



Privacy protection framework for face recognition in edge-based Internet of Things

Yun Xie¹ · Peng Li¹ · Nadia Nedjah² · Brij B. Gupta^{3,4,5} · David Taniar⁶ · Jindan Zhang⁷

Received: 30 October 2021 / Revised: 26 October 2022 / Accepted: 28 October 2022
© The Author(s) 2022

Abstract

Edge computing (EC) gets the Internet of Things (IoT)-based face recognition systems out of trouble caused by limited storage and computing resources of local or mobile terminals. However, data privacy leak remains a concerning problem. Previous studies only focused on some stages of face data processing, while this study focuses on the privacy protection of face data throughout its entire life cycle. Therefore, we propose a general privacy protection framework for edge-based face recognition (EFR) systems. To protect the privacy of face images and training models transmitted between edges and the remote cloud, we design a local differential privacy (LDP) algorithm based on the proportion difference of feature information. In addition, we also introduced identity authentication and hash technology to ensure the legitimacy of the terminal device and the integrity of the face image in the data acquisition phase. Theoretical analysis proves the rationality and feasibility of the scheme. Compared with the non-privacy protection situation and the equal privacy budget allocation method, our method achieves the best balance between availability and privacy protection in the numerical experiment.

Keywords Face recognition · Eigenface · Local differential privacy · Edge computing

1 Introduction

The advantages of FR technology in terms of non-contact and convenience have applied themselves to a greater extent in applications such as health testing, mobile payment, personal information collection, and identity authentication, especially since the outbreak of COVID-19. The vigorous development of machine learning (ML) [1, 2]

has greatly improved the accuracy and performance of FR in the era of big data, far surpassing traditional methods [3, 4]. However, the constraints caused by limited local storage and computing resources still exist, especially when dealing with large-scale face databases [5].

EC solves the above difficulties in a new way. It analyzes and processes data near the source of data, and there is no data circulation [6]. In EFR systems, face data still needs to be submitted to an untrusted third-party cloud

✉ Peng Li
lipeng@njupt.edu.cn

✉ Brij B. Gupta
gupta.brij@gmail.com

Yun Xie
2018040240@njupt.edu.cn

Nadia Nedjah
nadia@eng.uerj.br

David Taniar
David.Taniar@monash.edu

Jindan Zhang
zhangjindan83@163.com

² Department of Electronics Engineering and Telecommunications of the Engineering Faculty, State University of Rio de Janeiro, Rio de Janeiro, Brazil

³ International Center for AI and Cyber Security Research and Innovations & Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan

⁴ Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun, India

⁵ Lebanese American University, Beirut, Lebanon

⁶ Faculty of Information Technology, Monash University, Clayton, Australia

⁷ Xianyang Vocational Technical College, Xianyang, China

¹ School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

server for model training after edge processing [7]. The issue of privacy cannot be overlooked because face data carries or is closely related to personal sensitivities information [8]. Based on these concerns, federal agencies in the United States [9] have tried to promote new regulations to protect privacy, that is, banning FR systems.

Therefore, privacy protection is still a significant issue in face recognition systems in edge environments. Privacy protection for EFR systems faces several core issues:

- Do not rely on the existence of a trusted third-party server;
- The attacker cannot associate the acquired facial features with other sensitive data;
- Facial biometrics should be irreversible one-way conversion;
- Computational complexity shows friendliness to resource-constrained equipment and can be extended to large-scale data processing occasions.

Starting with secure data transmission and access control is the most traditional method to solve the privacy protection problem of the FR system, for example, ML frameworks based on homomorphic encryption technology, SecureML [10], and DeepZeroID [11]. In addition, although the loss of FR accuracy caused by encryption technology is tiny, its high time complexity and large memory consumption are not suitable for practical applications. Compared with traditional methods, differential privacy (DP) achieves lower computational complexity at the expense of proper utility. Especially in large-scale data processing, DP better reflects high efficiency [12].

Besides that, most FR functions based on encryption methods that provide privacy protection require an assumption that there exists one trusted third party [13, 14] in the server-based settings. However, there is no fully trusted party in the actual scenario. Generally, after the cloud server receives the encrypted data, it decrypts to get the plaintext and then performs matching and analysis operations [15]. There is a high possibility that private data leak on the server-side.

On the contrary, DP technology applies to the authentic situation where an untrusted third party exists, which has become a new focus in FR [16]. However, most existing schemes based on DP only consider data privacy protection in one or several stages of storage, release, and model construction in EFR systems [17]. There is still a lack of a systematic approach to address all the core issues mentioned above. For these reasons, this paper focuses on privacy protection throughout the entire life cycle of data in EFR systems. The main contributions of our work are summarized as follows:

- We propose a general privacy protection framework for an EFR system, in which the terminal device, the edge

network center, and the remote cloud server construct a three-level FR architecture. The privacy protection of face data in the entire life cycle is focused on and realized.

- We design a LDP algorithm that adaptively allocates a privacy budget according to the difference in the proportion of principal component feature information. The edge executes this algorithm after the dimensionality reduction of face images, which, on the one hand, protects the face feature data transmitted between edges and the cloud, and on the other hand, enhances the privacy security of the stored data and the published model on the cloud side.
- We add an authentication mechanism to control the legitimacy of terminal devices connected to the edge network center for higher security. This mechanism ensures the reliability and quality of the data source.

The rest of this article is organized as follows: Sect. 2 discusses related work, and Sect. 3 provides background knowledge. The EFR system and its existing security threats are explained in Sect. 4. Section 5 elaborates on the privacy protection scheme in detail. Section 6 discusses the experimental process and analyzes the results. Finally, Sect. 7 concludes the article.

2 Related work

Typical privacy protection methods in FR include encryption, de-identification (de-ID), and perturbation. We review the most relevant related works by category as follows.

2.1 Encryption for FR

Homomorphic encryption and secure multi-party computing are essentially encryption. In 2009, Erkin et al. [13] proposed a privacy-preserving FR scheme using Paillier and DGK cryptosystem. Since the recognition of the face image in the database is to process the homomorphically encrypted data, the computational complexity is very high. Sadeghi et al. [18] subsequently proposed a relatively effective improvement method. That is pulling in an obfuscation circuit in homomorphic encryption to improve the recognition efficiency. Xiang et al. [14] proposed a hybrid encryption scheme based on fully homomorphic for the scenario of FR outsourcing to cloud servers. The protocol provided higher privacy for faces and reduced the computational cost between the user and the face owner.

