Journal of Multimedia Information System VOL. 10, NO. 1, March 2023 (pp. 35-44): ISSN 2383-7632 (Online)
https://doi.org/10.33851/JMIS.2023.10.1.35

Online New Media Oriented Privacy Data Recognition Mechanism Based on Deep Learning

Jing Liu[1], Nali Yu[1,*]

Abstract

Although the current face de-recognition algorithm can effectively protect the user's identity, it will change the original attributes of the image, destroy the visual effect, or change the characteristics of the image to varying degrees. Traditional methods such as pixelation and occlusion can effectively realize face de-recognition, but the processed image cannot be used for basic processing such as face statistics and expression recognition, which greatly destroys the usability of the image in the field of online new media. In order to preserve more attributes of the original image and reduce the changes of facial skin color and texture features caused by the above de-recognition algorithm's operation on the whole facial area, this paper proposes a privacy protection model of face image based on generative adversarial network and facial feature analysis. Our model realizes face recognition based on changing the original image as little as possible. Specifically, we identify and extract features from fixed parts in face images, including eyes, nose, mouth, eyebrows, and cheeks. Then, we designed a face privacy recognition and protection model based on conditional generative adversarial networks. We verify our proposed method on two most commonly used face datasets in face research, namely CelebFaces Attributes and Labeled Faces in the Wild, and the results show that our proposed method achieve better performance compared with other face privacy protection methods.

Key Words: Face Recognition, GAN, New Media, Privacy Data Recognition.

I. INTRODUCTION

New media big data is faced with many security threats due to its rich value attribute [1]. The main threat to the new media big data production environment is the risk of ownership theft and abuse of media content producers. The risk of new media big data consumption environment is mainly the risk that consumers will be harassed by unsolicited bad information. The risk of security information being submerged in new media is interpreted from another perspective of the security of new media big data, which is also a hot topic in the current new media big data security research. The main motivation is to address how security information can be captured efficiently, accurately and in real time in a large volume of media data.

In the era of big data, the requirement of new media's liquidity and the traditional digital copyright protection mechanism are a pair of contradictions [2]. Traditional digital copyright protection technologies, such as DRM and Conditional Access (CA), cannot effectively solve this contradiction. The purpose of digital copyright protection technology is to protect the copyright of digital media. It technically prevents illegal copying of digital media, or makes copying very difficult to a certain extent. Consumers of digital media must be authorized to use digital media. The digital copyright protection technology is an effective means to control the unauthorized distribution of content, but it also restricts the circulation of media. Digital copyright protection technology is an effective way for the traditional media industry [3], which relies on the quantity of copies sold. However, the value of new media in the era of big data, especially the increasing value of we media, is mainly reflected in the speed and breadth of circulation. The copy income obtained through digital copyright protection technology will greatly reduce the value of new media itself, and a new technical means to change "blocking" into "thinning" is imperative. Media content fingerprint technology provides the technical basis for this. A content fingerprint is an extract from a piece of content that uniquely identifies the content in most contexts.

For video and image data [4], which account for the largest proportion of new media big data, privacy protection is much more difficult. With the emergence and popularization of the "Folksonomy" tagging method, users can freely choose custom tags to collaboratively classify video images. Thus, the cleaning of video images is simply converted to a

Manuscript received March 01, 2023; Revised March 11, 2023; Accepted March 18, 2023. (ID JMIS-23M-03-007)
Corresponding Author (*): Nali Yu, +8613930025962, yuchinali@163.com
[1]Handan Polytechnic College, Handan, China, liujing202208@126.com, yuchinali@163.com

cleaning method based on text marking. However, in many cases, these text tags cannot fully and truly reflect the content of the video or image. What's more, providers of bad information may label such information with seemingly normal and healthy labels. Therefore, in order to analyze and protect the privacy of video images from a deeper level, and to truly reflect the content of the video, it is necessary to extract feature patterns and semantics from the video. Most of the current video and image cleaning technologies are based on the basic features of the image for statistical learning and training, and are modeled by statistical learning methods such as decision trees, artificial neural networks, and support vector machines (SVM) to generate a repository of semantic models [5]. The semantic model library can automatically mark the image content after feature extraction, and filter and clean the marked content according to certain strategies.

