face images will inevitably be occluded by masks, glasses, hats, etc., and occlusion will significantly impact face recognition. In the experiment, Photoshop software is used to preprocess the image to be tested and simulate the occlusion of masks, glasses, and hats to test the resistance of the encrypted face recognition algorithm to occlusion attack.

The experimental data after being occluded by different occlusion areas are shown in Table 9.

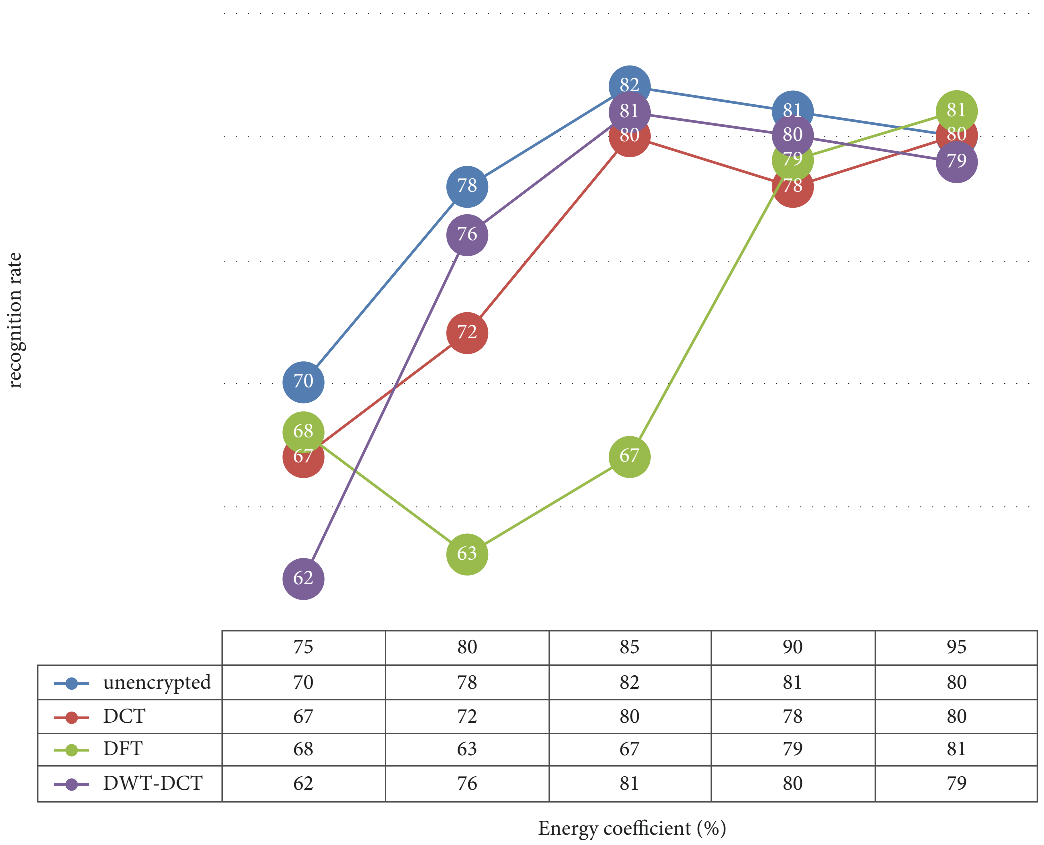
From the data in Table 9, it can be seen that for the occlusion of glasses, the person with the serial number 1 can be accurately identified before the occlusion area reaches Large. When the occlusion area is further expanded to *L*, it will be incorrectly recognized as the person with serial number 21 in the ORL face database. For mask occlusion, the encrypted face recognition algorithm can always accurately recognize, while the hat occlusion is always incorrectly recognized as the person with serial number 25. This shows that the designed algorithm has good resistance to glasses occlusion and mask occlusion, while the resistance to hat occlusion is relatively poor.

