IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 38, No. 6, December, 2021, pp. 1677-1687
Journal homepage: http://iieta.org/journals/ts

Non-Global Privacy Protection Facing Sensitive Areas in Face Images

Chao Liu[1,2], Jing Yang[1*], Yining Zhang[3], Xuan Zhang[4], Weinan Zhao[2], Fengjuan Miao[2], Yukun Shao[2]

[1] College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
[2] College of Communication and Electronic Engineering, Qiaihar University, Qiqihar 161000, China
[3] Department of Computer Engineering, DaQing Vocational College, Daqing 163000, China
[4] Information Center, First Affiliated Hospital of Qiqihar Medical College, Qiqihar 161000, China

Corresponding Author Email: yangjing@hrbeu.edu.cn

https://doi.org/10.18280/ts.380611

Received: 8 July 2021
Accepted: 2 November 2021

Keywords:
differential privacy, interactive framework, non-globality, landmark positioning, regional growth

ABSTRACT

Face images, as an information carrier, are naturally weak in privacy. If they are collected and analyzed by malicious third parties, personal privacy will leak, and many other unmeasurable losses will occur. Differential privacy protection of face images is mainly being studied under non-interactive frameworks. However, the ε-effect impacts the entire image under these frameworks. Besides, the noise influence is uniform across the protected image, during the realization of the Laplace mechanism. The differential privacy of face images under interactive mechanisms can protect the privacy of different areas to different degrees, but the total error is still constrained by the image size. To solve the problem, this paper proposes a non-global privacy protection method for sensitive areas in face images, known as differential privacy of landmark positioning (DPLP). The proposed algorithm is realized as follows: Firstly, the active shape model (ASM) algorithm was adopted to position the area of each face landmark. If the landmark overlaps a subgraph of the original image, then the subgraph would be taken as a sensitive area. Then, the sensitive area was treated as the seed for regional growth, following the fusion similarity measurement mechanism (FSMM). In our method, the privacy budget is only allocated to the seed; whether any other insensitive area would be protected depends on whether the area exists in a growing region. In addition, when a subgraph meets the criterion for merging with multiple seeds, the most reasonable seed to be merged would be selected by the exponential mechanism. Experimental results show that the DPLP algorithm satisfies ε-differential privacy, its total error does not change with image size, and the noisy image remains highly available.

1. INTRODUCTION

The rapid advancement of information technology makes it easier to acquire and share face images. People can easily obtain others' photos via online social networks, mobile payment, surveillance systems, and other channels. These digital images are rich in sensitive personal information. If they are collected and analyzed by malicious third parties, personal privacy will leak, and many other unmeasurable losses will occur [1]. Relevant stakeholders have expressed their concerns over the possible leak of personal privacy during the use of face images: a person may be kept in the dark about the public recognition and tracking of him/her, and about the collection, use, and sharing his/her personal data. To make matters worse, face image databases could be sold or shared by many parties to unknown buyers or sharers.

The image data query under privacy protection provides a solution to the above-mentioned privacy problems. For example, Fung et al. [2] and Xiao and Tao [3] created the k-same method, using the anonymization mechanism. However, there is a major weakness of the conventional anonymization mechanism: Prior to processing the data, it is necessary to set many prior conditions about the background knowledge and attack models of the attacker, many of which does not hold in the real world. For instance, Li et al. [4] restricted user access to images on social networks through access control. Instead of protecting image privacy, their strategy protects images from the angle of access setting. Terrovitis et al. [5] implemented same-state encryption of gray images. But data encryption still needs to make assumptions of the attacks. Focusing on anonymous images uploaded to Facebook, Sweeney [6] found that attackers can derive the social security number (SSN) of those in the anonymous images from Friendster, an extra feature of this social network.

Differential privacy [7], proposed by Dwork in 2006, adds noise to the output to disturb sensitive data. Under differential privacy, the effect of a single record can be concealed. Whether he record is in the dataset or not, the same result will always be outputted by the same probability, which prevents the attacker from further reasoning. Dwork further studied differential privacy in a series of papers [8-12], and disclosed the realization mechanism of differential privacy [13, 14]. McSherry noted that sequence combination and concurrent combination must be satisfied by the differential privacy algorithm for complex privacy problems [15].

The data protected by differential privacy can be published interactively or non-interactively, depending on the realization environment. The following are some representative interactive data publication methods: Roth and Roughgarden [16] Median algorithm, which can respond to multiple queries; Hardt and Rothblum [17] private multiplicative weights (PMW) mechanism, which increases the number of queries;

Gupta et al. [18] universal iterative dataset creation (IDC) framework; Fan and Xiong [19] filtering and adaptive sampling for releasing time series under differential privacy (FAST) algorithm; Kellaris et al. [20] flow data publication algorithm with an unlimited number of queries. Non-interactive data publication mainly uses histogram publication. The following are some representative non-interactive data publication methods: Xiao et al. [21] Privelet algorithm; Xu et al. [22] Noise First and Structure First algorithms; Li et al. [23] matrix mechanism; Li et al. [24] data- and workload-aware (DAWA) algorithm. Under the framework of differential privacy, the sensitive information in the protected images has only been researched tentatively, because the image data are highly complex. Currently, the additive noise for the differential privacy protection of images impacts the entire image. For face images, the sensitive information of the face only concentrates in the face area, and even in some specific parts of the face area. The other insensitive areas have nothing to do with privacy leak of face images.

Through the above analysis, this paper puts forward the differential privacy of landmark positioning (DPLP) algorithm, a non-global privacy protection method for sensitive areas in face images, details the realization of the algorithm, and experimentally verifies the performance of the DPLP in protecting the privacy of face images.

2. PRELIMINARIES

2.1 Differential privacy

Definition 1. Adjacent datasets of face image

For a given image X, the gray matrix X_{mn} can be obtained by normalizing the image. Then, there exists $X|X_{mn} = \begin{bmatrix} x_{11,}x_{12,} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1,}x_{m1,} & \cdots & x_{mn} \end{bmatrix}$, where x_{ij} in matrix X_{mn} represents the gray of the corresponding element. If there exists an X' with only one element difference from X, $|X - X'| = x_{ij}(1 \le i \le m, 1 \le j \le n)$, then X and X' are adjacent datasets.

Definition 2. Differential privacy

For a given random algorithm M of image data publication, with the output range of $\mathrm{Range}(M)$, the algorithm can provide ε- differential privacy, if its arbitrary outputs on two adjacent gray images X and X' satisfy:

$$\Pr[M(X) \in S] \le \exp(\varepsilon) \times \Pr[M(X') \in S] \tag{1}$$

Definition 3. Global sensitivity

Let Q be a random query function meeting $Q: D \to R^n$. Then, the global sensitivity of Q can be expressed as:

$$\Delta Q_{GS} = \max_{X,X'} ||Q(D) - Q(D')||_\rho \tag{2}$$

Theorem 1. Laplace mechanism

Let Q be a query series of the length d. The random algorithm M receives database D and outputs the following vector that satisfy ε-differential privacy:

$$M(D) = Q(D) + < \mathrm{Lap}_1\left(\frac{\Delta Q_{LS}}{\varepsilon}\right), \ldots, \mathrm{Lap}_d\left(\frac{\Delta Q_{LS}}{\varepsilon}\right) > \tag{3}$$

Theorem 2. Exponential mechanism

The exponential mechanism mainly handles the non-numeric outputs of the sampling algorithm. Under any exponential mechanism, the sampling algorithm M satisfies ε-differential privacy if it meets:

$$M(X,u) = \left\{r: \left| Pr[r \in S] \propto exp\left(\frac{\varepsilon u(X,r)}{2\Delta u_{LS}}\right)\right.\right\} \tag{4}$$

where, $u(X, r)$ is the scoring function; Δu_{LS} is the global sensitivity of the scoring function $u(X, r)$; S is the output domain of our algorithm; r is the selected output term of the output domain S. The higher the score of $u(X, r)$, the greater the probability for r being selected as the output.

