IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 January 2023, accepted 2 March 2023, date of publication 22 March 2023, date of current version 3 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3260260

RESEARCH ARTICLE

FaceIDP: Face Identification Differential Privacy via Dictionary Learning Neural Networks

LU OU[1], (Member, IEEE), YI HE[1], SHAOLIN LIAO[2,3], (Senior Member, IEEE), ZHENG QIN[4], (Member, IEEE), YUAN HONG[5], (Senior Member, IEEE), DAFANG ZHANG[4], AND XIAOHUA JIA[6], (Fellow, IEEE)

[1]School of Journalism and Communication, Hunan University, Changsha, Hunan 410082, China
[2]School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, Guangdong 510006, China
[3]Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616, USA
[4]College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan 410082, China
[5]Department of Computer Science and Engineering, University of Connecticut, Storrs, Mansfield, CT 06269, USA
[6]Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong

Corresponding author: Shaolin Liao (liaoshlin@mail.sysu.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2022YFB3103500, in part by the Guangdong Zhujiang Projects under Grant 2021ZT09X070 and Grant 2021CX02X011, in part by the National Natural Science Foundation of China under Grant 62002112 and Grant U20A20174, in part by the Natural Science Foundation of Hunan Province under Grant 2021JJ40117 and Grant 2019JJ50067, in part by the Science and Technology Key Projects of Hunan Province under Grant 2015TP1004, and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT In big-data era, large amount of facial images could be used to breach the face identification system, which demands effective Face IDentification Differential Privacy (FaceIDP) of the facial images for widespread adoption of the face identification technique. In this paper, to our best knowledge, we take the first step to systematically study an effective important FaceIDP approach via the help of Dictionary Learning (DL) for secure releasing of facial images. First, a Dictionary Learning neural Network (DLNet) has been developed and trained with the facial images database, to learn the common dictionary basis of the facial image database. Then, the coding coefficients of the facial images are obtained. After that, the sanitizing noise is added to the coding coefficients, which obfuscates the facial feature vector that is used to identify a user's identification. We have also proved that the FaceIDP is ε-differentially private. More importantly, optimal noise scale parameters have been obtained via the Lagrange Multiplier (LM) method to achieve better data utility for a given privacy budget ε. Finally, substantial experiments have been conducted to validate the efficiency of the FaceIDP with two real-life facial image databases.

INDEX TERMS Face-IDentification Privacy (FaceIDP), differential privacy, dictionary learning neural network.

I. INTRODUCTION

Face identification has been extensively used as a biometric authentication system in many fields such as public safety, finance, e-commerce, *etc.*, due to its super convenience [1]. Also, in the 5G and beyond era where images and videos on the internet clouds can be transmitted and shared in real time and faster speed than ever [2], [3]. This poses great threat to face identification systems because the adversaries could combine an individual's multiple facial images to form the 3D feature vectors and breaches the face identification system to identify the individual of interest [4]. This is especially true in the era of Artificial Intelligence (AI) [5], [6]: through training an AI system with large number of facial images of individuals, facial feature vectors could be learned accurately; then the face identification of the individual is carried out through deep learning, leading to privacy leakage from mining information of the publicly shared facial images [7]. However, the General Data Protection Regulations (GDPR) [8] clearly point out that individuals' privacy should be protected when

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Wei.

their data is used. Because the identification systems face the real risk of being breached, they are forbidden in many cities, such as San Francisco and Boston, in USA. Therefore, an effective face identification privacy protection approach is urgent for widespread adoption of face identification based applications.

However, there is lack of research on such face identification privacy problem, *i.e.*, adversaries may intrude face identification systems by utilizing falsified feature vectors generated from publicly released facial images through machine learning, although researches on other privacy problems other than the face identification privacy of publicly shared facial images exist. For example, in order to protect the facial image privacy, image obfuscation [9], [10], [11] such as pixelization and blurring, are adopted to protect image features. Unfortunately, these approaches could be re-identified. To fix this problem, a differentially private pixelization is proposed [12]. Furthermore, under the deep learning environment, adversarial perturbation generative network is proposed to preserve image features [13], [14]. However, these privacy protection approaches do not aim at protecting the face identification privacy with optimal utility.

To reduce the data space of facial images for the efficient face identification privacy algorithm, it is preferred that the basis set of the facial images can be learned in advance, which calls for the Dictionary Learning neural Network (DLNet) to learn the sparsifying basis set adaptively in real time [2], [15], [16], [17], [18].

To efficiently deal with the face identification privacy problem, we propose a novel Face-IDentification Privacy (FaceIDP) approach with the help of the DLNet. Without loss of generality, the 2D face identification, instead of the 3D face identification, is used to present the FaceIDP approach. Our major contributions are

- We integrate our recently developed effective DLNet [18] in the proposed FaceIDP approach to efficiently protect the face identification privacy, *i.e.*, to prevent adversaries from using the individuals' facial images to breach the face identification systems.
- To achieve the optimal DP performance, the DLNet is developed to adaptively learn the common dictionary facial image basis of the facial image database so that only weighted sanitizing noise is distributed to those face coding coefficients that correspond to the important dictionary facial image basis.
- The LM method is used to obtain the mathematical formula of the optimized distributed partial noise scale parameters of the face coding coefficients for the global constrained optimization problem of maximizing the data utility for a given global privacy budget ε.
- Extensive experiments have been conducted with the Labeled Faces in the Wild (LFW) database [19] and PubFig database [20], which show that the proposed FaceIDP approach outperforms other DP approaches.

II. RELATED WORK

The face identification system which is an important identity authentication system, has been widely used. Meanwhile, its privacy problem is also very important and challenging. Works have the cryptography-based face identification problems [1], [11]. These cryptography-based approaches can deal with facial image data securely. But the facial images collection center and the third party need to exchange secrets/keys in a secure channel. It does not fit into our non-interactive setting.

To the best of our knowledge, little research has been conducted on the face identification privacy protections. However, researches on other privacy problems of the facial images have been conducted. For example, to protect image privacy, researchers used pixelization [9] and blurring approaches to achieve image obfuscation. Unfortunately, McPherson et al. [10] studied pixelization and YouTube face blurring and concluded that the obfuscated images using those approaches can be re-identified. Furthermore, in order to deal with such problem, Fan [12] proposed the differentially private pixelization approach to protect image features. However, it doesn't focus on differentially private face identification problem.

Furthermore, regarding the deep learning, Tong and Zheng [13] proposed an adversarial perturbation generative network to generate perturbation to preserve image privacy. Yang et al. [14] proposed a facial image privacy protection approach by adding perturbation in the principal components of the facial images.

Therefore, it is necessary to study the optimal face identification privacy approach in order to achieve better data utility while still protecting the face identification system from being attacked by the adversaries, which is the focus of this paper.

III. PRELIMINARIES AND PROBLEM FORMULATION

In this section, we first provide preliminaries. It then presents the system model and the adversary model for technical discussions and the problem statement of the paper.

To start, **Table 1** lists some key variables used across this paper with their explanations.

A. THE DP FRAMEWORK

In this paper, we are interested only in whether there exists an effective FaceIP Privacy approach (FaceIDP) that can prevents the adversary to use a user's facial images to breach the face identification system, as shown in Fig. 1: without the FaceIDP, the adversary can use the publicly available facial images of a user to recognize the user, *i.e.*, to breach the face identification system (top of Fig. 1); while with the FaceIDP, the sanitizing noise is added in such a way that face identification system cannot recognize whether the facial images belong to the user or not. In the terminology of the differential privacy, the neighboring data records are a facial images set of an individual and a facial image set of the closest

TABLE 1. Notations and Definitions.

Symbol	Description
F	A facial image.
(A, B)	A neighboring facial image pair.
$\mathcal{F}$	$\{F\}$: The facial images set of a user.
$(\mathcal{A}, \mathcal{B})$	Facial image sets of a neighboring user pair.
F'	A noisy facial image.
$\overline{F}_M$	The 1D coding coefficients vector of length M.
$\mathbb{F}$	$\{\overline{F}_M\}$: the facial image coding coefficients dataset.
$\mathbb{F}_m$	$\{F_m\}$: the coding coefficient data subset.
$\overline{\overline{D}}_{N\times M}$	The $N \times M$ dictionary basis matrix.
$\overline{V}_L$	The feature vector of a facial image F with length L.
$\overline{P}_N$	A 1D pixel vector of a facial image F of length N.
$\mathbb{P}$	A set of facial image 1D pixel vectors $\{\overline{P}_N\}$.
f	The Probability Distribution Function (PDF).
Lap	The Laplace PDF.
CDF	The cumulative distribution function of Laplace distribution.
Ω	Probability space.
Pr	Probability over a probability space Ω
$\mathcal{U}$	Data utility.
$\overline{S}$	Partial sensitivity.
$\overline{b}_M$	The Laplace noise scale parameter vector of $\overline{F}_M$.
ε_m	Locus privacy budget.
ε	Loci privacy budget.

