Mathematical Biosciences and Engineering

MBE, 19(2): 1373–1387.
DOI: 10.3934/mbe.2022063
Received: 24 August 2021
Accepted: 28 October 2021
Published: 06 December 2021

http://www.aimspress.com/journal/MBE

Research article

Encrypted face recognition algorithm based on Ridgelet-DCT transform and THM chaos

Zilong Liu[1,2], Jingbing Li[1,*] and Jing Liu[3]

[1] School of Information and Communication Engineering, Hainan University, Haikou 570228, China
[2] Haikou University of Economics, Haikou 571127, China
[3] Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou 311121, China

* **Correspondence:** Email: toujipibs1842@163.com; Tel: +861363768206.

Abstract: With the popularization and application of face recognition technology, a large number of face image data are spread and used on the Internet. It has brought great potential safety hazard for personal privacy. Combined with the characteristics of tent chaos and Henon chaos, a THM (tent-Henon map) chaotic encrypted face algorithm based on Ridgelet-DCT transform is proposed in this paper. Different from conventional face recognition methods, this new approach encryptes the face images by means of using the homomorphic encryption method to extract their visual robust features in the first place, and then uses the proposed neural network model to design the encrypted face recognition algorithm. This paper selects the ORL face database of Cambridge University to verify the algorithm. Experimental results show that the algorithm has a good performance in encryption effect, security and robustness, and has a broad application prospect.

Keywords: ridgelet transform; tent-Henon-map; face recognition; neural network; encrypted face

1. Introduction

With the rapid development of computer image processing technology, artificial intelligence technology, cloud computing and cloud storage technology, face recognition technology has gradually replaced traditional passwords, electronic signatures and other authentication methods due to its biological uniqueness, convenience and particularity. It is widely used in the fields of mobile payment, financial management, process control and information security [1]. Compared with the traditional identity verification methods, face recognition conforms to people's visual recognition experience, convenient, fast, simple, and easy to be accepted by users. However, while face recognition technology brings a series of conveniences, there are also huge security risks. When recognizing faces, a large amount of original face data is stored and transmitted in the cloud, which can easily lead to the theft, leakage or tampering of face images and their personal related information [2]. It will cause certain losses and impacts on individuals and the society [3].

Due to the qualitative breakthrough of the underlying technology, the accuracy of face recognition has been greatly improved, and its application scenarios have seen explosive growth. However, the corresponding image information security and privacy protection measures have not kept pace with the development of face recognition technology in time. At present, there are still many security challenges. For example, using the adversarial examples which are imperceptible to the naked eye [4] can make the face recognition systems get wrong results with a higher recognition rate [5–7]. Through the AI face-changing technology or making three-dimensional high-precision facial feature models, we can also deceive the face recognition systems [8,9]. These attack methods all need to grasp the biometric information of the face images in advance. And encrypting the face images to hide the biological characteristics can resist these attacks effectively. However, the encrypted face images will cause most face recognition methods to fail or reduce the recognition rate. Therefore, in the environment of cloud storage and cloud transmission, it is of great significance to design an algorithm that can not only encrypt the face images, protect the security of the face images, but also have a higher recognition effect on the faces, for the privacy protection and information security protection of the face images. This is of great significance to the application and popularization of face recognition [3,8–10].

At present, there are many algorithms for face recognition and face encryption, but there are relatively few researches on recognition algorithms for encrypted face images, which are mainly divided into the following categories:

Encryption and recognition methods based on face image features. Such methods generally use linear transformation or frequency domain transformation and others to reduce the dimensionality of high-dimensional data [10]. And then, they represent the main features of the face images by extracting low-dimensional data feature information [11,12], to realize the encryption and recognition of the face images [13]. For example, G. Iovane et al. used the FIF algorithm to extract the fusion key from facial biometric information and digital information to achieve the purpose of encryption and recognition [10]. C. Liu et al. used logistic chaotic mapping to encrypt the face images, combined with the DFT domain to generate a "keyword" feature vectors. The algorithm realizes face recognition by calculating the NC values of the feature vectors of the original images and encrypted face images [11]. S. Guo used affine transformation to encrypt the images, and performed projection (feature extraction) in the encrypted domain to recognize the encrypted face images [13]. This type of methods is relatively easy to implement, and occupy a small space to generate feature vectors. However, they require relatively high requirements for the face images of the sample sets, have poor resistance to conventional attacks and geometric attacks, and the recognition effect of the algorithms are not ideal.

Face encryption and recognition system based on deep learning. The advent of high-performance computers makes it possible for processing large-scale face datasets. Coupled with a deep understanding of face recognition, the accuracy of face recognition algorithm based on deep learning has risen to a new level. In order to ensure the encryption and recognition efficiency of face images, the face encryption and recognition systems generally include two parts: client and data server [9–13]. The clients use algorithms such as Paillier algorithm [14,15] and asymmetric encryption algorithms [16] to encrypt face images. And then they deploy neural network models such as CNN [14,17] and

CycleGAN [16,18] on high-performance data servers to recognize the encrypted faces. This kind of methods has high encryption efficiency and good recognition effect. The pixe distributions of encryption images are uniform. The entropy of images is high. These methods have good visual scrambling performance, and can resist certain conventional attacks and geometric attacks. However, there are still several shortcomings: 1) Geometric features of encrypted face images have been hidden. It results in unstable training results of neural network models. And the quality of decoded images need to be improved [16]. 2) The performance requirements of the servers are high, and the feature vector elements of batch processing cannot be accessed separately, which limits the flexibility of the methods [19]. 3) The face templates are stored in the server by plain text. It is easy to cause information leakage or loss, once the servers are attacked [20]. In addition, C. Karri compared the recognition rate of several neural network models for encrypted faces in the cloud environment, and found that the recognition accuracy of AES, RSA and RCP is not ideal [21,22].

