Privacy-Preserving Facial Recognition Models: Retaining Learning Without Storing Facial Information

[1]He Yi, [2]Shi Lei, [3]Rowell Hernandez ,

[1]Batangas State University, The National Engineering University,4200, Batangas City,Philippines; 21-08297@g.batstate-u.edu.ph

[2]Batangas State University, The National Engineering University,4200, Batangas City,Philippines; 21-01463@g.batstate-u.edu.ph

[3]Batangas State University, The National Engineering University,4200, Batangas City,Philippines ;rowell.hernandez@g.batstate-u.edu.ph

Correspondence: Jeffrey S. Sarmiento ,Batangas State University, The National Engineering University,4200, Batangas City,Philippines; jeffrey.sarmiento@g.batstate-u.edu.

Abstract

At present, most application developers still need to save face images on the server, so they may still be stolen or stolen by service providers. Application service providers can use user facial information in specific visual scenes, but they cannot restrict service providers from using visual information on the server. This paper studies a server-oriented face image privacy protection technology. The research results of this paper are color-based face image perturbation algorithms, which will provide new ideas for solving face detection problems under complex backgrounds and improve the accuracy of detection. The face perturbation algorithm based on feature points can effectively overcome the shortcomings of existing algorithms that only focus on one feature and lack universality. The corresponding mathematical proof is also given in this paper, and the corresponding theoretical basis is given. Through experiments on face databases, we found that the accuracy of using different neural networks to detect images before and after perturbation is between 0.20% and 6.38%. Various different face image quality assessment methods are used and compared with the existing best face perturbation algorithms. The experimental results show that the image quality of the scrambled images is still greatly improved, and compared with the existing algorithms, it has better effects and can meet the needs of data availability.

Keywords : privacy protection; facial recognition ; face perturbation

I. Introduction

Face recognition is a very complex task, which involves processes such as face encoding and face matching. In these algorithms, face detection is used to determine the location of the face. Face alignment means identifying a person's facial information by identifying specific areas such as the nose, eyes and mouth. Face encoding technology converts the extracted facial pixels into recognizable feature vectors, which are so-called templates. Through face recognition, each person's identity is identified. In some application scenarios, service providers must disclose user image information, but if it is disclosed, it is easy to cause privacy leakage, and traditional methods such as mosaics will affect the availability of data. On the other hand, there are more and more regulations on user privacy, and operators are also trying to find a balance between data availability and facial visual privacy. In the process of face detection, image acquisition and storage face the risk of data leakage.

Existing research faces problems such as low data availability and high privacy computing overhead. Among the existing privacy protection algorithms, most of them achieve privacy protection by interfering with or encrypting image pixels. However, the encryption method of pixel points has a large loss of time and space complexity and cannot meet the needs of delay sensitivity or huge data scale. In addition, how to minimize image damage while maintaining image privacy is also a problem worth studying [1]. In response to the above problems, this paper studies an algorithm for low-destructive interference with facial images to ensure user privacy. Facial images are composed of three basic colors: red, green, and blue. Three different pixel channels together form facial images of different colors, and on this basis, the colors of different colors are analyzed. The design of privacy protection methods for facial images includes the following issues:

(1) Assume that there are M face images stored on the server. In practical applications, M is a very large number. In addition, when a face image is perturbed, it must be divided into three different pixel channels. In addition, the number of face image pixels stored in the database is in the order of 10^{5}. When a pixel in an image is perturbed, the time complexity required to perturb the image is approximately C* M*10^{5}, where C is a constant. If most pixels are directly perturbed, it will cause a high performance loss [2].

(2) From the perspective of availability, perturbing an image will inevitably change the pixel distribution of the original image, resulting in a decrease in data availability. How can we ensure that the perturbed image can still be detected while maintaining the privacy of the perturbation algorithm?

In order to solve the problem (1), this method does not need to interfere with all image pixels. Since facial images mainly contain important features such as eyes and noses, before interfering with the image, its position is determined first, and then it is interfered with. This can effectively reduce the number of interfering pixels, thereby achieving privacy protection and reducing the cost of the algorithm. When the same number of pixels are interfered, by reducing the interference area, the interference density of the critical area can be increased, thereby obtaining a better interference effect.