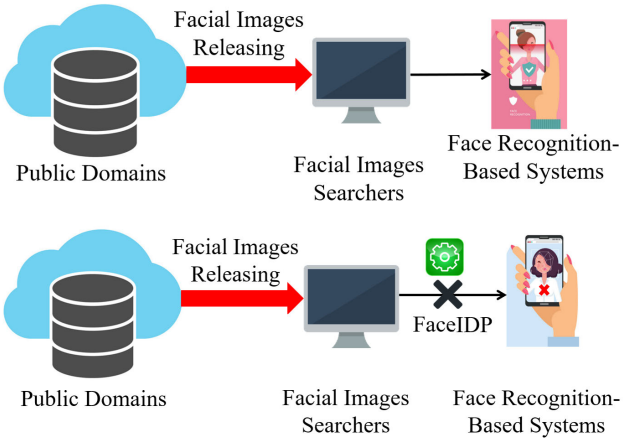


FIGURE 1. System Model.

individual, characterized by the ℓ_1-norm distance between their coding coefficients vectors.

Furthermore, the closest neighboring facial images are a pair of most similar facial images of the neighboring facial image sets in **Definition 1**, under the measure function $\mathcal{M}$. The definition is as **Definition 2**.

Definition 1 (The Neighboring Facial Image Sets): The neighboring facial image sets are the facial image set of an individual ($A \in \mathcal{A}$) and the facial image set of all other individuals ($B \in \mathcal{B}$),

$$\left(\left\{\overline{F}_M^{(A)} : A \in \mathcal{A}\right\}, \left\{\overline{F}_M^{(B)} : B \in \mathcal{B}\right\}\right) : \mathcal{B} \cup \mathcal{A} = \varnothing,$$

where the facial image is represented by its coding coefficients vector $\overline{F}_M$.

Definition 2 (The Closest Neighboring Face Images): The closest neighboring facial images pair is,

$$(A, B) : \underset{B}{argmin} \left\{\left|\mathcal{M}\left(\overline{F}_M^{(A)}\right) - \mathcal{M}\left(\overline{F}_M^{(B)}\right)\right|\right\}.$$

Definition 3 (Differential Privacy): Let $\mathcal{M}'$ be a obfuscating measure function with sanitizing random noise added, and O be any outcome of the measure function $\mathcal{M}$. For the two closest neighboring datasets A and B, the measure function $\mathcal{M}$ will be ε-differential private, if the following is satisfied

$$exp(-\varepsilon) \leq \frac{Pr\left(\mathcal{M}'(\overline{F}_M^{(A)}\right) = O)}{Pr(\mathcal{M}'\left(\overline{F}_M^{(B)}\right) = O)} \leq exp(\varepsilon).$$

Because the feature vector $\overline{F}_M^{(A)}$ and $\overline{F}_M^{(B)}$ consists of M elements, the privacy budget ε defined in **Definition 3** can be further expressed in terms of the partial differential privacy budgets of all M elements defined below [21], [22], [23],

Definition 4 (The Partial Differential Privacy): The obfuscating measure function $\mathcal{M}'$ adds noise to an element F_m of a facial image coding coefficients vector $\{\overline{F}_M : F_m \in \overline{F}_M, m = 1, \cdots M\}$, it is said to be ε_m-differentially private if the following probability condition is satisfied after the sanitizing noise is added to F_m,

$$\exp\left(-\varepsilon_m\right) \leq \frac{Pr\left\{\mathcal{M}'\left(F_m^{(i)}\right) = F_m'\right\}}{Pr\left\{\mathcal{M}'\left(F_m^{(j)}\right) = F_m'\right\}} \leq \exp\left(\varepsilon_m\right),$$

where in this paper, the obfuscating measure function $\mathcal{M}'$ adds independent Laplace noise to each element F_m.

It is clear that the total privacy is a function of the partial privacy budget vector, *i.e.*, $\varepsilon\left(\overline{\varepsilon}_M\right), \overline{\varepsilon}_M = [\varepsilon_1, \cdots, \varepsilon_M]^T$.

B. JOINT PROBABILITY BOUNDS

From **Definition 3** and **Definition 4**, it is clear that the privacy budget ε is closely related to the lower and upper bounds of numerator and denominator. So in this section, we will obtain the lower and upper bounds of the probabilities in **Definition 3** and **Definition 4**, which later will be used to prove that our FaceIDP satisfies the differential privacy.

The joint Probability Distribution Function (PDF) of the multivariate random variables vector $\overline{F}_M$ with length M, denoted as $f(\overline{F}_M)$, has its lower and upper bounds on a domain Ω given as follows,

Lemma 1 (Bounds of the Joint Probability): The lower and upper bounds of the joint probability $f(\overline{F}_M)$ on a domain Ω is

$$Pr(\overline{F}_N \in \Omega) \begin{cases} \geq \max\limits_{\Omega_{Fm}} \left\{\prod\limits_{m=1}^{M} Pr(X_m \in \Omega_{F_m})\right\}, \\ \leq Pr(\overline{F}_M \in \Omega) \leq \min_m \{Pr(F_m \in \Omega)\}, \end{cases}$$

where $\overline{\Omega} = \overline{I} - \Omega$ is the complementary domain with $\overline{I}$ being the entire domain of interest; and Ω_{F_m} is the sub-domain in which all $\overline{F}_M$ belongs to Ω.

Proof: The joint probability distribution can be expressed in terms of the conditional probability distribution,

$$f(\overline{F}) = f(F_m) f\left(\cdots F_{m-1}, F_{m+1}, \cdots | F_m\right) \leq f(F_m),$$

where the following conditional probability property has been used,

$$f\left(\cdots F_{m-1}, F_{m+1}, \cdots | F_m\right) \leq 1.$$

from which the probability in domain Ω is given by,

$$\begin{aligned} Pr(\overline{F} \in \Omega) &= \int_{F_1} \cdots \int_{F_M} f(\overline{F}) dF_1 \cdots dF_M \\ &\leq \int_{F_1} \cdots \int_{F_M} f(F_m) dF_1 \cdots dF_M \\ &= Pr(F_m \in \Omega), \end{aligned}$$

and the upper bound on the right hand side of **Lemma 1** is proved,

$$Pr(\overline{F} \in \Omega) \leq \min_m \left\{ Pr(F_m \in \Omega) \right\}.$$

The lower bound of the left hand side of **Lemma 1** can be obtained by finding the sub-domains of all F_n, denoted as Ω_{F_m}, in which all $\overline{F}_M$ belongs to Ω and the probability is given by,

$$Pr(\overline{F}_M \in \overline{\Omega}) \leq \min_m \left\{ Pr(F_m \in \overline{\Omega}) \right\},$$

from which the probability lower bound in domain Ω is given by,

$$\begin{aligned} Pr(\overline{F} \in \Omega) &\geq \int_{F_1} \cdots \int_{F_N} f(\overline{F}) dF_1 \cdots dF_M \\ &\geq \int_{\Omega_{F_1}} \cdots \int_{\Omega_{F_M}} f(F_m) dF_1 \cdots dF_M \\ &= \prod_{n=1}^{M} Pr(F_m \in \Omega_{F_m}), \end{aligned}$$

where independence has been assumed for all elements of $\overline{F}_M$ and the lower bound is thus obtained as,

$$Pr(\overline{F} \in \Omega) \geq \max_{\Omega_{F_m}} \left\{ \prod_{m=1}^{M} Pr(F_m \in \Omega_{F_m}) \right\},$$

from which **Lemma 1** is proved. □

C. DATA UTILITY

When the coding coefficients noise $\overline{n}_M$ is added to a facial image's coding coefficients $\overline{F}_M$, the noisy image is thus obtained as,

$$\overline{P}'_N = \overline{P}_N + \overline{D}_{N \times M} \overline{n}_M. \tag{1}$$

So, the data utility is thus defined as follows,

Definition 5 (Data Utility): The data utility is defined as the visual quality of the image [13]: here the expectation of the variance of the reconstructed noisy image from the original image,

$$\mathcal{U} = E\left\{ \left| \overline{P}'_N - \overline{P}_N \right|_2^2 \right\}. \tag{2}$$

Substituting Eq. (1) into Eq. (2), the data utility is obtained,

$$\mathcal{U} = \sum_{m=1}^{M} W_m \sigma_m^2 \quad W_m = \sum_{n=1}^{N} D_{n,m}^2 \tag{3}$$

where σ_m is the standard deviation of the noise component n_m, which is assumed to be independent of each other.

D. MODELS AND PROBLEM STATEMENT

1) SYSTEM MODEL

Again, the typical working scenarios of the FaceIDP problem are shown in Fig 1. Generally, a huge amount of facial images are available in the public domain for individuals, *i.e.*, facial images searchers, to download for entertainment and others. Without privacy protection, the searchers could use the downloaded facial images to analysis the facial feature vectors in order to breach some face identification system such as a smartphone, as shown on the top of Fig. 1. Furthermore, as shown on the bottom of Fig. 1, when an extra FaceIDP approach runs on the public domain side to sanitize the facial images before their releasing, the individuals' face identification systems could be well protected from the face identification leaking.