Inspired by the above limitations, this paper proposes an encrypted face recognition method based on Ridgelet-DCT transform and tent-Henon double chaos. The main contributions are as follows:

1) This paper proposes a new tent-Henon double chaos model, which has the characteristics of large key space, sensitive initial value, and high complexity.

2) A new method of face feature extraction in Ridgelet-DCT transform domain is proposed, and combined with Tent-Henon double chaos model to encrypt face images.

3) A neural network model is designed to recognize encrypted face images. The model can recognize encrypted face images under conventional attacks and geometric attacks, and has a good recognition effect.

4) It solves the problem that the existing algorithm cannot recognize the encrypted face image, or the recognition effect is not ideal. In addition, the initial images are not required for decryption, which protects the facial image information effectively.

The algorithm takes into account the characteristics of Ridgelet algorithm with higher approximation accuracy, better sparse expressive ability and DCT resistance to conventional attacks ability, ergodicity, robustness and so on. The tent-Henon double chaotic encryption system has the characteristics of large secret key space, high complexity, and sensitive initial values. The basic features of the encrypted face images have been hidden and they are difficult to crack. The PCA algorithm is used to extract the features of the encrypted face images. It eliminates the mutual influence between the original data components, and can reduce the complexity of the algorithm and save the time of neural network training. The algorithm proposed in this paper can achieve better recognition results while taking into account the protection of face images.

2. The fundamental theory

2.1. Ridgelet transform

Ridgelet transform is a non-adaptive high-dimensional function representation method. It has the ability of direction selection and recognition, and can represent directional singular features in signals more effectively [23,24]. Compared with wavelet transform, Ridgelet transform has higher approximation accuracy and better sparse representation performance for image processing. And it has stronger noise suppression ability. Its mathematical model is:

$$CRT_f(a,b,\theta)=\int_{R^2}\psi_{a,b,\theta}(z)f(z)dz \tag{1}$$

here, $\psi_{a,b,\theta}(x)=a^{-\frac{1}{2}}\psi\left(\frac{x\cos\theta+y\sin\theta-b}{a}\right)$ denotes the ridge function. Eq (1) denotes the continuous ridgelet transform of $f(z)$ on R^2. Ridgelet transform can be expressed as one-dimensional wavelet transform on Radon transform. The inverse transformation of Ridgelet transform is expressed as:

$$f(z)=\int_0^{2\pi}\int_{-\infty}^{\infty}\int_0^{\infty}CRT_f\left(a,b,\theta\right)\psi_{a,b,\theta}(z)\frac{da}{a^3}db\frac{d\theta}{4\pi} \tag{2}$$

2.2. Design of tent-Henon-map double chaotic systems

2.2.1. Tent map

Tent map is a piecewise function with linear mapping. It is sensitive (especially for the initial values), unrepeatable, uncertain, unpredictable and other characteristics. The mathematical model of Tent map is shown by Eq (3).

$$x_{n+1}=\begin{cases}\dfrac{x_n}{\alpha},0<x_n\le\alpha\\ \dfrac{1-x_n}{1-\alpha},\alpha\le x_n<1\end{cases} \tag{3}$$

Tent map is in the chaotic state, when $\alpha\in(0,1)$ and $x_n\in(0,1)$. Usually, the initial value x_0 takes a different value from the system parameter α in order to avoid forming a periodic system. The initial value is $x_0=0.001$, and the iteration is 300 times. When $\frac{1}{2}\le\alpha<1$, the branch diagram of chaotic mapping of Tent map is shown in Figure 1. However, Tent map has few variable parameters, simple structure, vulnerable to attacks, and low security [25,26].

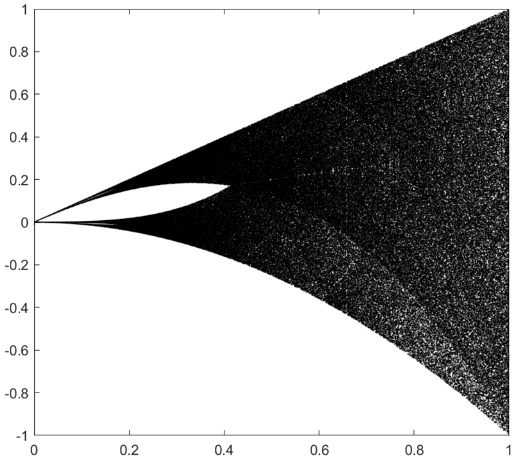


Figure 1. Branching diagram of chaotic mapping of tent map.

2.2.2. Henon map

Henon chaos is a discrete nonlinear dynamical system. Eq (4) is the mathematical model of Henon chaos.

$$\begin{cases} x_{n+1} = 1 - \alpha x_n^2 + y_n \\ y_{n+1} = \beta x_{n+1} \end{cases} \tag{4}$$

And α, β are system parameters, when $\alpha = 1.4$, $\beta = 0.3$, the system is in the chaotic state. Henon chaos is generated from variables and simultaneous iterations. It is more complex than the simultaneous creation of two independent one-dimensional chaos equations, as shown in Figure 2. Henon map is complex and easy to implement. It is suitable as a pseudo-random sequence generator for image encryption.