For problem (2), a pixel replacement algorithm is used. A face image segmentation algorithm based on wavelet transform is used. This algorithm uses the numerical values of pixels in various parts of the face image and performs spatial transformation on them [3]. This algorithm uses a new image processing technology, that is, improving the image quality by interfering with the image pixels.

In terms of algorithm structure, this paper divides the image into two parts: image data processing and pixel disturbance. The image data processing module performs format standardization on the image and converts the color image into a pixel allocation matrix of the red, green and blue channels, while the image disturbance module performs specific disturbance operations on the pixels of each color channel.

II. Methodology

2.1 Image Classification

Image classification based on image features is a basic problem in computer vision. The main task of face image detection is to distinguish faces from other objects, providing a basis for future applications such as face recognition and age recognition.

Euclidean distance, also known as Euclidean distance, is the true distance between two points in one-dimensional space, or in other words, a vector length [4]. Euclidean distance transformation is to transform a pixel value in a binary image into the distance between it and the nearest background point, thereby obtaining a binary image. The larger the Euclidean distance between two images, the greater the difference between the images. At present, most image recognition methods are based on Euclidean distance to judge the similarity of different images.

Suppose the pixel matrix of an image is I $_{mn}$, where m is the number of pixel matrices and n is the number of pixel matrix columns. Similarly, the pixel matrix of another image is I $_{mn}$ '. The Euclidean distance threshold for determining whether images belong to the same category is set to θ. When ||I $_{mn}$ -I $_{mn}$ '|| ^{2} ≈θ, the two images belong to the same category; when ||I $_{mn}$ -I $_{mn}$ '|| ^{2} > θ , the two images are not in the same category; ||●|| ^{2} represents the square of the 2D Euclidean distance [5].

2.2 Design of face color image perturbation algorithm

The goal of this method is to visually distinguish the original image from the interference image by perturbing each pixel. The method proposed in this paper can effectively protect the visual privacy of the original image while making the interfered image still recognizable. This method changes the pixel values of the local area by transforming the pixel points in the key area between the pixels, thereby protecting the visual privacy of the face[6].

$_{S0}$ containing M facial images and the number of times n the pixel is disturbed, read out their 3-D RGB matrices from each image imagei of S0 , perform secondary processing on the pixel matrix, and obtain the pixel matrix of three channels, each of which is a two-dimensional matrix; among which, the red channel is represented by ima ^{R} i, the green channel is represented by ima ^{G} i, and the blue channel is represented by ima ^{B} i;

Second, arrange the three pixel matrices ima ^{R} i, ima ^{G} i, ima ^{B} i in row order into a large column vector to locate the face in the image; among them, L is the leftmost position of the face in the column vector; similarly, R, U, D represent the rightmost, topmost, and bottommost positions in the column vector, respectively, and according to the area calculated in step 5, perform non-repetitive permutation operations on the pixels in the selected area; similarly, perform the same spatial permutation on the vectors of the other two columns; and restore the three column vectors according to the format of the pixel matrix.

Third, the three pixel matrices are perturbed to obtain a color face image and output the new image data set S $_d$. The following will perform specific numerical calculations on the perturbation algorithm and analyze the size of its threshold [7].

2.3 Variables in facial feature extraction

(1) Average face

In S0 , for M face images, the 2D pixel matrix of each image consists of m rows and n columns, and they are converted into m n * 1 column vectors. The pixel matrix of the two-dimensional image is represented as $\{\Gamma_1, \Gamma_2, \cdots, \Gamma_M\}$. Then the average face is defined as

$$\Psi = \frac{1}{M}\sum_{i=1}^{M} \Gamma_i$$

(2) Definition of pixel difference matrix

In the process of calculating the Euclidean distance, the dimension of the original pixel matrix is very large, so it must be reduced in dimension. The basic idea is to extract the most critical k features from the matrix (k can be set according to actual needs) to replace the original large-dimensional matrix. First, the principal component analysis method is used to reduce the dimension of the image, and the experiment verifies whether the Euclidean distance of the image before and after the dimension reduction is maximized.

(3) Matrix projection vector

Assume that , then $\mathrm{A} = \{\Gamma_1, \Gamma_2, \cdots, \Gamma_M\}$ the dimension reduction projection vector of $u_l = \sum_{k=1}^{M} \nu_{lk}\phi_k$the pixel difference matrix is; Here, vlk is $\{\phi_1, \phi_2, \cdots, \phi_M\}$the M eigenvalues of L = A $^{\mathrm{T\,A,\,l = 1,\,2,\,...,}}$ M.