Compared with homomorphic encryption technology, secure multi-party computing technology is more suitable for face data privacy protection in application

scenarios with multiple cloud servers [19–21]. In [19], the authors presented an application of FR technology based on secure multi-party computing in CloudID and designed a K -d tree structure processing biometrics in the encrypted domain. In [20], a secure outsourcing FR method for the joint-environment has been given, which can still effectively protect the user's private data under the semi-honest model. The main idea is that two semi-honest and conflict-free cloud servers perform FR based on eigenface algorithms in a privacy-protecting manner. Ma et al. [21] also proposed a secure FR system, in which a deep neural network is for extracting facial features. To reduce the computational burden, lightweight computing schemes have been proposed: POR [22] and PE-MIU [23]. POR is a lightweight-adaptive enhancement AdaBoost classification framework based on additive secret sharing. PE-MIU implements privacy enhancement based on the smallest information unit.

2.2 De-ID for FR

The de-ID method realizes privacy protection by removing the correspondence between the user's face data and individual identities. K -same based on K -anonymity is an early method [24]. Then, some new de-ID methods appeared. Binod et al. [25] proposed a method to de-identify the face images by adding designed noise patterns. Letournel et al. [26] proposed an adaptive filtering method to de-identify face images. Sun et al. [27] focused on diversity to avoid de-IDed faces all looking similar. More recently, generative adversarial networks (GAN) have been used for face de-ID. The work in [28] used GAN to generate de-IDed faces. In [29], a GAN-based in-painting method was used to partially replace the original face.

2.3 Perturbation for FR

Early face image privacy protection based on DP technology mainly solved the privacy protection problem during publishing face data by confusing the visual identity in the image. For example, Othman and Ross [30] interfered with the face image to hide age, gender, and race information. Although adding Laplace noise directly to all values in the real field matrix of the image can satisfy DP, it will cause excessive distortion of the images. To reduce the noise error, Zhang et al. [16] proposed an image compression method based on discrete Fourier transform, adding the corresponding Laplacian noise to the compressed image. However, reconstruction error is incited in the image compression process. To balance the noise error and the reconstruction error, they proposed an improved scheme based on matrix decomposition, which improved the robustness of the gray scale face image [31] but failed

to fundamentally eliminate the reconstruction error in the compression process. In [32], Fan added pixelation to face images based on DP to achieve safe sharing while obtaining strong privacy guarantees. However, the confusing images are no longer similar to the original category of the object, resulting in poor visual quality of the output image. William et al. [33] applied DP to a generative model to blur facial images, and then extended this method to general images [34]. Liu et al. [35] adopted a data stream method to process images and finally realized the dynamic allocation of privacy budget based on the similarity of adjacent data, which improves the image data to a certain extent availability.

However, the above ways tend to focus on the research and application of theoretical methods in the scenes of trusting a third-party. In actual applications, third parties are usually untrustworthy. In response to this problem, Chamikara et al. [17] proposed the PEEP protocol to achieve resistance to member reasoning attacks and model memory attacks, in which the third-party server only receives and stores the disturbed eigenface data to perform a standard recognition algorithm.

3 Preliminaries

3.1 Local differential privacy

Definition 1 (ϵ -LDP) [36] Assuming there are N users, each user has a data record. For privacy algorithm F , its defined domain is $Dom(F)$, and its output range is $Ran(F)$. If the same output result t^* ($t^* \subseteq Ran(F)$) which is obtained by the algorithm F on two arbitrary records t and t' ($t, t' \subseteq Dom(F)$) satisfies the condition of formula (1). Then we say that the algorithm F satisfies ϵ -LDP.

$$\Pr[F(t) = t^*] \leq e^\epsilon \times \Pr[F(t') = t^*] \quad (1)$$

LDP is a branch of the ϵ -DP framework. LDP does not rely on a trusted data collector, and its privacy protection occurs on the user side. Each user submits only the disturbed data to an aggregator. The aggregator cannot distinguish whether t^* is from the real record t or another record t' with high confidence, regardless of the background information it possesses. Even if the aggregator is malicious, the privacy of each user is still protected. Moreover, since the data is randomly disturbed at each user, users can use DP parameter values to achieve personalized privacy protection based on their own needs.

LDP inherits important properties of DP: such as post-processing immunity, which states that arbitrarily

transforming the output of DP by some data-independent functions will not affect its privacy guarantee.

Theorem 1 (Post-processing) [37] *Let M be an ε -differentially private mechanism and g be an arbitrary mapping from the set of possible outputs of M to an arbitrary set. Then, $g \circ M$ is ε -differentially private.*

3.2 Principal component analysis (PCA)

The PCA method is especially useful when the variables in the dataset are highly correlated, reducing the original variables to a smaller number of new variables (principal components). That is, PCA removes variables that are strongly correlated with other variables, leaving more representative variables. Compared with LDA and a few other dimensionality reduction methods [38], PCA can retain the original information to the greatest extent and minimize the loss of information while reducing the features.

Suppose the data set $D = [D_1, D_2, \dots, D_n]$ has a total of n samples, and each sample, such as the i th sample $D_i \in \mathbb{R}^d$, contains d characteristic attributes, then the original data set $D \in \mathbb{R}^{n \times d}$ can be represented in a $n \times d$ matrix form.

Definition 2 (Covariance matrix (CM)) Assuming that the l_2 norm of the vector D_i satisfies the condition: $\|D_i\|_2 \leq 1$, the l_2 norm of any vector $x \in \mathbb{R}^d$ is $\|x\|_2 = \sqrt{\sum_{i=1}^d x_i^2}$. The CM of the original data $D = [D_1, D_2, \dots, D_n]$ is:

$$A = \frac{1}{n} D^T D = \frac{1}{n} \sum_{i=1}^d D_i^T D_i \quad (2)$$

Here, A is a $d \times d$ symmetric matrix. A represents the correlation between variables, and the correlation indicates that there is redundancy in the data.

