Mathematical Biosciences and Engineering

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

MBE, 19(7): 7314–7336.
DOI: 10.3934/mbe.2022345
Received: 18 March 2022
Revised: 07 May 2022
Accepted: 11 May 2022
Published: 18 May 2022

Research article

Privacy protection generalization with adversarial fusion

Hao Wang[1], Guangmin Sun[1], Kun Zheng[1], Hui Li[1], Jie Liu[1] and Yu Bai[2,*]

[1] Beijing University of Technology, Beijing 100124, China
[2] Beijing Friendship Hospital, Beijing 100050, China

* **Correspondence:** Email: lab@nnir.net; Tel: +86-01067392193.

Abstract: Several biometric privacy-enhancing techniques have been appraised to protect face image privacy. However, a face privacy protection algorithm is usually designed for a specific face recognition algorithm. When the structure or threshold of the face recognition algorithm is fine-tuned, the protection algorithm may be invalid. It will cause the network bloated and make the image distortion target multiple FRAs through the existing technology simultaneously. To address this problem, a fusion technology is developed to cope with the changeable face recognition algorithms via an image perturbation method. The image perturbation is performed by using a GAN-improved algorithm including generator, nozzles and validator, referred to as the Adversarial Fusion algorithm. A nozzle structure is proposed to replace the discriminator. Paralleling multiple face recognition algorithms on the nozzle can improve the compatibility of the generated image. Next, a validator is added to the training network, which takes part in the inverse back coupling of the generator. This component can make the generated graphics have no impact on human vision. Furthermore, the group hunting theory is quoted to make the network stable and up to 4.8 times faster than other models in training. The experimental results show that the Adversarial Fusion algorithm can not only change the image feature distribution by over 42% but also deal with at least 5 commercial face recognition algorithms at the same time.

Keywords: privacy protection; neural network; facial recognition; adversarial attacks; decoding; transferability; algorithm fusion

1. Introduction

The risk of privacy leakage is often encountered in the exchange of medical data, especially between institutions. Because auxiliary algorithms used by institutions come from different manufacturers, some data analysis tools even need to be connected to the Internet. Commercial biometric estimators with face recognition algorithms (FRAs) may steal facial data to a third party during transmission. Biometric Privacy-Enhancing Techniques (PETs) have been invented, but none can cope with all situations. There are three classifications to hit the target. One is parts shelter. The characteristic is that the human can see the local content, and the information of the specific information is hidden. Additional computational overhead is required while the image is restored, e.g., pixelation and blurring. Another is in pixels recoding. Anyone can hardly recognize the content in the image unless they know the cipher. For this reason, a password is required whenever the image is used, e.g., chaos [1] or RCDP [2] method. And the most suitable for daily use is cloak perturbation. It can not only hide specific features but also be recognizable to humans, e.g., Fawkes [3] and federated privacy [4]. The first two categories are almost impeccable, but in most cases, face images still need some readability in daily research, e.g., medical institutions exchange toddler images to record the relationship between eye distance and height. In contrast, the desensitization of children's images deserves more attention than the research itself. However, if the face image is hidden roughly, it may bring inconvenience to doctors to identify patients.

Table 1. Accuracy of famous FRAs on difficult benchmarks. "*" indicates that the data is quoted from the original paper.

FRA name	Year	Training	Accuracy (%)				
		dataset	LFW2	IJB-C	AndyLau	CFP-FP	iQIYI-VID
Fisherface [6]	1936	--	93.5 [7]	--	93.6	--	--
Phenogram [8]	1987	--	97.6	--	98.1	--	--
Eigenface [9]	1991	--	64-96*	--	95.56	--	--
LBP [10,11]	1996	--	87.62	--	88.12	--	--
Color Segmentation [12]	2001	--	96.27	--	93.47	--	--
DeepFace [13]	2014	LFW1	97.35*	79.88–90.49	98.81	97.26	--
DeepID [14]	2014	LFW1	97.45	79.91–90.88	98.81	95.08	--
DeepID2 [15]	2014	LFW1	99.15	79.94–90.98	98.81	95.31	--
DeepID2+ [16]	2015	LFW1	99.47	81.36–90.96	98.98	95.43	97.52
FaceNet [17]	2015	LFW1	99.63*	84.76–90.28	91.17	--	--
Baidu [18]	2015	--	99.85	98.21–98.66	99.98	99.71	98.11
Face++ [19]	2016	--	99.6–99.8*	90.73–96.12	99.96	99.74	98.09
SphereFace [20]	2017	LFW1	99.17–99.42	73.58–93.77	97.89	--	--
Cosface [21]	2018	YTF/LFW1	99.33–99.51	89.25–95.96	99.27	--	--
ArcFace [22]	2018	--	99.41–99.5*	88.5–95.74	99.94	98.27	98.2
PyramidBox [23]	2018	WIDER FACE	88.7–95.6	79.51–89.41	96.17	97.11	97.39
ElasticFace [24]	2019	MS1MV2	99.8–99.82*	96.4–98.96*	99.89	98.61-98.73*	97.41
MagFace [25]	2021	MS1MV2	99.83*	89.26–90.24*	99.68	98.46*	98.07
MixFaceNets [26]	2021	MS1MV2	99.53–99.68*	90.43–93.08*	99.93	98.37	98.11
PocketNet [27]	2022	MS1MV2	99.5–99.58*	90.79–91.62*	99.71	93.78–94.21*	97.75–98.01

PET methods are currently formulated for one or several types of FRAs. Hence, those excellent cases become helpless once the scenes are changed. These studies were not widely adopted because FRAs upgraded and developed rapidly, and the computing power and network update for face tasks were also fast. Further, the average annual compound growth rate of the face recognition market alone is 30.7% from 2010 to 2018, and the market scale will exceed 7 billion dollars by 2024 [5]. More importantly, everyone can get and collect FRAs easily. Since 2014, commercial FRAs have sprung up, and they have a perfect development to after-sales process, so their recognition accuracy is approaching 99.99% as shown in Table 1. After the COVID-19 outbreak, FRAs for deep occlusion have also emerged. They can identify covered faces (gauze mask), even the face covered over 50%. We can't conclude whether a camera applies an FRA, and manufacturer of the FRA.

The classification of PET can be roughly divided into 6 groups [28]: 1) Data applicable, 2) Mapping type, 3) Biometric attributes, 4) Ways to address biometric utility, 5) Guarantee of the possibility of reconstructing information, 6) Hidden biometric targets (humans and/or machines). As for the specific response measures, only three categories are widely used. Only Image means, representation means and inference means can produce effective algorithms.

Image means are used to process graphics or videos. Their target may be humans or machines. Confusion, confrontation and synthesis technology is used to change visual data to protect privacy [29,30]. Representation means are based on the method of transformation and elimination. It suppresses some target aspects of data by transforming the original template into another form. It can also delete the meta element with the largest amount of information about the target attribute in the template [31], and used only for a pre-defined purpose [28]. Inference means usually change the biometric template and the comparison/classification process used to drive the similarity/comparison score [32]. Unlike image means PET, this group's technology is specifically aimed at automatic machine learning models rather than humans. However, our research mainly focuses on an image processing method that allows human beings to know who's that in the picture while the machine cannot, so we need to combine both image and inference. It is more important to disable many machine recognition algorithms as much as possible, rather than a certain class.

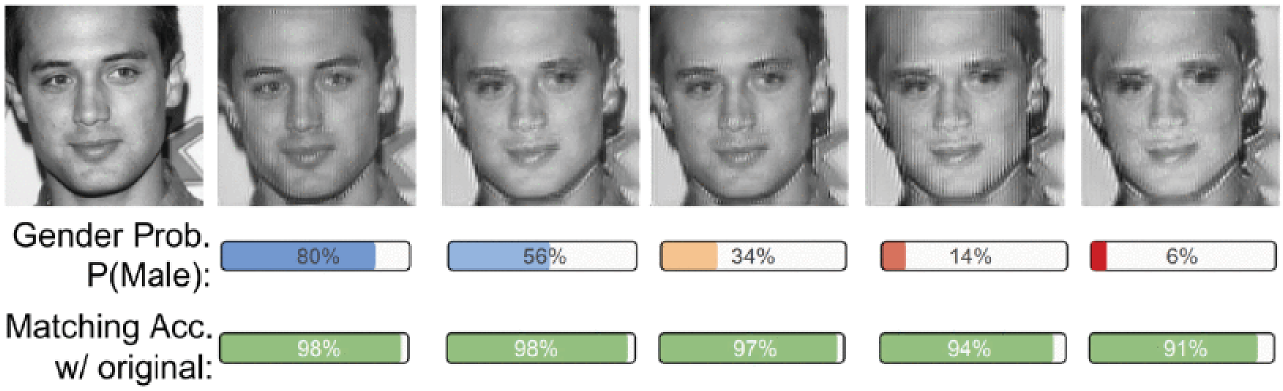

Figure 1. The illustration of the FlowSAN model, after completely hiding the gender attribute, the generated person can hardly be recognized by humans.