Proof: A matrix uses a principal component analysis method, the purpose of which is to find a set of M-dimensional unit orthogonal vectors u that can characterize the data distribution of A matrix. The M-dimensional vector u must satisfy $\lambda_k = \frac{1}{M}\sum_{k=1}^{M} (u_k^T\phi_n)^2$, where

$$u_l^k u_k = \delta_{l,k} = \begin{cases} 1 & if l = k \\ 0 & otherwise \end{cases}$$

The covariance matrix C is defined as follows:

$$C = \frac{1}{M}\sum_{k=1}^{M} \phi_k\phi_k^T = AA^T$$

Since the dimension of matrix C is mn, it is difficult to solve its eigenvalues and eigenvectors. In addition, since the data set has M images, and in reality M is usually much smaller than mn, if the M eigenvalues and eigenvectors can be converted into eigenvalues and eigenvectors of an M-dimensional matrix, the amount of calculation can be greatly reduced.

Construct an M*M matrix L = A $^{\mathrm{T}}$ A, and obtain $u_l = \sum_{k=1}^{M} \nu_{lk}\phi_k$ the M L feature vectors vl that determine the linear combination of the training set pixel matrix, that is, the projection vector of the pixel matrix, where l = 1, 2, ..., M. [8]

From (1) to (3), we can see that the Euclidean distance has a threshold before and after the interference, and the value of the threshold is given. In practical applications, we only need to ensure that the maximum Euclidean distance before and after the interference does not exceed the maximum Euclidean distance that the detection model can distinguish. This ensures data availability and meets visual privacy.

2.4 Experimental Setup

LFPW is a widely used facial image library. It is obtained from natural scenes, so it is difficult to recognize. The LFW dataset contains 6487 face images. Each image contains multiple faces, with the main face in the middle as the training sample, and the remaining non-important faces as disturbances. Due to differences in individual age, gender, skin color and other factors, this study has raised new challenges to the study of this problem. The LFW sample set has a total of 18,974 face photos, all of which are 250x250 color photos named with corresponding names and numbers. The effectiveness of the disturbed images is verified from two aspects: face detection effect and image quality evaluation.

2.5 Detection model selection

This paper adopts two target detection methods, FasterRCNN and YOLOv3, which have high detection accuracy, fast speed and strong robustness to complex scenes. FasterR-CNN is developed on the basis of R-CNN and Fast R-CNN. It is an end-to-end detection architecture. Fast R-CNN detects and recognizes the region candidate area based on the region candidate box generated by the fast response [9]. Compared with the existing methods, this method has completed the positioning and recognition of the object when constructing the region candidate point, thereby effectively improving the recognition accuracy of the entire framework. As can be seen from Figure 1.[10]