In this model, an individual's facial image is characterized by its 1D pixel vector denoted as $\overline{P}_N$ of length N. What's more, the facial image set $\mathbb{P}$ consists of all individuals' facial images, $\mathbb{P} = \left\{ \overline{P}_N | N = 0, 1, \cdots \right\}$.

2) PROBLEM STATEMENT

In this paper, we study the privacy problem of the face identification: our goal is to prevent adversaries from using individuals' facial images to breach the face identification systems, which is characterized by the Euclidean norm measure $\mathcal{M}$ on the face identification feature vector space $\overline{V}$, which is a function of the coding coefficient components $\overline{F}_M$. For example, if a facial image belongs to user $A(\mathcal{A})$ if the following statement holds

$$\overline{F}_M \in \mathcal{A}: \ \mathcal{M}\left\{\overline{V}_L\right\} = \left|\left|\overline{V}_L\right|\right|_2 \in \left\{\Omega_{\mathcal{A}} = \left|\left|\overline{V}_L\right|\right|_2 \leq R\right\}, \tag{4}$$

where R is the radius of user $A(\mathcal{A})$.

Our purpose is to design an efficient face identification privacy protection approach by adding random perturbation on the original facial images, denoted by $\mathbb{P}$, to hide the face

identification feature vector space $\overline{V}$ from the adversaries. Under the face identification privacy protection approach, the face identification system cannot distinguish whether a set of noisy facial images belong to the certain individual or not, with some confidence probability level or $\varepsilon-$differential privacy has been achieved.

Finally, optimal data utility should be obtained for a given global differential privacy level ε.

3) ADVERSARY MODEL

For the well-known semi-honest adversary model, adversaries are honest but curious. In our paper, the facial image searchers are considered as adversaries. They can access the facial images on public domains and may be interested in breaching an individual's face identification systems. Once adversaries obtain the images, they may analyze the user's facial data set $\mathcal{F}$ which is the unique identification of an individual. Furthermore, the face identification could be represented by the coding coefficients vector $\overline{F}_M$, *i.e.*, $\left\{\overline{F}_M\right\} : F \in \mathcal{F}$. Then, through the face identification query measure function, which is to validate an individual's identification, adversaries could intrude the face identification systems. With the facial images obtained by the adversaries as input, the query measure function gives the outcome of "1" if it can validate the individual's identification or "0" otherwise.

4) THE DLNet

The authors recently developed a concise DLNet that can obtain the coding coefficients vector $\overline{F}_M$ effectively [18]. As shown in Fig. 2, the DLNet consists of mainly 2 sub-networks:

1) The sparse representation sub-network: it consists of multiple Fully Connected Layers (FCL) with their basis denoted as $\overline{\overline{D}}^{(k)}_{M_{i+1}\times M_k}, k = 1, K$ and the corresponding coding coefficients denoted as $\overline{\overline{F}}^{(k)}_{M_k}$. The initially reconstructed image $\overline{P}^0_N$ can be expressed as follows,

$$\overline{P}^0_N = \overline{\overline{D}}_{N\times M_K}\left(\prod_{k=1}^{K}\overline{\overline{D}}_{M_{k+1}\times M_k}\right)\overline{\overline{D}}_{M_1\times M}\overline{F}_M.$$

2) The smoothing Convolutional Neural Network (CNN) sub-network: it takes the initially reconstructed image $\overline{P}^0_N$ as input and makes the Total Variation (TV) of the output image $\overline{P}'_N$ smooth,

$$TV\left(\overline{\overline{P'}}\right) = \sum_i^n\sum_j^m\left[\left(\nabla^h_{i,j}\overline{\overline{P'}}\right)^2 + \left(\nabla^v_{i,j}\overline{\overline{P'}}\right)^2\right];$$
$$\bigvee_{i,j}^{h}\overline{\overline{P'}} = P'_{i+1,j} - P'_{i,j},\quad \nabla^v_{i,j}\overline{\overline{P}}' = P'_{i,j+1} - P'_{i,j}.$$

The purpose of the sparse representation sub-network is to learn the sparse representation of the facial images' details and the smoothing CNN sub-network is used to fill in the area between the facial images' details.

During the DLNet training process, both the dictionary basis and the coding coefficients can be trained through minimizing the two error functions, *i.e.*, the mean square error of the reconstructed image E and the ℓ_1 norm of the sparse code $\overline{\overline{F}}^{(k)}_{M_k}$ Specifically, the DLNet is trained through two sequential steps: 1) updating of the parameters through the Stochastic Gradient Descent (SGD) method; and 2) performing the ℓ_1 norm sparsification operation.

1) The SGD updating: first, the gradient of parameter x, denoted as $\nabla_x E$, can be obtained through the chain rule,

$$\nabla_x E = -2\sum_{n=1}^{N}\left(P_n - P'_n\right)\nabla_x P'_n,$$

and the parameter x is updated as follows

$$x = x - \eta\nabla_x E,$$

with η being the learning rate and the parameter x is either the dictionary bases or the coding coefficients,

$$x = \left\{\overline{\overline{D}}_{M_k\times M}, \overline{\overline{F}}^{(k)}_{M_k}\right\}.$$

2) The ℓ_1-norm sparsification operation: Then, the ℓ_1-norm Operation is performed on the SGD updated coding coefficients $\overline{\overline{F}}^{(k)}_{M_k}$ through the Iterative Soft Thresholding Algorithm (ISTA) to achieve the sparsity of the coding coefficients,

$$\overline{\overline{F}}^{(k)}_{M_k} = sign\left\{\overline{\overline{F}}^{(k)}_{M_k}\right\}\max\left\{0, \overline{\overline{F}}^{(k)}_{M_k} - \lambda\right\},$$

where λ is the thresholding value.

Finally, after the training of the DLNet, the total dictionary basis $\overline{\overline{D}}_{N\times M}$ is obtained as follows,

$$\overline{\overline{D}}_{N\times M} = \overline{\overline{D}}_{N\times M_K}\left(\prod_{k=1}^{K}\overline{\overline{D}}_{M_{k+1}\times M_k}\right)\overline{\overline{D}}_{M_1\times M}.$$

According to the definition of the privacy budget in **Definition 3**, the privacy budget ϵ is an implicit function of the partial privacy budget ϵ_m given in **Definition 4** whose relation depends on the face identification measure function $\mathcal{M}$, which is usually nonlinear. Also, according to **Definition 5**, the data utility $\mathcal{U}$ is also an implicit function of the partial privacy budget ϵ_m. Thus there exists the constrained optimization problem of finding the optimal data utility $\mathcal{U}$ given a partial privacy budget ϵ_m, which is the focus of this paper.

Now let's calculate the privacy budget defined in **Definition 3** and **Definition 4**.

According to **Section III-B**, it is known that the lower bound and upper bound of two probabilities have to be computed: 1) the probability that a noisy facial image of user B, denoted as $B'(\mathcal{B})$, is mistakenly assigned to user $A(\mathcal{A})$; and 2) the probability that a noisy image of user A, denoted as

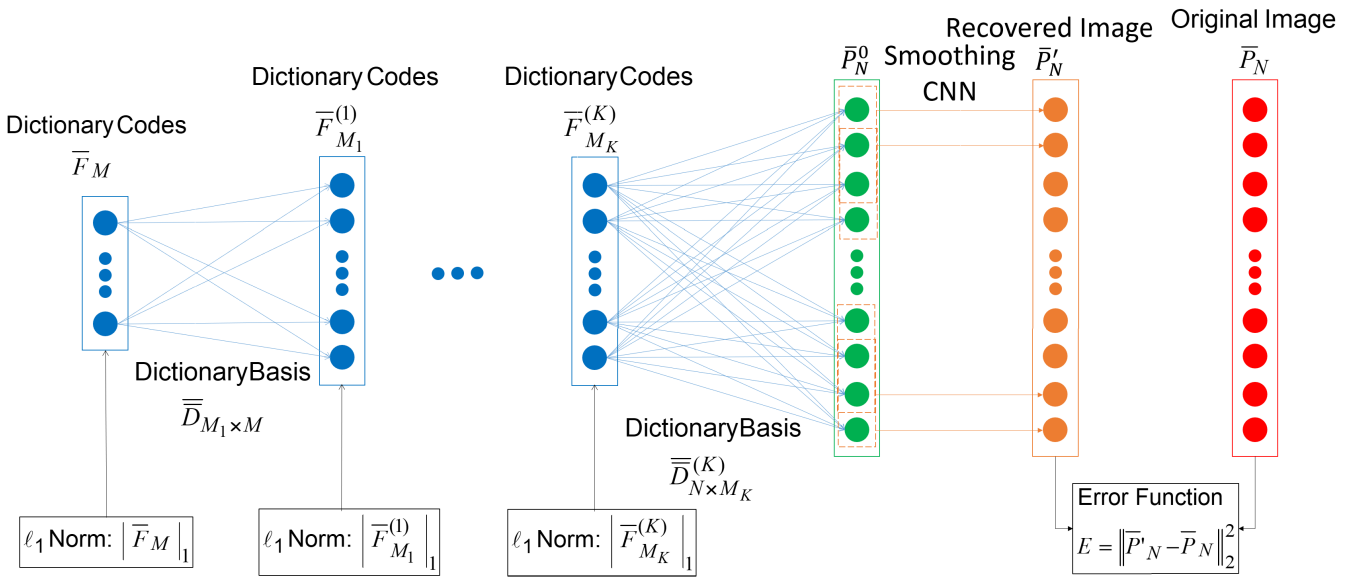


FIGURE 2. The working principle of the DLNet to learn the sparse dictionary basis of the facial images.