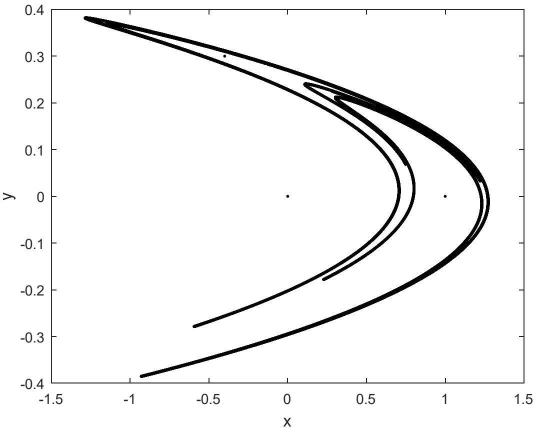


Figure 2. Henon mapping space.

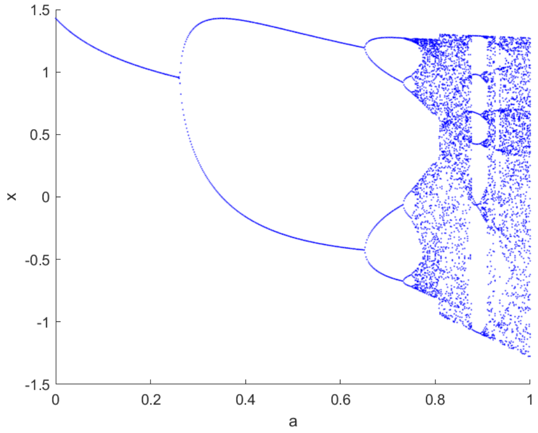


Figure 3. The bifurcation diagram of Henon map.

However, Henon mapping has two security problems: first, no matter what the initial values are, there will be a blank window in the chaos region, as shown in Figure 3. Second, there is a "stable window". In other words, the generated sequence values will be clustered within a certain region, while the other regions are blank.

2.2.3. Design of tent-Henon-map double chaotic systems

In this paper, a tent-Henon double chaotic system (THM) is designed according to the characteristics of large key space of Tent Map and high complexity of Henon map, which are suitable for two-dimensional images. The system uses THM for encryption twice, which makes up for the deficiency of tent map and Henon map. It is simple in structure, very sensitive to initial values, large in key space, fast in calculation. The system also can generate chaotic sequence which is difficult to predict, and more flexible in application. Moreover, THM double chaotic system can change the dynamic behavior of chaotic system, avoid the periodic degradation problem of low chaotic system, and it can effectively resist the model reconstruction, exhaustive and other attacks.

Here, the initial values $x_0 = 0.36$ and $a = 0.998$ are seted to generate Tent chaotic sequence, which is transformed into matrix T_1. And initial values $\alpha = 1.4$, $\beta = 0.314$, $x_0 = 0$ and $y_0 = 0$ are seted to generate chaotic matrix H_1. T_1 and H_1 are transformed into binary matrices T_2 and H_2 by Eqs (5) and (6).

$$T_2(i,j) = \begin{cases} T_1(i,j) = 0, T_1(i,j) < T_{average} \\ T_1(i,j) = 1, T_1(i,j) \geq T_{average} \end{cases} \tag{5}$$

$$H_2(i,j) = \begin{cases} H_1(i,j) = 0, T_1(i,j) < H_{average} \\ H_1(i,j) = 1, T_1(i,j) \geq H_{average} \end{cases} \tag{6}$$

Then T_2 and H_2 perform XOR operation and dot product operation respectively, and Key_1 and Key_2 are obtained by Eqs (7) and (8).

$$Key_1 = T_2 \oplus H_2 \tag{7}$$

$$Key_2 = T_2.*H_2 \tag{8}$$

2.3. PSNR

Peak signal-to-noise ratio (PSNR) is a widely used measurement method to evaluate image quality. It represents the ratio of the maximum possible power of the signal to the destructive noise power that affects its representation accuracy, as shown in Eq (9). The peak signal to noise ratio (PSNR) is usually used as the objective evaluation standard of image quality.

$$PSNR = 10\lg\left[\frac{MN \max\limits_{i,j}\left(\mathrm{I}(i,j)\right)^2}{\sum\limits_{i}\sum\limits_{j}\left(\mathrm{I}(i,j) - \mathrm{I}'(i,j)\right)^2}\right] \tag{9}$$

Here, $I(i,j)$ and $I'(i,j)$ are the pixel values of each point of the original image and the transformed image respectively.

3. The proposed algorithm

The algorithm proposed includes two parts: face image encryption and encrypted face image recognition.

3.1. THM double chaotic encryption algorithm based on Ridgelet-DCT transform

This paper designed a face image encryption algorithm under the transform domain based on Ridgelet transform and DCT transform, and its main process is shown in Figure 4.

(1) $Image_{\mathrm{Rid}}$ is obtained by Ridgelet transform of the original face image $Image(w,h)$.

(2) The encrypted data $Image_{\mathrm{Rid\_k1}}$ is obtained by the dot product of key_1 and $Image_{\mathrm{Rid}}$.

(3) DCT transform is used to encrypt $Image_{\mathrm{Rid\_k1}}$ to obtain $Image_{\mathrm{Rid\_k1\_dct}}$, and then $Image_{\mathrm{Rid\_k1\_dct}}$ takes the dot product with key_2.

(4) DCT inverse transformation to obtain the encrypted image $EImage$. The decryption process of the algorithm is the inverse of the encryption process.