At present, face images are the main component of new media data. The concept of face privacy recognition and face recognition differ in their intended purposes and outcomes. Face recognition is used to identify individuals, while face privacy recognition is used to protect individuals' identities and privacy. Face recognition plays an important role in various fields and industries of necessities of life. Moreover, face privacy protection is a very important research hotspot in new media art. However, compared with iris and fingerprints, facial features are a relatively weak biological feature. Face images can be obtained through a variety of channels, and it is not difficult to forge 3D avatars of others [6]. Various information leakage incidents in the recent period also indicate the urgency of users to strengthen personal privacy protection. This paper uses deep learning technology to design a face privacy protection mechanism. We anonymize the facial features and retain more facial features of the original image. Then, we design a privacy-preserving mechanism for face images using differential privacy. Differential privacy can adjust the privacy protection ability of publishing and querying data through privacy budget.

II. RELATED WORK

This chapter reviews the research on security and privacy in facial image recognition. Face recognition is an identity authentication technology based on pattern recognition based on biometrics and determines a person's identity in an information system [7]. Face recognition technology mainly involves information security and pattern recognition, that is, information security focuses on the security analysis of face recognition technology. Pattern recognition provides the principle and algorithm for extracting features based on face picture information. Modern face recognition algorithms mainly rely on deep learning technology [8-9], for example, DeepFace [10], DeepID [11], FaceNet [12]. The latest face recognition algorithm can exceed the level of human recognition on the face dataset LFW (Labeled Faces in the Wild, a widely used standard face dataset). The recognition rate of face recognition algorithms has continuously improved and reached the practical stage in recent years. For LFW, the recognition rate of the face recognition algorithm based on eigenfaces could reach 60%. By 2014, the recognition rate of face recognition algorithms based on deep learning had reached 97%. At the same time, face recognition algorithms are constantly improving security and ease of use, including occlusion recognition and live detection [13]. In short, the continuous improvement of face recognition technology has been able to meet the needs of practical application scenarios such as identity authentication, monitoring, and evidence collection, and more and more application systems or Internet services have begun to support face recognition.

From the perspective of information security, the face recognition application system as an information system needs to satisfy authenticity, confidentiality, integrity, usability, and non-repudiation. The general information system security mechanism is still applicable, but the new security and privacy issues caused by the face recognition mechanism make the face recognition application system face greater technical challenges. Face images are private. On the one hand, the face image itself, as a kind of identity information, can be used to identify individuals, and it is necessary to prevent malicious collection and abuse. On the other hand, various personal information such as age, gender, race, facial disability, health status, emotion, and even kinship can be analyzed from face datasets through image processing and data mining algorithms [14].

The commonly used protection methods to achieve face identity de-recognition include: editing images, face anonymization, face de-recognition based on deep learning, and image privacy protection based on differential privacy. Image editing [15-16] refers to the direct protection of images by means of blur, pixelation, occlusion, encryption, disturbing and other methods. Blur is the application of functions on the image, such as Gaussian function, under the action of adjacent pixels, to modify the image pixel. Pixelation is the replacement of an entire existing pixel by averaging pixels. Occlusion is to use other image areas to directly cover the sensitive area to achieve occlusion. These three methods are the simplest and effective methods to protect the sensitive area of the image. They are often used as the baseline algorithm to compare with other algorithms in face image privacy protection algorithms. However, these algorithms cause obvious damage to the visual effects of images and are often used to protect witnesses and victims in news pro-

grams or documentaries. Encryption and Scrambling are scrambling images using related algorithms. Image encryption algorithm is usually a regular encoding of the image; it can be restored to the original image through decryption. This method has the characteristics of relatively complex calculation and high security performance. It is often used in the process of image transmission. The sender encrypts the image before transmission, and the receiver decrypts the original image after receiving the image to ensure that the image cannot be stolen by a third-party during transmission [17]. Image perturbation [18] is the addition of invisible perturbation. The difference between blur and pixelation is that the former disturbs the image through different formats, such as frequency domain, spatial domain, and feature vector, while the latter disturbs the RGB pixels of the image directly. Ref. [17] encrypts the face region in the frequency domain, which requires less computation. The degree of disturbance is a key indicator for realizing privacy protection and visual effect of images. In [19], the author proposed to measure the degree of disturbance of images by the Boltzmann entropy (i.e., thermodynamic entropy), which proved the effectiveness of this scheme in gray scale images.