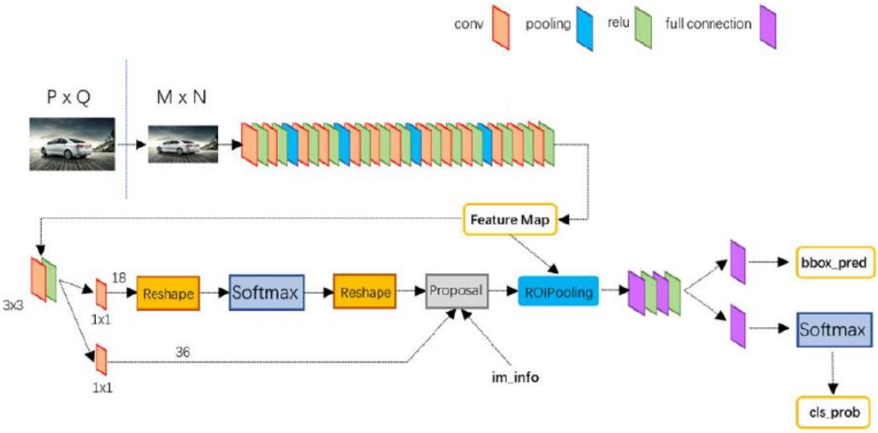

Figure 1 FasterRCN network structure

The YOLOv3 architecture uses the DarkNet-53 convolutional neural network. Figure 2 is an example of the main operation process of 416x416X3x3X3X3x3. First, the input image is scaled and the feature extraction network is used to extract features from it to generate a feature map with a specific size. Finally, three feature maps with different scales are generated. 1) After 5 downsampling, DBL (convolutional layer-batch normalization-leakyrelu activation function) is used for feature extraction, and finally a 13x13x255 feature map is obtained through convolution [11]. The second feature map is first upsampled from the first feature map, then the data of the second to last feature map is concatenated, and then feature extraction and convolution are performed on DBL to obtain a 26x26x255 feature map; the third feature map is first upsampled from the second feature map, then it is concatenated with the results of the last three downsamplings, and then feature extraction and convolution are performed on DBL to obtain a 52x52x255 feature map. Finally, the three images are input into the detection network[12].

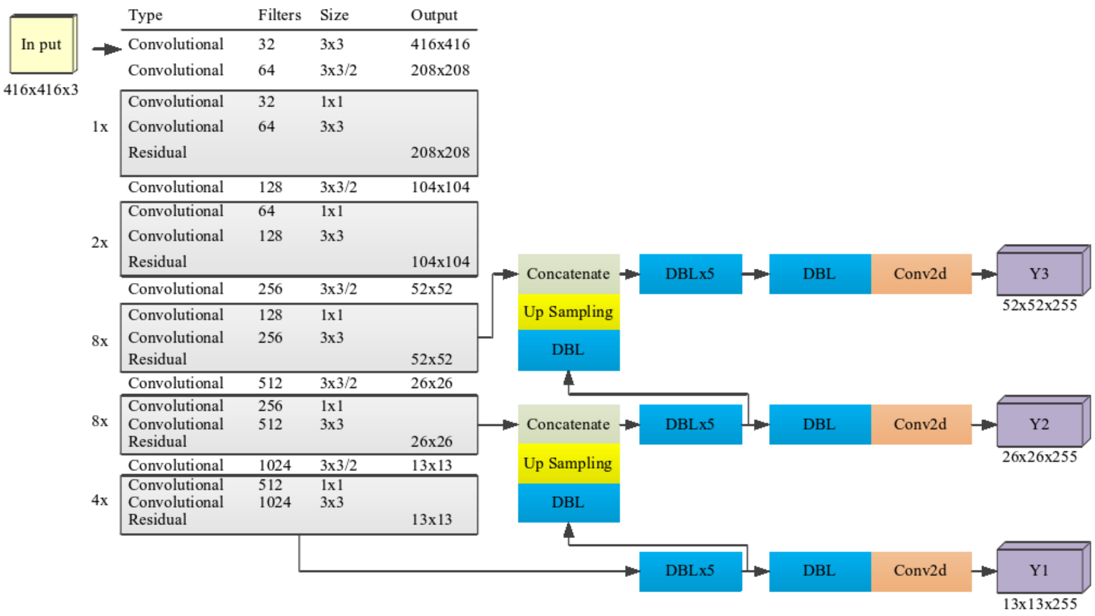

Figure 2 YOLO v3 algorithm flow chart

When the intersection-over-union ratio is 0.5, the YOLOv3 framework can achieve the same accuracy as the RetinaNet framework and greatly exceeds the SSD framework, showing the strong advantage of YOLOv3 in detection. Finally, we will use two different image processing architectures, FasterRCNN and YOLOv3, and verify the proposed method through experiments.

2.6 Evaluation indicators

(1) Precision and recall

Precision and recall are the two most important indicators in research fields such as machine vision. Precision is also called "accuracy" or "correctness". According to the definition of precision, the precision in this article is equal to the proportion of facial images in which the "face label" is detected [13]. Recall, also known as "recall rate", refers to the number of facial images accurately identified in the test sample set, which is used to represent the total number of facial images of the subject.

Accuracy = 60/80 = 75%;

Recall rate = 60/100 = 60%;

From the definition of precision and recall, we can see that there is a certain relationship between accuracy and recall. Under ideal conditions, the system can achieve high accuracy and recall. In reality, there is an inverse relationship between accuracy and recall. AP value and F value are used to comprehensively evaluate recall and precision respectively, which can better reflect the recognition effect of the target.

(2) AP value

The AP value is the area under a curve (that is, accuracy is the horizontal axis and recall is the vertical axis), which is used to evaluate the detection effect of the trained model on a certain type of object.