All privacy protection networks based on neural networks are easily affected by the neural network itself. Therefore, even if the PET algorithm is extremely advanced, it cannot keep up with the frequently upgraded FRA. PET algorithms are usually targeted for research and development. Take Fawkes [3] for example, the training for ArcFace V1 has been outstanding, and the success probability (SP) can reach over 90%. However, this algorithm is failed to work with V2 soon after it was proposed. Even if we retrained the model, SP dropped below 50%. FlowSAN [33] as representative of semi-advertising networks will make the face look more and more strange with the high threshold. Thus, some face attributes are hidden. As shown in Figure 1. Later, some algorithms were compared. Few PETs can cope with multiple types of FRAs at the same time.

As shown in Table 2, almost every method is not competent for non-anticipatory situations. If the retrained model copes with the new FRA version, it may lead to data rewriting. It's necessary to study a sustainable PET without retraining. Algorithm convergence leads to complex and huge networks. Therefore, no ideal neural network can be fast and flexible for multiple FRAs. High intensity GAN often leads to output distortion to the eyes or failure to FRAs.

Table 2. Characteristics of PETs.

PET name	Adversary	Year	SP	Conclusion
De-identifying [34]	All	2005	99.9%	Characteristic irreversibility. Not suitable for eyes. Key is easy to be leaked.
Outsourced computation [35]	All	2016	99%	Not suitable for eyes.
Multi-target adversary [36]	All	2017	90–98%	It requires a large number of training samples and huge parameters.
Similarity-sensitive noise [37]	SphereFace/Dlib	2019	95%	Only used in SphereFace & Dlib.
LightFace [38]	All CNN based FRAs	2019	96.2–98.5%	Only one FRA can be dealt with, slow training speed. Not suitable for eyes.
Differential [39]	Eigenface	2020	70–90%	Limited to single white box applications
Pixel perturbation [3]	Black box based FRAs	2020	97–98%	For specific versions of commercial FRAs only or need to retrain the model. Some algorithms fail after the image is compressed
Synthetic face replacement [40]	U-net based FRAs	2021	98.1–98.4%	Become another person. Not suitable for eyes.

In short, the main point is to keep the generator adapting to the newly added discriminator (black box FRAs) continuously. It is more important to find a fast gradient descent method when the parameters are increasing.

The main contributions of this work can be summarized as follows:

1) The model can integrate many face recognition algorithms without caring about their structure and training sets.

2) The algorithm proposes an inverse back coupling mechanism to make the output play the opposite role to the input and automatically balance the target error.

3) Keeping the network stable with the help of the principle of social animal hunting.

4) Use the validator to score and maintain a stable visual effect.

2. Related works

2.1. Privacy and security technology

Privacy-Preserving and Security Mining Framework (PPSF) offers algorithms for data anonymity, privacy-preserving data mining, and privacy-preserving utility mining [41]. It comprises 13 data anonymity algorithms. However, these state-of-the-art algorithms mainly hide sensitive information [42], making the targets they try to read become incomprehensible, including humans.

Lin et al. proposed an ant colony optimization (ACO) method [43], which uses multiple objectives and transaction deletion to protect confidential and sensitive information. This method mainly deletes transactions to protect confidential and sensitive information, which belongs to representation means. That protected information will not apply to the data without dedicated tools, e.g., CT graphics.

Shan et al. [3] use the Generative Adversarial Networks to cheat the ArcFace algorithm at the image level. As a result, they can magically disable the specific FRA, to protect the textured face ID from being collected. The biggest disadvantage of this method is that it can only be used for a certain FRA. If FRA changed, the network needs to be retrained.

Wang et al. [44] introduced the nearest neighbor method to calculate the cosine similarity of feature vectors into edge computing, which can effectively improve the security of face data in the cloud. The fault tolerance of identity authentication systems is improved by the secret sharing of homomorphism technology of distributed computing.

The research of soft biometrics considers the use of feature templates to infer information about a person's gender, age, race, sexual orientation, and health status [32]. The server preserves a full amount of face feature templates [45]. In the business process, face privacy is safe, but if the server receives an intrusion, there is still a risk of privacy disclosure.

In brief, the existing privacy protection methods are described for a certain pattern of FRA, and most of them are for machine recognition.

2.2. Information fusion

Damer et al. suggested the concept of algorithm fusion in 2013 [46]. The algorithm results from different sources are normalized, and then the scores are fused to improve compatibility. However, after our evaluation, the time to reach the deviation of multiple algorithms is unacceptable, especially in the black box state. Baseline weighting algorithms [47] were applied in the second year. Although the robustness has been improved, the experimental results show significant differences for different data sets.

Subsequently, Damer then focused on an asynchronous combination-based score-level weighted-sum fusion approach [48]. Its focus is on the trusted model, not the attack model. We believe that the attack model is the key to protect privacy. Face Morphing Attacks were invoked [49] by the minimum, maximum, and mean fusion rules, and at most 3 detectors of different protocols can be fused. The new method is totaling up to six fused detectors in different attacks.

Literature [50] gives us some enlightenments. Even if we integrate some algorithms, some repair methods can still judge the changed area in the image, resulting in the attack's failure. There must be a network structure with both automatic mechanism and manual intervention mechanism to prevent the generated attack image from being seen through.

3. Methods

A face image should be blocked by some cloaks so that the corresponding FRA recognition can be prevented as shown in Figure 2. Considering the variety and self-renewal of FRA, the algorithm should be compatible. The overall goal is to make function f that exerts some perturbation on the input image x to satisfy the following properties:

It believes that the facial feature template corresponding to each algorithm is different. We define the characteristic set of each FRA as the two-dimensional representation of its feature template, and its mapping to image *x* is **s**. The original image feature $c_x \in \boldsymbol{s}$ and the output image feature $\boldsymbol{c}_y \notin \boldsymbol{s}$.

If the feature set of x in FRA1 and FRA2 are $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ respectively, then the output image meets $\boldsymbol{c}_y \notin (\boldsymbol{s}_1 \cup \boldsymbol{s}_2)$.

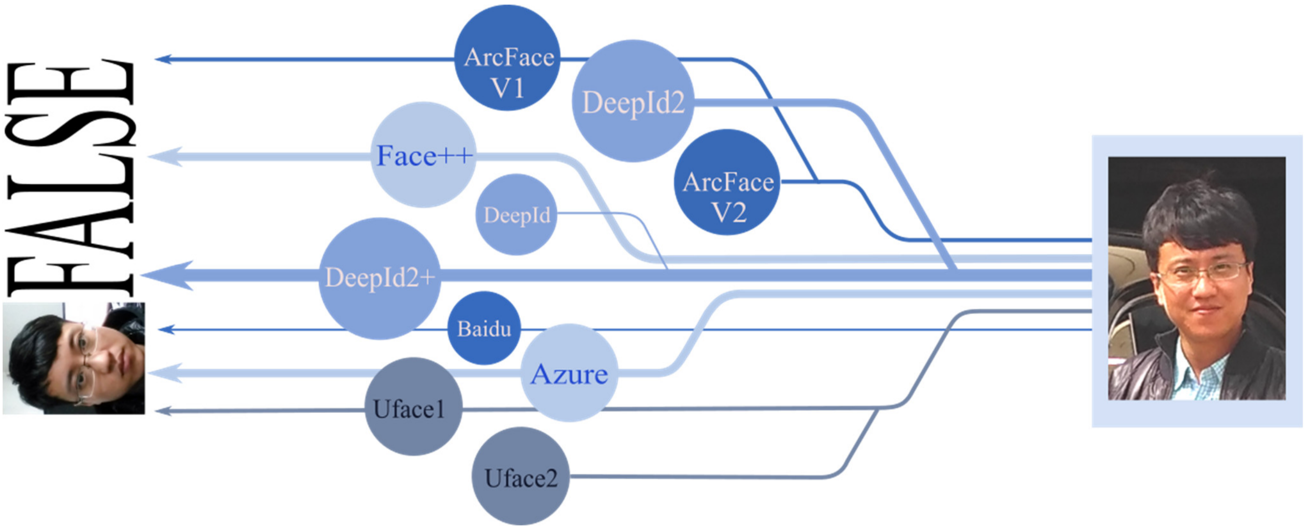

Figure 2. Overall target diagram: the protected face image can disable multiple FRAs at the same time without affecting human vision.

3.1. Adversarial fusion network

The best way to inherit human visual recognizance is to add small perturbations to the image, therefore the main research objective is to utilize the cloak pixels to encrypt the image. The proposed Adversarial Fusion Network (AFN) is divided into two categories: build a generative adversarial network (GAN) and inverse back coupling validator. In order to improve the compatibility of the algorithm, the adversary nozzles are used to carry out black box attacks instead of the discriminator. True and false images at the nozzles can be docked to parallel FRAs and compared constantly until they are decided to be different results completely by FRAs. To keep the visibility of the output image, a validator scores the output image to determine the generation effect, as shown in Figure 3.