Face Anonymization is characterized by removing the personal identity identifier in the face data, while retaining some attributes of the face that have nothing to do with identity information. Aiming at the defects of the black box and occlusion methods, Ref. [20] proposed the k-Same image privacy protection algorithm, which determines the similarity between faces through the distance measure, averages the image components that may be the original image pixels, and create a face pixel or image feature vector from the mean. Experiments have proved that even if k-Same retains a lot of facial details, the face recognition system cannot accurately identify faces. The k-Same algorithm is an important basis for face anonymization. Ref. [21] proposed a new face anonymization algorithm, which realizes k-anonymity by adding noise to data values, and realizes k-anonymity by randomizing classified data, so that the images generated by face anonymization have better visual effects. Ref. [22] compared eight face image privacy protection algorithms in three scenarios of fuzzy face recognition, verification, and reconstruction, including Gaussian blur, median blur, pixelation, k-same, k-same-net, UPGAN, P3 and scrambling. It is proved by experiments that the method based on k-same is better than other image editing algorithms.

With the introduction of deep learning, network models based on deep learning have been widely used in various fields. The generation model based on generative adversarial network and autoencoder has made further progress in image privacy recognition and protection. Ref. [23] proposed an EPD-Net network model based on the idea of conditional generation adversarial network. Ref. [24] used structural similarity index and improved generative adduction network to generate better face recognition images to solve the problem of face anonymization image quality. Ref. [25] proposed the Secret Face Gan (SF-GAN) based on the generative adversarial network, which uses the superficial face attribute information and the deep face attribute information to process the attributes of different faces in different ways. Ref. [26] proposed a model combining attribute untangling and generating network, which disturbed the identity and expression features of face images respectively to achieve the effect of face recognition. Ref. [27] proposed a face recognition method based on depth generation model. Ref. [28] proposed a AnonymousNet framework to generate privacy protection images in different demand scenarios from four parts, including the facial attribute estimation, privacy-metric oriented face estimation, directional natural image synthesis, and adversarial disturbance. Based on the depth generation model, the image structure can be continuously trained by the network model, which is more advantageous than other face image privacy protection algorithms to a certain extent. Ref. [29] put forward a neural network model including encoder and generator, which utilizes the encoder pairs to convert face images into high-semantic potential code vectors and add differential privacy.

DP was originally proposed for the protection of published data [30]. It has the property of not relying on the background knowledge of the attacker. No matter how much information the attacker has about the data, it is impossible to deduce otherwise accurate original data. The essence of differential privacy is to protect data by adding an appropriate amount of noise to the data. Adding noise directly to image pixels will destroy the structure of the image, and converting the image to other forms can minimize the impact of noise. Ref. [31] uses image segmentation technology to convert the image grayscale matrix into a one-dimensional ordered data stream and then performs differential privacy processing, which enables the image to achieve the goal of privacy protection without causing major damage to the image vision. Ref. [32] utilize differential privacy to perturb eigenfaces, which avoids privacy attacks on information inference and model memory. Ref. [33] achieved the same effect as anonymization by blurring facial images through formal differential privacy. Ref. [34] directly introduces the differential privacy noise of the Laplacian mechanism in the frequency domain of the image, and reduces the image error based on the discrete Fourier technology to generate an image with privacy protection.

III. MECHANISM DESIGN

This section describes in detail the face recognition

method for smart teaching management mechanism proposed in this paper. We propose a face image privacy recognition and protection algorithm based on facial feature extraction and analysis. Specifically, we identify and extract features from fixed parts in face images, including eyes, nose, mouth, eyebrows, and cheeks. Then, we designed a face privacy recognition and protection model based on conditional GAN.

3.1. Face Feature Extraction

Studies have shown that when using the ROI for partial recognition of facial expression images, local features play an important role in facial expression recognition. For face recognition, the basic steps include face detection, facial feature extraction, face recognition or matching. The extracted features include facial contours, facial features (i.e., eyes, nose, mouth, eyebrows, etc.), texture features (e.g., wrinkles) [35]. Wrinkle texture features affect the detection of age and health. Eyes, nose, mouth, eyebrows, and other facial features affect facial recognition. Facial contours affect the overall structure of the face. When performing face recognition, the effect of forehead and face is far less than that of facial features such as eyes, nose, mouth, and eyebrows. Therefore, in face identity protection, the role of facial features is greater than that of other parts.