(3) F value

The letter P is used to express precision, and the letter R is used to express recall, which is the F value. In other words, F-measure is expressed as the sum of the weighted average of precision (P) and recall (R). The detailed definition is as follows:

$$F = \frac{(\alpha^2 + 1)^* P^* R}{\alpha^2 * (P + R)}$$

Here, α represents the weight, which is used to adjust the influence of P and R on the final effect of the F-value function. When the weight coefficient is 1, the F-value is the most commonly used case. In the following experiments, α=1.

(4) FaceQnet Scores

The basic idea of the face recognition evaluation index based on deep learning is to score the face Qnet model established by convolutional neural network to evaluate its application effect in face recognition. The research of FaceQnet shows that the score is in the range of [0,1], which is very similar to a commercial face recognition software called Face++. When the score is close to 0, it means that the input image is not suitable for face recognition, and vice versa, the value is also correct.

(5) Peak signal-to-noise ratio

Peak signal-to-noise ratio (PSNR) is the ratio of the image branch signal energy to the MSE, which is used to evaluate the quality of the image [14].

$$PSNR = 10\log \frac{MAX^2}{\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} \parallel O(i,j) - R(i,j) \parallel^2}$$

Here, O represents the original image, R represents the image after interference, the size of both images is m*n, and MAX is the maximum pixel of the image. An 8-bit binary string is usually used to express each pixel in the image, so the value of the pixel is [0,255], that is, the value of MAX is 255. A higher PSNR value indicates that the difference between the image before and after interference is small, that is, the quality of the image after interference is improved.

(6) Structural similarity index

Structural similarity (SSI) is an important indicator for measuring image quality. It comprehensively considers the image's brightness, structure, contrast and other characteristics [15]. The SSIM parameter is calculated using the following formula:

$$SSIM(x,x') = [l(x,x')]^{\alpha}[c(x,x')]^{\beta}[s(x,x')]^{\gamma}$$

Among them, l, c, s represent brightness, contrast, and structure, and x and x′ represent the original image and the image after interference. Among them, α , β , γ >0, respectively adjust the weights of the brightness, structure, and contrast of the image in the image. The following defines the three contrast indicator functions l, c, and s:

$$l(x,x') = \frac{2u_x u_{x'} + C_1}{u_x^2 + u_{x'}^2 + C_1}$$

$$c(x,x') = \frac{2\sigma_x \sigma_{x'} + C_2}{\sigma_x^2 + \sigma_{x'}^2 + C_2}$$

$$s(x,x') = \frac{\sigma_{xx'} + C_3}{\sigma_x \sigma_{x'} + C_3}$$

Here C1, C2, and C3 are all constants, u', u' are the averages of the input images x and x', and σ xx' is the covariance matrix of the input images x and x'.

The SSIM index function can be in the range of [-1,1]. When the two images are completely matched, the output of the SSIM index function is 1. Therefore, the closer the output of SSIM is to 1, the smaller the difference between x and x′ is, which means that the interference picture quality is better, which is more in line with the algorithm goal proposed in this paper. Therefore, we hope that in the next experiment, SSIM will be as close to 1 as possible, which means that the perturbation method will not cause too much damage to the structure of the image itself.

III. Results

3.1 Verification of face detection accuracy on LFW dataset after perturbation

This experiment aims to study whether LFPs can still be detected after interference and their positions can be accurately determined under interference conditions. This paper uses two different convolutional neural networks, Alexnet and Resnet101. (1) Alexnet first used RELU for convolutional neural networks and proved that this method is better than Sigmoid in deeper networks. (2) Alexnet uses the Dropout method to randomly remove local neurons, thereby effectively preventing overfitting during learning; (3) Alexnet first used overlapping maximum pooling for convolutional neural networks; (4) Graphics processing units (GPUs) are used to accelerate network calculations. It is precisely because of these characteristics that this system has shown excellent performance in practical applications. ResNet101 is built on Resnet, which can well solve the problem of reduced accuracy due to depth in the deep process.

In Figure 3, the yellow frame is the recognition result of the face recognition system, where "face" represents the type of object in the rectangular box, and the score represents the possibility that the framework thinks the object can be recognized. The highest score is 1 and the lowest is 0. The higher the score, the greater the possibility that the object in the rectangular box is considered a "face".