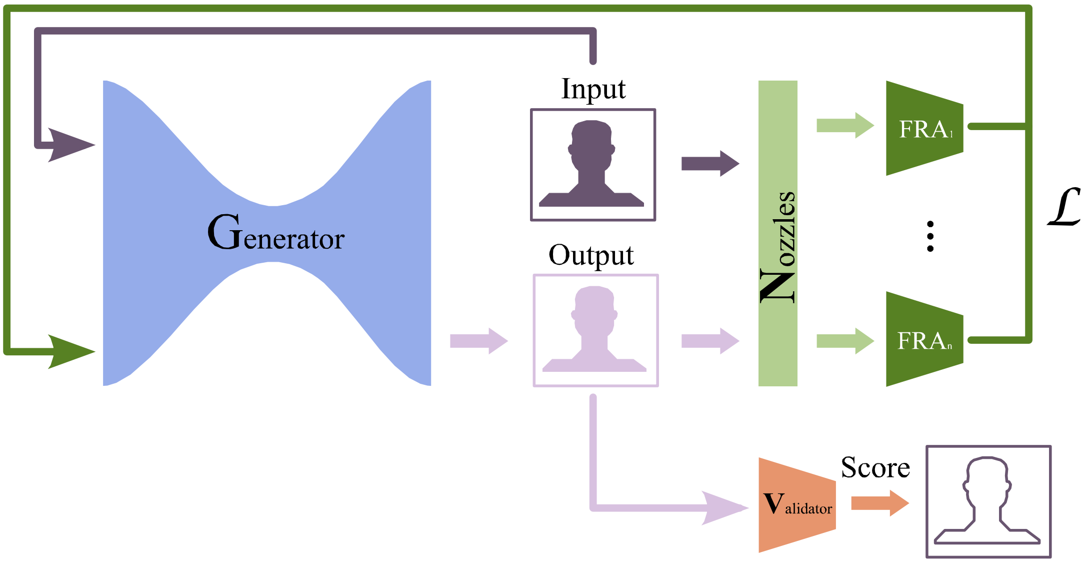

Figure 3. Schematic representation of Adversarial Fusion Network architecture.

The output contains random factors related to the distribution of feature points corresponding to the target FRA. The greater the Euclidean distance between the output vector and the original vector, the weaker FRA's ability. If multiple FRAs are compatible, try to keep the output vector consistent with the original image when the current FRA fails. The original image can be restored by printing random factors and calculating with the protected image. According to this idea, we assume that the regression function f is the feature point mapping learned in an FRA. In the training stage, the same mask template distribution needs to be got from images of different scales, and the complete feature space should comply with Eq (1). Vector $\boldsymbol{\varphi}$ is the n_{th} feature distribution of different scales (s) in the original images. Equation (2) makes the network learn the hyperparameters. The relatively simple idea is the translation and scaling for the aim function in Eq (3).

$$\phi = \sum_1^n \varphi_n^s \tag{1}$$

$$f(\varphi_n^s) = f(\varphi_n^{s'}) \tag{2}$$

$$f_*(\phi) = \omega_*^T \cdot I \tag{3}$$

Set I represent input eigenvector, ω_* is hyper parameter, * refers regional coordinate of the feature point, f_* is predicted value, which should have the smallest Euclidean distance from the real value t_*, Eq (4) is the loss function for adversary nozzles, which distinguishes the difference between the generated image and the original image. The function optimization goal is defined as Eq (5).

$$L_n = \sum_i^m (t_*^i - \omega_*^T \cdot I^i)^2 \tag{4}$$

$$W_* = argmin_{\omega_*} \sum_i^m (t_*^i - \omega_*^T \cdot I^i)^2 + \lambda \|\omega_*\|^2 \tag{5}$$

Input images are samples of different scales and distinct faces which are mapped to a fixed size landmark template image, and the feature output is given by the same FRA. The feature points region output by the algorithm is pre-processed in 4 × 4 × 3 pixels or 4 × 4 × 1 pixels to reduce the amount of computation (the result of a grey scale image is sometimes not ideal, because some algorithms are sensitive to color channels). Normalizing a random facial mask model is expected to have 30 million super parameters, so it is necessary to establish a simple network. Each layer adopts batch normalization layer to speed up model training and prevent over fitting [51]. We use a filter of 4 × 4 pixels and the same convolution (stride is 2). After 2 consecutive convolutions with 16 filters, the image is compressed to 128 × 128 × 32 pixels through the pooling layer. Then there are several convolution layers again, by using 64 filters and some same convolution. After pooling, it becomes a 64 × 64 × 64 matrix. Subsequently, matrix data of 16 × 16 × 128 pixels are gained through 128 filters and maximum pooling twice respectively. After passing through two full connection layers, it is input into the Softmax layer for activation, as shown in Figure 4.

The concept of adversarial example transferability was first proposed by Szegedy et al. [52], in that the training models with different structures on different subsets set results in the target model have high confidence error classification. If the trained model is universal, Feature-representation-transfer [53] can be used as a node to fit different FRAs. Adversary nozzles establish a connection between the generator and FRAs, it aggregates the vectors with close feature distance into a subset that reduces the network parameters. The set $\boldsymbol{\varphi}$ is used to describe the characteristics of FRAs. The regrouped distribution $f_{(x,y)}$ is continuously fed back to the generator and compares the distance of the same feature with the real image. e.g., the tip and wing of nose are mapped to vector $\boldsymbol{\tau}$ for different FRAs as shown in Figure 5. Next, more new FRAs can be added, and old memories are stored in the set $\boldsymbol{\varphi}$.

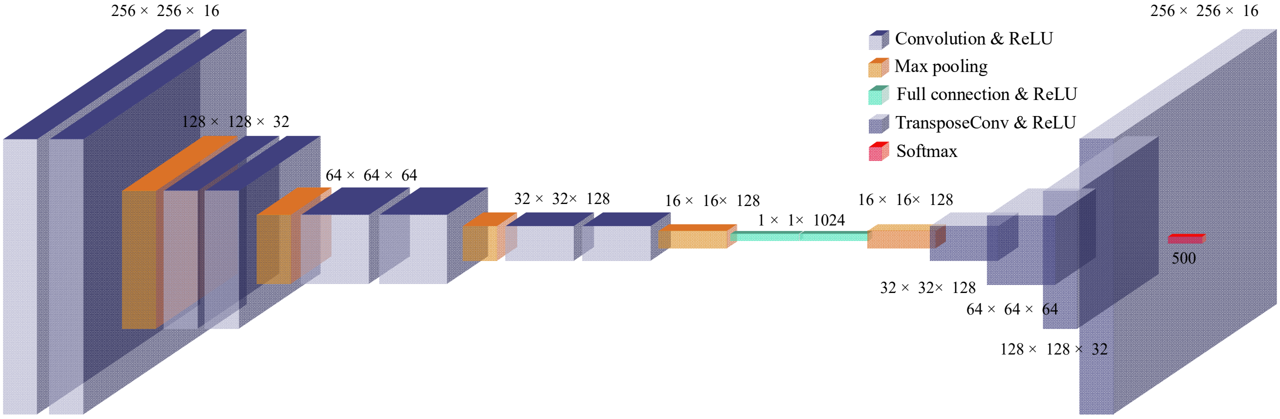

Figure 4. The detailed architecture of the generator.

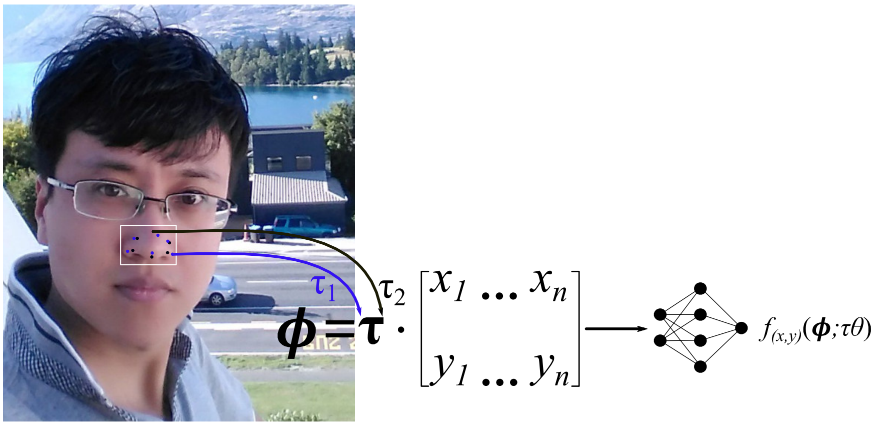
τ_1
τ_2
$\boldsymbol{\phi}=\boldsymbol{\tau}\cdot\begin{bmatrix} x_1 \dots x_n \\ y_1 \dots y_n \end{bmatrix}$
$f_{(x,y)}(\boldsymbol{\phi};\tau\theta)$

Figure 5. The principle of the adversary nozzle.

However, feeding data only through the nozzle will make the output image unattractive with high probability. If the generated image is approaching an unacceptable level, the nozzle should be closed in time. In the formula, the distribution parameter θ comes from the validator which makes the Euclidean distance between desired distribution t_* and measurement f_* as small as possible. The validator comprises six deconvolution layers and a human face tracking network. On the one hand, the deformation degree of the generated image is detected by the visual semi supervised window [54]. On the other hand, if the face cannot be detected, the training will be stopped by nozzles.

The generated template can be regarded as a reserved room. If it is filled with noise, the image is encrypted. Using the template to do XOR operation with the encrypted image can also restore the image.

3.2. Group hunting in AFN

When carrying out multi-objective AFN tasks, training time is a thorny problem. Attacker, barrier, chaser, and driver are simulated in expectation, extreme value, data distribution, and minimum loss [55]. We use the division of labor of chimpanzees in hunting behavior to improve the cooperation ability of the network. Each hidden layer in AFN is treated as a chimpanzee. The characteristic distribution plane is considered as a tree.