Since facial contours have an impact on face detection and the overall structure of the face, the facial contours are considered as facial features and are not analyzed for facial features. The facial feature analysis algorithm proposed in this method mainly considers the influence of facial features and the correlation of eyes, nose, mouth, and eyebrows on facial identity. When protecting the privacy of face identity, only the facial features can be processed, and the structure of other regions and more attributes of the original image can be preserved. In this regard, we propose a facial feature analysis algorithm, the structure of which is shown in Fig. 1.

In order to avoid other calculation errors caused by pixelization that is far from the original image, try to pixelate the positioning features with pixels that are close to the skin color of the face to form pixelated eye images, pixelated eyebrow images, pixelated nose images, pixelated mouth image. Then calculate the similarity between the pixelated eye image, pixelated eyebrow image, pixelated nose image, pixelated mouth image and the original face image respectively. The Euclidean distance is used to calculate the similarity between images. The greater the similarity between the two images, the smaller the impact of contrasting pixelated features on the face matching. According to the calculation results, the features with a low degree of matching with the face are regarded as facial features. Facial feature analysis is the image preprocessing of the face image privacy protection algorithm. After the facial feature analysis of the face image, the facial features can be processed in the process of face image privacy protection.

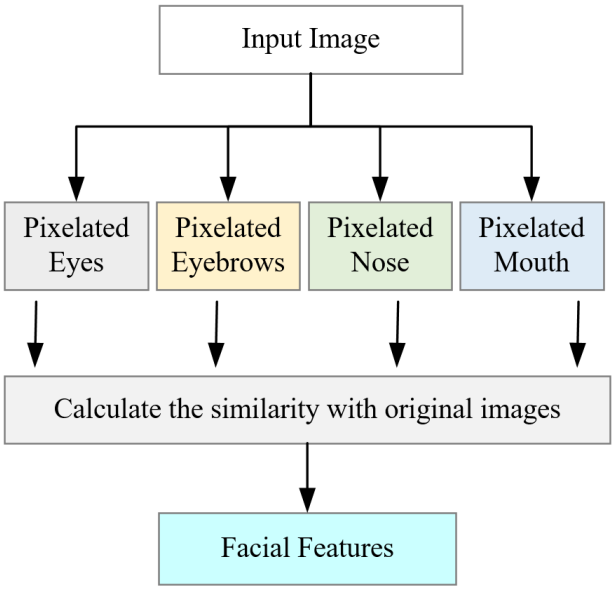

Fig. 1. The overflow of the facial feature analysis.

3.2. Model Design

In order to retain more other features of the original image, we propose a facial feature model based on the GAN model, which embeds the facial feature analysis into the preprocessing layer of the GAN model, generates and changes the facial features, and retains other facial attributes of the face image. Our proposed model is a conditional generative adversarial network model based on image anonymization. The input image of the model is divided into two parts, one is the feature localization map and facial mask map of the original face, and the other is the target image that does not contain the original face. The preprocessing of the original image by this model is to process it into a feature localization image and a facial mask map. After the model is analyzed, the facial features are preprocessed, and the preprocessing gets the feature mask map and feature label map as input. The features in the feature mask map and feature marker currently include facial contours. The model structure is shown in Fig. 2.

In Fig. 2, the feature mask image and feature tag image are images obtained based on the facial feature analysis algorithm. The target image is a real image set that does not contain the original face, which is used to anonymize the generated image, and the anonymized area is the mask area. Feature mask images and strong feature labeled images are processed by downsampling and fed into the generator. At the same time, the target image is processed by a transposed neural network and input to the generator. The input data is