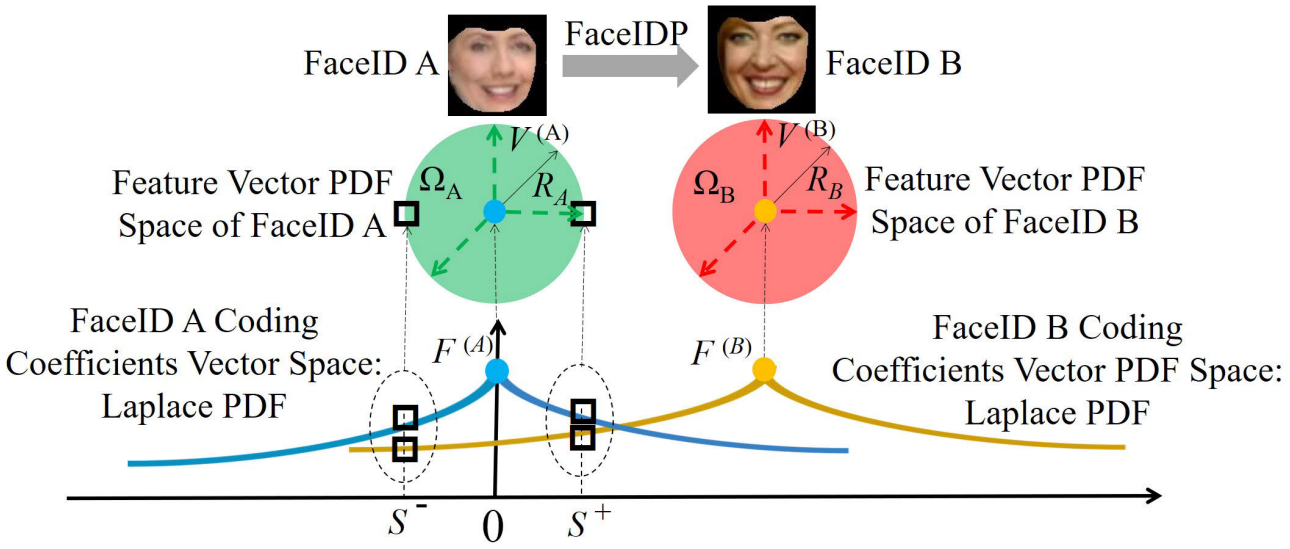


FIGURE 3. PDF spaces of the feature vectors for the closest neighboring facial image pair ($A \in \mathcal{A}$, $B \in \mathcal{B}$) showing the sensitivities of the FaceIDP.

$A' \in \mathcal{A}$, is still assigned the correct user $A(\mathcal{A})$. These probabilities are related to the face identification feature vector space $\overline{V}_L$ of length L, which is a function of the first M significant coding coefficient components $\overline{F}_M$: $\overline{V}_L\left(\overline{F}_M\right)$, as shown in Fig. 3. First, the user $A(\mathcal{A})$ is assigned to a facial image F through the Euclidean norm measure $\mathcal{M}$ on the feature vector $\overline{V}_L$, as shown in Eq. (4).

Then, the probability of a face F assigned user $A(\mathcal{A})$ is given by,

$$P_F = Pr\left(\mathcal{M}\left\{\overline{V}_L\right\} \in \Omega_{\mathcal{A}}\right). \tag{5}$$

Also, the feature vector space $\overline{V}_L$ is related to the first M significant face coding coefficients components $\overline{F}_M$. For example, when the change of a single face coding coefficients element F_m corresponds to a probability curve $\left|\left|\overline{V}_L\right|\right|_2$ in the feature vector space $\overline{V}_L$, as shown in Fig. 3.

Definition 6 (Probability Boundary Edges): The probability boundary edges define the probability space within which the noisy image B' is assigned user $A(\mathcal{A})$, while other coefficients elements are set to zeros, i.e., $F_{m'}^{(B')} = 0, m' \neq m$,

$$\left(s_m^-, s_m^+\right) \equiv F_m^{(B')} \in \left(s_m^-, s_m^+\right) \in \Omega_{\mathcal{A}}. \tag{6}$$

5) PROBABILITY OF THE NOISY FACE B ASSIGNED TO $\mathcal{A}$

The probability that a noisy facial image from its original facial image $B(\mathcal{B})$ is mistakenly assigned to $\mathcal{A}$ is

given by,

$$P_B \equiv Pr\left(\overline{F}_M^{(B')} : B' \in \mathcal{A} \middle| \overline{b}_M\right) = Pr\left(\mathcal{M}\left\{\overline{F}_M^{(B')}\right\} \in \Omega_{\mathcal{A}}\right)$$
$$= \int_{\mathcal{M}\left\{\overline{F}_M^{(B')}\right\} \in \Omega_{\mathcal{A}}} \cdots \int f_{\overline{b}_M}\left(F_1^{(B')}, \cdots, F_M^{(B')}\right) d\overline{F}_M^{(B')},$$

where $f_{\overline{b}_M}$ is the joint Laplace PDF of $\overline{F}_M^{(B')}$ with the noise scale parameter vector of $\overline{b}_M$,

$$f_{\overline{b}_M}\left(F_1^{(B')}, \cdots, F_M^{(B')}\right) = Lap\left(\overline{F}_M^{(B')} \middle| \overline{b}_M\right) = \prod_{m=1}^{M} Lap\left(F_m^{(B')} \middle| b_m\right),$$

where independence has been assumed for $\overline{F}_M$.

Now look at the lower and upper bounds of the probability according to **Lemma 1**. First, the upper bound is given by,

$$P_B^+ \equiv \max\left\{Pr\left(\mathcal{M}\left\{\overline{F}_M^{(B')}\right\} \in \Omega_{\mathcal{A}}\right)\right\}$$
$$= \min_m \int_{F_m \in \Omega_{\mathcal{A}}} \cdots \int Lap\left(F_m^{(B')} - F_m^{(B)} \middle| \overline{b}_m\right) dF_m^{(B')},$$
$$= \min_m \left\{CDF\left(s_m^+ - F_m^{(B)}\right) - CDF\left(s_m^- - F_m^{(B)}\right)\right\}, \quad (7)$$

where CDF is the cumulative distribution function of the Laplace distribution; and s_m^- and s_m^+ are the left and right probability boundary edges of coding coefficients element m in $\Omega_{\mathcal{A}}$ given in **Definition 6**.

Similary, according to according to **Lemma 1**, the probability lower bound is given by,

$$P_B^- \equiv \min\left\{Pr\left(\mathcal{M}\left\{\overline{F}_M^{(B')}\right\} \in \Omega_{\mathcal{A}}\right)\right\}$$
$$= \max_{\Omega_{\mathcal{A},m}}\left\{\prod_{m=1}^{M} Pr\left(F_m^{(B')} \in \Omega_{\mathcal{A},m}\right)\right\}, \quad (8)$$

where the private probability domain $\Omega_{\mathcal{A},m}$ is obtained as follows,

Definition 7 (The Private probability Domain): The private probability domain is defined as the maximum linear scaling of space bounded by the probability boundary edges such that the noisy image B' is assigned the $\mathcal{A}$,

$$\Omega_{\mathcal{A},m} = \alpha\left(s_m^-, s_m^+\right) : \alpha = \underset{\alpha}{argmax}\left\{B' \to \mathcal{A}\right\},$$

for all coding coefficients elements $m = 1, \cdots M$ and α is the linear scaling parameter.

Now the probability lower bound in Eq. (8) reduces to

$$P_B^- = \prod_{m=1}^{M}\left\{CDF\left(\alpha s_m^+ - F_m^{(B)}\right) - CDF\left(\alpha s_m^- - F_m^{(B)}\right)\right\}. \quad (9)$$

6) PROBABILITY OF THE NOISY FACE A ASSIGNED TO $\mathcal{A}$

Similarly, the probability that a noisy image A' from $A \in \mathcal{A}$ is still assigned correctly to $\mathcal{A}$ are bounded as follows

$$P_A \equiv Pr\left(\mathcal{M}\left\{\overline{F}_M^{(A')}\right\} \in \Omega_{\mathcal{A}}\right)$$
$$P_A^+ \equiv \max\left\{Pr\left(\mathcal{M}\left\{\overline{F}_M^{(A')}\right\} \in \Omega_{\mathcal{A}}\right)\right\}$$
$$= \min_m\left\{CDF\left(s_m^+\right) - CDF\left(s_m^-\right)\right\},$$
$$P_A^- \equiv \min\left\{Pr\left(\mathcal{M}\left\{\overline{F}_M^{(A')}\right\} \in \Omega_{\mathcal{A}}\right)\right\}$$
$$= \prod_{m=1}^{M}\left\{CDF\left(\alpha s_m^+\right) - CDF\left(\alpha s_m^-\right)\right\}. \quad (10)$$

7) PRIVACY BUDGET BOUNDS

With the above probability bounds, the privacy budget bounds can be obtained.