In nature, there are two main differences between chimpanzee groups and other biological groups: 1) Individual diversity: in a group of chimpanzees, the abilities and intelligence of individuals are not similar, but they are all members of the hunting team, and there is no discrimination when performing tasks. In view of their different abilities, chimpanzees will be responsible for different hunting operations according to their special abilities. In the algorithm, different models with different curvature, slope, and interception points are used to give chimpanzees different behaviors, just like in natural hunting tasks.
2) Sexual motivation: besides the great advantages of group hunting, research shows that the hunting behavior of chimpanzees is also affected through the social benefits brought by obtaining meat. After obtaining meat, chimpanzees have a certain reputation. They can use the meat for corresponding returns, such as sex, being groomed by their companions, and so on. Unfortunately, chimpanzees will shuffle their duties after each round of hunting. The chaos stimulates them to obtain meat quickly. This unconditional behavior improves the exploitation and convergence speed in the final.

Attackers need more cognitive effort to predict the subsequent movement of prey, so after successful hunting, they will get a larger piece of meat. This aggressive behavior is positively correlated with initial position, empirical value, and time. In addition, chimpanzees can choose roles in each round of hunting according to their advantages [56].

Different FRAs are regarded as prey in AFN. The target FRA can appear simultaneously or separately, depending on the distance between the pursuer and the prey in the initial stage. Of course, every chimpanzee is constantly changing its position for driving and chasing its prey. The driver followed the FRA without trying to catch. And the barrier places itself on a tree to prevent FRA from escaping (Upgrading). The chaser chased the FRA and explored its route. Finally, the attacker predicts the FRA's downward escape route and grabs it at the shortest distance.

The driving model d in the exploration and exploitation phase represents the relative distance between the position of driver x_c and the position of prey x_p. Where *t* (< 500) stands for the iteration sequence number, a, m, and *c* are the coefficient vectors in [0, 2]. The smaller d, the better, but it cannot be 0. Its goal is to make prey move, the Eqs (6) and (7) are proposed.

$$\mathrm{d} = \left|c.x_p(t) - m.x_c(t)\right| \tag{6}$$

$$x_p(t+1) = x_p(t) - ad \tag{7}$$

According to experience, let the initial value *x* of *f* be 0.1 and the nonlinear descent space be [3.57, 4]. In which, $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ are the random vectors in the range of [0, 1]. Equations (8)–(10) respectively.

$$\boldsymbol{a} = (2\boldsymbol{r}_1 - 1)f \tag{8}$$

$$\boldsymbol{c} = \boldsymbol{r}_2 f \tag{9}$$

$$\boldsymbol{m} = f(x) \coloneqq \mathrm{logistic}(x) \tag{10}$$

Finally, $\boldsymbol{m}$ is a logistic mapped vector that represents the effect of the chaotic stimulates (sexual motivation) of chimpanzees after hunting. Convergence rate is improved via the chaotic function in complex and high-dimensional problems. All particles behave similarly in both local and global searches, so individuals can be considered as a single population with a common search strategy.

Chimpanzees can be divided into several hunting groups. The roles of each group are the same, and the members of the group can be adjusted after several rounds of hunting. In Table 3, where *t* refers to the current iteration and T indicates the maximum number of iterations.

Table 3. The coefficient of *f* vector.

Groups	Plan 1	Plan 2
1	$1.95 - 2\frac{t^{1/4}}{T^{1/3}}$	$2.5 - \frac{2\log(t)}{\log(T)}$
2	$1.85 - 3\frac{t^{1/3}}{T^{1/4}}$	$2.5 - 2\left(\frac{t}{T}\right)^3$
3	$1.5 - 3\left(\frac{t}{T}\right)^3$	$0.5 + 2\exp\left[-16\left(\frac{t}{T}\right)^2\right]$
4	$1.5 - 2\left(\frac{t}{T}\right)^3$	$2.5 + 2\left(\frac{t}{T}\right)^2 - 4\frac{t}{T}$

There are no known parameters of an FRA. In order to compare gaining FRA characteristics to chimpanzees hunting, it is assumed that any member can be a chaser to report the location $\boldsymbol{x}$. These recommended role models are applied and the other members update their positions based on the recommended initial values to get the best formation. The relational model is expressed by the Eqs (11)–(13).

$$\mathbf{d}_R = |\boldsymbol{c}_n \boldsymbol{x}_R - \boldsymbol{m}_n \boldsymbol{x}| \tag{11}$$

$$\boldsymbol{x}_n = \boldsymbol{x}_R - \boldsymbol{a}_n \mathbf{d}_R \tag{12}$$

$$\boldsymbol{x}(t+1) = \frac{1}{4}\sum_{\mathbf{1}}^{n} \boldsymbol{x}_n \tag{13}$$

The hunting role of chimpanzees is represented by subscript R; n is the group number of the next change. When the prey weight $\boldsymbol{c} > 1$, the hunting group hunts (encircle and intercept), otherwise, it will divide food or reassign roles. This parameter also contributes to the randomization of the optimization process and reduces the probability of local minimization. Note that the $\boldsymbol{c}$ vector follows the same random function mapping from the beginning to the end of the iteration.

3.3. Ensemble training

Federated learning [39] and transfer learning [4] can also deal with multiple FRA attacks. However, their parameters are relatively large, and the gradient explosion or gradient disappearance often occurs. Too many training rounds will often lead to an unsatisfactory feeling for the human being. ChOA theory can realize rapid gradient descent, and the acceptance of the output image can be effectively optimized.

All the feature points can't be clustered separately [57], because there will always be some unknown data. Chimpanzees need to know the focus of each FRA. According to the assumption, if the key points of an image correspond to the positions of different prey, the way to reduce the network parameters is to drive the prey to a certain position and then attack. It can reduce the capture time (training speed) and make the focus on the prey closer to the attacker (gradient explosion).

Attackers attack the prey on the grassland named σ, the lowest gradient acceptable to the human.

After AFN began, chimpanzees entered the stage of exploration. They search for prey (local extremum) separately and attack intensively. The vector ***a*** with a random value from -1 to 1, so that searchers focus on tracking prey far away from others. When inequality |***a***| > 1 the chimpanzees abandon the current route to find new prey, as shown in Figure 6.

As mentioned earlier, after several iterations of hunting activities, each chimpanzee adjusts its weight and position (satisfaction after eating), and then released or inherited its previous responsibilities. Therefore, the chaotic way helps to balance the division of labor among hunting groups. This chaotic behavior helps chimpanzees to further ease falling into local optimization and slow convergence speed in solving high-dimensional problems. Once the prey is captured, the nearest four groups of chimpanzees will regroup and start new exploitation.

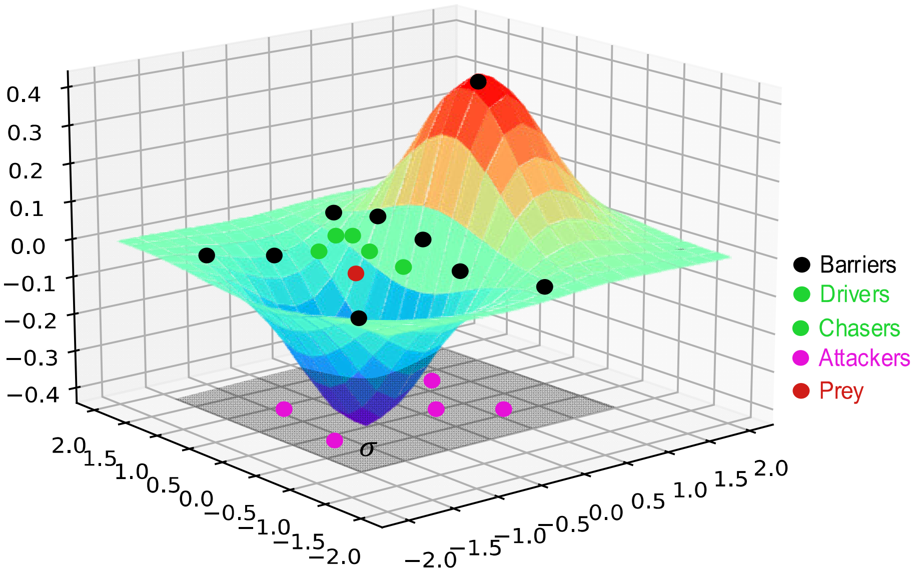

Figure 6. Fast gradient descent method based on hunting model.