Definition 3 (Eigenvalue decomposition) The relationship among CM A , eigenvalue λ and eigenvector U satisfies:

$$A = U \Lambda U^T \quad (3)$$

Among them, Λ is a diagonal matrix composed of A 's all eigenvalues; U is an orthogonal matrix composed of A 's all eigenvectors in columns, which constitutes a new vector space as the coordinate axis of new variables (principal components). Principal components can be obtained by calculating the eigenvalue λ and the corresponding eigenvector U of A .

Start with the order polynomial of the eigenvalue λ :

$$|\lambda I - A| = 0 \quad (4)$$

Among them, I is an identity matrix, the eigenvalue λ of A are solved, and then by the formula:

$$A u_i = \lambda_i u_i, (i = 1, 2, \dots, d) \quad (5)$$

Eigenvectors of A can be solved. Denote the set of eigenvectors as $U = (u_1, u_2, \dots, u_d)$. Here, $\lambda_i (1 \leq i \leq d)$ is the i th eigenvalue corresponding the i th eigenvector u_i , which can represent the proportion of the information contained in the corresponding component, the larger the value λ_i , the more important the information contained in the corresponding component.

Definition 4 (Accumulative contribution) [39] Accumulative Contribution is used to reflect the proportion of information contained in the first k eigenvalues when the number of principal components is selected as k , expressed as:

$$\eta_k = \sum_{i=1}^k \lambda_i / \sum_{i=1}^d \lambda_i \quad (6)$$

Introduce $\eta (0 \leq \eta \leq 1)$ as the threshold, and make $\eta_k \geq \eta$ to determine the appropriate value of k . Then, extract the eigenvectors corresponding to the first k eigenvalues to form a matrix $U_k = (u_1, u_2, \dots, u_k)$, in which u_i and u_j are orthogonal ($i \neq j$).

4 System framework

This section introduces the architecture of the EFR system and analyzes its existing security issues and design goals.

4.1 System model

The EFR system framework is divided into three layers according to functions, as shown in Fig. 1.

- The first layer is the local terminals, which collect face images and uploads them to the edge.
- The second layer is the edge, which receives the face image uploaded by the local terminal and uploads it to the server after preprocessing.
- The third layer is the cloud server, which receives the face image information submitted by the edge, carries out model training, or uses the trained model for recognition, and feeds back the recognition result to the edge.

This framework, on the one hand, can use the existing data and computing capabilities on the cloud server to

complete model training; on the other hand, it reduces the pressure of data transmission between the local terminal and the cloud server and improves communication efficiency. Thus, the response time of the recognition result is greatly shortened.

4.2 Threat model

We illustrate the security threats in the face recognition system based on edge computing from two aspects: user privacy and data reliability.

- (1) Threats to user privacy. As an untrusted third party, the cloud server is curious about the face data submitted by the edge. In the process of model training or recognition, it may use some intermediate information to further analyze the associated private information. Correspondingly, an attacker can easily obtain facial images, training models, and other associated private information by accessing the cloud server.
- (2) Threats to data reliability. The local terminal is the source of face data. If it is used by an attacker, the reliability of the data will not be guaranteed. On the one hand, the attacker may submit forged facial data through illegal local terminals; on the other hand, legitimate local terminals may also submit low-quality or invalid facial data (due to the poor objective environment of the image acquisition equipment, the image quality poor, or the user's maliciousness) will reduce the accuracy of model training, which in turn affects the effectiveness of system functions. In addition, multiple attackers may

conspire to send invalid data to disrupt the operation of the system.

4.3 Security goals

In order to effectively solve the user privacy threats and data reliability threats in the system, the designed privacy protection scheme needs to achieve the following security goals:

- (1) Protect user data privacy. The third-party server or attacker cannot obtain user privacy information. First, the face image data submitted by the edge to the cloud server cannot be raw data, but data processed by privacy protection algorithms. Then submit it to the cloud server for normal model training or recognition so that the system functions are not affected. In addition, a third party or an attacker cannot infer the user's original face image or related private information through the obtained intermediate information.
- (2) Ensure data reliability and improve data quality. The edge reviews the authority of the local terminal, and only legal users who have passed the registration can submit data to the edge or receive feedback information from the edge. The edge does not exchange any information with illegal terminals. In addition, the edge preprocesses the image data submitted by the legal local terminal to ensure that the quality of the face image data can meet the needs of model training and recognition.
- (3) Reduce communication load and improve system response time. Although the data quality of the face image after edge preprocessing is guaranteed, it is still high-dimensional data. If the edge directly submits high-dimensional data, it will put a lot of pressure on network communication, and it will also cause a long system response delay, especially in large-scale data scenarios. Therefore, it is necessary for the edge to perform further dimensionality reduction processing on the face image, reduce the amount of data transmitted between the remote server and itself, reduce the communication burden, and effectively improve the communication efficiency.

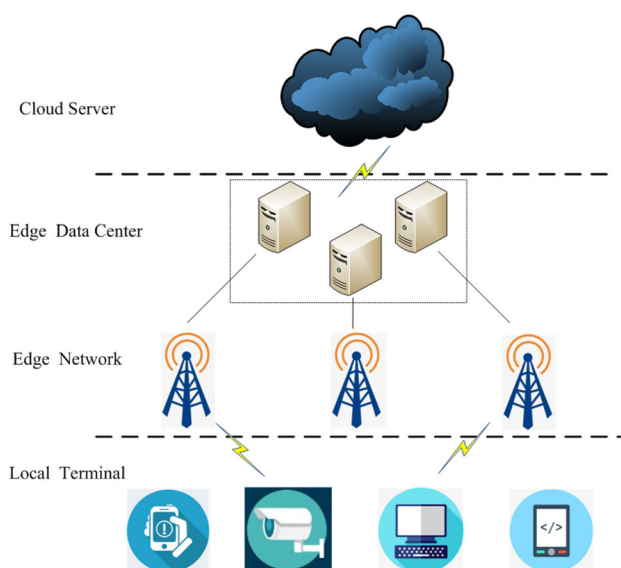


Fig. 1 The architecture of EFR system

5 Our proposed framework

In this section, we discuss the privacy protection framework of the entire face image processing process under the three-level FR system architecture. The flow chart of our framework is shown in Fig. 2.