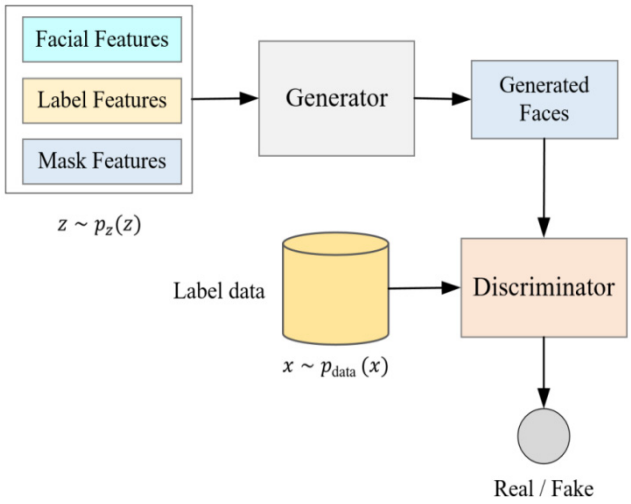

Fig. 2. The overall structure of our proposed model based on GAN.

upsampled in the generator to generate an adversarial image. The generated image is input to the discriminator for discrimination. The identity director is used to identify the identity of the user, and distinguish between the generated image and the given expected image, making the generated image and the expected image as indistinguishable as possible. In the end, the face image generated by the GAN model meets the two characteristics that it is difficult to identify the authenticity of the image, and it is difficult for the machine to distinguish the identity of the image.

In the process of facial feature analysis, calculating the matching degree between the pixelated feature image and the original face image is an important criterion for analyzing the importance of features. We use the Euclidean distance to discriminate the similarity between the pixelated feature image and the original image. The formula of Euclidean distance to calculate the similarity of two images in N-dimensional space is as follows.

$$ED = \sqrt{\sum_{i=1}^{N} (x_i - y_i)^2}. \tag{1}$$

When calculating Euclidian distance, the image needs to be transformed into grayscale image. x_i and y_i are the corresponding grayscale values of the image respectively, namely, the corresponding pixel points of the two images. The larger the calculation result, the larger the space distance between two points, and the lower the similarity between two images. The smaller the calculation result, the greater the similarity between the two images. According to the data given by FaceNet in the image matching experiment, when the matching result is greater than or equal to 1.1, the matching rate of two images is very low and they are regarded as different faces. When the matching result is less than 1.1, the two face images are regarded as a successful match, that is, a face. In the face features and the original face image matching process, because the face features are largely combined at the same time affect face recognition, so cannot be a single successful matching result to the 1.1 standard to calculate. Considering that each feature will affect each other, the minimum similarity value of the four calculation results is far less than the average value of the four results, so the feature with the minimum calculation result is taken as the feature of facial recognition without influence. When the calculated results of all eigenvalues are not different, mask processing is performed on all facial features.

We perform feature location and feature mask processing on the face image analyzed by facial features, and obtain a strong facial feature location map and a strong facial feature mask map, which are spliced and input to the generator. The image discriminator and identity director in the discriminator part constitute a Siamese neural network, that is, both use the same loss function. We pre-train the identity director with a loss such that the generated image yields the desired identity given the desired image, and then fine-tune the network with a contrastive loss. The loss functions for the image discriminator and generator are computed as follows.

$$\min_D V(D) = \frac{1}{2} E_{x \sim p_{data}(x)}(x)[(D(x) - b)^2] \frac{1}{2} E_{z \sim p_z(z)}(x)[(D(G(z)) - a)^2]. \tag{2}$$

$$\min_G V(G) = \frac{1}{2} \mathrm{E}_{z \sim p_z(z)}(z)[(D(G(z)) - b)^2], \tag{3}$$

where G is the generator, D is the discriminator, a and b are the labels of the generated image and the real image, respectively. $x \sim p_{\text{data}}(x)$ is the distribution that satisfies the original image, and $z \sim p_z(z)$ represents the distribution that satisfies the noise. In the model, the facial feature localization map and facial feature mask image are first concatenated and then processed by downsampling. At the same time, the target image is input to the generator after being processed by the transposed neural network.

IV. EXPERIMENTS AND RESULTS

4.1. Dataset and Setting

In order to avoid unnecessary errors caused by insufficient training and testing images and incomplete face identities, this experiment uses the two most commonly used face datasets in face research, namely CelebFaces Attributes (Celeb A) and Labeled Faces in the Wild (LFW). Celeb A is a large-scale open-source face dataset published by the research team of the Chinese University of Hong Kong [36], which includes 202,599 face images, and the images cover complex and changeable poses and backgrounds.