Every one-dimensional vector can be regarded as a chimpanzee to indicate the candidate points in AFN. Further, the weights are the coefficients of social roles, in which the total length is equal to the vector's in $\boldsymbol{\varphi}$, in Equation 14, where h is the number of neurons in the hidden layer and n is the number of inputs [58]. As an example of this analogy, the ensemble training is shown in Figure 7. Mean square error (MSE) is used to measure the fitness of the chimpanzee, which calculates the difference between the expected value f and evaluation value $\hat{f}$ of all training in Eq (15). Where n is the number of instances in the training dataset.

$$\mathrm{L} = (n \times h) + (2 \times h) + 1 \tag{14}$$

$$MSE = \frac{1}{n}\sum_{1}^{n}\left(f - \hat{f}\right)^{2} \tag{15}$$

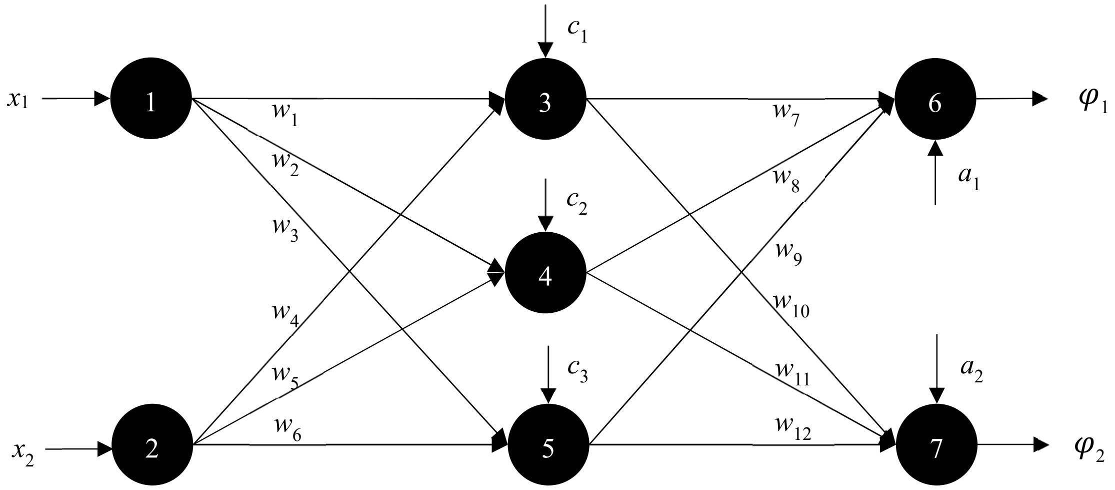

Figure 7. Diagrammatic sketch of ensemble training.

3.4. Template application

The captured prey is mapped to a two-dimensional grassland. It not only affects the behavior of chimpanzees' social factor but also stores it in a room to generate templates. In other words, the main purpose of the attack is to determine the position of the prey on the σ plane, which continuously forms a template corresponding to the feature points collected by FRAs. And the template is transformed into printed patch [59] by texture visualization technology as shown in Figure 8..

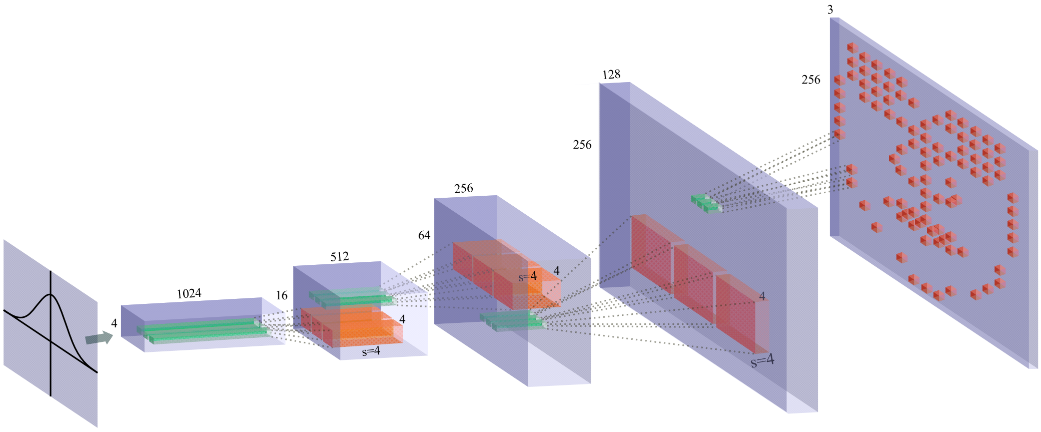

Figure 8. Template mapping.

Because the location of prey driven to the ground is random, each template file is different. They are combined with perturbation technology to encrypt face images. For the generator, in order to improve the quality of samples and the speed of convergence, all pooling layers and full connection layers are cancelled [60]. This method can reduce the difficulty of search σ. The only problem is that it will produce noise pollution.

By mapping Gaussian noise onto the template file and XOR with the original image, the features concerned by FRAs can be hidden. In order to make the generated image more realistic, we conduct Y-axis mapping on the images of less than 2KB in CelebA dataset, convert them into Gaussian noise and give them to AFN. The protected image is a set of pixels at specific regions generated by random noise. If template file XOR with the disturbed image again and the pure image can be restored. The template file can be saved again through image encryption technology [61] to increase its security.

4. Results

4.1. Datasets and experimental setup

This section compares the effects of several famous privacy protection methods, famous FRAs will also take part in the experiments. Distributed training conducted by the GPU of ARM mali-t860 MP4 and the development board of 16 core NPUs. CelebA, LFW, and Andy_Lau datasets are used to assess the performance.

Privacy protection methods include: Chaos [62] and cryptography [2], zero-watermark [63], Feature area twist [6], Fawkes [3], ADVHAT [64] in the image level. Parameters of paper [65] are used in the inference experiment.

FRAs include: Baidu [18], Azure face [66], Face++ [19], ArcFace [22] and open source face recognition algorithm based on Dlib [67]. They are renamed as M_B, M_{Az}, M_F, M_{Ar}, M_D for convenience.

4.2. Visual effect experiments

This experiment is aimed at implementing ArcFace algorithm. ADVHAT and Fawkes algorithms are not updated for other FRAs. Principal component analysis (PCA) [68] method is used to reduce dimensionality to accept a two-dimensional space of visual features. To keep the interpretation of the original data to the greatest extent, this paper uses the minimum loss theory to make the first principal component have the largest variance, and each subsequent principal component is orthogonal to the previous ones. An image covered by every protection shows that chaos and cryptography are strongest and zero-watermark almost impossible to protect privacy, the algorithms of changing the eigenvector with cloak all work well, as shown in Figure 9. Although from the mathematical, most algorithms have the basic elements of hiding privacy. However, the printed image can't be recognized except ADVHAT, Fawkes, and the mask template.

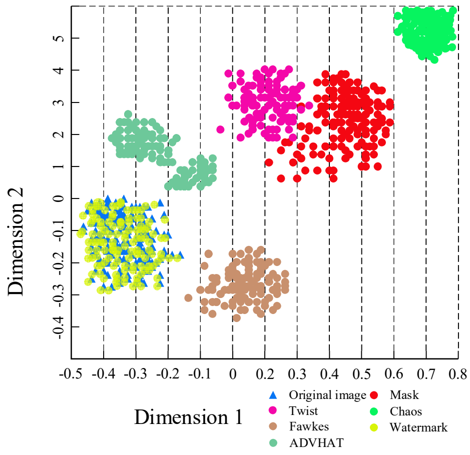

Figure 9. Visual 2D feature space. The Euclidean distances are different, indicating that it has reached the expectation in principle.

4.3. *Template mapping deviation experiments*

We refer to [65] and use 70% of CelebA as a data training set and 30% as a test set. Performance evaluation is conducted with a test set. Images from LFW are used to assess the generalization capabilities of AFN. To have a consistent evaluation setup, face recognition, gender, and age are organized into the experiments Learning-based and Strict (LBS) evaluation protocol [69] is used to train, and the dataset is organized into 5 folds. The commercialized FRA will not abide by the rules. The only way to prove whether the privacy protection is effective is whether the attacked FRA outputs the correct face ID. We use *err* to analyze the average ratio of genuine pair comparison.

Privacy-gain identity-loss coefficient (PIC) is used to evaluate the performance of the model. Where fic' and eer' were computed from the attribute suppressed representations, whereas the errors *fic* and *eer* were calculated from the original (unmodified) face representations [37], shown in Eq (16) [37], the higher value of *PIC* the performance is better. The model maps the initial face representations into disentangled representations z, z_{id}, and z_{att}, where z represents the template information of a face, z_{id} shows identity information and z_{att} encodes information about biometric attributes.

$$PIC = \frac{fic'-fic}{fic} - \frac{eer\prime-eer}{eer} \tag{16}$$

The fraction of incorrectly classified images *fic* and equal error rates *err* are reported for the face id and attribute recognition. In table 4, the impact of the model on potential space is concentrated on z_{id}, and the information of z_{att} includes age and gender are not been affected. The experimental results show our model does not care about the specific attributes of the face, we only care about whether FRA can output face ID. Existing state-of-the-art e.g., PE-MIU [32], Unsupervised privacy-enhancement (PE-UP) [37], feature disentanglement (PE-FD) [65], prefer to hide some key attributes and preserve the recognizability of face.

Table 4. Privacy-gain identity-loss coefficient on CelebA, LFW and Andy_Lau. Computed over 5 folds.

Datasets	z	z_{id}	z_{att}
CelebA	25.077 ± 1.130	422	1
LFW	24.478 ± 0.189	348	1
Andy_Lau	29.635 ± 1.484	1024	256

This implies that the total privacy cost remains unchanged. It is important to apply an adaptive iterative privacy budget allotment to a fixed allotment [70]. In terms of latent space, the goal is to maneuver latent space to achieve a given image's transformations [71]. After mapping, the template coordinates of Arcface algorithm are output in the training network as shown in Figure 10, where x_s is the original image and x_t is the image template in AFN. It can be seen that the feature distribution of the processed image has changed. All the test samples are collected as shown in Table 5. We have added liveness (images of volunteers) experiments to deal with reality.