## 5. Analysis and Discussion

The recognition rates of three algorithms (unencrypted, DCT, DFT, and DWT-DCT) are compared with the recognition rates of the algorithms without encryption. The face image recognition rates of various algorithms under different energy coefficients are shown in Figure 7.

It can be seen from the data in Figure 7 that the recognition rates of the three encrypted face image recognition methods are different under different energy coefficients.

When the selected energy coefficient reaches 85%, the recognition rate of the encrypted face recognition algorithm based on DCT transform and DWT-DCT transform reaches the maximum, which are 80% and 81%, respectively, and the difference between the recognition rate of the algorithm



| | 75 | 80 | 85 | 90 | 95 |
|---|---|---|---|---|---|
| ● unencrypted | 70 | 78 | 82 | 81 | 80 |
| ● DCT | 67 | 72 | 80 | 78 | 80 |
| ● DFT | 68 | 63 | 67 | 79 | 81 |
| ● DWT-DCT | 62 | 76 | 81 | 80 | 79 |

Figure 7: The image recognition rates of various algorithms under different energy coefficients.

without encryption and 82% is only within 2%. The maximum recognition rate of the encrypted face image recognition algorithm based on the DFT transform appears at the energy coefficient of 95%, reaching 81%.

For different encrypted face recognition algorithms, it is necessary to select the appropriate energy coefficient to optimize the algorithm's performance. The security of face image data is effectively protected after chaotic encryption.

## 6. Conclusions

This paper proposes an image recognition and encryption algorithm based on an artificial neural network and multidimensional chaotic sequence. It adopts the combination of high-dimensional chaos and one-dimensional chaos to enhance the security of the key. And, complete the image encryption in the DWT-DCT transform domain and use PCA and BP neural network to achieve face recognition. Then, the key sensitivity, algorithm recognition rate, and robustness of the encryption algorithm were analyzed and tested. Finally, the algorithm recognition rate and robustness of the three encrypted face recognition algorithms and unencrypted face recognition are compared and analyzed. The results show that the recognition rate of the face recognition method using transform domain encryption is not much different from that of the unencrypted face recognition method, and it has good robustness. And, after encryption, the security of face image data on the Internet is greatly improved.

## Data Availability

The data used to support the study are included in the paper.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

[1] L. Ma, Y.-jian Kang, and J.-ping Liu, "Network information security privacy protection system in big data era Lecture Notes of the Institute for Computer Sciences, social-informatics and telecommunications engineering 2019," in *Proceedings of the advanced hybrid information processing - 3rd EAI international conference*, Nanjing, China, September2019.

[2] Q. Pan, J. Wu, A. K. Bashir et al., "Joint protection of energy security and information privacy for energy harvesting: an incentive federated learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3473–3483, 2022.

[3] T. Feng, Pu. Yang, C. Liu, J. Fang, and R. Ma, "Blockchain data privacy protection and sharing scheme based on zero-knowledge proof," *Wireless Communications and Mobile Computing*, pp. 1–11, 2022.

[4] T. Zhang, K. Zhao, M. Yang, T. Gao, and X. Wanyu, "Research on Privacy Security Risk Assessment Method of Mobile Commerce Based on Information Entropy and Markov," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–11, 2020.

[5] L. Pang, “Research on the Privacy Security of Face Recognition Technology,” *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[6] Y. Wang, X. Liang, X. Hei, W. Ji, and L. Zhu, “Deep Learning Data Privacy Protection Based on Homomorphic Encryption in AIoT,” *Mobile Information Systems*, 2021.

[7] T. Xiao, J. Li, J. Liu, J. Cheng, and U. A. Bhatti, “A robust algorithm of encrypted face recognition based on DWT-DCT and tent map Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),2018,” in *Proceedings of the Cloud Computing and Security - 4th International Conference*, pp. 508–518, Haikou, China, June2018.

[8] L. Li, B. Lei, and C. Mao, “Digital twin in smart manufacturing,” *Journal of Industrial Information Integration*, vol. 26, no. 9, Article ID 100289, 2022.