Property 1. Differential privacy-serial combination property

For a given dataset X and a set of differential privacy algorithms $M_1(X), M_2(X), \ldots, M_m(X)$ related to X, if algorithm $M_i(D)$ satisfies ε_i - differential privacy, and the random processes of any two algorithms are independent of each other, then the algorithm combined from these algorithms satisfies $\sum_{i=1}^{m} \varepsilon_i$- differential privacy.

Property 2. Differential privacy-parallel combination property

Let $M_1(X_1), M_2(X_2), \ldots, M_m(X_m)$ be a series of ε - differential privacy algorithms with input datasets $X_1, X_2, \ldots, X_m$, respectively. Suppose the random processes of any two algorithms are independent of each other. Then, the algorithm combined from these algorithms satisfies ε - differential privacy.

2.2 Face landmark positioning

Face landmark positioning can automatically detect the landmarks (positions) in representative sensitive areas (eyebrows, eyes, ears, noise, mouth, and face contours) in face-containing images, using some algorithms. This technique is of great significance to research fields like face identification, expression analysis, three-dimensional (3D) face modeling, face synthesis, and face image coding. Yang and Huang [25] realized the mosaic algorithm with the aid of edge tracking. Meng et al. [26] were the first to position face landmarks through geometric projection. On this basis, Feng and Zhou developed face landmark positioning using variance projection function (VPF) [27] and integral projection function (IPF) [28], respectively. Zhang and Lenders [29] introduced binarization to position landmarks in reference to pupil positions. Considering the symmetry of face, Reisfeld et al. [30] proposed the generalized symmetric transform (GST), which takes the eyes as center points, to position face landmarks. Wu et al. [31] established multiple Snake models for different face organs, and fitted the locally converging Snake models into a complete set of face landmarks. Yuile et al. [32] replaced the traditional edge prediction algorithm with a more stable approach, namely, the peak-valley variation frequency of face image gray value, and put forward a face landmark positioning method based on deformable template (DT). Lanitis et al. [33] suggested using principal distribution model (PDM) algorithm to realize face landmark positioning. Cootes et al. [34] designed the active shape model (ASM) algorithm, a statistical point distribution model. Dollár et al. [35] positioned landmarks in images through cascaded pose regression (CPR). With the development of convolutional neural network (CNN) [36], many scholars utilized the strong feature extraction power of the CNN to pinpoint face landmarks. The representative methods include deep CNN

(DCNN) [37], tasks-constrained deep convolutional network (TCDCN) [38], multitask cascaded convolutional networks (MTCNN) [39], and tweaked CNN (TCNN) [40]. In addition, some scholars solved face landmark positioning with principal component analysis (PCA) [41], support vector machine (SVM) [42], back propagation network (BPN) [43], dynamic link architecture (DLA) [44], and Gabor wavelet network (GWN) [45]. Table 1 analyzes the performance of the above methods.

Table 1. Performance of different face landmark positioning methods

Algorithm	Image quality	Computational complexity	Accuracy
Mosaic image	Strongly high	Strongly complex	Strongly low
VPF	Strongly high	Slightly simple	Slightly low
IPF	Strongly high	Slightly simple	Slightly low
Binarization	Strongly high	Slightly simple	Slightly low
GST	Strongly high	Strongly complex	Slightly high
Snake	Strongly high	Strongly complex	Slightly high
DT	Strongly high	Slightly complex	Slightly high
ASM	Slightly high	Slightly complex	Strongly high
CPR	Slightly high	Strongly complex	Strongly high
DCNN	Strongly low	Strongly complex	Strongly high
TCDCN	Strongly low	Strongly complex	Strongly high
MTCNN	Strongly low	Strongly complex	Strongly high
TCNN	Strongly low	Strongly complex	Strongly high
PCA	Strongly low	Strongly complex	Strongly high
SVM	Strongly low	Strongly complex	Strongly high
BPN	Slightly low	Slightly complex	Strongly high
DLA	Slightly low	Slightly complex	Strongly high
GWN	Slightly low	Slightly complex	Strongly high

3. METHODOLOGY

3.1 Laplacian (LAP) algorithm

This paper proposes the LAP algorithm based on the Laplace mechanism. Without changing any of the original data, this algorithm directly disturbs the two-dimensional (2D) matrix generated from the original image with Laplace noise, and publishes the disturbed image straightforwardly. In the LAP algorithm, every pixel x_{ij} in the gray matrix $X_{m\times n}$ is considered an independent individual, laying the basis for applying the interactive mechanism to privacy protection. Provided that the pixels do not disturb each other, and the privacy budget is allocated evenly, each $x_{ij}(1\leq i\leq m,\ 1\leq j\leq n)$ consumes a privacy budget of $\varepsilon/(m\times n)$. The LAP algorithm is detailed as follows:

Different from the original image X, the privacy protected image X' contains an additive noise of $2m\times n\times(\Delta Q\times m\times n/\varepsilon)^2$. Although the LAP algorithm satisfies ε-differential privacy, a huge error will arise if the algorithm is directly applied for privacy protection of an excessively large image, making the noisy image strongly unavailable. The LAP algorithm applies to noise addition to the subgraphs of an image, but the noise level of a subgraph depends on the size of that subgraph.

Most of the existing methods face the same problem as the LAP algorithm: the algorithm feasibility is limited by image size. Besides, there are two more defects with these methods: an excessively high computing load, and the low availability of the noisy image.

Algorithm 1: LAP

Input: original image X, privacy budget ε,parameters m and n, subgraph similarity expectation Th

Output: Image X' satisfying differential privacy

Read the original image X, convert the image into gray matrix and store it in matrix $X_{m\times n}$

for i=1 to m

for i=1 to n

$X_{(i,j)}{}'=X_{(j,i)}+\mathrm{lap}(\Delta Q\times m\times n/\varepsilon)$

end for

end for

Output privacy protected image X'

3.2 ASM algorithm

The ASM model abstracts the target by a shape model. It is an algorithm based on point distribution model (PDM). In the PDM, the geometry of objects with similar shapes, such as face, hands, heart, and lungs, can be described by a shape vector, which is formed by serial connected coordinates of several landmarks. Before implementing the ASM algorithm, it is necessary to manually label the training images, obtain the shape model through training, match specific objects with landmarks. The ASM algorithm is realized in two stages: training and search.