This dataset is robust to studying publicly available face images. The image resolution in the Celeb A dataset is all 178×218. LFW is a face dataset completed by a research team at the University of Massachusetts. The face images in this dataset come from face images on the Internet. Each image also has complex and changeable character poses and backgrounds. There are more than 13,000 face images in total, and the resolution of the images is 250×250.

We take the common metrics for face classification and identification as performance indicators in our experiments, including the structural similarity (SSIM) and classification metrics: Recall, Precision, Accuracy, and F1-score. They are respectively defined as follows.

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_x\sigma_y+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x{}^2\sigma_y{}^2+C_2)}, \tag{4}$$

$$\mathrm{Recall} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}, \tag{5}$$

$$\mathrm{Precision} = \frac{TP}{TP+FP}, \tag{6}$$

$$\mathrm{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}, \tag{7}$$

$$\mathrm{F1}-score = \frac{2\times Precision\times Recall}{Precision+Recall}, \tag{8}$$

where C_1 and C_2 are constants, μ_x and μ_y are the means of x and y, σ_x and σ_y are the standard deviations of x and y, and xy is the covariance of x and y. SSIM is one of the most common metrics for evaluating image similarity and is widely used to generate visual structure evaluations of images. SSIM mainly compares the similarity of two images from three aspects: image contrast, image structure and image brightness. At the same time, these three aspects are relatively close to the human eye's visual perception of the image, so it has certain theoretical significance to evaluate the difference between the human eye's perception of the two images. When comparing two images with SSIM, the two images need to be gray scaled first. When calculating SSIM, the pixel values of the two images are regarded as x and y respectively, the standard deviation of the gray level is used as the measurement of the image contrast, the average gray level is used as the measurement of the image brightness, and the structure measurement is used to calculate the structure of the two images. In other metrics, TP is the true positive prediction, TN is the true negative prediction, FP is the false positive prediction, FN is the false negative prediction.

4.2. Results

Table 1 calculates and compares the SSIM similarity between the image generated by various image protection algorithms and the original image. The algorithms compared include unprocessed (original), pixelated, facial occlusion (masked), CIAGAN model [37] and the generation model based on GAN proposed in this paper.

It can be seen from Table 1 that the result of calculating the SSIM index value of the unprocessed face image is 1, which means that the two images are exactly the same. From the results of the pixelation method and the occlusion method, it can be seen that the SSIM value of the occluded image is smaller, which indicates that occlusion has a great effect on the masking of image information. Compared with the images processed by the pixelated, occluded, and CIAGAN models, the proposed model achieves the largest SSIM value, which shows that the difference between the face image generated by our model and the original face image is smaller than that produced by other comparison algorithms.

Table 2 shows the results of face recognition on the Facenet model for images generated by different models. From the Table, we can see that: (1) compared with other processing methods, our proposed method has achieved the best results on the four indicators; (2) the Pixelated method is better than the Masked method, which shows that the masked manner will lose a lot of facial information. The face matching module in the Facenet model is a calculation process for the similarity of two face images, which is widely used in traditional face matching models, which is of great significance for measuring the effect of protected images in matching models. Face image privacy protection is an important requirement of face recognition. In order to verify the de-recognition performance of the proposed algorithm, the famous Facenet model was used to evaluate

Table 1. Comparison results with different processing mothds.

Method	SSIM
Original	1.0
Pixelated	0.264
Masked	0.134
CIAGAN	0.281
Ours	0.328

Table 2. The classification results of Facenet model under different processing methods.

Method	Recall (%)	Precision (%)	Accuracy (%)	F1 (%)
Original	70.6	65.4	75.3	67.9
Pixelated	30.1	29.3	33.6	29.7
Masked	5.64	6.89	6.17	6.2
CIAGAN	26.3	24.8	29.4	25.5
Ours	40.8	38.9	43.7	39.8

the de-recognition ability of the generated face image. Facenet model can realize face alignment, face matching, face recognition and other functions. With its good face recognition performance, Facenet model has been used by many face privacy protection models to evaluate the de-recognition performance. We use the face recognition module and face matching module of the Facenet to evaluate the de-recognition effect of the generated images. Face recognition module uses image to realize Iception-Resnet to Facenet model for pre-training, its recognition principle is to measure the nearest neighbor from the same category of sample rate, the output result is the recognition rate. The higher the output value, the worse the privacy protection of the model generating the face image. On the contrary, the lower the recognition rate of the face image, the better the privacy protection of the model generating the image.