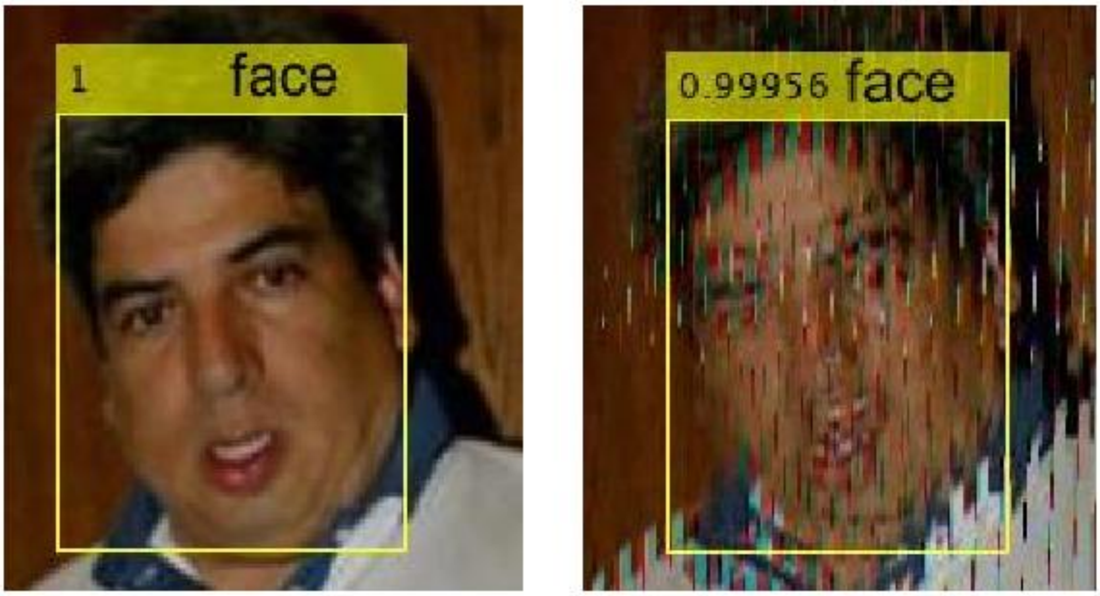

Figure 3 Face detection effect

In terms of face recognition, we randomly selected 6487 LFPW samples from LFW, and only selected the main face in the center of each image in LFPW. Among the remaining images, 1000 non-repeated face images were selected as training samples. On this basis, we will select two different types of faces, with a merging ratio of more than 0.5 and a score of more than 0.8, and consider them correct (this condition is that they are determined to be faces by the framework). We used two different detection frames, FasterR-CNN and YOLOv3. The experimental results of the original image and the disturbed image are shown in Table 1:

Table 1 Frame detection of face images before and after perturbation

Whether to disturb	frame	network	Accuracy	Recall	AP Value	F-number
no	Faster R-CNN	Alexnet	91.68%	93.67%	0.8718	0.9297
		ResNet101	92.41%	97.44%	0.9087	0.9437
	YOLO v3	DarkNet-53	92.06%	93.31%	0.8722	0.9215
yes	Faster R-CNN	Alexnet	87.21%	94.40%	0.8239	0.9034
		ResNet101	89.47%	92.77%	0.8340	0.9088
	YOLO v3	DarkNet-53	93.52%	92.38%	0.8664	0.9265

From the data shown in Table 1, it can be seen that when the number of disturbed pixels is 8000, the difference in accuracy before and after the interference is between 0.20% and 6.38%, which is not much lower than the original image. Among them, since the detection architecture of this paper is a single category, it has a higher accuracy rate. By disturbing a large number of pixels, the minimum correct rate of the face recognition algorithm for the disturbed image reaches 87.21%, and the maximum reaches 93.52%, which has good practical value and can meet the accuracy requirements of most face detection. The experimental results show that the proposed method is feasible from the perspective of facial recognition accuracy. In addition, by comparing the recall rate, AP value, and F value before and after the interference, it is found that compared with the original image, the image recall rate and AP value after the interference have not changed much, and the F value also shows that there is a good balance between the accuracy and recall rate before and after the interference. Therefore, from the performance indicators before and after the interference, it can be seen that the interference method proposed in this paper is effective.