Lemma 2: The privacy budget has the lower bound and upper bound of

$$\varepsilon^-\left(\overline{b}_M\right) \le \varepsilon\left(\overline{b}_M\right) \le \varepsilon^+\left(\overline{b}_M\right),$$

where ε^- and ε^+ are the lower bound and upper bound given below.

Proof: The privacy budget ε is obtained from **Definition 3**,

$$\varepsilon\left(\overline{b}_M\right) = -\ln\left(\max_{(A,B)}\left\{\frac{P_B}{P_A}\right\}\right).$$

From Eq. (7) and Eq. (10), the privacy budget lower bound is

$$\varepsilon^- = \max_{(A,B)}\left\{\ln\left(\frac{P_A^-}{P_B^+}\right)\right\} = \max_{(A,B)}\left\{\ln\left(\frac{P_A^-}{\min\left\{P_B^{+o}, P_B^{+i}\right\}}\right)\right\},$$

where

$$P_A^- = \prod_m\left\{1 - \frac{\exp\left(-\frac{\alpha s_m^+}{b_m}\right) + \exp\left(\frac{\alpha s_m^-}{b_m}\right)}{2}\right\},$$
$$P_B^{+o} = \min_{F_m^B \notin (s_m^-, s_m^+)}\left\{\frac{\left|\exp\left(-\frac{S_m^+}{b_m}\right) - \exp\left(-\frac{S_m^-}{b_m}\right)\right|}{2}\right\},$$
$$P_B^{+i} = 1 - \max_{F_m^B \in (s_m^-, s_m^+)}\left\{\frac{\exp\left(-\frac{S_m^+}{b_m}\right) + \exp\left(-\frac{S_m^-}{b_m}\right)}{2}\right\},$$

and S_m^- and S_m^+ are the distances from the left and right probability boundary edges given below,

$$S_m^- = \left|F_m^B - s_m^-\right|; \quad S_m^+ = \left|F_m^B - s_m^+\right|.$$

Similarly, from Eq. (9) and Eq. (10), the upper bound of the privacy budget is given by,

$$\varepsilon^+ = \max_{(A,B)}\left\{\ln\left(\frac{P_A^+}{P_B^{-i} P_B^{-o}}\right)\right\},$$

where

$$P_A^+ = \min_m \left\{ 1 - \frac{\exp\left(-\frac{S_m^+}{b_m}\right) + \exp\left(-\frac{S_m^-}{b_m}\right)}{2} \right\},$$

$$P_B^{-o} = \prod_{F_m^B \notin (s_m^-, s_m^+)} \left\{ \frac{\left| \exp\left(-\frac{\tilde{S}_m^+}{b_m}\right) - \exp\left(-\frac{\tilde{S}_m^-}{b_m}\right) \right|}{2} \right\},$$

$$P_B^{-i} = \prod_{F_m^B \in (s_m^-, s_m^+)} \left\{ 1 - \frac{\exp\left(-\frac{\tilde{S}_m^+}{b_m}\right) + \exp\left(-\frac{\tilde{S}_m^-}{b_m}\right)}{2} \right\}, \quad (11)$$

where $\tilde{S}_m^+$ and $\tilde{S}_m^-$ are defined as follows,

$$\tilde{S}_m^+ = \left| F_m^B - \alpha s_m^+ \right|, \quad \tilde{S}_m^- = \left| F_m^B - \alpha s_m^- \right|.$$

After some mathematics calculation, the upper bound of the privacy budget can be expressed as follows,

$$\varepsilon^+ = \delta + \sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m}{b_m},$$

with

$$\delta = \max_{(A,B)} \left\{ \ln\left(\frac{P_A^+}{\prod P_B^{-i} \prod \tilde{P}_B^{-o}} \right) \right\}$$

$$\tilde{P}_B^{-o} = \prod_{F_m^B \notin (s_m^-, s_m^+)} \left\{ \frac{\left| 1 - \exp\left(-\frac{\left| \tilde{S}_m^+ - \tilde{S}_m^- \right|}{b_m} \right) \right|}{2} \right\},$$

where the partial sensitivity S_m is defined as follows,

Definition 8 (Partial Sensitivity): The partial sensitivity is defined as closest distance from the coding coefficients elements to their probability boundary edges,

$$S_m = \min\left\{ \tilde{S}_m^-, \tilde{S}_m^+ \right\}. \quad (12)$$

□

Now, it is ready to show that the FaceIDP noise mechanism satisfies the ε-differentially private guarantee,

Theorem 1: The noise mechanism of the FaceIDP satisfies ε-differential privacy,

$$\exp(-\varepsilon) \le \frac{Pr\left(\overline{F}_M^{(B')} : B \in \mathcal{A}\right)}{Pr\left(\overline{F}_M^{(A')} : A \in \mathcal{A}\right)} \le \exp(\varepsilon),$$

with

$$\varepsilon = \delta + \sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m}{b_m}.$$

Proof: From **Lemma 2**, the privacy budget satisfies

$$\varepsilon\left(\overline{b}_M\right) \le \delta + \sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m}{b_m},$$

from which **Theorem 1** is proved. □

IV. THE FACEIDP OPTIMIZATION

In this Section, the optimal noise distribution over elements of the facial imaging coding coefficients vector is obtained for a given global privacy budget ε and the FaceIDP algorithm is presented.

A. OPTIMAL NOISE DISTRIBUTION FOR BETTER UTILITY

For joint Laplace distribution of $\overline{F}_M$, the data utility $\mathcal{U}$ in **Definition 5** is reduced to the following,

$$\mathcal{U} = \sum_{m=1}^{M} 2 W_m b_m^2, \quad (13)$$

where the Laplace distribution variance $\sigma_m^2 = 2\, b_m^2$ has been used.

The data utility in **Definition 5** and the privacy budget in **Definition 3** are a balanced pair: if the data utility is high ($\mathcal{U}$ is low), the privacy is low (ε is high) and vice versa. Also they are both functions of the noise scale parameter of $\overline{n}_M$, denoted as $\overline{b}_M$. So it is desire to optimize the data utility $\mathcal{U}$ for the given privacy budget $\varepsilon = \varepsilon_0$, which is the constrained optimization problem,

Lemma 3: The constrained optimization of the data utility $\mathcal{U}$ for a given privacy budget ε can be done through the Lagrange Multiplier (LM) method,

$$\frac{\partial}{\partial \overline{b}_M} \mathcal{L}(\overline{b}_M) = 0; \quad \varepsilon(\overline{b}_M) = \varepsilon_0,$$
$$\mathcal{L}(\overline{b}_M) = \mathcal{U}(\overline{b}_M) + \lambda \left[\varepsilon(\overline{b}_M) - \varepsilon_0 \right],$$

Proof: The constrained optimization problem is given as follows,

$$\min\left\{ \mathcal{U}(\overline{b}) \right\}, \quad s.t. \ \ \varepsilon(\overline{b}) = \varepsilon_0,$$

whose solution is obtained when **Lemma 3** is satisfied. □

From **Lemma 3**, the data utility $\mathcal{U}$ can be optimized to obtain the optimal noise scale parameter $\overline{b}_M$, for a given privacy budget ε,

$$\min_{\overline{b}_M} \left\{ \mathcal{U} = \sum_{m=1}^{M} 2 W_m b_m^2 \,\middle|\, \varepsilon(\overline{b}_M) = \varepsilon_0 \right\}. \quad (14)$$

With the probabilities given in Eq. (11), the LM optimization problem in Eq. (14) can be solved numerically. Under the approximation that P_A^+, P_B^{-i} and P_B^{-i} are constants, the privacy budget factor δ is also a constant and an effective privacy given budget ε_0' can be defined according to **Theorem 1**

$$\varepsilon_0' = \varepsilon_0 - \delta = \sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m}{b_m},$$

and the LM optimization problem in Eq. (14) reduces to the following,

$$\frac{\partial}{\partial \overline{b}_M} \mathcal{L}(\overline{b}_M) = 0\,; \quad \sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m}{b_m} = \varepsilon_0' = \varepsilon_0 - \delta,$$

$$\mathcal{L}(\overline{b}_M) = \sum_{F_m^B \notin (s_m^-, s_m^+)} 2W_m b_m^2 + \lambda \left[\sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m}{b_m} - \varepsilon_0' \right]. \tag{15}$$