V. CONCLUSION

This paper introduces a privacy protection model of face image based on facial features. Firstly, the theoretical logic of the proposed facial feature analysis algorithm is introduced, which aims at processing the features that have important influence on the face image. Then the facial feature analysis algorithm is embedded into the GAN model. The facial features of the image are generated by the condition generation based on anonymization against the network generation, and the identity is close to the given expected image. The resulting protected image preserves image features other than facial features. It can be seen from the experimental results that the protective image generated by the proposed model retains image features other than facial features, so that the posture and action of the figure in the image are basically consistent with the original image. In the SSIM index, our model is superior to pixelated, occluded and CIAGAN model protected face images. The advantages of our proposed method lie in the following two points: (1) facial features extraction can well express individual details; (2) GAN model can learn the feature distribution state of data by opposing ideas, which provides the basis for generating diversified facial images. In the face recognition model based on deep learning, the image protected by the proposed model significantly reduces the recognition rate and plays a certain role in the recognition.

REFERENCES

[1] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," *Future Generation Computer Systems*, vol. 86, pp. 914-925, 2018.

[2] S. González-Bailón, "Social science in the era of big data," *Policy & Internet*, vol. 5, no. 2, pp. 147-160, 2013.

[3] J. Waldfogel, "Copyright protection, technological change, and the quality of new products: Evidence from recorded music since Napster," *The Journal of Law and Economics*, vol. 55, no. 4, pp. 715-740, 2012.

[4] T. Ko, "A survey on behavior analysis in video surveillance for homeland security applications," in *2008 37th IEEE Applied Imagery Pattern Recognition Workshop*, *IEEE*, 2008, pp. 1-8.

[5] M. A. Hearst, S. T. Dumais. and E. Osuna et al., "Support vector machines," *IEEE Intelligent Systems and Their Applications*, vol. 13, no. 4, pp. 18-28, 1998.

[6] S. Streuber, M. A. Quiros-Ramirez, and M. Q. Hill, et al., "Body talk: Crowdshaping realistic 3D avatars with words," *ACM Transactions on Graphics (TOG)*, vol. 35, no. 4, pp. 1-14, 2016.

[7] W. Fang, L. Ding, and H. Luo, et al., "Falls from heights: A computer vision-based approach for safety harness detection," *Automation in Construction*, vol. 91, pp. 53-61, 2018.

[8] X. X. Li and R. H. Liang, "A review for face recognition with occlusion: From subspace regression to deep learning," *Chinese Journal of Computers*, vol. 41, no. 1, pp. 177-207, 2018.

[9] Y. Wen, K. Zhang, and Z. Li, et al., "A comprehensive study on center loss for deep face recognition," *International Journal of Computer Vision*, vol. 127, no. 6, pp. 668-683, 2019.

[10] Y. Taigman, M. Yang, and M. A. Ranzato, et al., "Deepface: Closing the gap to human-level performance in face verification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1701-1708.

[11] Y. Sun, X. Wang, and X. Tang, "Deep learning face representation from predicting 10,000 classes," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1891-1898.

[12] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, pp. 815-823.

[13] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Computing Surveys (CSUR)*, vol. 50, no. 1, pp. 1-37, 2017.

[14] Z. Akhtar and A. Rattani, "A face in any form: ew challenges and opportunities for face recognition technology," *Computer*, vol. 50, no. 4, pp. 80-90, 2017.

[15] B. Meden, P. Rot, and P. Terhörst, et al., "Privacy-enhancing face biometrics: A comprehensive survey," *IEEE Transactions on Information Forensics and Security*, 2021.

[16] L. Rakhmawati, "Image privacy protection techniques: A survey," in *TENCON 2018–2018 IEEE Region 10 Conference*, *IEEE*, pp. 0076-0080, 2018.