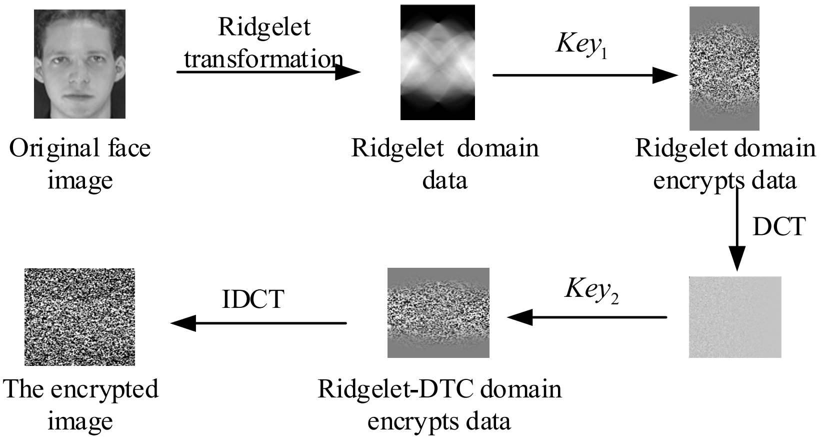


Figure 4. The main steps of the Ridgelet-DCT double chaotic encryption algorithm.

3.2. Neural network face recognition algorithm based on feature extraction

To improve the recognition rate of encrypted face images and reduce the complexity of the algorithm, this paper use PCA to extract the features of encrypted face images. BP neural network is widely used in the fields of data mining and pattern recognition. It has the characteristics of simple structure, fast running speed, small resource consumption, and can meet the low latency in the cloud environment. The main process of the algorithm is shown in Figure 5, and its main steps are as follows:

Step 1: Build encrypted face database. Face images are encrypted by using the encryption algorithm, and the encrypted face image database is obtained. Then, PCA algorithm is used to extract the features of encrypted face data, and the projection matrix T is obtained after feature dimension reduction.

Step 2: Create and train the neural network. The samples are divided into training set and testing set. The structure neural network includes one input layer, two hidden layers and one output layer. Data features of training set are extracted, dimensionality reduction matrixes are obtained, and then the trained neural network is established.

Step 3: Testing the neural network. We use the encryption algorithm to encrypt the testing set, and then extract the feature information to get the projection matrixes E, put E into the trained neural network to complete the learning.

Step 4: Recognize the encrypted face images. The encrypted face images to be recognized are put into the trained neural network to get the final results.

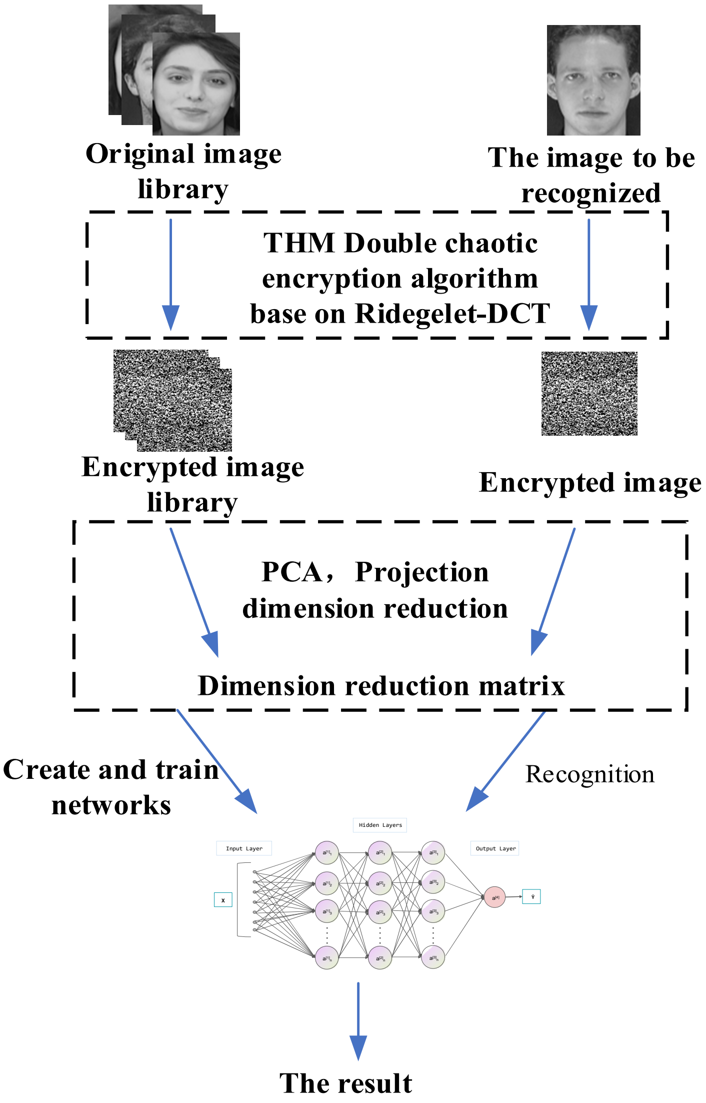

Original image library
The image to be recognized
THM Double chaotic encryption algorithm base on Ridegelet-DCT
Encrypted image library
Encrypted image
PCA，Projection dimension reduction
Dimension reduction matrix
Create and train networks
Recognition
Input Layer
Hidden Layers
Output Layer
x
y
The result