First, in the data aggregation stage, the terminal device submits the collected face images to the edge through an encrypted communication channel to form a face database. Second, in the model training phase, the edge sequentially performs the following operations on the face image: pre-processing, eigenface generation, and eigenface perturbation. Then, the output perturbed eigenface is sent to the cloud server for classification model training to obtain a privacy-protected recognition model. Finally, in the face recognition stage, the terminal submits the test image, and the edge performs image processing and disturbance according to the above steps and submits the result to the cloud. The cloud uses the trained model to get the recognition results and feed them back to the edge. The terminal device obtains the recognition response from the edge.

Based on the key exchange protocol and LDP technology, we solve the problem of data reliability and user privacy protection throughout the life cycle of face images in recognition processing.

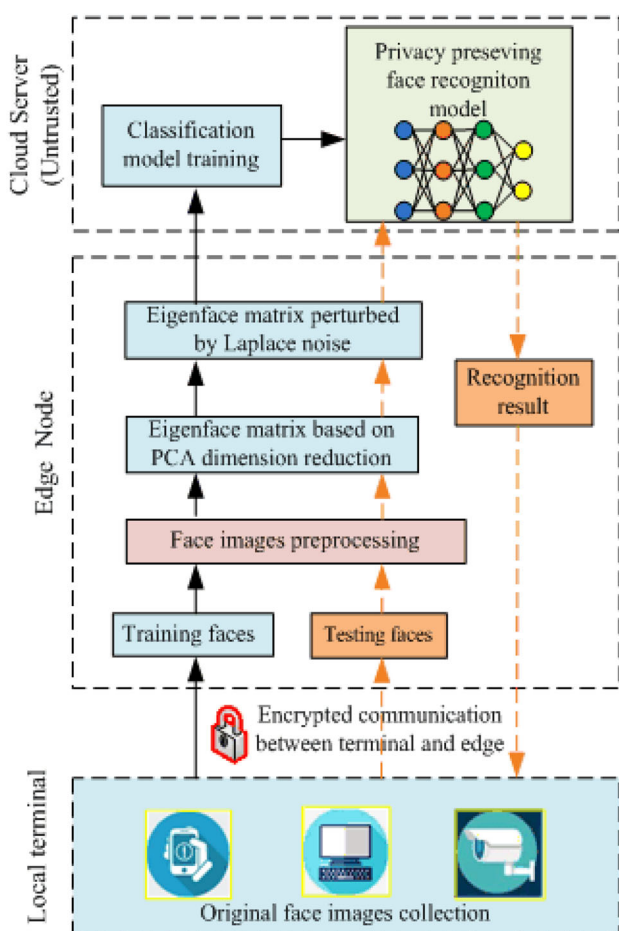


Fig. 2 The flowchart of our proposed framework of EFR system

5.1 Encrypted communication and authentication

To prevent attackers from submitting forged data to the system through illegal terminals to achieve the purpose of disrupting the normal operation of the system or stealing key intermediate information. At the same time, to further ensure the quality of the data and improve the reliability of the data, it is necessary to authenticate the local terminal and establish a secure data exchange channel between the local terminal device and the edge node.

The process of establishing secure communication and identity authentication between the terminal device and the edge node based on the key exchange protocol is briefly described as follows:

- (1) First, the terminal device and the edge node are based on a key exchange protocol, namely the Diffie–Hellman protocol to generate a temporary key. This key is only owned by the edge and the device to ensure subsequent communication security. The temporary key generation process is:
 - (a) The device sends its own ID_i to the edge, requesting a temporary key.
 - (b) The edge node randomly selects three numbers g, p, a , where a is a private parameter; sends g, p and $A = (g^a) \bmod p$ to the device.
 - (c) After the device receives the above data set, it also selects a private parameter b and replies $B = (g^b) \bmod p$ to the edge node as a response. At this time, the device can calculate its temporary key: $K = (A^b) \bmod p$, and the edge node also calculates its own temporary key: $X = (B^a) \bmod p$. Because of $K = X$, the edge and the device got the same temporary key.
- (2) The device applies to the edge node for registration.
 - (a) The device encrypts its own ID_i with the temporary key K and sends it to the edge node as a registration application;
 - (b) After receiving the registration application from the device, the edge node extracts ID_i and uses the private key key and a one-way hash function H with a 64-bit output to generate a registration key for it: $pw_i = H(ID_i, key)$, then sends $c_1 = X(pw_i)$ to the device.

At this point, the device has completed the registration on the edge network.
- (3) The edge node authenticates the device.

- (a) The device receives pw_i , calculates $\delta_i = H(t \oplus pw_i)$, $c = (ID_i, \delta_i, t)$, and replies $c_2 = K(c)$ to the edge node as a response, where t is the current system time.
- (b) The edge node receives feedback from the device at the moment t' . First, check the validity of ID_i . If the format is incorrect, the identity authentication will fail. Secondly, determine the validity of the time interval $\Delta t = t' - t$ and determine whether it is within the expected effective transmission delay time interval. If it times out, the device will be denied access to the edge network.
- (c) When both ID_i and the time interval Δt are valid, the edge node will carry out further calculations:

$$pw_i = H(ID_i, key) \tag{7}$$

$$\delta'_i = H(t \oplus pw_i) \tag{8}$$

If δ'_i matches with δ_i , the terminal device has passed the identity authentication and can access the edge network, and the edge will send the network key to the terminal device. Otherwise, the edge network rejects the terminal device.

- (4) The terminal device and the edge node use AES algorithm to realize data encryption communication.
 - (a) The terminal device computes hash value of the original face D_i , $h_i = H_1(D_i)$, then sends $K(D_i, h_i)$ to the edge node. Edge node decrypts the ciphertext to obtain face image for subsequent processing(model training or recognition).
 - (b) The edge feeds back the recognition result $X(r_i, h'_i)$ containing the hash of original face. The terminal device accepts this result r_i only when h_i and h'_i are equal.

5.2 Image processing and privacy protection

The collected face image is uploaded to the edge computing node via encrypted communication by the registered terminal device. The edge computing node preprocesses the face image, including correcting the angle of the face to a standardized direction, cutting out redundant data, filter out the interference noise, scale the size of the face image

to a predetermined size, etc. Since it is not the focus of this article, the specific process is omitted here.