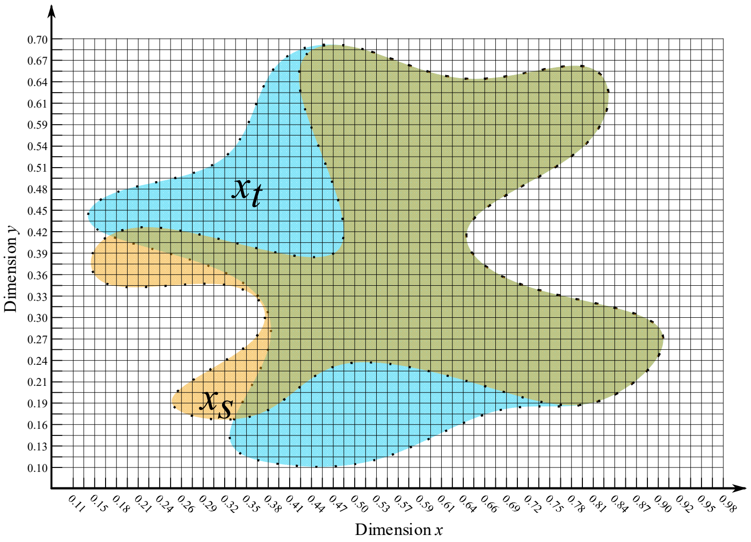

Figure 10. 2D coordinates of feature template. The test dataset is Andy_Lau and target FRA is Arcface v2.

Table 5. Change rate of feature distribution.

Dataset	M_B	M_{Az}	M_F	M_{Ar}	M_D
CelebA	13.6% ± 1.1%	24.4% ± 0.8%	10.2%	27.1% ± 0.5%	99%
LFW	9.3% ± 0.8%	23.6% ± 0.8%	12.4%	18.6% ± 0.1%	99%
Andy_Lau	15.2% ± 2.7%	33.3% ± 0.1%	25.8% ± 0.9%	42.0% ± 1.2%	99%
Liveness	5.8%	10% ± 0.2%	4.5%	38.1% ± 3.5%	99%

It can be seen from the experiment that the single FRA algorithm can change the image feature distribution and make the detector ineffective. The best experimental result is Andy_ Lau's data set has a change rate of over 40% in the Arcface V2 algorithm. *M_D* is not intelligent, so it is only recorded and not included in the experimental data.

4.4. Cheat experiments

The comparison processes adopt the black box method, and the evaluation index uses the protection score s_p, which objectively evaluates the effect of algorithm output on the targeted FRA. F_p represents error samples on target FRA, T_p means accuracy given by FRA authors. F_t^n stands for the correct samples of the image after the protection algorithm in other FRA. β is the perception coefficient, which is based on the subjective evaluation of the tester comparing all the experimental results' weight from 0.10 to 0.99, *n* is FRA's ID. Shown as Eq (17), 1500 samples were tested in Table 6.

$$s_p = \beta^n \frac{F_p}{F_p+T_p+\sum_1^n F_t^n} \tag{17}$$

Table 6. Cheat experiments. The values in brackets have β participation.

	M_B	M_{Az}	M_F	M_{Ar}	M_D
Chaos	0.999(0.001)	0.999(0.001)	0.999(0.001)	0.999(0.001)	0.999(0.001)
Zero-watermark	0.001(0.999)	0.001(0.999)	0.001(0.999)	0.001(0.999)	0.001(0.999)
Twist	0.414(0.238)	0.230(0.138)	0.377(0.137)	0.798(0.701)	0.816(0.803)
Fawkes	0.001(0)	0.327(0.310)	0.199(0.013)	0.986(0.837)	0.997(0.986)
ADVHAT	0.001(0)	0.001(0)	0.333(0.334)	0.894(0.803)	0.960(0.960)
Mask Template	0.834(0.811)	0.852(0.633)	0.883(0.675)	0.901(0.897)	0.998(0.998)

The results indirectly proved that the method proposed in this paper has compatibility when dealing with multiple FRAs. Chaos method is more efficient without considering the visual effect.

4.5. FRAs superposition experiments

There is a catastrophic forgetting (feature confusion) phenomenon. Obviously, the pixel coordinates have shifted, as shown in Figure 11. Intuitively, it should be substantial differences in landmarks specifications of these enumerated FRAs, which may be related to the initial chaotic function of the chimpanzee hunting group. Logistic chaotic mapping with values of [0.01, 0.4] is used. If Singer mapping was used, the effect is much better. If users do more chaotic mapping experiments, they can save a lot of time, because they often find that the vision is affected after many rounds of model training.

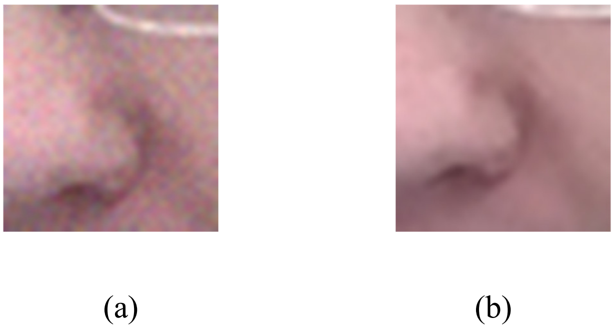

Figure 11. Catastrophic forgetting after hunting. (a) Feature confusion when Logistic mapping was used. (b) The image is smoother by singer mapping.

The output image results from the XOR operation between the noise and the original image through the mask template in Figure 12. Therefore, in order to restore the image, we only need to make the output image XOR with the mask template again. The mask template can be saved by image encryption. When the image needs to be decoded, restore the graphical mask template by decryption, to ensure the security of the mask template key.

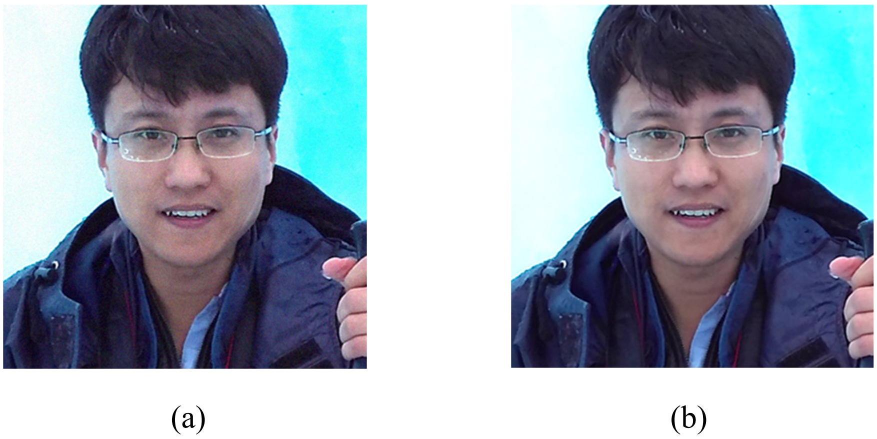

Figure 12. Multi model superposition reduction experiment. (a). Images generated for $M_{B+Az+F+Ar+D}$. (b). Restored image.

The average error rate of cumulative FRAs $\bar{F}_p$ proves the generality of the algorithm studied in this paper. Even if the generated image is far from expected, it must be able to restore to the original state. Table 7 records the results of accumulating different FRAs, where Perception is the author's subjective opinion, and $\bar{R}_{\boldsymbol{p}}$ is the recognition accuracy after restoring. It can be demonstrated that the number of FRA is not directly proportional to the training time.

Table 7. Training results.

FRAs	Training time(min)	$\bar{F}_p$	$\bar{R}_p$
$M_{B+Az+F+Ar+D}$	32,698	0.512	0.989
$M_{B+Az+F+D}$	31,058	0.838	0.989
$M_{B+Az+F+Ar}$	32,136	0.892	0.995
M_{B+Az+F}	31,274	0.977	0.998
M_{B+Az}	28,013	0.984	0.998
M_{F+Ar}	29,137	0.996	0.997
M_b	21,638	0.999	0.998
M_{Ar}	19,333	0.998	0.998

To investigate the performance of the algorithm switching between different versions of FRA from the same manufacturer, V1 and V2 of M_{Ar} is chosen because these two versions are easy to download and have different interfaces. V1 training took 19,333 minutes to generate a template, but it is invalid when applied to V2. Then V2 is directly turned into prey without changing the network structure and protected image. The result can be successful and takes another 6010 minutes. In contrast, Fawkes takes 61,028 minutes to train on V1 and AdvHat takes 93,110 minutes (two gradient explosions).

5. Discussion

The facial mask from AFN has great efficiency, but the solution to the template coordinate drift is only to change the chaotic function. The main reason is that we do not fully use the social behavior of chimpanzees. In other words, when the target features are captured, the weight of various roles in the network does not form an effective replacement. This causes that if the roles and tasks assigned at the beginning are not reasonable and the follow-up work is not tuned, we can only get good results from the random chaotic function. In the next work, we will focus on the optimization of task allocation and let the network adjust the weight of hunting members automatically.