During ASM training, the first step is to establish a shape model that matches any face shapes. The model construction requires the collection of sufficient training samples, and manual labeling of face landmarks (In this paper, 68 landmarks are labeled on each training image). After labeling, all landmarks are combined into a shape vector $g_i=\left(x_1^i,y_1^i,x_2^i,y_2^i,\dots,x_k^i,y_k^i\right)(i=1,2,\dots,n)$, where $k=68$, and $\left(x_j^i,y_j^i\right)$ is the position of landmark j on training sample i, and n depends on the number of training samples. In this way, a $2\times n$-dimensional vector a can be obtained:

$$g_i=(x_1,\dots x_n,y_1\dots y_n)^T \tag{5}$$

The high dimensionality of vector (5) is not conducive to the subsequent computing. But the different dimensions have

a strong correlation, owing to the natural similarity of face features, even if the landmarks come from different faces. However, there is no excessively large position changes between the landmarks with the same label. To solve the excessively high dimensionality, the vector is subjected to dimensionality reduction and principal component extraction by the PCA. Hence, any set of landmarks can be viewed as a point in the principal component space. The mean of the point set is the origin. Thus, any point can be described as the sum of the origin and a vector. Thus, we have:

$$g_i \approx \bar{g} + Pb \tag{6}$$

During the PCA, the mean shape vector needs to be calculated:

$$\bar{g} = \frac{1}{n}\sum_{i=1}^{n} g_i \tag{7}$$

Then, the covariance matrix can be derived:

$$S = \frac{1}{n}\sum_{i=1}^{n} (g_i - \bar{g})^T \cdot (g_i - \bar{g}) \tag{8}$$

After that, the eigenvalues of the covariance matrix S are calculated, and sorted to obtain $\tau_{1,}\tau_{2,} \ldots . \tau_{q,}$, where any $\tau_i > 0$. The P in formula (6) is a covariance matrix containing the top-t principal components. The matrix P and the corresponding eigenvalue satisfy:

$$\frac{\sum_{i=1}^{t} \tau_i}{\sum_{i=1}^{q} \tau_s} > f_v V_T \tag{9}$$

where, f_v is a proportionality coefficient depending on the number of eigenvectors (the value of f_v is usually 95%); V_T is the sum of all eigenvalues. The b in formula (6) is a t-dimensional vector controlling the variation in landmark shape:

$$b_i = P^T \cdot (g_i - \bar{g}) \tag{10}$$

when b=0, x is the origin (mean shape). To prevent the shape variation from exceeding the preset range, the b value should be limited by:

$$D_m^2 = \sum_{i=1}^{t} (\frac{{b_i}^2}{\tau_i}) \le D_{max}^2 \tag{11}$$

where, D_{max} is usually set to 3. Thus, $|b_i| < 3\sqrt{\tau_i}$.

After setting up the shape model, it is necessary to establish the local features of each landmark, such as to match the shape model with the new point set. For a given face image X, the image matching process aims to rotate, scale, and translate the shape model:

$$X = T_{X_t,Y_t,s,\theta}(\bar{g} + Pb) \tag{12}$$

where, $T_{X_t,Y_t,s,\theta}$ is the matching operation matrix:

$$T_{X_t,Y_t,s,\theta}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} X_t \\ Y_t \end{pmatrix} + \begin{pmatrix} s\cos\theta & -\ s\sin\theta \\ s\sin\theta & s\cos\theta \end{pmatrix} \tag{13}$$

To match the landmark set Y (the results after translation, scaling, and rotation) and model X, i.e., minimize the difference between model X and image landmark set Y, it is necessary to solve the minimum of the following formula:

$$|Y - T_{X_t,Y_t,s,\theta}(\bar{g} + Pb)|^2 \tag{14}$$

Note that, if the model point positions are given in X, and if the nearest adjacent point to each model point is X', then the error metric can be expressed as:

$$F(b, X_t, Y_t, s, \theta) = |X - X'|^2 \tag{15}$$

During ASM search, the mean shape needs to go through affine transformation to obtain an initial model:

$$X = M(s, \theta)[g_i] + X_c \tag{16}$$

The initial model X (16) refers to the results of the mean shape after being rotated counterclockwise by θ degrees, scaled by a ratio of s, and translated by a distance of X_c. Using the initial model, the search stage looks for the target shape in image Y, aiming to minimize the gap between the landmark position of the target shape and the actual landmark position. The final results of the search are obtained by adjusting the variation of parameter b and implementing affine transformation. The specific steps of the ASM search are explained in Algorithm 2.

Algorithm 2: ASM search

$L = \mathrm{L}_{\max}$
while (L $\geq$ 0)
  Calculate the position of the model point in the L-th layer of the image
  Search n sampling points on both sides of the model point
  Update the position and adjust the parameters to fit the model to the new point
  if (the preset number of iterations is exceeded or no closer feature point is found at the current position)
    Return to line 2
  if (L > 0) then L $\rightarrow$ (L $-$ 1)
if (convergence of layer 0 function)
  Output result

3.3 DPLP algorithm

Non-interactive data publication is the research hotspot of the data publication under differential privacy. In this form of data publication, the entire image is influenced by ε-effect. As a result, the noise level obeys uniform distribution across the image. However, the sensitive information only exists in specific areas of real-world face images. For an image, different parts require different degrees of privacy protection. Thus, it is meaningful to realize non-global privacy protection of human images, and reduce the noise impact on the protected image. This paper combines landmark positioning, regional growth, and differential privacy into a novel face image privacy protection method called DPLP. Our algorithm adopts the ASM algorithm to estimate the areas of sensitive information, and implements non-global noise disturbance to the specific areas containing sensitive face information. Under the premise of satisfying ε-differential privacy, the DPLP algorithm mitigates the influence of Laplace noise on the

privacy protected image, and balances image availability and the degree of privacy protection.

To ensure the realization of the DPLP algorithm, four key problems must be solved during the algorithm design: selecting landmark positioning algorithm, setting the rules for regional growth, allocation of privacy budget, and selecting the best target out of multiple seeds available for a subgraph.

The setting of the rules for regional growth is crucial to regional growth. Due to the limitations of the traditional regional growth rules, this paper adopts the fusion similarity measurement mechanism (FSMM) [46] as regional growth rules. The $FSMM(X,Y)$ can be calculated by:

$$FSMM(X,Y) = \frac{\varphi \times (d(X,Y)/\,\rho(X,Y) + \sigma) \times (2u_X u_Y + C_1) \times (2\sigma_X\sigma_Y + C_2)}{(u_X^2 + u_Y^2 + C_1) \times (\sigma_X^2 + \sigma_Y^2 + C_2)} \quad (17)$$

The regional growth of the DPLP algorithm needs to allocate a suitable portion of the privacy budget to each seed, using the Laplace mechanism of differential privacy. Whether an adjacent subgraph should be merged into the growing region of the current seed depends on the similarity between the subgraph and the region meets the preset threshold. In our method, the privacy budget is only allocated among the seeds. For an insensitive area, if it belongs to a growth region, it will be protected; otherwise, it will not be protected. In addition, when a subgraph can be merged with multiple seed areas, the most suitable seed area to be merged needs to be selected through the exponential mechanism. The realization of the DPLP algorithm is as follows:

Lines 1-5 convert the original image into a gray image, divide the gray image into β subgraphs of the same size, and call the ASM algorithm to position 68 landmarks and to find the seeds needed for regional growth. Line 5 adjusts the position of seed regions to ensure the growth direction. Line 6 divides the total privacy budget ε into two parts: the part ε_1 for adding Laplace noise to seed regions, and the part ε_2 for implementing the exponential mechanism. Line 7 defines the possibility of $\leq S$: a subgraph may cover multiple landmarks, because the subgraph size is too large. Lines 8-20 overcome the defect of traditional regional growth technique: the adjacent subgraph can be merged to the growth region of the current seed, as long as the subgraph satisfies the growth rules; when multiple seed areas are available for merging the subgraph, the traditional technique depends both on growth rules and the sequence of seed selection. To solve the problem, Lines 15-16 take the Euclidean distance as the scoring function between each subgraph and each seed, and choose the most suitable seed by the exponential mechanism. The nearest seed is not preferred for region fusion. Otherwise, the attacker can deduce the distribution of landmarks, a prediction result of face identification, leading to privacy leak.