5.2.1 Constructing eigenface

The vector dimension after vectorization of face images is generally high, so face image recognition is a classic high-dimensional small sample problem. PCA can be used to reduce the dimensionality, and the resulting low-dimensional subspace is generally called the “face space”. Dimensionality reduction based on PCA can find a set of basis vectors used to define the “face space”. These vectors can describe the distribution of face images in space.

Assuming that the number of face image samples is n , the dimension is d , which constitutes an original sample set $D_{n \times d}$, and the vector generated by the i th face image is recorded as x_i , then the average image vector of the sample set is:

$$\mu = \frac{1}{n} \sum_{i=1}^n x_i \tag{9}$$

Then, center the sample data according to μ :

$$x_i = x_i - \mu \tag{10}$$

Further obtain the covariance matrix A :

$$A = \frac{1}{n} \sum_{i=1}^n (x_i - \mu)(x_i - \mu)^T = \frac{1}{n} CC^T \tag{11}$$

Among them, is the set of relative mean image difference of each image:

$$C = [x_1 - \mu, x_2 - \mu, \dots, x_n - \mu] \tag{12}$$

Let the non-zero eigenvalue of matrix CC^T be $\lambda_i (i = 1, 2, \dots, n)$, v_i is the eigenvector corresponding to the non-zero eigenvalue λ_i . The matrix CC^T is orthogonalized and normalized, and the calculated eigenvector u_i is:

$$u_i = \frac{1}{\sqrt{\lambda_i}} \sum_{i=1}^n C v_i, (i = 1, 2, \dots, n) \tag{13}$$

The calculated eigenvectors are sorted by size, and the first k largest eigenvalues and their corresponding orthogonal normalized vectors u_1, u_2, \dots, u_k are selected to form the eigenface space. Algorithm 1 describes the basic process of constructing low-dimensional eigenface based on PCA.

Algorithm 1 Dimension reduction of PCA based face image.

Input: Face image matrix $D \in R^{n \times d}$, number of sample n , attributes d , threshold η for selecting a specific k value.

Output: Low-dimensional spatial dimensions K , Eigenvector matrix U_k as "principal component face".

- 1: Begin:
- 2: Centralize all samples: $x_i \leftarrow x_i - \frac{1}{n} \sum_{i=1}^n x_i$ form a new matrix C ;
- 3: Compute covariance matrix $A = \frac{1}{n} CC^T$;
- 4: Perform eigenvalue decomposition on the covariance matrix A :
 $Au_i = \lambda u_i$, get d eigenvalues λ_i and corresponding eigenvectors u_i ,
 $1 \leq i \leq d$;
- 5: According to the given threshold η , ($0 \leq \eta \leq 1$) select top k
eigenvectors u_i of A to form the eigenface space $U_k = (u_1, u_2, \dots, u_k)$.
- 6: End.

5.2.2 Eigenface perturbation algorithm

The face image after PCA dimensionality reduction, that is, the projection matrix is quite different from the original face. However, because the "eigenface" still retains the main feature information that can reflect the

only in the transmission process, but also in the cloud storage, processing, and publishing process. In [17], the authors proposed an output perturbation method based on the Laplacian mechanism. We review the algorithm in the paper, as follows.

Algorithm 2 Differential privacy eigenface algorithm (PEEP)

Input: Face image matrix $D \in R^{n \times d}$, number of sample n , attributes d , privacy budget parameter ε .

Output: Privacy preserving facial recognition model $DPFRS$.

- 1: Begin:
- 2: Call algorithm 1.
- 3: Output the top k eigenvalues λ_i and their corresponding eigenvectors u_i , such that, $\|u_i\| = 1$, ($1 \leq i \leq k$).
- 4: Form eigenvector matrix (eigenface) $U_k = (u_1, u_2, \dots, u_k)$.
- 5: Generate a random noise column vector e obeys Laplace distribution:
 $\frac{\varepsilon}{2\Delta f} e^{\frac{|x - FSV_i| \varepsilon}{\Delta f}}$, where the sensitivity Δf equals 1, FSV_i represents an index of the flattened image vectors scaled between 0 and 1.
- 6: Add noise to every eigenvector u_i from eigenvector matrix U_k ,
such that, $u'_i = u_i + e$, $1 \leq i \leq k$.
- 7: Produce eigenface matrix after disturbance U'_k .
- 8: Feed perturbed eigenface matrix U'_k to computing center.
- 9: Train the classification model using the randomized data.
- 10: Release the differentially private classification model $DPFRS$.
- 11: End.

corresponding human face, the attacker can completely recover the approximate face image close to the original data through the "eigenface". Therefore, if the edge node directly submits the "characteristic face" to the untrusted server, there will be a greater risk of privacy leakage, not

According to the previous analysis, the larger the feature value, the larger the proportion of the information contained in the corresponding component, which means that the information contained in the corresponding component is more important. However, Algorithm 2

(PEEP) [17] adopts equal noise addition for eigenvector matrix elements, which will introduce some risk. On the one hand, the amount of noise introduced will increase with the increase of the number of matrix elements, which reduces the availability of data; On the other hand, adopting consistent equal noise addition, ignoring the difference in the importance of the information contained between the principal components, resulting in excessive loss of privacy budget.

Based on these considerations, we propose a novel LDP budget allocation algorithm for eigenface based on the parallel characteristics and the output disturbance mechanism of DP [36, 40]. The main idea is to adopt DP budget divisions according to the sensitivity and importance of the information contained in the principal components and add different amounts of noise to different column elements of the eigenvector matrix. Algorithm 3, called PEPI, allocates the LDP budget according to the difference in the proportion of principal component feature information.

6 Theoretical analysis

6.1 PEPI provides ϵ -LDP protection

Theorem 2 In PEPI algorithm, given original data set $D \in R^{n \times d}$ and top k eigenvectors matrix U_k , denote $f(D) = U_k$; then, the sensitivity of the function $f(D)$ equals \sqrt{k} .