6. Conclusions

The model proposed in this paper can ensure that the target face recognition algorithm cannot recognize the protected Face ID. the model improves the existing algorithms that can only protect the privacy for specific face recognition algorithms, and can deal with multiple recognition algorithms at the same time. In addition, a negative feedback network is added to intervene in image distortion, so that it can ensure that human beings can recognize the protected Face ID. In order to speed up the speed, the optimization algorithm of chimpanzee group hunting is introduced. Experiments show that the model can change the feature distribution of the facial image by up to 42% without obvious visual changes. It can be connected in parallel at least five commercial face recognition algorithms. Using a chaotic function to initialize network parameters can reduce the difficulty of network design, but it will produce slight noise on the output image. This will reduce the possibility of a gradient explosion. Compared with other biological privacy protection methods based on small perturbation, our method can improve the training speed by 4.8 times.

Acknowledgments

This research was partially funded by the Strategic Priority Research Program of the Chinese Academy of Sciences, grant number XDB41020104 and Scientific Research Project of Beijing Educational Committee, grant number KM202110005024.

Conflict of interest

The authors declare no conflict of interest.

References

1. R. M. Mizanur, M. A. Hossain, H. Mouftah, A. EI Saddik, E. Okamoto, Chaos-cryptography based privacy preservation technique for video surveillance, *Multimedia Syst.*, **18** (2012), 145–155. https://doi.org/10.1007/s00530-011-0246-9
2. G. Sun, H. Wang, Image encryption and decryption technology based on rubik's cube and dynamic password, *J. Beijing Univ. Technol.*, **47** (2021), 833–841. https://doi.org/10.11936/bjutxb2020120003
3. S. Shan, E. Wenger, J. Zhang, H. Li, H. Zheng, B. Y. Zhao, Fawkes: protecting privacy against unauthorized deep learning models, in *29th USENIX Security Symposium (USENIX Security 20)*, (2020), 1589–1604. Available from: https://www.usenix.org/conference/usenixsecurity20/presentation/shan.

4. J. Yang, J. Liu, R. Han, J. Wu, Transferable face image privacy protection based on federated learning and ensemble models, *Complex Intell. Syst.*, **7** (2021), 2299–2315. https://doi.org/10.1007/s40747-021-00399-6
5. 2021 White Paper of Innovation in Face recognition industry. Available from: https://www.vzkoo.com/read/11206bd95038173b5831540e5982e1b2.html.
6. R. A. Fisher, The use of multiple measurements in taxonomic problems, *Ann. Eugen.*, **7** (1936), 179–188. https://doi.org/10.1111/j.1469-1809.1936.tb02137.x
7. G. Cheng, Z. Song, Robust face recognition based on sparse representation in 2D fisherface space, *Optik*, **125** (2014), 2804–2808. https://doi.org/10.1016/j.ijleo.2013.11.042
8. L. Sirovich, M. Kirby, Low-dimensional procedure for the characterization of human faces, *J. Opt. Soc. Am. A*, **4** (1987), 519–524. https://doi.org/10.1364/JOSAA.4.000519
9. M. Turk, A. Pentland, Eigenfaces for recognition, *J. Cognit. Neurosci.*, **3** (1991), 71–86. https://doi.org/10.1162/jocn.1991.3.1.71
10. T. Ojala, M. Pietikainen, D. Harwood, A comparative study of texture measures with classification based on fea-tured distributions, *Pattern Recognit.*, **29** (1996), 51–59. https://doi.org/10.1016/0031-3203(95)00067-4
11. Q. Zhang, H. Li, M. Li, L. Ding, Feature extraction of face image based on LBP and 2-D Gabor wavelet transform, *Math. Biosci. Eng.*, **17** (2020), 1578–1592. https://doi.org/10.3934/mbe.2020082
12. Z. Peng, L. Tao, G. Xu, H. Zhang, Detecting facial features based on color segmentation and KL transform, *J. Tsinghua Univ. (Sci. Technol.)*, **41** (2001), 218–221. https://doi.org/10.16511/j.cnki.qhdxxb.2001.z1.052
13. Y. Taigman, M. Yang, M. A. Ranzato, L. Wolf, Deepface: closing the gap to human-level performance in face verification, in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, (2014), 1701–1708. https://doi.org/10.1109/CVPR.2014.220
14. Y. Sun, X. Wang, X. Tang, Deep learning face representation from predicting 10,000 classes, in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, (2014), 1891–1898. https://doi.org/10.1109/CVPR.2014.244
15. Y. Sun, Y. Chen, X. Wang, X. Tang, Deep learning face representation by joint identification-verification, in *Advances in Neural Information Processing Systems*, **27** (2014). Available from: https://proceedings.neurips.cc/paper/2014/file/e5e63da79fcd2bebbd7cb8bf1c1d0274-Paper.pdf.
16. Y. Sun, X. Wang, X. Tang, Deeply learned face representations are sparse, selective, and robust, in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (2015), 2892–2900. https://doi.org/10.1109/CVPR.2015.7298907
17. F. Schroff, D. Kalenichenko, J. Philbin, FaceNet: a unified embedding for face recognition and clustering, in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (2015), 815–823. https://doi.org/10.1109/CVPR.2015.7298682
18. J. Liu, Y. Deng, T. Bai, Z. Wei, C. Huang, Targeting ultimate accuracy: face recognition via deep embedding, preprint, arXiv: 1506.07310.
19. H. Fan, E. Zhou, Approaching human level facial landmark localization by deep learning, *Image Vision Comput.*, **47** (2016), 27–35. https://doi.org/10.1016/j.imavis.2015.11.004
20. W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, L. Song, Sphereface: deep hypersphere embedding for face recognition, in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (2017), 6738–6746. https://doi.org/10.1109/CVPR.2017.713

21. H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, et al., Cosface: large margin cosine loss for deep face recognition, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, (2018), 5265–5274. https://doi.org/10.1109/CVPR.2018.00552
22. J. Deng, J. Guo, N. Xue, S. Zafeiriou, ArcFace: additive angular margin loss for deep face recognition, in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, (2019), 4685–4694. https://doi.org/10.1109/CVPR.2019.00482
23. X. Tang, D. K. Du, Z. He, J. Liu, PyramidBox: a context-assisted single shot face detector, in *Computer Vision – ECCV 2018*, (2018), 812-828. https://doi.org/10.1007/978-3-030-01240-3_49
24. F. Boutros, N. Damer, F. Kirchbuchner, A. Kuijper, ElasticFace: elastic margin loss for deep face recognition, preprint, arXiv:2109.09416.
25. Q. Meng, S. Zhao, Z. Huang, F. Zhou, MagFace: a universal representation for face recognition and quality assessment, in *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, (2021), 14220–14229. https://doi.org/10.1109/CVPR46437.2021.01400
26. F. Boutros, N. Damer, M. Fang, F. Kirchbuchner, A. Kuijper, MixFaceNets: extremely efficient face recognition networks, in *2021 IEEE International Joint Conference on Biometrics (IJCB)*, (2021), 1–8. https://doi.org/10.1109/IJCB52358.2021.9484374
27. F. Boutros, P. Siebke, M. Klemt, N. Damer, F. Kirchbuchner, A. Luijper, PocketNet: extreme lightweight face recognition network using neural architecture search and multistep knowledge distillation, *IEEE Access*, **10** (2022), 46823–46833. https://doi.org/10.1109/ACCESS.2022.3170561
28. B. Meden, P. Rot, P. Terhorst, N. Damer, A. Luijper, W. J. Scheirer, Privacy–enhancing face biometrics: a comprehensive survey, *IEEE Trans. Inf. Forensics Secur.*, **16** (2021), 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024
29. A. Chattopadhyay, T. E. Boult, PrivacyCam: a privacy preserving camera using uCLinux on the blackfin DSP, in *2007 IEEE Conference on Computer Vision and Pattern Recognition*, (2007), 1–8. https://doi.org/10.1109/CVPR.2007.383413
30. P. Terhorst, D. Fahrmann, N. Damer, F. Kirchbuchner, A. Luijper, Beyond identity: what information is stored in biometric face templates, in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, (2020), 1–10, https://doi.org/10.1109/IJCB48548.2020.9304874
31. Z. Zhang, Y. Xu, L. Shao, J. Yang, Discriminative block-diagonal representation learning for image recognition, *IEEE Trans. Neural Networks Learn. Syst.*, **29** (2018), 3111–3125. https://doi.org/10.1109/TNNLS.2017.2712801
32. P. Terhorst, K. Riehl, N. Damer, P. Rot, B. Bortolato, F. Kirchbuchner, et al., PE-MIU: a training-free privacy-enhancing face recognition approach based on minimum information units, *IEEE Access*, **8** (2020), 93635–93647. https://doi.org/10.1109/ACCESS.2020.2994960
33. V. Mirjalili, S. Raschka, A. Ross, FlowSAN: privacy-enhancing semi-adversarial networks to confound arbitrary face-based gender classifiers, *IEEE Access*, **7** (2019), 99735–99745. https://doi.org/10.1109/ACCESS.2019.2924619
34. E. M. Newton, L. Sweeney, B. Malin, Preserving privacy by de-identifying face images, *IEEE Trans. Knowl. Data Eng.*, **17** (2005), 232–243. https://doi.org/10.1109/TKDE.2005.32
35. C. Xiang, C. Tang, Y. Cai, Q. Xu, Privacy-preserving face recognition with outsourced computation, *Soft Comput.*, **20** (2016), 3735–3744. https://doi.org/10.1007/s00500-015-1759-5
36. F. Tramer, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, P. McDaniel, Ensemble adversarial training: attacks and defenses, preprint, arXiv:1705.07204.