Algorithm 3: DPLP

Input: original image X, privacy budget ε, preset parameters β, subgraph similarity expectation Th

Output: image X' satisfying differential privacy

Read the original image X, convert the image into gray matrix and store it in matrix $X_{m\times n}$

$X_{m\times n}$ according to preset parameters β, split into subgraph sets with the same structure $T_{(I,J)}$

Extracting facial feature point $K_S = (K_1, K_2, \ldots K_{68})$ using ASM algorithm_ S

If K_S belongs to a subgraph $T_{(i,j)}$ $(1 \leq \mathrm{i} \leq I, 1 \leq \mathrm{j} \leq J)$

Set $T_{(i,j)}$ as the backup seed, optimize the position of $T_{(i,j)}$, and add it to the $Seed_N$,

$$\varepsilon = \varepsilon_1 + \varepsilon_2$$

Find all backup $Seed_N = (Seed_1, Seed_2, \ldots Seed_n)$ $(N \leq S)$

$\widetilde{Seed} = 0$

Create the list to record the status of the current seed region merging process

$while(\widetilde{Seed} \leq N)$

$if\ list\_head == NULL$

Randomly select unmarked $Seed_n$ and add noise to it, $Seed'_n = Seed_n + lap(\Delta Q \times N/\varepsilon_1)$

If $(FSMM(Seed'_n, T_{(i,j)}) \leq Th \&\& T_{(i,j)}$ is unmarked

Calculate all $Seed_M$ that meets the condition by $FSMM\left(Seed'_N, T_{(i,j)}\right) \leq Th$ ($Seed_M \in Seed_N | Seed_M = (\ldots, Seed_m | Seed_m = T_{(x,y)}, \ldots)$

$u\left(T_{(i,j)}, Seed_M\right) = -\sqrt{(i-x)^2 + (j-y)^2}$

Extract $Seed_m | Seed_m \in Seed_M$ ($\mathrm{P} \propto \exp\left(\varepsilon_2 u\left(T_{(i,j)}, Seed_M\right)/2\Delta u\right)$)

$T'_{(i,j)} = Seed_m + lap(\Delta Q \times N/\varepsilon_1)$

$Seed_n$ as marked, $T_{(i,j)}$ as marked

$\widetilde{Seed} = \widetilde{Seed} + 1$

Release all data in the list, and the consolidation of this sub region is comple

Theorem 3. In DPLP, the privacy budget under the Laplace mechanism will not surpass ε_1.

Proof: According to the constraint of $N \leq S$ in Line 7, Algorithm 3, when each seed only contains one landmark, $N = (S = 68)$. Then, there exists:

$$\varepsilon_1^1 + \varepsilon_1^2 + \varepsilon_1^3 + \cdots + \varepsilon_1^{68} = \varepsilon_1$$

when each seed contains more landmarks, $N < (S = 68)$. Then, there exists:

$$\varepsilon_1^1 + \varepsilon_1^2 + \varepsilon_1^3 + \cdots + \varepsilon_1^N < \varepsilon_1$$

Q.E.D.

Theorem 4. DPLP satisfies ε- differential privacy.

Proof:

In the DPLP, the total privacy budget ε is divided into two parts: $\varepsilon=\varepsilon_1+\varepsilon_2$. Among them, ε_2 is used to select the target seed by the exponential mechanism. The selection probability is positively proportional to $exp\left(\frac{\varepsilon_2 u(T_{(i,j)}, Seed_M)}{2\Delta u}\right)$. For convenience, the scoring function $u\left(T_{(i,j)}, Seed_M\right)$ is replaced with ΔQ, that is, there exists:

$$Pr[M(Seed_M, \Delta Q) = Seed_m] = \frac{exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m)}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)} \quad (18)$$

Given $Seed_M$ and its adjacent $Seed_M{}'$, for any $Seed_m$ value ($Seed_m \in O$), the following can be derived from formula (18):

$$
\begin{aligned}
&\frac{Pr[M(Seed_M, \Delta Q) = Seed_m]}{Pr[M(Seed_M{}', \Delta Q) = Seed_m]} \\
&= \frac{\dfrac{exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m)}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}}{\dfrac{exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M{}', Seed_m)}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M{}', Seed_m{}')}{2\Delta u}\right)}} \\
&= \left(\frac{exp\left(\frac{\varepsilon_2 \Delta Q((Seed_M, Seed_m))}{2\Delta u}\right)}{exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M{}', Seed_m)}{2\Delta u}\right)}\right) \\
&\times \left(\frac{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M{}', Seed_m{}')}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}\right) \\
&= exp\left(\frac{\varepsilon_2 \begin{pmatrix} \varepsilon_2 \Delta Q(Seed_M, Seed_m) \\ -\varepsilon_2 \Delta Q(Seed_M{}', Seed_m) \end{pmatrix}}{2\Delta u}\right) \\
&\times \left(\frac{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M{}', Seed_m{}')}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}\right) \\
&\leq \exp\left(\frac{\varepsilon_2}{2}\right) \\
&\times \left(\frac{exp\left(\frac{\varepsilon_2}{2}\right)}{\sum_{Seed_m{}' \in O} \times exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}\right) \\
&\leq \exp\left(\frac{\varepsilon_2}{2}\right) \times exp\left(\frac{\varepsilon_2}{2}\right) \\
&\times \left(\frac{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}{\sum_{Seed_m{}' \in O} exp\left(\frac{\varepsilon_2 \Delta Q(Seed_M, Seed_m{}')}{2\Delta u}\right)}\right) \\
&= exp(\varepsilon_2)
\end{aligned}
$$

Therefore, the DPLP satisfies ε_2-differential privacy during the selection of unlabeled subgraphs under the exponential mechanism. In addition, the proof of Theorem 3 suggests that the DPLP satisfies ε_1 -differential privacy during noise addition. According to Property 1, the whole process of the DPLP satisfies ε-differential privacy.

Q.E.D.

Theorem 5. The error of the DPLP is no greater than that of the LAP, i.e.:

$$Error(DPLP) < \mathrm{Error}(LAP)$$

Proof:

In the DPLP, the privacy protected image contains three types of subgraphs, namely, noise-free subgraph $P_{(i,j)}$, seed $Seed_n$, and subgraph merged in regional growth $T_{(i,j)}$. Under the Laplace mechanism, $Seed_n$ and $T_{(i,j)}$ are mixed with an additive noise to form $Seed'_n$ and $T'_{(i,j)}$. Then, it is necessary to prove that $Error(DPLP) \leq \mathrm{Error}(LAP)$ for each type of subgraph.

(1) For $P_{(i,j)}$ in DPLP:

$$P'_{(i,j)\_DPLP} = 0$$

$$P'_{(i,j)\_LAP} = P_{(i,j)} + lap(\Delta Q \times I \times J/(\varepsilon_1 + \varepsilon_2))$$

Subtracting the two formulas above, we have: $Error\big(DPLP(P_{(i,j)})\big) < \mathrm{Error}\big(LAP(P_{(i,j)})\big)$.