Proof In PEPI, the input is a face image, and each face image can be regarded as each vector, which is scaled to the interval $[0,1]$ and then subjected to PCA dimensionality reduction processing. And, a set of feature vectors orthogonal to each other are generated, that is, eigenfaces (select the top K with the highest proportion of eigenvalue information). In PEPI, noise is added to these feature vectors. So, the sensitivity of PEPI can understand the maximum difference between eigenvectors. This can be expressed by the equation:

Algorithm 3 Differential privacy eigenface algorithm based on the proportion of feature information (PEPI).

Input: Face image matrix $D \in R^{n \times d}$, number of sample n , attributes d , threshold η for selecting a specific k value, privacy budget parameter ϵ .

Output: Privacy preserving facial recognition model *PEPIM*.

- 1: Begin:
 - 2: Call Algorithm 1.
 - 3: Output the top k eigenvalues λ_i and corresponding eigenvectors u_i , $1 \leq i \leq k$;
 - 4: Calculate the sum of the top k eigenvalues: $\lambda_{sum} = \sum_{i=1}^k \lambda_i$;
 - 5: **for** $i=1$ to k **do**
 - 6: Compute: $\Delta_i = \frac{\lambda_i}{\lambda_{sum}}$;
 - 7: Take: $\epsilon_i = \Delta_i \epsilon$;
 - 8: Generate a random noise column vector e_i where the whole n elements are i.i.d samples from $Lap(0, \Delta f / \epsilon_i)$;
 - 9: **endfor**
 - 10: Combine all noise column vectors e_i , ($1 \leq i \leq k$) to generate the noise matrix $E = (e_1, e_2, \dots, e_k)$;
 - 11: Add noise to eigenface matrix: $U'_k = U_k + E$.
 - 12: Feed perturbed eigenface matrix U'_k to computing center (the third-party server).
 - 13: Train the classification model using the randomized eigenface.
 - 14: Release privacy preserving face recognition model *PEPIM*.
 - 15: End.
-

$$\Delta f = \max \left\{ \|u'_i - u_i\|_1 \right\}, \tag{14}$$

As shown in the formula (14), u_i represents a flat image vector scaled in the interval $[0, 1]$, and u'_i is adjacent to u_i , $\|u_i\|_2 = 1$, $\|u'_i\|_2 = 1$, $1 \leq i \leq k$.

$$\begin{aligned} \|u'_i - u_i\|_1^2 &= \left(\sum_{j=1}^k |u'_{i,j} - u_{i,j}| \right)^2 \\ &\leq k \sum_{j=1}^k |u'_{i,j} - u_{i,j}|^2 \\ &\leq k \|u'_i - u_i\|_2^2 \\ &\leq k \end{aligned} \tag{15}$$

So, $\|u'_i - u_i\|_1 \leq \sqrt{k}$, where k is the main component.

At this point, the proof of Theorem 2 is completed. \square

Theorem 3 Allocating the LDP budget according to the difference in the proportion of principal component feature information satisfies ϵ -LDP and can provide ϵ -level privacy protection for face images.

Proof According to Algorithm 3, the expression of the noise eigenface matrix is:

$$U' = U + E, \tag{16}$$

where $E = (e_1, e_2, \dots, e_k)$, $e_i (1 \leq i \leq k)$ means a noise column vector in which the whole n elements are i.i.d samples from $Lap(0, \epsilon_i / \Delta f)$.

Let $D_{n \times d}$ and $D'_{n \times d}$ are two arbitrary neighbor matrices, only one data record, that is, one vector is different, for example D_i and D'_i , $1 \leq i \leq n$. There is a mapping relationship: $f : D \rightarrow U_k$, such that, $f(D) = U_k = (u_1, u_2, \dots, u_k)$, and $f(D') = U'_k = (u'_1, u'_2, \dots, u'_k)$. The disturbance output results O on D and D' can be expressed as:

$$O = A(D) = f(D) + \left(Lap_1 \left(\frac{\Delta f}{\epsilon_1} \right), Lap_2 \left(\frac{\Delta f}{\epsilon_2} \right), \dots, Lap_k \left(\frac{\Delta f}{\epsilon_k} \right) \right)$$

. In order to simplify the following description, we remember the output vector $O = (y_1, y_2, \dots, y_k)$.

Then there is:

$$\Pr[A(D) = O] = \prod_{i=1}^d \frac{\epsilon_i}{2\Delta f} e^{-\frac{\epsilon_i}{2\Delta f} |u_i - y_i|} \tag{17}$$

$$\Pr[A(D') = O] = \prod_{i=1}^d \frac{\epsilon_i}{2\Delta f} e^{-\frac{\epsilon_i}{2\Delta f} |u'_i - y_i|} \tag{18}$$

So, we can further get:

$$\begin{aligned} \frac{\Pr[A(D) = O]}{\Pr[A(D') = O]} &= \frac{\prod_{i=1}^k \frac{\epsilon_i}{\Delta f} e^{-\frac{\epsilon_i}{\Delta f} |u_i - y_i|}}{\prod_{i=1}^k \frac{\epsilon_i}{\Delta f} e^{-\frac{\epsilon_i}{\Delta f} |u'_i - y_i|}} \\ &= \prod_{i=1}^k e^{-\frac{\epsilon_i}{\Delta f} (|u_i - y_i| - |u'_i - y_i|)} \\ &= e^{\frac{\epsilon}{\Delta f} \sum_{i=1}^k (|u'_i - y_i| - |u_i - y_i|)} \end{aligned} \tag{19}$$

However, for each $|u'_i - y_i| - |u_i - y_i|$, we regard y_i as a variable. According to the absolute value inequality, the following relationship exists:

$$\begin{aligned} \sum_{i=1}^k (|u'_i - y_i| - |u_i - y_i|) &\leq \sum_{i=1}^k |u'_i - u_i| \\ &\leq \max_{D, D'} \left(\sum_{i=1}^k |u'_i - u_i| \right) \\ &= \Delta f \end{aligned} \tag{20}$$

In the end, we get:

$$\frac{\Pr[A(D) = O]}{\Pr[A(D') = O]} \leq e^\epsilon \tag{21}$$

This completes the proof of Theorem 3. \square

Theorem 4 PEPI (Algorithm 3) provides ϵ -LDP protection for output.