3.2 Image quality evaluation

First, the generated image is compared with the other four algorithms. Figure 4 shows the interference image generated when the number of disturbed pixels is 8000 and the interference effect of other algorithms. On the left side of Figure 4 is an original face image. In the case of interference, the features of the face such as eyes, eyebrows and nose have changed greatly, and it is almost impossible to recognize the original face information visually.

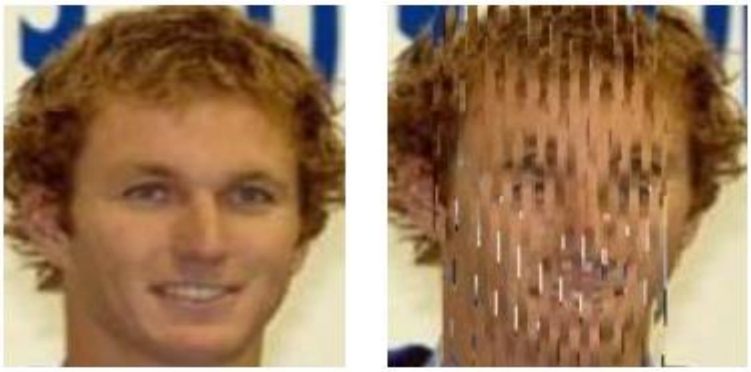

Figure 4. Protection results of face privacy protection algorithm

Table 2 shows the image size of SSIM and PSNR index under different algorithm interference. Without any processing, the SSIM score is 1, while the PSNR value is positive and infinite; due to the poor quality of face images after Gaussian noise interference, the quality of face images extracted by Gaussian interference method is poor, which limits the promotion of this method. In addition, due to the advancement of image filtering technology, the image after noise processing will also be restored to its original appearance, thereby increasing the risk of privacy leakage. The super-correction algorithm, CAE algorithm and the algorithm proposed in this paper are used to improve SSIM and PSNR, and higher SSIM and PSNR values are obtained. Therefore, the images generated by the algorithm are verified from the two aspects of SSIM and PSNR.

Table 2 Comparison of image quality of different privacy protection algorithms

Privacy Preservation Algorithm	SSIM	PSN R
Unprocessed	1	I nf
Face occlusion	0.7614	15.78
Noise(σ2=0.2)	0.5238	12.98
Noise(σ2=0.8)	0.1576	3.49
Super-Pixel(16*16)	0.8 1 39	22.67
Super-Pixel(24*24)	0.8247	19.86
CAE	0.8 254	23. 44
This method	0.8 549	23.89

Table 3 FaceQNet scores of different privacy protection algorithms

Privacy Preservation Algorithm	Super-Pixel (16*16)	Super-Pixel (24*24)	CAE	Noise(σ2=0.2)
Score	0.3 8 08	0.37 56	0.4921	0.4077

The FaceQNet score is used to test the proposed algorithm, see Table 3. This study uses the AT&T face image database as the research object. For different perturbation pixels, the face quality network score of the face image is calculated.

Figures 5 and 6 show the PSNR and SSIM averages of each image when different numbers of pixels are perturbed in the AT&T dataset. It can be seen from the images that when 4500 perturbed pixels are perturbed, the PSNR and SSIM scores are the largest, and when the perturbation amount is 9360, the PSNR and SSIM scores are the smallest, and both decrease with the increase in the number of perturbed pixels. The maximum and minimum values of the peak signal-to-noise ratio are 29.9478 and 20.7846 respectively. The maximum and minimum values of the SSIM curve are 0.6989 and 0.5465 respectively, and the average SSIM score is between 0.55 and 0.75. In terms of the score after perturbation, the image can still maintain a good structure under the perturbation of 4500-9000 pixels, and the image quality will also decrease with the increase in the number of perturbed pixels. The experimental results show that the perturbation method proposed in this paper can effectively improve the quality of the image.