(2) For $Seed_n$ in DPLP:

$$Seed'_{n\_DPLP} = Seed_n + lap(\Delta Q \times N/\varepsilon_1)$$

$$Seed'_{n\_LAP} = Seed_n + lap(\Delta Q \times I \times J/(\varepsilon_1 + \varepsilon_2))$$

Since $N \ll I \times J$, the numerical gap between ε_1 and $\varepsilon_1 + \varepsilon_2$ is so small as to be negligible. Subtracting the two formulas above, we have: $Error(DPLP(Seed_n)) < \mathrm{Error}(LAP(Seed_n))$.

(3) For $T_{(i,j)}$ in DPLP:

$$
\begin{aligned}
Error\big(DPLP(T_{(i,j)})\big) &= T'_{(i,j)\_DPLP} \\
&= Seed_n + lap\left(\Delta Q \times \frac{N}{\varepsilon_1}\right) - T_{(i,j)}
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{Error}\big(LAP(T_{(i,j)})\big) &= T'_{(i,j)\_LAP} \\
&= lap(\Delta Q \times I \times J/(\varepsilon_1 + \varepsilon_2))
\end{aligned}
$$

Subtracting the two formulas above, we have:

$$
\begin{aligned}
&Error\big(DPLP(T_{(i,j)})\big) \\
&\quad - \mathrm{Error}\big(LAP(T_{(i,j)})\big) = Seed_n \\
&\quad + lap\left(\Delta Q \times \frac{N}{\varepsilon_1}\right) - T_{(i,j)} \\
&\quad - lap(\Delta Q \times I \times J/(\varepsilon_1 \\
&\quad + \varepsilon_2)) = (Seed_n \\
&\quad + lap\left(\Delta Q \times \frac{N}{\varepsilon_1}\right)) - (T_{(i,j)} \\
&\quad + lap(\Delta Q \times I \times J/(\varepsilon_1 + \varepsilon_2))) \\
&\quad = Seed'_{n\_DPLP} - T'_{(i,j)\_LAP}
\end{aligned}
$$

The maximum and minimum of the image gray matrix are 255 and 0, respectively. Under the noise effect, all values greater than 255 will be converted into 255, and all values smaller than 0 will be converted into 0. Under the Laplace mechanism, when the privacy budget approaches zero, $Error(T'_{(i,j)\_LAP})$ is equivalent to $Error(Seed'_{n\_LAP})$. Thus, we have:

$$
\begin{aligned}
&Seed'_{n\_DPLP} - T'_{(i,j)\_LAP} \\
&\quad = Seed'_{n\_DPLP} \\
&\quad - Seed'_{n\_LAP} = Seed_n \\
&\quad + lap\left(\Delta Q \times \frac{N}{\varepsilon_1}\right) - Seed_n \\
&\quad - \ lap(\Delta Q \times I \times J/(\varepsilon_1 + \varepsilon_2)) \\
&\quad = lap\left(\Delta Q \times \frac{N}{\varepsilon_1}\right) \\
&\quad - \ lap(\Delta Q \times I \times J/(\varepsilon_1 + \varepsilon_2)) < 0
\end{aligned}
$$

Thus, we have: $Error\left(DPLP(T_{(i,j)})\right) < Error\left(LAP(T_{(i,j)})\right)$.

Q.E.D.

4. EXPERIMENTS AND RESULTS ANALYSIS

4.1 Experiments

The feasibility of the DPLP was tested on 17-2m.jpg (480*640) from the IMM Face Database. During the execution of the algorithm, the subgraph size was set to 10*10, and the original image was split into 3,072 subgraphs. To realize the DPLP, the first step is to convert the original image (Figure 1) into a gray image (Figure 2). Then, the ASM algorithm was adopted to label 68 landmarks (Figure 3) in the face of the gray image. To satisfy the regional growth requirements of the DPLP, the face image needs to be divided into multiple subgraphs of the same size, using the preset parameters (Figure 4). If the landmark position overlaps the area contained in a subgraph (Figure 5), the subgraph will be treated as a sensitive area, and selected as a seed for regional growth (Figure 6).

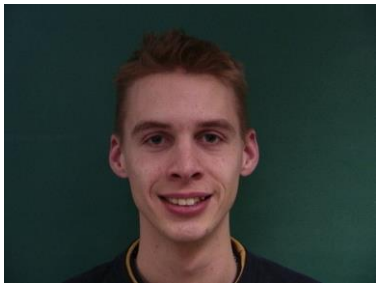

Figure 1. Original image

Figure 2. Gray image

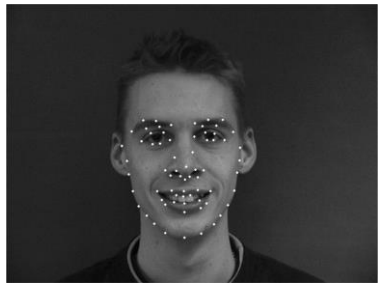

Figure 3. Face landmark positioning

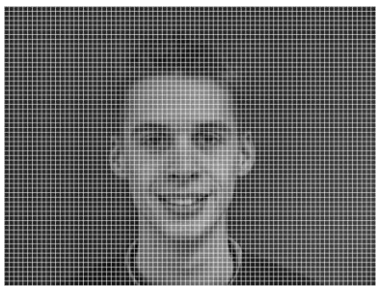

Figure 4. Subgraph division

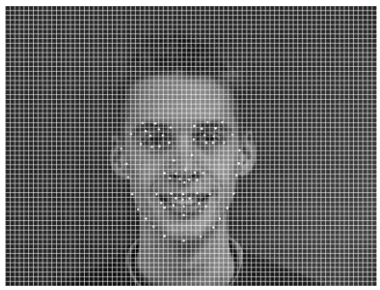

Figure 5. Overlapping region

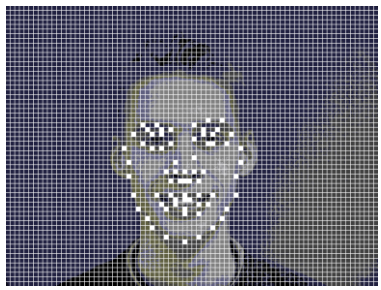

Figure 6. Sensitive area (seed)

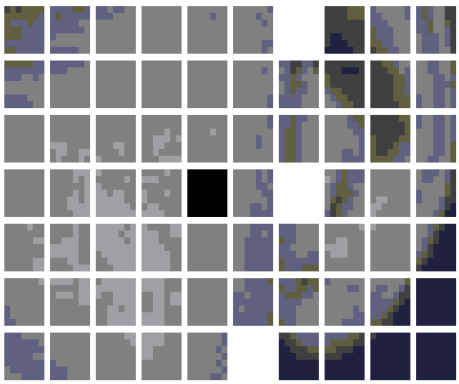

Figure 7. Candidate areas for merging

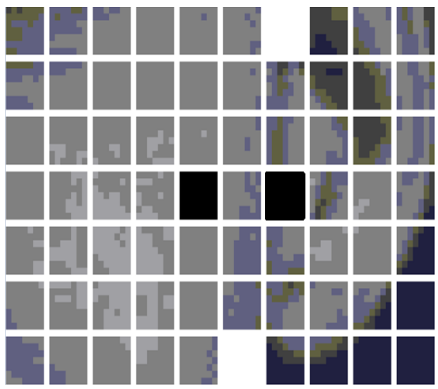

Figure 8. Ideal areas for merging

Figure 9. Results of the LAP

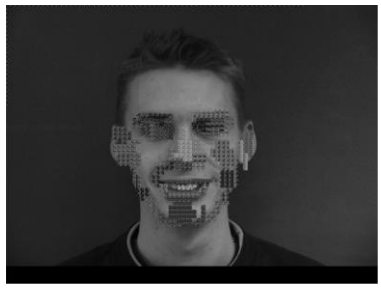

Figure 10. Results of the DPLP

As shown in Figure 7, when a subgraph (black area) could be merged with multiple seeds (white area) in the DPLP, the merging result depends too much on the sequence of seed selection. To prevent the attacker from predicting the target face from landmark distribution, the Euclidean distance between each subgraph and each seed is adopted as the scoring function of the exponential mechanism to guide the selection of areas to be merged. Figure 8 shows the most reasonable merging method under ε_2.