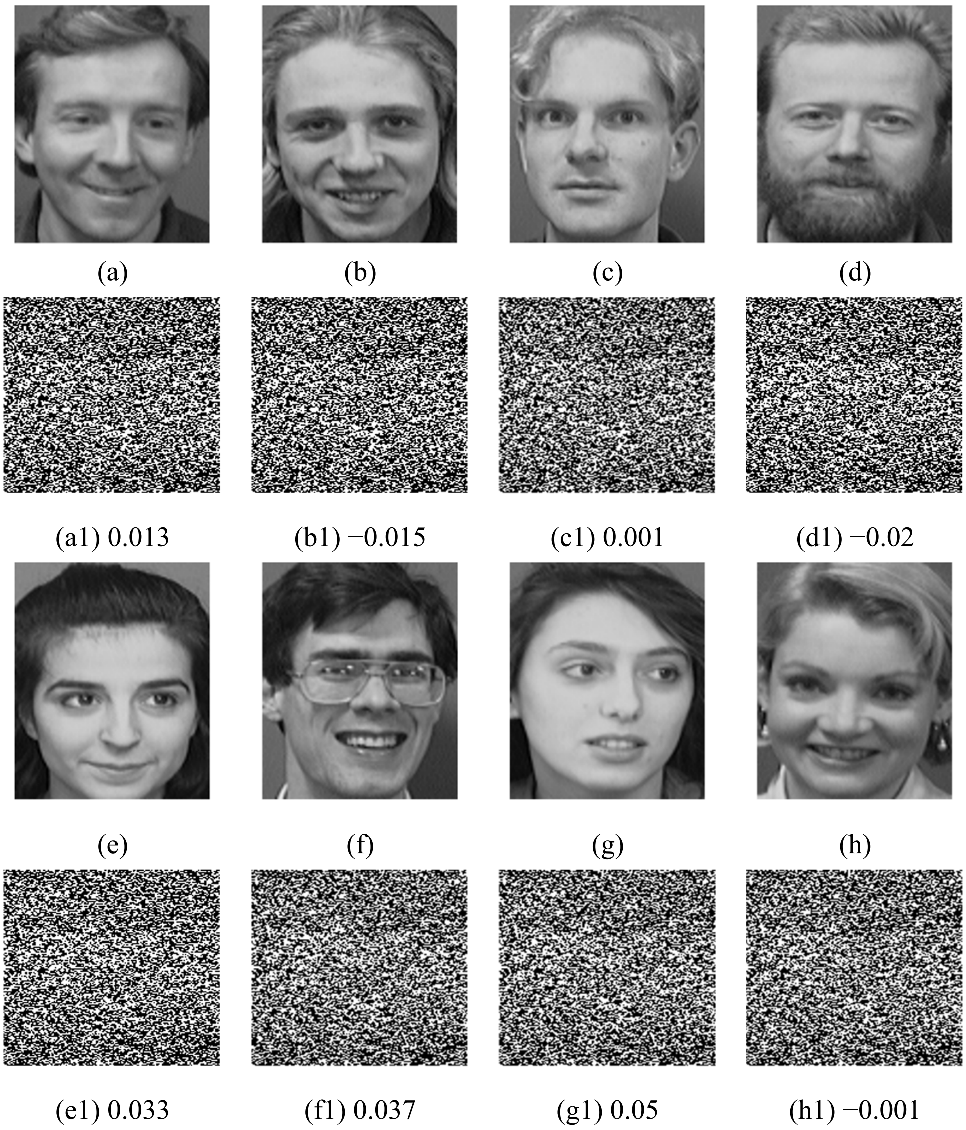
Figure 5. The flow of the recognition algorithm.

4. Simulation results

Combined with the specific requirements of this paper, the ORL face database is selected to verify the algorithm. The original image data is taken from the ORL face database, which contains 40 individuals with serial numbers. Taking the first ORL face image as an example, we verify the sensitivity and robustness of the proposed algorithm.

4.1. The results of encryption algorithms

The original and encrypted face images of the following 8 people are randomly displayed, as shown in Figure 6.



(a) (b) (c) (d)

(a1) 0.013 (b1) −0.015 (c1) 0.001 (d1) −0.02

(e) (f) (g) (h)

(e1) 0.033 (f1) 0.037 (g1) 0.05 (h1) −0.001

Figure 6. The original face images and their encrypted face images (The values behind the images are the correlation coefficients between the original images and the encrypted images).

By observing it can be found that the encrypted images compared with the original images, great changes have taken place. In the case that only the encrypted images are mastered, it is not possible to associate them with any face map, nor to determine the specific images content they represent.

4.2. Sensitivity analysis of algorithm

The THM double chaotic system designed in this paper has 8 initial values, and it is highly sensitive to the initial values. So even small changes in the keys, we cannot get the correct decryption image, which will cause the images encryption to fall into a chaotic state. When other parameters are kept unchanged, the initial parameter of Tent Map is changed to $x_0 = 0.36 + 10^{-16}$ or the initial parameter of Henon Map is changed to $a = 1.4 + 10^{-16}$, it can be found that neither of them can get the correct face image, as shown in Figure 7.