Theorem 2 (Optimal Noise Scale Parameters): The optimal noise scale parameters vector b_m^* is given by,

$$b_m^* = \frac{S_m}{\varepsilon_m'},$$

with

$$\varepsilon_m' = p_m \varepsilon_0' \; p_m = \frac{W_m^{1/3} S_m^{2/3}}{\sum_{F_m^B \notin (s_m^-, s_m^+)} W_m^{1/3} S_m^{2/3}}.$$

Proof: From Eq. (15),

$$\frac{\partial}{\partial \overline{b}_M} \mathcal{L}(\overline{b}_M) = 0 \rightarrow b_m = \left(\frac{\lambda S_m}{4W_m} \right)^{1/3}, \tag{16}$$

from which the constraint of the privacy budget is given by,

$$\sum_{F_m^B \notin (s_m^-, s_m^+)} \frac{S_m^{2/3} (4W_m)^{1/3}}{(\lambda)^{1/3}} = \varepsilon_0', \tag{17}$$

and

$$\lambda = \left(\frac{\sum_{F_m^B \notin (s_m^-, s_m^+)} S_m^{2/3} (4W_m)^{1/3}}{\varepsilon_0'} \right)^3. \tag{18}$$

Substituting Eq. (18) into Eq. (16), the noise scale parameters are obtained and **Theorem 2** is proved. □

B. FaceIDP ALGORITHM

In this section, we give the algorithm for the FaceIDP approach.And the whole work pipeline of our proposed approach is clearly stated in Algorithm 1.

Algorithm 1 FaceIDP

Input: Face images $\mathbb{P}$ and privacy budget ε.
Output: Sanitized facial images $\mathbb{P}'$ satisfying DP.

$\mathbb{P}' = \varnothing$
Learn the sparse dictionary basis $\mathbb{D}$ of the facial images data set through the DLNet.
for each facial image $\overline{P}_N \in \mathbb{P}$ **do**
  Decompose the facial image $\overline{P}_N$ into the product of the selected dictionary basis $\overline{\overline{D}}_{N\times M}$ and coding coefficients vector $\overline{F}_M$.
  Compute the weight vector $\overline{W}_M$ according to Eq. (3).
  Calculate the sensitivity vector $\overline{S}_M$ according to Eq. (12).
  Compute the optimal noise scale parameters $\overline{b}_M$ according to **Theorem 2**.
  Obtain the coding coefficients noise through the joint Laplace distribution: $\overline{\delta}_M = \prod_{m=1}^{M} Lap(F_m|b_m)$.
  Obtain the sanitized noisy image $\overline{P}_N'$ according to Eq. (1).
  Update the sanitized image dataset: $\mathbb{P}' = \mathbb{P}' \cup \overline{P}_N'$.
return $\mathbb{P}'$.

V. EXPERIMENTAL RESULTS

During the FaceIDP experiment, the pre-trained model of Dlib, a ResNet based neural network, is used in Python 3.7 to perform the face identification. The neural network has been trained and tested with two databases: 1) LFW database [19] and 2) PubFig database [20]. On one hand, LFW is a database of face photographs designed for studying the problem of unconstrained face identification. On the other hand, unlike most other existing face databases, these images of the PubFig database are taken in completely uncontrolled situations with non-cooperative subjects.

The face identification consists of 4 common stages: face detection, face eqnarray, face encoding representation and face verification. The face encoding feature vector $\overline{V}_L$ has a dimension of $L = 128$ and the Euclidean distance is used to recognize the faces with a threshold of 0.6.

To show the efficiency of our optimal FaceIDP approach, we compared it to the standard-DP approach and the partial-DP approach where sanitizing noise is added to partial coding coefficients that lie outside of the Probability Boundary Edges according to **Definition 6**: $F_m^B \notin (s_m^-, s_m^+)$, *i.e.*, sanitizing noise is added to coding coefficients that have the most significant effect on the face encoding feature vectors, as shown in **Theorem 1**.

A. THE DLNet

First, the common bases of the facial images $\overline{\overline{D}}_{N\times M}$ are learned through the DLNet in **Section III-D4**. 1000 facial images of the LFW database are used to train the DLNet to obtain 100 face dictionary bases. During the training, the learning rate of the SGD η and the ISTA thresholding value λ are set as follows,

$$\eta = 0.01; \;\; \lambda = 0.01 \max \left\{ \overline{\overline{F}}_{M_k}^{(k)} \right\}, \;\; k = 1, 2, \cdots, K.$$

B. THE SANITIZED FACE IMAGES

Then, we obtained the closest neighboring facial image pair according to **Definition 2**, *i.e.*, the minimum Euclidean distance difference. For the LFW database, the obtained closest neighboring facial images are shown in the 1st column of Fig. 4, which are labeled as Face *A* and Face *B*. Next, the sanitizing noise for a given data utility $\mathcal{U} = 13$ in Eq. (13) is added to the closest neighboring facial images with the 3 DP approaches, *i.e.*, the Standard-DP sanitized facial images in the 2nd column; the Partial-DP sanitized facial images in the 3rd column; and the optimal FaceIDP sanitized facial images in the 4th column. To show the difference clearly, Fig. 5 zooms in the left eye of Face *A* and mouth of Face *B*,

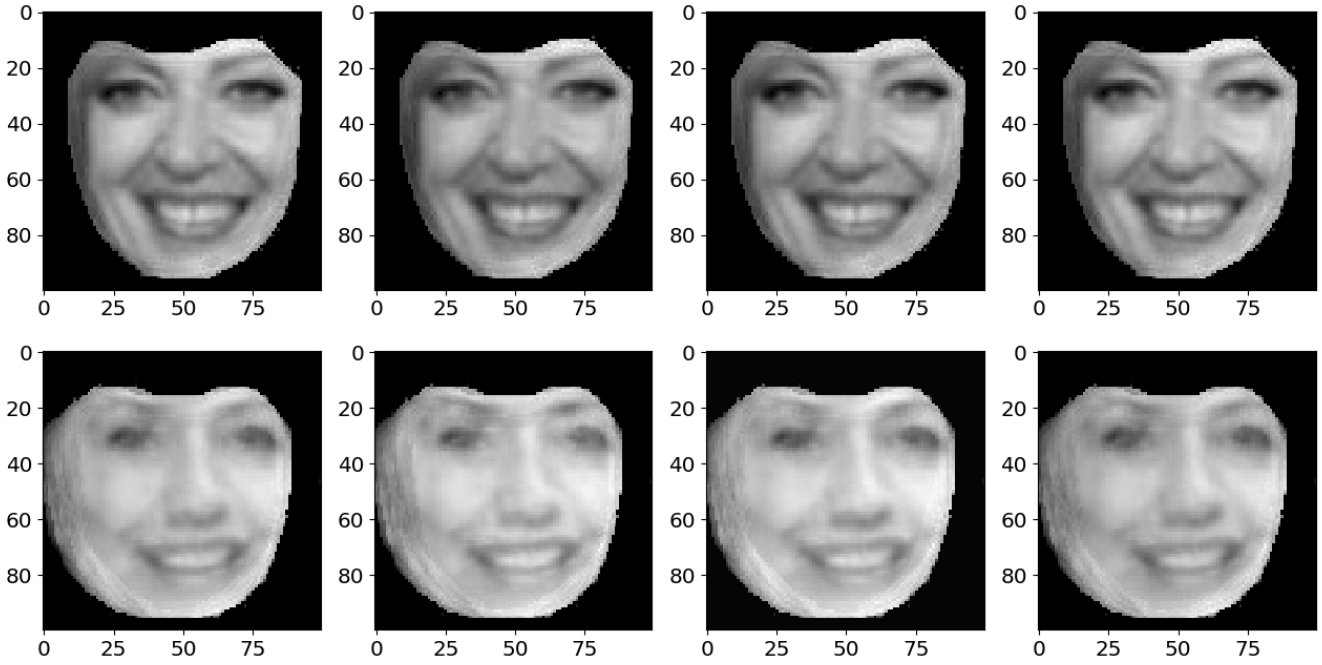


FIGURE 4. The closest neighboring face pair for a given data utility $\mathcal{U} = 13$ (LFW Database).