Figure 9 presents the results of the LAP algorithm, and Figure 10 displays the results of the DPLP under the same privacy budget. It can be observed that the DPLP only functions within the regional growth range with face landmarks as seeds, while the LAP acts on the entire image.

4.2 Results analysis

To verify the feasibility of our algorithm, some multi-face images were selected from IMM Face Database, Aberdeen Face Database, and LFW Face Database, and compiled into test sets. The experimental environment includes Intel® Core i9-9900K CPU @ 3.60 GHz, 32G memory, GTX 21080TI GPU, and Windows 10. During the experiments, the faces were recognized by TensorFlow + AlexNet CNN. The privacy budget ε was set to 0.5, 1, 1.5, 2, 2.5, and 3, in turn. The performance was measured by Precision, Recall, and F1-score. The experimental results are displayed in Figures 11-19.

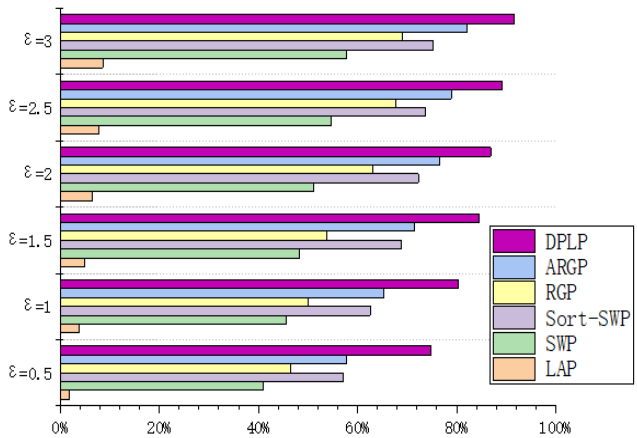

Figure 11. Precision on IMM

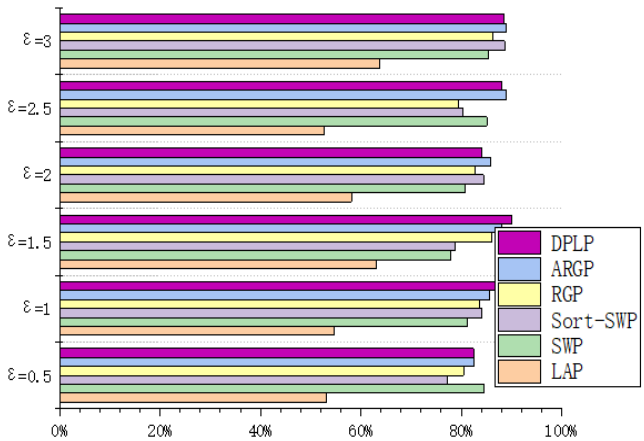

Figure 12. Recall on IMM

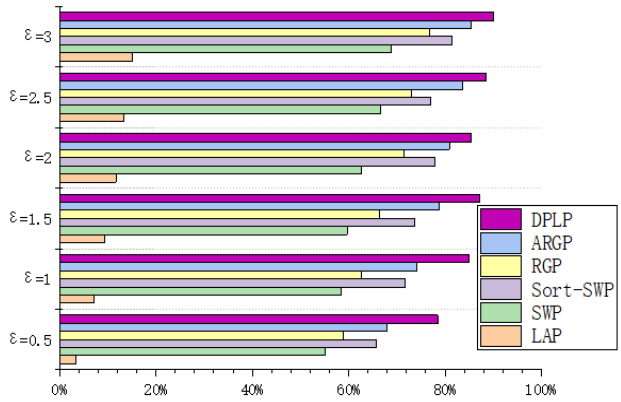

Figure 13. F1-score on IMM

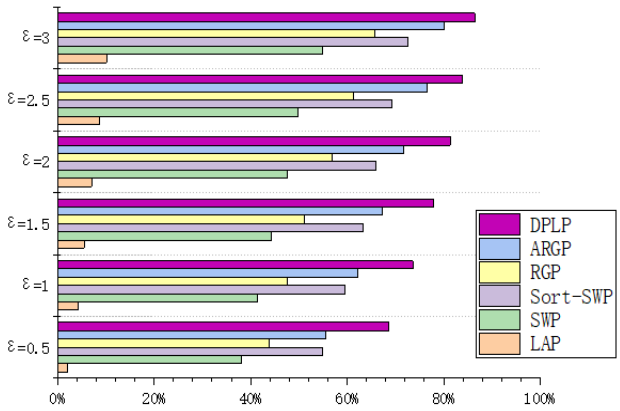

Figure 14. Precision on Aberdeen

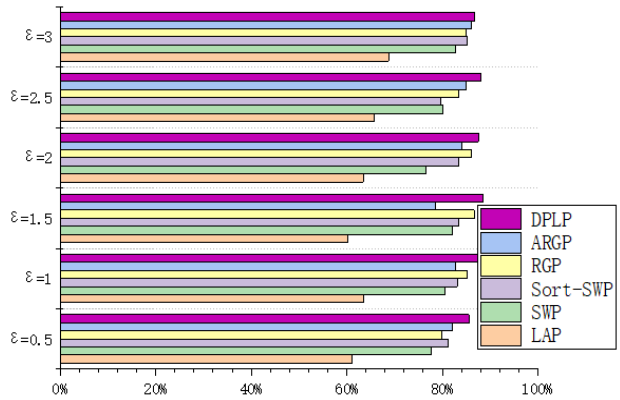

Figure 15. Recall on Aberdeen

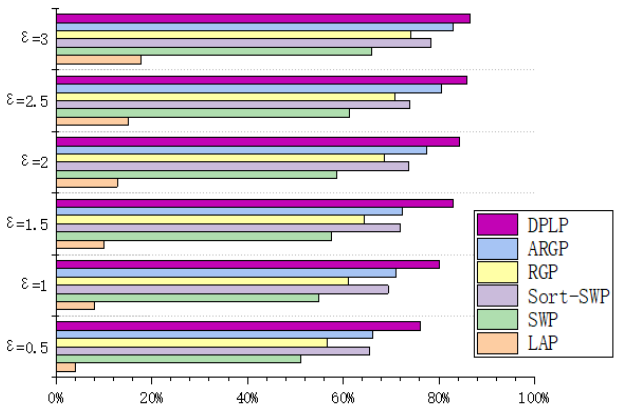

Figure 16. F1-score on Aberdeen

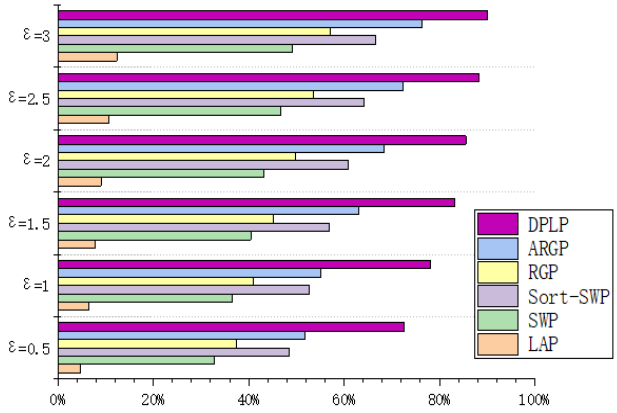

Figure 17. Precision on LFW

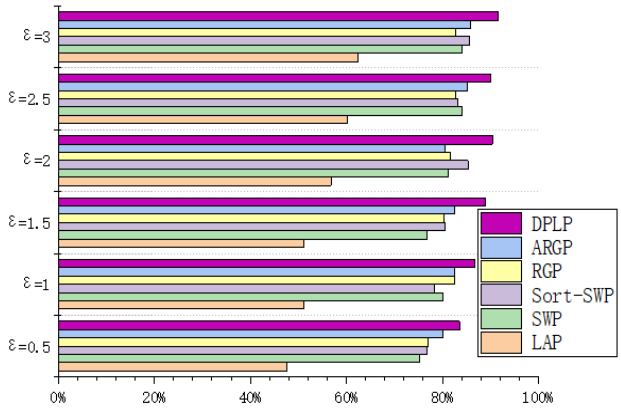

Figure 18. Recall on LFW

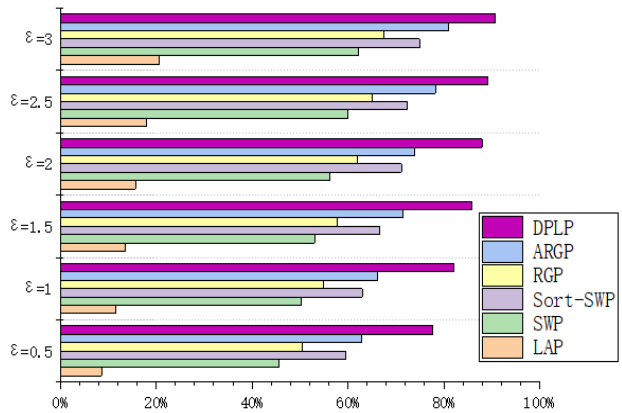

Figure 19. F1-score on LFW

Under the same privacy budget (ε=0.5), the LAP performed the best on LFW (250*250) (Precision=4.7%), followed by Aberdeen (400*550) (Precision=2.1%), and worked the worst on IMM (480*640) (Precision=1.8%). This is because the total error of the LAP depends on the image size. For sliding window publication (SWP) algorithm, sort-SWP algorithm, region growing publication (RGP), and atypical RGP (ARGP) algorithm, the total error hinges on the regional growth results. Under the same privacy budget and Th, the results of regional growth depend on the complexity of the image. All four algorithms had the worst performance (Precision=32.7%, 48.6%, 37.5%, 51.8%) on LFW, due to the complex background of images in the database. Their performances on IMM (Precision=40.9%, 57.2%, 46.6%, 57.7%) and Aberdeen (Precision=38.2%, 54.9%, 43.8%, 55.5%) were similar, both were better than the performance on LFW. This is attributable to the fact that region merging is easier due to the pure color backgrounds of images in these two databases. In addition, the experimental results show that the error of the DPLP is independent of image size, but affected by the percentage of face area in the entire image. That is, the proportion of face area is negatively correlated with Precision, Recall, and F1-score. The result is consistent with the previous expectation.