37. P. Terhorst, N. Damer, F. Kirchbuchner, A. Luijper, Unsupervised privacy-enhancement of face representations using similarity-sensitive noise transformations, *Appl. Intell.*, **49** (2019), 3043–3060. https://doi.org/10.1007/s10489-019-01432-5
38. Y. Li, Y. Wang, D. Li, Privacy-preserving lightweight face recognition, *Neurocomputing*, **363** (2019), 212–222. https://doi.org/10.1016/j.neucom.2019.07.039
39. M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, S. Camtepe, Privacy preserving face recognition utilizing differential privacy, *Comput. Secur.*, **97** (2020), 101951. https://doi.org/10.1016/j.cose.2020.101951
40. Z. Kuang, Z. Guo, J. Fang, J. Yu, N. Babaguchi, J. Fan, Unnoticeable synthetic face replacement for image privacy protection, *Neurocomputing*, **457** (2021), 322–333. https://doi.org/10.1016/j.neucom.2021.06.061
41. J. C. LIN, P. Fournier-Viger, L. Wu, W. Gan, Y. Djenouri, J. Zhang, PPSF: an open-source privacy-preserving and security mining framework, in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, (2018), 1459–1463. https://doi.org/10.1109/ICDMW.2018.00208
42. K. Zheng, J. Shen, G. Sun, H. Li, Y. Li, Shielding facial physiological information in video, *Math. Biosci. Eng.*, **19** (2022), 5153–5168. https://doi.org/10.3934/mbe.2022241
43. J. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, M. Aloqaily, Privacy-preserving multiobjective sanitization model in 6G IoT environments, *IEEE Internet Things J.*, **8** (2021), 5340–5349. https://doi.org/10.1109/JIOT.2020.3032896
44. X. Wang, H. Xue, X. Liu, Q. Pei, A privacy-preserving edge computation-based face verification system for user authentication, *IEEE Access*, **7** (2019), 14186–14197. https://doi.org/10.1109/ACCESS.2019.2894535
45. W. Shen, Z. Wu, J. Zhang, A face privacy protection algorithm based on block scrambling and deep learning, in *Cloud Computing and Security*, (2018), 359–369. https://doi.org/10.1007/978-3-030-00012-7_33
46. N. Damer, A. Opel, A. Shahverdyan, An overview on multi-biometric score-level fusion, in *Proceedings of the 2nd International Conference on Pattern Recognition Applications and Methods (BTSA-2013)*, (2013), 647–653. https://doi.org/10.5220/0004358306470653
47. N. Damer, A. Opel, A. Nouak, Biometric source weighting in multi-biometric fusion: towards a generalized and robust solution, in *2014 22nd European Signal Processing Conference (EUSIPCO)*, (2014), 1382–1386. Available from: https://ieeexplore.ieee.org/abstract/document/6952496.
48. N. Damer, F. Maul, C. Busch, Multi-biometric continuous authentication: a trust model for an asynchronous system, in *2016 19th International Conference on Information Fusion (FUSION)*, (2016), 2192–2199. Available from: https://ieeexplore.ieee.org/abstract/document/7528154.
49. N. Damer, S. Zienert, Y. Wainakh, A. M. Saladié, F. Kirchbuchner, A. Kuijper, A multi-detector solution towards an accurate and generalized detection of face morphing attacks, in *2019 22th International Conference on Information Fusion (FUSION)*, (2019), 1–8. Available from: https://ieeexplore.ieee.org/abstract/document/9011378.
50. X. Zhang, C. Shi, X. Wang, X. Wu, X. Li, J. Lv, et al., Face inpainting based on GAN by facial prediction and fusion as guidance information, *Appl. Soft Comput.*, **111** (2016), 107626. https://doi.org/10.1016/j.asoc.2021.107626

51. K. Simonyan, A. Zisserman, Very deep convolutional networks for large-scale image recognition, preprint, arXiv:1409.1556.
52. C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, et al., Intriguing properties of neural networks, preprint, arXiv:1312.6199.
53. R. Mutegeki, D. S. Han, Feature-representation transfer learning for human activity recognition, in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, (2019), 18–20. https://doi.org/10.1109/ICTC46691.2019.8939979
54. Y. Li, M. Zhu, G. Sun, J. Chen, X. Zhu, J. Yang, Weakly supervised training for eye fundus lesion segmentation in patients with diabetic retinopathy, *Math. Biosci. Eng.*, **19** (2022), 5293–5311. https://doi.org/10.3934/mbe.2022248
55. M. Khishe, M. R. Mosavi, Chimp optimization algorithm, *Expert Syst. Appl.*, **149** (2020), 113338. https://doi.org/10.1016/j.eswa.2020.113338
56. C. Boesch, Cooperative hunting roles among taï chimpanzees, *Hum. Nat.*, **13** (2002), 27–46. https://doi.org/10.1007/s12110-002-1013-6
57. J. M. Wu, J. C. Lin, P. Fournier-Viger, Y. Djenouri, C. Chen, Z. Li, The density-based clustering method for privacy-preserving data mining, *Math. Biosci. Eng.*, **16** (2019), 1718–1728. https://doi.org/10.3934/mbe.2019082
58. I. Aljarah, H. Faris, S. Mirjalili, Optimizing connection weights in neural networks using the whale optimization algorithm, *Soft Comput.*, **22** (2018), 1–15. https://doi.org/10.1007/s00500-016-2442-1
59. M. Pautov, G. Melnikov, E. Kaziakhmedov, K. Kireev, A. Petiushko, On adversarial patches: real-world attack on ArcFace-100 face recognition system, in *2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, (2019), 0391–0396. https://doi.org/10.1109/SIBIRCON48586.2019.8958134
60. A. Radford, L. Metz, S. Chintala, Unsupervised representation learning with deep convolutional generative adversarial networks, preprint, arXiv:1511.06434.
61. C. Sharma, A. Bagga, R. Sobti, M. Shabaz, R. Amin, A robust image encrypted watermarking technique for neurodegenerative disorder diagnosis and its applications, *Comput. Math. Methods Med.*, **2021** (2021), 8081276. https://doi.org/10.1155/2021/8081276
62. Z. Liu, J. Li, J. Liu, Encrypted face recognition algorithm based on Ridgelet-DCT transform and THM chaos, *Math. Biosci. Eng.*, **19** (2022), 1373–1387. https://doi.org/10.3934/mbe.2022063
63. C. Wang, X. Wang, Z. Xia, C. Zhang, Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm, *Inf. Sci.*, **470** (2019), 109–120. https://doi.org/10.1016/j.ins.2018.08.028
64. S. Komkov, A. Petiushko, AdvHat: Real-world adversarial attack on arcface face ID system, in *2020 25th International Conference on Pattern Recognition (ICPR)*, (2021), 819–826. https://doi.org/10.1109/ICPR48806.2021.9412236
65. B. Bortolato, M. Ivanovska, P. Rot, J. Križaj, P. Terhörst, N. Damer, et al., Learning privacy-enhancing face representations through feature disentanglement, in *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020)*, (2020), 495–502. https://doi.org/10.1109/FG47880.2020.00007
66. S. Li, F. Liu, J. Liang, Z. Cai, Z. Liang, Optimization of face recognition system based on azure IoT edge, *Comput. Mater. Continua*, **61** (2019), 1377–1389. https://doi.org/10.32604/cmc.2019.06402

67. G. Gamage, I. Sudasingha, I. Perera, D. Meedeniya, Reinstating Dlib correlation human trackers under occlusions in human detection based tracking, in *2018 18th International Conference on Advances in ICT for Emerging Regions (ICTer)*, (2018), 92–98. https://doi.org/10.1109/ICTER.2018.8615551
68. P. Baldi, K. Hornik, Neural networks and principal component analysis: learning from examples without local minima, *Neural Networks*, **2** (1989), 53–58. https://doi.org/10.1016/0893-6080(89)90014-2
69. P. Terhörst, M. Huber, N. Damer, P. Rot, F. Kirchbuchner, V. Struc, et al., Privacy evaluation protocols for the evaluation of soft-biometric privacy-enhancing technologies, in *BIOSIG 2020 - Proceedings of the 19th International Conference of the Biometrics Special Interest Group*, (2020), 215–222. http://dl.gi.de/handle/20.500.12116/34330
70. K. Owusu-Agyemang, Z. Qin, A. Benjamin, H. Xiong, Z. Qin, Guaranteed distributed machine learning: privacy-preserving empirical risk minimization, *Math. Biosci. Eng.*, **18** (2021), 4772–4796. https://doi.org/10.3934/mbe.2021243
71. R. N. Abiram, P. Vincent, Identity preserving multi-pose facial expression recognition using fine tuned VGG on the latent space vector of generative adversarial network, *Math. Biosci. Eng.*, **18** (2021), 3699–3717. https://doi.org/10.3934/mbe.2021186