Proof The training of classification models based on perturbed eigenfaces can be seen as an independent transformation process for the output of ϵ -LDP (Theorem 3). Since DP has the property of post-processing immunity, which means that the model training result (PEPIM) and the model testing result (recognition result) are still protected by DP.

Thereby, the PEPI (Algorithm 3) satisfies ϵ -LDP, which completes the proof of Theorem 4. \square

6.2 System security analysis

The system considers the actual application scenarios, and does not assume that the cloud server is completely credible as a third party. Moreover, as a shared storage space, there are other resource users and visitors, and it is not ruled out that individual attackers want to access the image data information in the cloud space and obtain valuable information from it. The system can ensure the safety of the following aspects:

- (1) The transmission of terminal data to the edge is secure.

- (a) The temporary key provides a guarantee for the establishment of secure communication.
 - (b) A terminal device that wants to access the edge network must register by submitting its own ID in order to obtain a legal identity. Then, in the data preprocessing stage, once the edge node finds that a certain device submits fake data, it immediately prohibits its access, refuses to provide it with subsequent functional services, and conducts identity tracking. In this way, it can resist poisoning attacks and collusion attacks.
 - (c) In the identity authentication phase, the edge node judges the validity of the response time from the terminal device. If it times out, even if the ID and registration key provided by the device are correct, it will still be rejected by the edge node. In this way, the terminal device's replay attack on the system is avoided.
 - (d) The encrypted transmission based on the AES algorithm further ensures the security of data communication between the terminal device and the edge node.
- (2) During the transmission process from the edge node to the cloud platform, the transmission data stolen by the attacker is the principal component characteristic data protected by LDP, so that the attacker cannot directly obtain and infer the original face image data. Therefore, this process can ensure that the face image data is safe.
 - (3) User privacy is guaranteed because the edge node submits a face feature data set that meets differential privacy protection, and does not carry any other identifying information associated with the user terminal device, such as *ID* or *location*. Therefore, even if the cloud server leaks relevant information in

the face image processing, the attacker cannot associate the user with the leaked information.

7 Experimental

7.1 Data set

We choose two open source datasets to test the performance of the algorithm, namely a small-scale face image dataset named fetch—olivetti—faces (Olivetti) and a larger-scale face image dataset named lfw—funneled people (LFW). The Olivetti data set is taken by the Cambridge Laboratory in the UK and contains photos of 40 different individuals. The LFW data set is a database compiled by the Computer Vision Laboratory of Massachusetts State University Amherst, and is usually used to study face recognition problems in unrestricted environments. LFW contains more than 13,000 gray-scale face images collecting on the Internet.

7.1.1 Feature extraction

We use PCA to reduce the dimensionality of high-dimensional images, which can drop the complexity of subsequent image processing while maximizing the preservation of the original information. Of course, the more features are retained at the end, the less information is lost, but the computational complexity is higher. We implement parameters tuning using the accumulative contribution threshold η . Figure 3 shows the cumulative explained variance ratio with the number of principal components K .

Figure 4 shows the proportion of the eigenvalues of the top 10 principal components in their respective data sets. Usually, we select the first K eigenvectors corresponding to the eigenvalues to describe the original face space. This set of orthogonal vectors is called eigenface. Eigenface shows the basic features of the input image, and any face image is a combination of a group of eigenface. Figure 5 shows the eigenface belonging to the above two data sets when $K=10$.

7.1.2 Eigenface disturbance

The eigenface hides the most important biological characteristics of the face database, and with the help of effective face reconstruction technology, the original face image information can be restored through the eigenface. Therefore, it is necessary to protect the privacy of eigenfaces. Figure 6 shows the eigenface (Fig. 5b) after implementing the PEPI algorithm to add noise perturbation (privacy budget $\epsilon = 0.1$). As shown in the figure, at this time, it is no longer possible to detect any biological

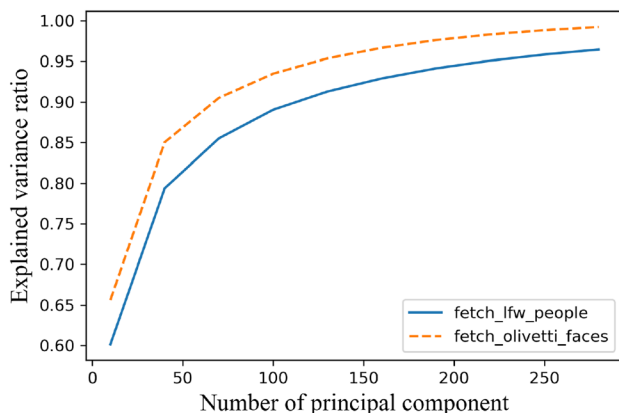


Fig. 3 Explained variance ratio varies with K

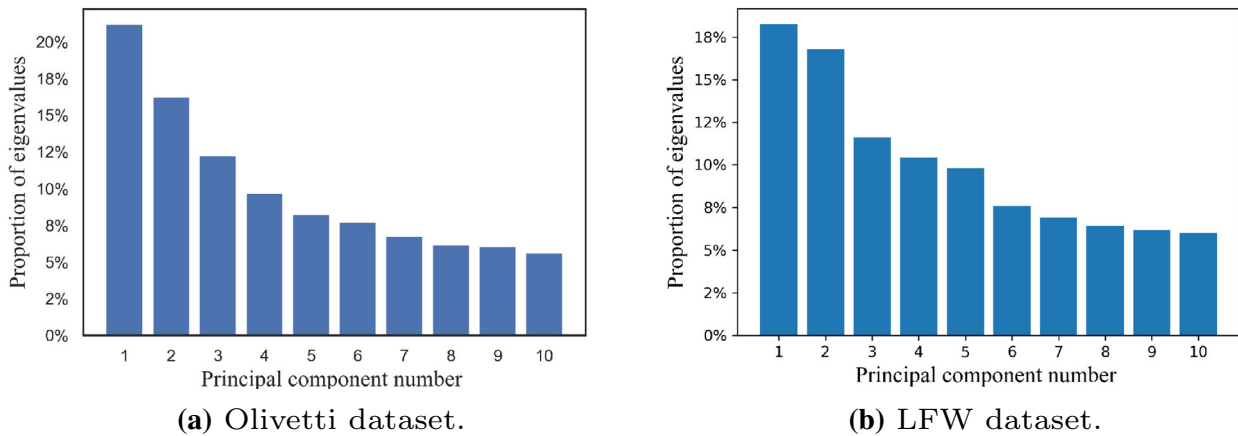
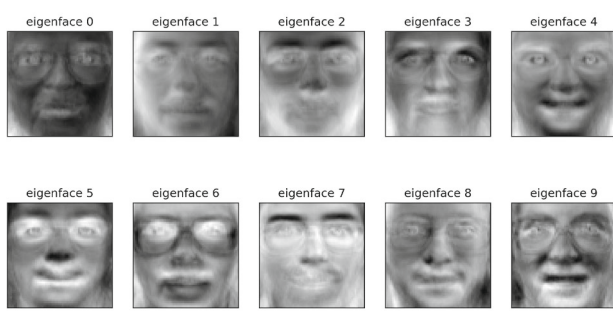
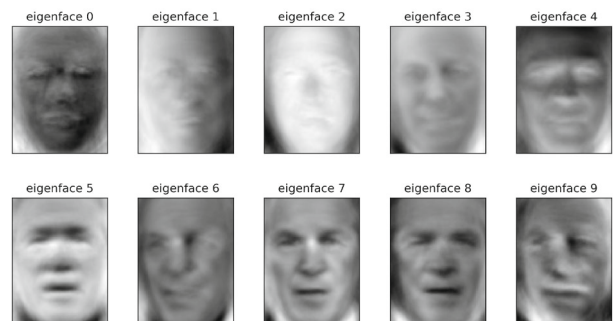