5. CONCLUSIONS

To solve the problems in privacy protection of face images, this paper integrates face landmark positioning, regional growth, and Laplace mechanism in differential privacy to add noise to local sensitive areas in the original image, and thus realizes the non-global privacy protection of face images under the interactive framework. Through comparative experiments on several face databases (IMM, Aberdeen, and LFW), the proposed DPLP achieved better Precision, Recall, and F1-score than LAP, SWP, Sort-SWP, RGP, and ARGP. The results suggest that DPLP-based privacy protection of face images improves the availability of the protected image. Using DPLP, the protected areas in the original image only depend on landmark positions and growth rules. Thus, the noise error induced by privacy protection does not change with image size.

Notably, although the DPLP can effectively protect the face information in face images, the algorithm is unable to pinpoint the landmarks in multiple faces, if the original image contains more than one faces, and the face areas only account for a small portion of the image. In this case, some face information in the image may be leaked. To prevent the privacy leak, the future research will further improve the face image privacy protection framework for multi-face images.

ACKNOWLEDGMENT

The authors thank the project of the National Natural Science Foundation of China (Grant No.: 61672179), Natural Science Foundation of Heilongjiang Province (Grant No.: LH2021D022, 2019F004), and Fundamental Research Funds in Heilongjiang Provincial Education Department (Grant No.: 145109216).

REFERENCES

[1] Liu, C., Yang, J., Zhao, W., Zhang, Y., Li, J., Mu, C. (2021). Face image publication based on differential privacy. Wireless Communications and Mobile Computing, (9): 1-20. https://doi.org/10.1155/2021/6680701

[2] Fung, B.C., Wang, K., Philip, S.Y. (2007). Anonymizing classification data for privacy preservation. IEEE Transactions on Knowledge and Data Engineering, 19(5): 711-725. https://doi.org/10.1109/TKDE.2007.1015

[3] Xiao, X., Tao, Y. (2006). Anatomy: Simple and effective privacy preservation. In Proceedings of the 32nd International Conference on Very Large Data Bases, pp. 139-150. https://doi.org/10.3390/met11020309

[4] Li, T., Li, N., Zhang, J., Molloy, I. (2010). Slicing: A new approach for privacy preserving data publishing. IEEE