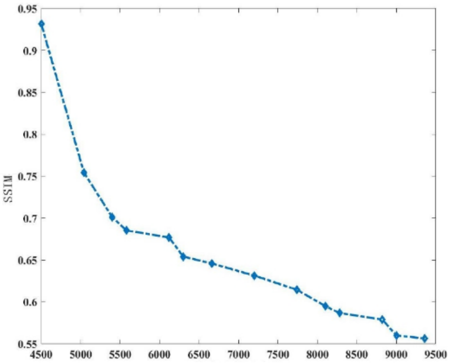

Figure 5 SSIM scores when perturbing different numbers of pixels in the AT&T dataset

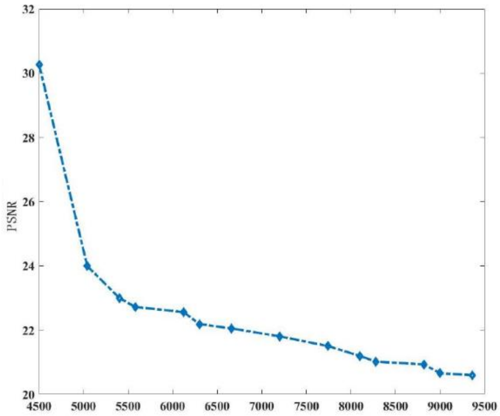

Figure 6 PS R scores when perturbing different numbers of pixels in the AT&T dataset

IV. Conclusion

This paper studies a face recognition method for image environments. The algorithm first divides the color image into two-dimensional pixel matrices of multiple channels, and then performs spatial transformation on each pixel matrix to achieve the distortion of the face image. Through this algorithm, the attacker cannot directly obtain the detailed information in the image, nor can it be reconstructed through vision, so the privacy of the face can be effectively protected. We tested this method using FasterRCNN and YOLOv3, and conducted experiments on LFPW. The results show that this method can effectively identify blurred faces. Although it has declined compared to the original method, the degree of decline is not obvious. This means that the method proposed in this paper can not only simultaneously ensure the data availability of face images, but also ensure the privacy of images.

References

[1] Zhang Nan. Kohler Bathroom secretly captured customers' facial recognition feature information and sold job seekers' resumes on recruitment platforms such as Zhaopin.com [N]. Beijing Daily, 2021-07-06(04).

[2] Shi Jiayou, Liu Siqi. Personal information protection in facial recognition technology: On the construction of dynamic consent model[J]. Finance and Economics, 2021(02):60-78.

[3] Yue Ye, Wen Ruiping, Wang Chuanlong. Face recognition algorithm with feature information convolutional neural network[J]. Journal of Engineering Mathematics, 2024, 41(03): 410-420.

[4] Hu Yuchen, Li Qiusheng. Research on facial expression recognition based on structured deep clustering network[J]. Journal of Gannan Normal University, 2023, 44(06): 56-63.

[5] Zhang Tuo. Research on face recognition algorithm based on multi-path fusion[J]. Intelligent Computers and Applications, 2024, 14(07): 64-70.

[6] Ma Xinyan, Zhang Chuancai. The Practical Dilemma and Countermeasures of Informed Consent Rules[J]. Journal of Shanghai University of Political Science and Law (Rule of

Law), 2021(05):99-109.

[7] Lin Ling. "Information and Consent" and "Data Utilization" Rules in Facial Recognition Information Protection[J]. Contemporary Communication, 2022(01):108-112.

[8] Qin E, He Jiayao, Liu Yinwei, et al. Low-resolution occluded face recognition based on densely connected channel hybrid PCANet[J]. High Technology Letters, 2024, 34(06): 602-615.

[9] Cheng Sifan. Analysis of concerns and countermeasures of information dissemination based on biometric recognition[J]. Journal of Editing, 2021, (01): 57-62.

[10] Gao Ting. Risks and liability determination of infringement of face recognition information[J]. Journal of Beijing Vocational College of Political Science and Law, 2023, (02): 88-93.

[11] Fang Shijian. Research on improvement of multi-task convolutional neural network algorithm in face recognition[J]. Wireless Internet Technology, 2023, 20(22): 96-100+111.

[12] He Ao. Theoretical basis, technical support and implementation path of educational reform in the era of artificial intelligence [J]. Journal of Shunde Vocational and Technical College, 2022, 20(01): 45-49.

[13]Luo Fugui, Song Qian, Qin Yunchu, et al. Research on application of convolutional neural network in image recognition[J]. Computer and Information Technology, 2024, 32(03): 51-54.

[14] Feng Zhanbo, Shan Chaoying. Research on visual recognition technology based on K210[J]. Digital Communication World, 2024, (06): 21-23.

[15] Liu Jiaming. Questioning the legitimacy and necessity of face recognition technology[J]. Journal of Dalian University of Technology (Social Science Edition), 2021(6):90-96.