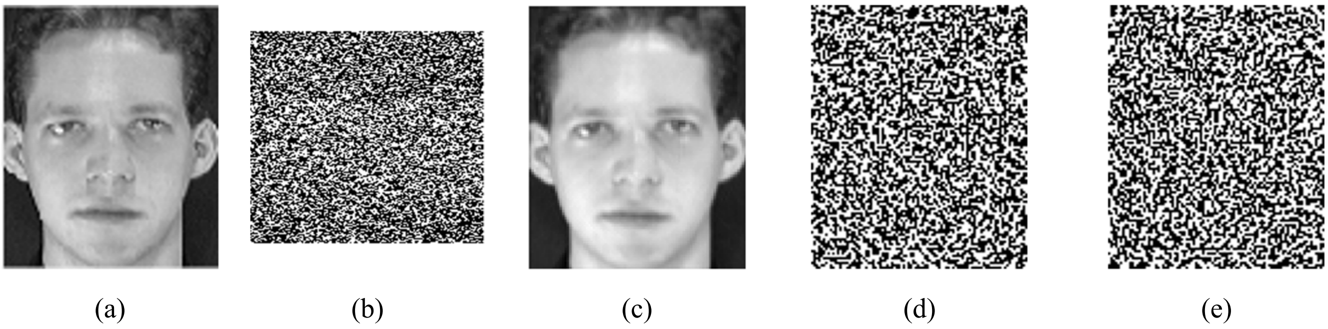


Figure 7. The sensitivity testing of the encryption algorithm. (a) Original image, (b) Encrypted Image, (c) Decrypt correctly, (d) Decrypt incorrectly ($x_0 = 0.36 + 10^{-16}$), (e) Decrypt incorrectly($a = 1.4 + 10^{-16}$).

The key space of the algorithm is 10^{116}, which is much higher than other key Spaces in the references [3,27–29], as shown in Table 1. It shows that the face encryption algorithm proposed in this paper is safe and reliable. It can protect the security of face image data well in the cloud environment.

Table 1. Comparison of the key spaces.

THM Double chaotic encryption	Other algorithm in [3]	Other algorithm in [27]	Other algorithm in [28]	Other algorithm in [29]
10^{116}	10^{96}	10^{32}	2^{256}	10^{100}

4.3. Robust analysis of the algorithm

The robustness of the proposed algorithm is verified from the aspects of anti-noise attacks, anti-geometry attacks and anti-occlusion attacks. The images of different attacks and their encrypted images are shown in Figure 8.

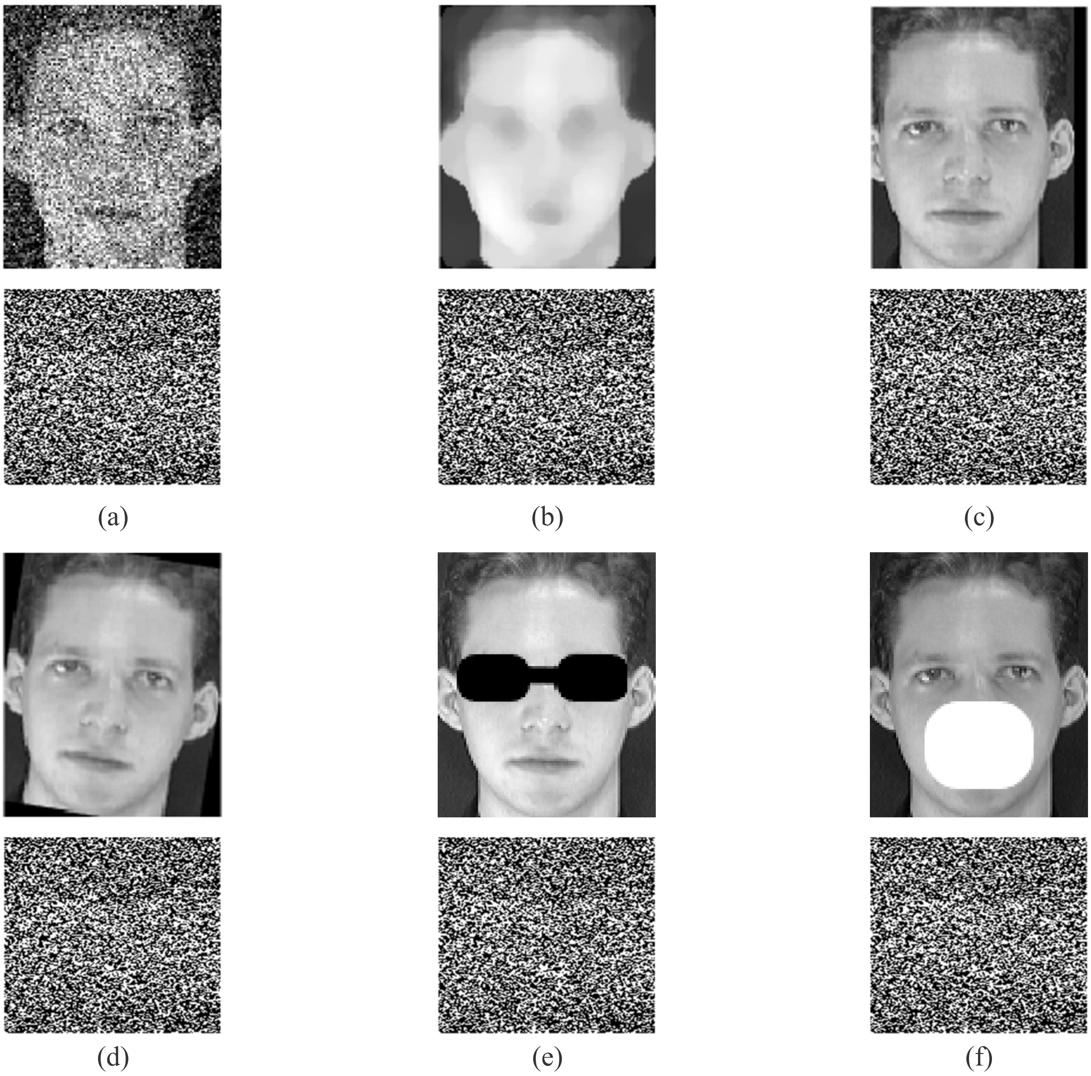


Figure 8. Various attacks on face images and their encrypted images. (a) Gaussian noise attack, (b) Median filtering attack, (c) Horizontal shift to the left, (d) clockwise rotation, (e) Occlusion (Glass), (f) Occlusion (Mask).