Transactions on Knowledge and Data Engineering, 24(3): 561-574. https://doi.org/10.1109/TKDE.2010.236
[5] Terrovitis, M., Liagouris, J., Mamoulis, N., Skiadopoulos, S. (2012). Privacy preservation by disassociation. arXiv preprint arXiv:1207.0135.
[6] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5): 557-570. https://doi.org/10.1142/S0218488502001648
[7] Dwork, C. (2006). Differential privacy. In International Colloquium on Automata, Languages, and Programming, pp. 1-12. https://doi.org/10.1007/11787006_1
[8] Dwork, C. (2008). Differential privacy: A survey of results. In International Conference on Theory and Applications of Models of Computation, pp. 1-19. https://doi.org/10.1007/978-3-540-79228-4_1
[9] Dwork, C. (2009). The differential privacy frontier. In Theory of Cryptography Conference, pp. 496-502.
[10] Dwork, C., Lei, J. (2009). Differential privacy and robust statistics. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, pp. 371-380. https://doi.org/10.1145/1536414.1536466
[11] Dwork, C. (2010). Differential privacy in new settings. In Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms, pp. 174-183. https://doi.org/10.1137/1.9781611973075.16
[12] Dwork, C. (2011). The promise of differential privacy a tutorial on algorithmic techniques. In 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, pp. 1-2.
[13] Dwork, C., McSherry, F., Nissim, K., Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography Conference, pp. 265-284. https://doi.org/10.1007/11681878_14
[14] McSherry, F., Talwar, K. (2007). Mechanism design via differential privacy. In 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07), pp. 94-103. https://doi.org/10.1109/FOCS.2007.66
[15] McSherry, F.D. (2009). Privacy integrated queries: an extensible platform for privacy-preserving data analysis. In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, pp. 19-30. https://doi.org/10.1145/1559845.1559850
[16] Roth, A., Roughgarden, T. (2010). Interactive privacy via the median mechanism. In Proceedings of the forty-second ACM symposium on Theory of Computing, pp. 765-774. https://doi.org/10.1145/1806689.1806794
[17] Hardt, M., Rothblum, G.N. (2010). A multiplicative weights mechanism for privacy-preserving data analysis. In 2010 IEEE 51st Annual Symposium on Foundations of Computer Science, pp. 61-70. https://doi.org/10.1109/FOCS.2010.85
[18] Gupta, A., Roth, A., Ullman, J. (2012). Iterative constructions and private data release. In Theory of Cryptography Conference, pp. 339-356. https://doi.org/10.1007/978-3-642-28914-9_19
[19] Fan, L., Xiong, L. (2012). Real-time aggregate monitoring with differential privacy. In Proceedings of the 21st ACM International Conference on Information and Knowledge Management, pp. 2169-2173. https://doi.org/10.1145/2396761.2398595
[20] Kellaris, G., Papadopoulos, S., Xiao, X., Papadias, D. (2014). Differentially private event sequences over infinite streams. Proceedings of the VLDB Endowment, 7(12): 1155-1166. https://doi.org/10.14778/2732977.2732989
[21] Xiao, X., Wang, G., Gehrke, J. (2010). Differential privacy via wavelet transforms. IEEE Transactions on Knowledge and Data Engineering, 23(8): 1200-1214. https://doi.org/10.1109/TKDE.2010.247
[22] Xu, J., Zhang, Z., Xiao, X., Yang, Y., Yu, G., Winslett, M. (2013). Differentially private histogram publication. The VLDB Journal, 22(6): 797-822. https://doi.org/10.1007/s00778-013-0309-y
[23] Li, C., Miklau, G., Hay, M., McGregor, A., Rastogi, V. (2015). The matrix mechanism: Optimizing linear counting queries under differential privacy. The VLDB Journal, 24(6): 757-781. https://doi.org/10.1007/s00778-015-0398-x
[24] Li, C., Hay, M., Miklau, G., Wang, Y. (2014). A data- and workload-aware algorithm for range queries under differential privacy. Proceedings of the VLDB Endowment, 7(5): 341-352. https://doi.org/10.14778/2732269.2732271
[25] Yang, G., Huang, T.S. (1994). Human face detection in a complex background. Pattern recognition, 27(1): 53-63. https://doi.org/10.1016/0031-3203(94)90017-5
[26] Meng, W.L., Mao, C.Z., Zhang, J., Wen, J., Wu, D.H. (2019). A fast recognition algorithm of online social network images based on deep learning. Traitement du Signal, 36(6): 575-580. https://doi.org/10.18280/ts.360613
[27] Feng, G.C., Yuen, P.C. (1998). Variance projection function and its application to eye detection for human face recognition. Pattern Recognition Letters, 19(9): 899-906. https://doi.org/10.1016/S0167-8655(98)00065-8
[28] Zhou, Z.H., Geng, X. (2004). Projection functions for eye detection. Pattern Recognition, 37(5): 1049-1056. https://doi.org/10.1016/j.patcog.2003.09.006
[29] Zhang, L., Lenders, P. (2000). Knowledge-based eye detection for human face recognition. In KES'2000. Fourth International Conference on Knowledge-Based Intelligent Engineering Systems and Allied Technologies. Proceedings (Cat. No. 00TH8516), (1): 117-120. https://doi.org/10.1109/KES.2000.885772
[30] Reisfeld, D., Yeshurun, Y. (1992). Robust detection of facial features by generalized symmetry. In International Conference on Pattern Recognition, pp. 117-117. https://doi.org/10.1109/ICPR.1992.201521
[31] Wu, H., Yokoyama, T., Pramadihanto, D., Yachida, M. (1996). Face and facial feature extraction from color image. In Proceedings of the Second International Conference on Automatic Face and Gesture Recognition, pp. 345-350. https://doi.org/10.1109/AFGR.1996.557289
[32] Yuille, A.L., Hallinan, P.W., Cohen, D.S. (1992). Feature extraction from faces using deformable templates. International Journal of Computer Vision, 8(2): 99-111. https://doi.org/10.1007/BF00127169
[33] Lanitis, A., Taylor, C.J., Cootes, T.F. (1995). A unified approach to coding and interpreting face images. In Proceedings of IEEE International Conference on Computer Vision, pp. 368-373. https://doi.org/10.1109/ICCV.1995.466919
[34] Cootes, T.F., Hill, A., Taylor, C.J., Haslam, J. (1993). The use of active shape models for locating structures in medical images. Image and Vision Computing, 12(6): 355-365. https://doi.org/10.1007/BFb0013779

[35] Dollár, P., Welinder, P., Perona, P. (2010). Cascaded pose regression. In 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 1078-1085. https://doi.org/10.1109/CVPR.2010.5540094
[36] LeCun, Y., Bottou, L., Bengio, Y., Haffner, P. (1998). Gradient-based learning applied to document recognition. Proceedings of the IEEE, 86(11): 2278-2324. https://doi.org/10.1109/5.726791
[37] Sun, Y., Wang, X., Tang, X. (2013). Deep convolutional network cascade for facial point detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 3476-3483.
[38] Zhang, Z., Luo, P., Loy, C.C., Tang, X. (2014). Facial landmark detection by deep multi-task learning. In European Conference on Computer Vision, pp. 94-108. https://doi.org/10.1007/978-3-319-10599-4_7
[39] Zhang, K., Zhang, Z., Li, Z., Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. IEEE Signal Processing Letters, 23(10): 1499-1503. https://doi.org/10.1109/LSP.2016.2603342
[40] Wu, Y., Hassner, T., Kim, K., Medioni, G., Natarajan, P. (2017). Facial landmark detection with tweaked convolutional neural networks. IEEE Transactions on Pattern Analysis and Machine Intelligence, 40(12): 3067-3074. https://doi.org/10.1109/TPAMI.2017.2787130
[41] Reddy, C., Reddy, U.S., Kishore, K. (2019). Facial emotion recognition using NLPCA and SVM. Traitement du Signal, 36(1): 13-22. https://doi.org/10.18280/ts.360102
[42] Liu, C., Yang, J., Wu, J. (2020). Web intrusion detection system combined with feature analysis and SVM optimization. EURASIP Journal on Wireless Communications and Networking, (1): 1-9. https://doi.org/10.1186/s13638-019-1591-1
[43] Yow, K.C., Cipolla, R. (1996). A probabilistic framework for perceptual grouping of features for human face detection. In Proceedings of the Second International Conference on Automatic Face and Gesture Recognition, pp. 16-21. https://doi.org/10.1109/AFGR.1996.557238
[44] Wiskott, L., Krüger, N., Kuiger, N., Von Der Malsburg, C. (1997). Face recognition by elastic bunch graph matching. IEEE Transactions on pattern analysis and machine intelligence, 19(7): 775-779. https://doi.org/10.1109/34.598235
[45] Feris, R.S., Gemmell, J., Toyama, K., Kruger, V. (2002). Hierarchical wavelet networks for facial feature localization. In Proceedings of Fifth IEEE International Conference on Automatic Face Gesture Recognition, pp. 125-130. https://doi.org/10.1109/AFGR.2002.1004143
[46] Liu, C., Yang, J., Zhao, W., Zhang, Y., Shi, C., Miao, F., Zhang, J. (2021). Differential privacy protection of face images based on region growing. Traitement du Signal, 38(5): 1385-1401. https://doi.org/10.18280/ts.380514