[17] Q. Jiang, W. Zeng, and W. Ou, et al., "A scrambling and encryption algorithm for selective block of identification photo," in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*, *IEEE*, 2016, pp. 1-5.

[18] S. J. Oh, M. Fritz, and B. Schiele, "Adversarial image perturbation for privacy protection a game theory perspective," in *2017 IEEE International Conference on Computer Vision (ICCV)*, *IEEE*, pp. 1491-1500, 2017.

[19] X. Cheng and Z. Li, "Using Boltzmann entropy to measure scrambling degree of grayscale images," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, *IEEE*, 2021, pp. 181-185.

[20] E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 2, pp. 232-243, 2005.

[21] F. Song, T. Ma, and Y. Tian, et al., "A new method of privacy protection: Random k-anonymous," *IEEE Access*, vol. 7, pp. 75434-75445, 2019.

[22] H. Hao, D. Güera, and J. Horváth, et al., "Robustness analysis of face obscuration," in *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020)*, *IEEE*, 2020, pp. 176-183.

[23] A. Aggarwal, R. Rathore, and P. Chattopadhyay, et al., "EPD-Net: A GAN-based architecture for face de-identification from images," in *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, *IEEE*, 2020, pp. 1-7.

[24] J. Song, Y. Jin, and Y. D. Li, et al., "Learning structural similarity with evolutionary-gan: A new face de-identification method," in *2019 6th International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC)*, *IEEE*, 2019, pp. 1-6.

[25] Y. Li, Q. Lu, and Q. Tao, et al., "SF-GAN: face de-identification method without losing facial attribute information," *IEEE Signal Processing Letters*, vol. 28, pp. 1345-1349, 2021.

[26] S. Yang, W. Wang, and Y. Cheng, et al., "A systematical solution for face de-identification," in *Chinese Conference on Biometric Recognition*, Cham, 2021, pp. 20-30.

[27] D. Cho, J. H. Lee, and I. H. Suh, "CLEANIR: Controllable attribute-preserving natural identity remover," *Applied Science*s, 2020, vol. 10, no. 3, p. 1120.

[28] T. Li and L. Lin, "Anonymousnet: Natural face de-identification with measurable privacy," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2019.

[29] Y. Zhao, B. Liu, and T. Zhu, et al., "Private-encoder: Enforcing privacy in latent space for human face images," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 3, p. e6548, 2022.

[30] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*, Berlin, Heidelberg, 2008, pp. 1-19.

[31] X. Zhang and W. Q. Yan, "Comparative evaluations of privacy on digital images," in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE*, 2018, pp. 1-6.

[32] M. A. P. Chamikara, P. Bertok, and I. Khalil, et al., "Privacy preserving face recognition utilizing differential privacy," *Computers & Security*, vol. 97, p. 101951, 2020.

[33] W. L. Croft, J. R. Sack, and W. Shi, "Obfuscation of images via differential privacy: From facial images to general images," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1705-1733, 2021.

[34] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 925-951, 2015.

[35] R. Sithara and R. Rajasree, "A survey on Face Recognition Technique," in *2019 IEEE International Conference on Innovations in Communication, Computing and Instrumentation (ICCI), IEEE*, 2019, pp. 189-192.

[36] Z. Liu, P. Luo, and X. Wang, et al., "Deep learning face attributes in the wild," in *Proceedings of the IEEE International Conference on Computer Vision*, 2015, pp. 3730-3738.

[37] M. Maximov, I. Elezi, and L. Leal-Taixé, "Ciagan: Conditional identity anonymization generative adversarial networks," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 5447-5456.

Journal of Multimedia Information System VOL. 10, NO. 1, March 2023 (pp. 35-44): ISSN 2383-7632 (Online)
https://doi.org/10.33851/JMIS.2023.10.1.35

AUTHORS

Jing Liu is currently an associate professor at Handan Polytechnic College with a vice director of computer department. She has published more than 20 journal articles and hold two projects. Her main research interests include digital media, big data, etc.

Nali Yu received her B.S at Hebei Normal University in 2001 and received her M.S at Hebei University in 2006. She is currently an associate professor at Handan Polytechnic College. She has published more than 20 journal/conference articles and taken part in more than 10 projects. Her research interests include media design, data analysis, art education, etc.