Under the attacks of Gaussian noise and mean filtering, the recognition results of the algorithm designed in this paper is shown in Table 2. When the noise is increased to 20%, the algorithm can still correctly recognize the face image whose serial number is 1. When the noise intensity increases by 50%, the algorithm identifies errors. Under the attacks of median filtering, the algorithm can accurately recognize the serial number of face images as 1. The results show that the algorithm has good robustness under the attacks of Gaussian noise and mean filtering.

After the rotation attacks, the algorithm can correctly recognize the encrypted face images within 10° clockwise and 12° counterclockwise. It shows that the algorithm has a certain ability of resisting rotation attack and has strong robustness, as shown in Table 3.

In the mobile attacks, the left and right movement within 9% to 3%, the algorithm can correctly recognize the face images. Both up and down movements are within 4%, it can also be accurately identified. It indicates that the algorithm has good robustness against mobile attacks, as shown in Table 4.

Table 2. The results of Gaussian noise attackS and median filtering attacks.

Attacks	Intensity	PSNR (dB)	Serial number
Noise (%)	10	10.7232	1
	20	8.8570	1
	50	7.10	18
Median filtering (10Times)	[3 × 3]	29.20	1
	[5 × 5]	24.02	1
	[7 × 7]	20.01	1

Talbe 3. The results of rolling attacks.

Clockwise	Rotation (°)	8	9	10	11
	PSNR (dB)	16.69	16.23	15.83	15.47
	Serial number	1	1	1	24
Contrarotate	Rotation (°)	10	11	12	13
	PSNR (dB)	15.83	15.47	15.16	14.87
	Serial number	1	1	1	12

Table 4. The results of mobile attacks.

Attacks	Direction	Percentage shift(%)	PSNR (dB)	Serial number
Horizontal movement	Left	8	14.23	1
		9	12.86	1
		10	12.69	8
	Right	2	22.90	1
		3	19.59	1
		4	17.78	18
Vertical movement	Up	3	16.36	1
		4	15.44	1
		5	14.68	13
	Donw	3	19.46	1
		4	18.31	1
		5	17.42	24

Table 5. The result of occlusion attacks.

Attacks	Keep out area	S	M	L
Occlusion (Glass)	PSNR (dB)	15.53	12.32	9.99
	Serial number	True	True	False
Occlusion (Mask)	PSNR (dB)	18.52	17.47	13.11
	Serial number	True	True	True
The recognition algorithm in [3]	PSNR (dB)	20.78	17.64	15.68
	Serial number	True	True	False
The recognition algorithm in [27]	PSNR (dB)	18.78	17.99	15.77
	Serial number	True	True	False

Occlusion attack is one of the most common situations and difficult problem in face recognition. As the main facial features are occluded, the recognition effect and robustness of the algorithm will decrease significantly. This paper aims at the most common glasses occlusion attacks and masks occlusion attacks to verify the recognition effect of the algorithm. The range of occlusion are divided into S, M and L from large to small. Under the condition that data encryption is guaranteed, the algorithm designed in this paper can be correctly identified except for the cover of the L mask and the cover of the L glasses. In the case of a lower PSNR, the algorithm proposed in this paper is better than the algorithms in references [3] and [16], as shown in Table 5. It shows that the algorithm has good robustness under occlusion attack.

5. Conclusions

In order to protect the security of face data storage and transmission in cloud environment, this paper proposed a tent-Henon double chaotic encryption face recognition algorithm based on Ridgelet-DCT transform. Combined with PCA feature extraction and neural network model, the encrypted face recognition algorithm proposed in cloud environment is robust. The experimental results show that the algorithm designed in this paper has good performance in encryption effect, security and robustness. However, the structure of the neural network used in the algorithm is relatively simple, so it is feasible to transplant the idea and design of the algorithm to a more advanced neural network. This will be the direction of further research in the future.

Acknowledgments

This work was supported by the Hainan Provincial Natural Science Foundation of China (620QN286).

Conflict of interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. K. M. Hosny, M. Abd Elaziz, M. M. Darwish, Color face recognition using novel fractional-order multi-channel exponent moments, *Neural Comput. Appl.*, **33** (2021), 5419–5435. doi: 10.1007/s00521-020-05280-0.
2. A. R. Javed, Z. Jalil, Byte-level object identification for forensic investigation of digital images, in *IEEE 2020 International Conference on Cyber Warfare and Security (ICCWS)*, (2020), 1–4. doi: 10.1109/ICCWS48432.2020.9292387.
3. J. Hu, J. Li, S. A. Nawaz, Q. Lin, Research on encrypted face recognition algorithm based on new combined chaotic map and neural network, *Innovation Med. Healthcare*, **2020** (2020), 105–115. doi: 10.1007/978-981-15-5852-8_10.
4. B. Zhang, B. Tondi, M. Barni, Adversarial examples for replay attacks against CNN-based face recognition with anti-spoofing capability, *Comput. Vision Image Understanding*, **197** (2020), 102988. doi: 10.1016/j.cviu.2020.102988.