[9] L. Li, T. Qu, Y. Liu et al., “Sustainability assessment of intelligent manufacturing supported by digital twin,” *IEEE Access*, vol. 8, pp. 174988–175008, 2020.

[10] L. Li and C. Mao, “Big data supported PSS evaluation decision in service-oriented manufacturing,” *IEEE Access*, vol. 8, no. 99, pp. 154663–154670, 2020.

[11] L. Li, C. Mao, H. Sun, Y. Yuan, and B. Lei, “Digital twin driven green performance evaluation methodology of intelligent manufacturing: hybrid model based on fuzzy rough-sets AHP, multistage weight synthesis, and PROMETHEE II,” *Complexity*, vol. 2020, no. 6, pp. 1–24, 2020.

[12] Z. Yu, Y. Dong, J. Cheng, M. Sun, and S. Feng, “Research on Face Recognition Classification Based on Improved GoogleNet,” *Security and Communication Networks*, vol. 2022, 2022.

[13] G. Wu, “Masked face recognition algorithm for a contactless distribution cabinet,” *Mathematical Problems in Engineering*, pp. 2021–11, 2021.

[14] M. H. Siddiqi, K. Asghar, U. Draz et al., “Image Splicing-Based Forgery Detection Using Discrete Wavelet Transform and Edge Weighted Local Binary Patterns,” *Security and Communication Networks*, vol. 2021, 2021.

[15] S. Chen, B. Qiu, F. Zhao, C. Li, and H. Du, “Fast compressed sensing mri based on complex double-density dual-tree discrete wavelet transform,” *International Journal of Biomedical Imaging*, pp. 1–13, 2017.

[16] Z. He, “Vocal Music Recognition Based on Deep Convolution Neural Network,” *Scientific Programming*, 2022.

[17] P. Gupta, R. K. Singh, H. P. Thethi, B. Singh, and S. K. Nanda, “Discrete cosine transform matrix based SLM algorithm for OFDM with diminished PAPR for M-PSK over different subcarriers,” *Journal of Computer Networks and Communications*, pp. 1–10, 2019.

[18] Y. Dong, X. Huang, Q. Mei, and Y. Gan, “Self-Adaptive Image Encryption Algorithm Based on Quantum Logistic Map,” *Security and Communication Networks*, 2021.

[19] C. B. B. Quiroga and C. E. Cantón, “Generation of dynamical S-boxes for block ciphers via extended logistic map,” *Mathematical Problems in Engineering*, pp. 1–12, 2020.

[20] X. Huang, L. Liu, X. Li, M. Yu, and Z. Wu, “A new two-dimensional mutual coupled logistic map and its application for pseudorandom number generator,” *Mathematical Problems in Engineering*, pp. 1–10, 2019.

[21] Z. Tang, Ye. Yang, S. Xu, C. Yu, and X. Zhang, “Image Encryption with Double Spiral Scans and Chaotic Maps,” *ecurity and Communication Networks*, S, 2019.

[22] S. Ajili, M. A. Hajjaji, and A. Mtibaa, “Crypto-watermarking Algorithm Using Weber’s Law and AES: A View to Transfer Safe Medical Image,” *Scientific Programming*, 2021.

[23] J. Chandrasekaran and S. J. Thiruvengadam, “A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images,” *Security and Communication Networks*, 2017.

[24] H. Song and K. Rajakani, “Analysis of winning experience and technical training effect of badminton match based on BP neural network,” *Journal of Healthcare Engineering*, pp. 1–8, 2022.

[25] W. Yu, G. Guan, J. Li et al., “Claim afpautomobile insurance based on the BP neural network,” *Complexity*, pp. 2021–17, 2021.

[26] Y. Jin, Y. Yang, B. Yang, and Y. Zhang, “An adaptive BP neural network model for teaching quality evaluation in colleges and universities,” *Wireless Communications and Mobile Computing*, pp. 2021–7, 2021.