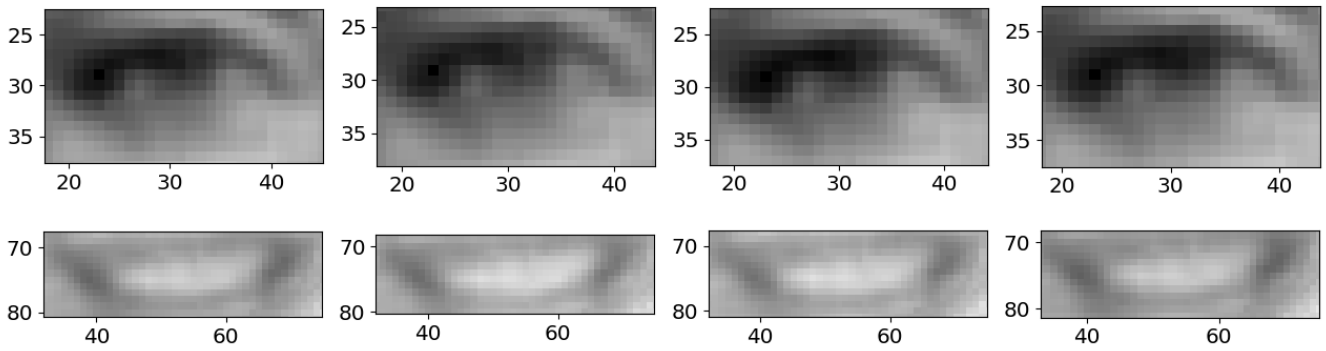


FIGURE 5. The zoom-in view of the left eye and mouth of the closest neighboring Face *A* and Face *B* of Fig. 4, for a given data utility $\mathcal{U} = 13$ (LFW Database).

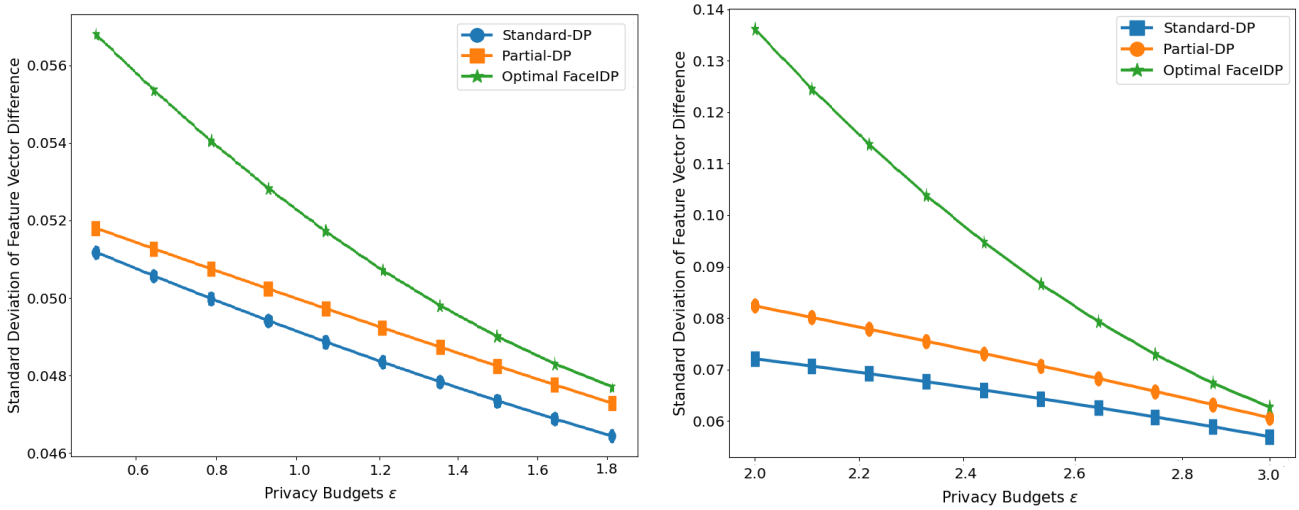
from which we can see that the optimal FaceIDP approach obtain the most significant difference from the original facial images, providing better protection for the face identification privacy or smaller privacy budget ε, for a given data utility $\mathcal{U}$. Similar results are obtained for the PubFig database, which are not shown here.

C. THE SANITIZED FEATURE VECTORS

After that, to show the quantified results of the privacy protection, the standard deviation of the sanitized feature vectors difference from its original value: the larger the standard deviation, the better the privacy protection. Fig. 6 shows results for both the LFW database (left) and the PubFig database (right) for 3 approaches, from which one can see better face identification privacy protection has been achieved for the optimal FaceIDP approach.

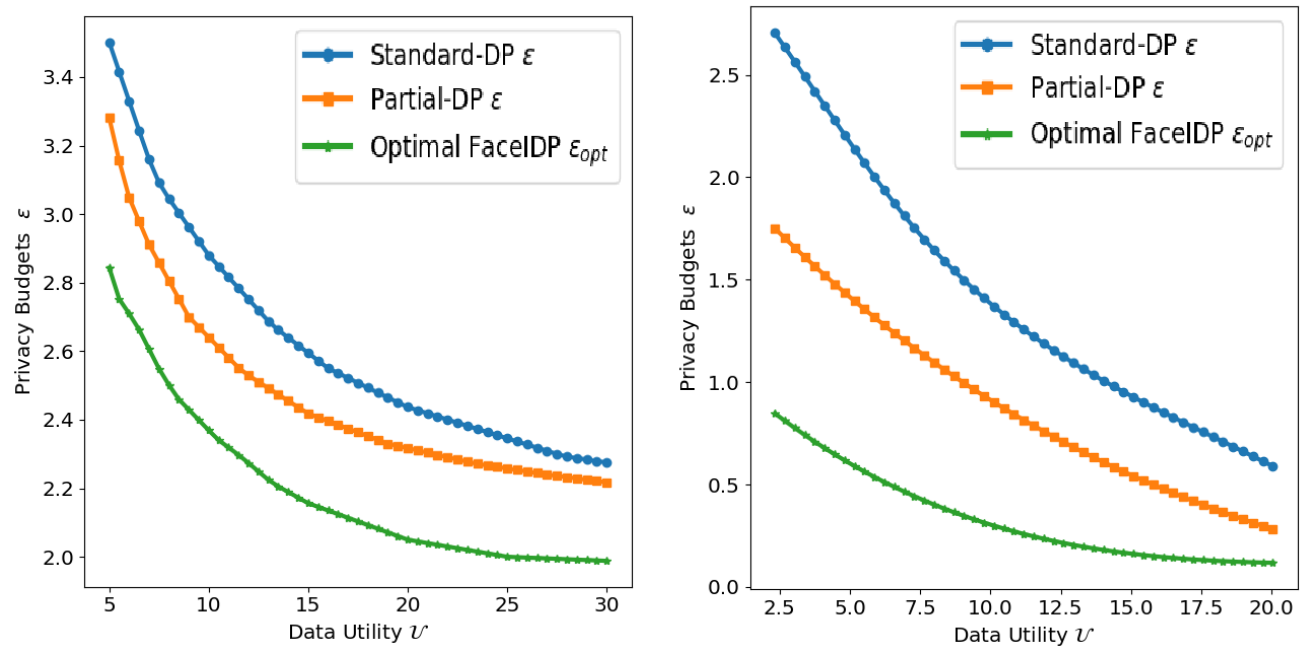
D. THE PRIVACY BUDGET AND DATA UTILITY

To show the performance of the optimal FaceIDP, the privacy budgets ε for different data utilities have been obtained. For the LFW database, ε is calculated for $\mathcal{U} = [5, 30]$ and the result is shown on the left plot of Fig. 7, from which it can be seen that the face identification privacy protection of the FaceIDP approach is the best among all approaches, *i.e.*, it has the smallest privacy budget ε (green stars). Also, the Partial-DP approach is better than the Standard-DP approach, which is because that only the most significant coding coefficients are used in the Partial-DP approach to achieve better privacy protection with smaller data utility $\mathcal{U}$. Also, on the right plot



(a) LFW Database (b) PubFig Database

FIGURE 6. Standard deviation of feature vector difference vs. privacy budget ε.



(a) LFW Database (b) PubFig Database

FIGURE 7. Privacy budget ε vs. data utility $\mathcal{U}$.

of Fig. 7, the data utility $\mathcal{U}$ is plotted against the privacy budget ε, which again shows that the optimal FaceIDP has the smallest data utility (the best data utility) for a given privacy budget $\varepsilon = (2.2, 2.9)$. Also, the Partial-DP approach shows better performance than the Standard-DP approach, *i.e.*, for a given privacy budget ε, the data utility $\mathcal{U}$ is smaller (better). Similarly, for the PubFig database, the left and right plots of Fig. 7 show the privacy budget ε for different data utility $\mathcal{U}$ and vice versa respectively, from which again it can be seen that the optimal FaceIDP outperforms the other 2 approaches.

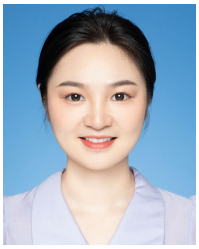
VI. CONCLUSION

In this paper, the differential privacy problem of face identification, *i.e.*, the FaceIDP, has been studied. First, the DLNet is built to learn the dictionary basis of the facial images. After that, the sanitizing noise is added to the coding coefficients of the facial images. Then the FaceIDP is proved to be

ε-differentially private and the lower and upper bounds of the privacy budget are obtained. What's more important, the formulas of the optimal noise parameters to achieve better data utility have been derived. Also, experiment has been carried out with 2 facial images database, *i.e.*, the LFW and the PubFig databases, to confirm the efficiency of the FaceIDP to protect the face identification privacy while still achieving good data utility. Although only 2D face identification privacy problem is studied in this paper, the FaceIDP approach can be readily extended to the 3D face identification privacy problem. At last, the FaceIDP can be deployed in many scenarios, including facial images transfer between the cloud server and the smartphones, point-to-point facial images transmission, as well as face-to-face real-time video chat.