5. A. Athalye, L. Engstrom, A. Ilyas, K. Kwok, Synthesizing robust adversarial examples, preprint, arXiv:1707.07397.
6. Z. Zhu, Y. Lu, C. K. Chiang, Generating adversarial examples by makeup attacks on face recognition, in *2019 IEEE International Conference on Image Processing (ICIP)*, (2019), 2516–2520. doi: 10.1109/ICIP.2019.8803269.
7. A. Nguyen, J. Yosinski, J. Clune, Deep neural networks are easily fooled: High confidence predictions for unrecognizable images, preprint, arXiv:1412.1897.
8. Y. Wang, X. Chen, J. Zhu, W. Chu, Y. Tai, C. Wang, et al., *HifiFace: 3D shape and semantic prior guided high fidelity face swapping*, 2021. Available from: https://johann.wang/HifiFace/.
9. F. Ding, G. Zhu, Y. Li, X. Zhang, P. K. Atrey, S. Lyu, Anti-forensics for face swapping videos via adversarial training, *IEEE Trans. Multimedia*, **2021** (2021), 1–13. doi: 10.1109/TMM.2021.3098422.
10. G. Iovane, C. Bisogni, L. D. Maio, M. Nappi, An encryption approach using information fusion techniques involving prime numbers and face biometrics, *IEEE Trans. Sustainable Comput.*, **5** (2020), 260–267. doi: 10.1109/TSUSC.2018.2793466.
11. C. Liu, J. Li, Y. Duan, A face image recognition algorithm based on DFT encryption domain, in *2017 First International Conference on Electronics Instrumentation and Information System*s, (2017), 1–6. doi: 10.1109/EIIS.2017.8298669.
12. M. Chamikara, P. Bertok, I. Khalil, D. Liu, S. Camtepe, Privacy preserving face recognition utilizing differential privacy, *Comput. Secur.*, **97** (2020), 1–12. doi: 10.1016/j.cose.2020.101951.
13. S. Guo, T. Xiang, X. Li, Towards efficient privacy-preserving face recognition in the cloud, *Signal Proc.*, **164** (2019), 320–328. doi: 10.1016/j.sigpro.2019.06.024.
14. Y. Ma, L. Wu, X. Gu, J. He, Y. Zhou, Secure face-verification scheme based on homomorphic encryption and deep neural networks, *IEEE Access*, **2017** (2017), 16532–16538. doi: 10.1109/ACCESS.2017.2737544.
15. F. A. Khan, A. Bouridane, S. Boussakta, R. Jiang, S. Almaadeed, Secure facial recognition in the encrypted domain using a local ternary pattern approach, *J. Inf. Secur. Appl.*, **59** (2021), 1–5. doi: 10.1016/j.jisa.2021.102810.
16. Z. Bao, R. Xue, Y. Jin, Image scrambling adversarial autoencoder based on the asymmetric encryption, *Multimedia Tools Appl.*, **2021** (2021), 1–37. doi: 10.1007/s11042-021-11043-3.
17. H. Chabanne, R. Lescuyer, J. Milgram, C. Morel, E. Prouff, Recognition over encrypted faces, in *International Conference on Mobile, Secure, and Programmable Networking*, (2018), 174–191. doi: 10.1007/978-3-030-03101-5_16.
18. J. Yang, J. Liu, R. Han, J. Wu, Transferable face image privacy protection based on federated learning and ensemble models, *Complex Intell. Syst.*, **2021** (2021), 1–17. doi: 10.1007/s40747-021-00399-6.
19. P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch, On the application of homomorphic encryption to face identification, in *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, (2019), 1–8.
20. X. Yang, H. Zhu, R. Lu, X. Liu, H. Li, Efficient and privacy-preserving online face recognition over encrypted outsourced data, in *2018 IEEE Confs on Internet of Things*, (2018), 366–373. doi: 10.1109/Cybermatics_2018.2018.00089.
21. C. Karri, Secure robot face recognition in cloud environments, *Multimed Tools Appl.*, **80** (2021), 18611–18626. doi: 10.1007/s11042-020-10253-5.

22. C. Karri, M. S. R. Naidu, Deep learning algorithms for secure robot face recognition in cloud environments, in *IEEE International Conference on Big Data and Cloud Computing (BdCloud)*, (2020), 1021–1028. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00154.
23. X. Zhang, Ridgelet analysis and its application in image compression, Ph.D thesis, Xidian University, 2006.
24. M. N. Do, M. Vetterli, The finite ridgelet transform for image representation, *IEEE Trans. on Image Proc.*, **12** (2003), 16–28. doi: 10.1109/TIP.2002.806252.
25. Z. Hua, Y. Zhou, One-dimensional nonlinear model for producing chaos, *IEEE Trans. Circuits Syst.*, **1** (2018), 235–245. doi: 10.1109/TCSI.2017.2717943.
26. H. Wang, D. Xiao, X. Chen, H. Huang, Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map, *Signal Proc.*, **3** (2018), 444–452. doi: 10.1016/j.sigpro.2017.11.005.
27. T. Xiao, J. Li, J. Liu, J. Cheng, U. A. Bhatti, A robust algorithm of encrypted face recognition based on DWT-DCT and tent, in *International Conference on Cloud Computing and Security*, (2018), 508–518. doi: 10.1007/978-3-030-00009-7_46.
28. H. Zhu, B. Pu, Z. Zhu, Y. Zhao, Y. Song, Two-dimensional sine-tent-based hyper chaotic map and its application in image encryption, *J. Chin. Comput. Syst.*, **7** (2019), 1510–1517.
29. C. Zhu, G. Wang, K. Sun, Cryptanalysis and improvement onan image encryption algorithm design using a novel chaos based s-box, *Symmetry*, **10** (2018), 1–15. doi: 10.3390/sym10090399.