REFERENCES

[1] Z. Ma, Y. Liu, X. Liu, J. Ma, and K. Ren, "Lightweight privacy-preserving ensemble classification for face recognition," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5778–5790, Jun. 2019.
[2] L. Ou, S. Liao, Z. Qin, and H. Yin, "Millimeter wave wireless Hadamard image transmission for MIMO enabled 5G and beyond," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 134–139, Dec. 2020.
[3] H. Wang, S. Xie, and Y. Hong, "Videodp: A flexible platform for video analytics with differential privacy," in *Proc. Privacy Enhancing Technol.*, vol. 4, Jul. 2020, pp. 277–297.
[4] V. Mirjalili, S. Raschka, and A. Ross, "PrivacyNet: Semi-adversarial networks for multi-attribute face privacy," *IEEE Trans. Image Process.*, vol. 29, pp. 9400–9412, 2020.
[5] S. Shan, E. Wenger, J. Zhang, H. Li, H. Zheng, and B. Y. Zhao, "Fawkes: Protecting privacy against unauthorized deep learning models," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1589–1604.
[6] K. Hill and A. Krolik, "How photos of your kids are powering surveillance technology," The New York Times, Oct. 2019.
[7] A. Tonge and C. Caragea, "Image privacy prediction using deep neural networks," *ACM Trans. Web*, vol. 14, no. 2, pp. 1–32, Apr. 2020.
[8] EU Commission. (2018). *2018 Reform of EU Data Protection Rules*. [Online]. Available: https://www.eeas.europa.eu/node/44451_en
[9] S. Hill, Z. Zhou, L. Saul, and H. Shacham, "On the (In) effectiveness of mosaicing and blurring as tools for document redaction," in *Proc. Privacy Enhancing Technol.*, 2016, pp. 403–417.
[10] R. McPherson, R. Shokri, and V. Shmatikov, "Defeating image obfuscation with deep learning," 2016, *arXiv:1609.00408*.
[11] M. R. Ra, R. Govindan, and A. Ortega, "P3: Toward privacy-preserving photo sharing," in *Proc. 10th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2013, pp. 515–528.
[12] L. Fan, "Image pixelization with differential privacy," in *Data and Applications Security and Privacy XXXII*. Cham, Switzerland: Springer, 2018, pp. 148–162.
[13] C. Tong, M. Zhang, C. Lang, and Z. Zheng, "An image privacy protection algorithm based on adversarial perturbation generative networks," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 17, no. 2, pp. 1–14, May 2021.
[14] J. Yang, J. Liu, and J. Wu, "Facial image privacy protection based on principal components of adversarial segmented image blocks," *IEEE Access*, vol. 8, pp. 103385–103394, 2020.
[15] C. Jiang, Q. Zhang, R. Fan, and Z. Hu, "Super-resolution CT image reconstruction based on dictionary learning and sparse representation," *Sci. Rep.*, vol. 8, no. 1, p. 8799, Jun. 2018.
[16] S. Tariyal, A. Majumdar, R. Singh, and M. Vatsa, "Deep dictionary learning," *IEEE Access*, vol. 4, pp. 10096–10109, 2016.
[17] S. Liao and L. Ou, "High-speed millimeter-wave 5G/6G image transmission via artificial intelligence," in *Proc. IEEE Asia–Pacific Microw. Conf. (APMC)*, Dec. 2020, pp. 655–657.
[18] Y. Qiu, C. Zhang, R. Huang, H. Tian, C. Xiong, and S. Liao, "DL-CSNet: Dictionary learning based compressed sensing neural network," in *Proc. J. Phys., Conf.*, vol. 2245, 2022, Art. no. 012015.
[19] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Univ. Massachusetts, Amherst, MA, USA, Tech. Rep. 07-49, Oct. 2007.
[20] N. Kumar, A. C. Berg, P. N. Belhumeur, and S. K. Nayar, "Attribute and simile classifiers for face verification," in *Proc. IEEE 12th Int. Conf. Comput. Vis.*, Sep. 2009, pp. 365–372.
[21] L. Ou, Z. Qin, S. Liao, T. Li, and D. Zhang, "Singular spectrum analysis for local differential privacy of classifications in the smart grid," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5246–5255, Jun. 2020.
[22] L. Ou, Z. Qin, S. Liao, Y. Hong, and X. Jia, "Releasing correlated trajectories: Towards high utility and optimal differential privacy," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 1109–1123, Sep. 2020.
[23] L. Ou, Z. Qin, S. Liao, H. Yin, and X. Jia, "An optimal pufferfish privacy mechanism for temporally correlated trajectories," *IEEE Access*, vol. 6, pp. 37150–37165, 2018.

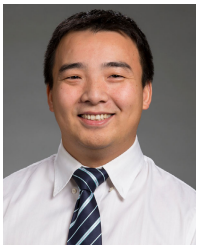


LU OU (Member, IEEE) received the Ph.D. degree in software engineering from Hunan University, Changsha, China, in 2018. From 2015 to 2016, she was a Visiting Student with the Department of Computer Science, The University of Texas at Arlington, Arlington, TX, USA. She was a Postdoctoral Fellow with the College of Computer Science and Electronic Engineering, Hunan University. She is currently an Associate Professor with the School of Journalism and Communication, Hunan University. Her research interests include data security, privacy and big data, as well as signal, image, and video analysis.

YI HE received the bachelor's degree in radio and television from the Nanjing University of Aeronautics and Astronautics, in 2021. She is currently pursuing the master's degree with the School of Journalism and Communication, Hunan University. Her research interests include short video communication, data security and privacy, and social media science.

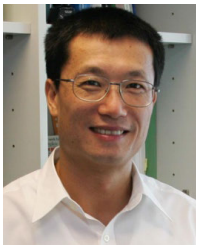
SHAOLIN LIAO (Senior Member, IEEE) received the B.S. degree in material science and engineering from Tsinghua University, Beijing, China, in 2000, and the Ph.D. degree in electrical engineering from the University of Wisconsin–Madison, USA, in 2008. He is currently a Professor with the School of Electronics and Information Technology, Sun Yat-sen University (SYSU), Guangzhou, Guangdong, China, and an Adjunct Faculty with the Department of Electrical and Computer Engineering, Illinois Institute of Technology (IIT), Chicago, IL, USA. Before joining SYSU, he was with the Argonne National Laboratory. He was also a Postdoctoral Fellow with the Department of Physics, The City University of New York (CUNY), from 2008 to 2010. His research interests include artificial intelligence (AI) techniques for big data analysis, algorithms for signal processing, and efficient methods for multiphysics simulation, including computational electromagnetics (CEM). He was an Associate Editor of IEEE Access.

ZHENG QIN (Member, IEEE) received the Ph.D. degree in computer software and theory from Chongqing University, China, in 2001. From 2010 to 2011, he was a Visiting Scholar with the Department of Computer Science, Michigan University. He is currently a Professor with the College of Computer Science and Electronic Engineering, Hunan University, where he serves as the Vice Dean. He is also the Director of the Hunan Key Laboratory of Big Data Research and Application and the Vice Director of the Hunan Engineering Laboratory of Authentication and Data Security. His research interests include network and data security, privacy, data analytics and applications, machine learning, and applied cryptography. He is a member of the China Computer Federation (CCF).



YUAN HONG (Senior Member, IEEE) received the Ph.D. degree in information technology from Rutgers, The State University of New Jersey. He is currently an Associate Professor with the Computer Science and Engineering Department, University of Connecticut. His research was supported by the National Science Foundation. His research interests include the intersection of privacy, security, optimization, and data mining.

DAFANG ZHANG received the Ph.D. degree in application mathematics from Hunan University, Changsha, China, in 1997. He is currently a Professor with the College of Computer Science and Electronic Engineering, Hunan University. His current research interests include dependable systems/networks, network security, big data, and privacy.



XIAOHUA JIA (Fellow, IEEE) received the B.Sc. and M.Eng. degrees from the University of Science and Technology of China, in 1984 and 1987, respectively, and the D.Sc. degree in information science from The University of Tokyo, in 1991. He is currently a Chair Professor with the Department of Computer Science, City University of Hong Kong. His research interests include cloud computing and distributed systems, data security and privacy, computer networks, and mobile computing. He was the General Chair of ACM MobiHoc, in 2008, the TPC Co-Chair of IEEE GlobeCom—Ad Hoc and Sensor Networking Symposium, in 2010, and the Area-Chair of IEEE INFOCOM, in 2010 and from 2015 to 2017. He was an Editor of IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, from 2006 to 2009, *Wireless Networks*, *World Wide Web Journal*, and *Journal of Combinatorial Optimization*.