Fig. 4 The proportion of eigenvalues of the top 10 principal components



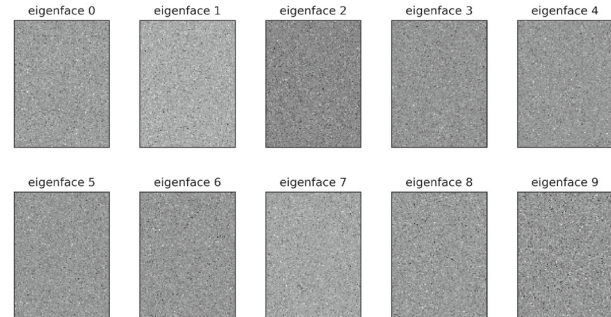
(a) Eigenfaces of Olivetti dataset ($K=10$)



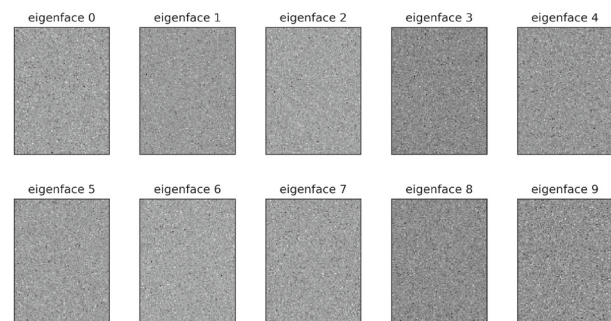
(b) Eigenfaces of LFW dataset ($K=10$)

Fig. 5 Part of the sample images in the source input data set (the training set used to build the PCA model) are processed for dimensionality reduction, and only a set of eigenfaces generated by the first 10 most important eigenvalues are retained

features of the face image from the eigenface with naked eyes. Even in the most relaxed situation (privacy budget $\varepsilon = 10$), the disturbed feature face still cannot be observed by naked eyes, as shown in Fig. 6b.



(a) Eigenfaces after disturbance, $\varepsilon=0.1$

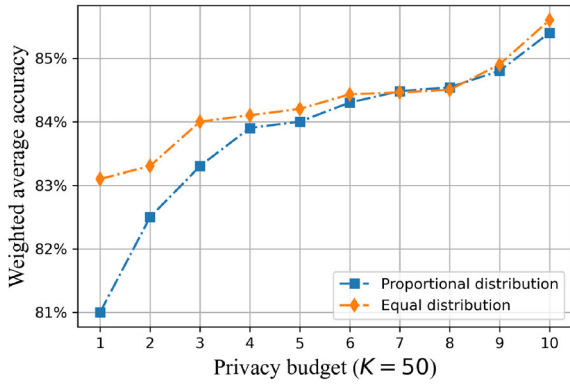


(b) Eigenfaces after disturbance, $\varepsilon=10$

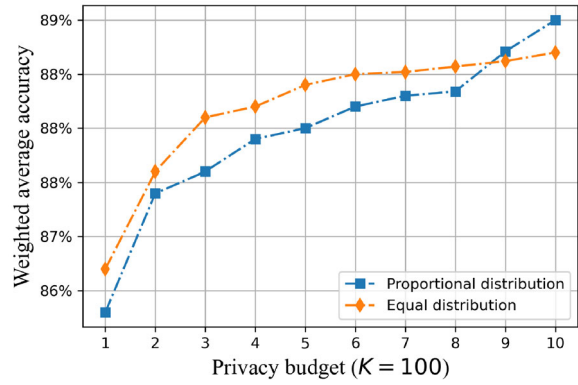
Fig. 6 Perturb the eigenface (LFW dataset), $\varepsilon = 0.1, 10$. The smaller the privacy budget ε , the more obscure the feature information

7.2 Model training and recognition

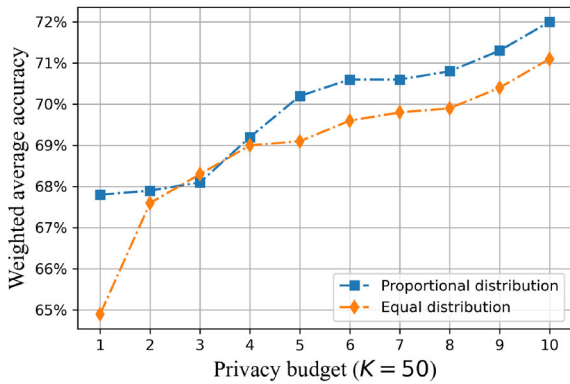
We use Tensorflow environment and Python language programming for simulation experiments. The server used has the following resource configuration: CPU Intel Xeon CPU E5-2620 v4 2.10 GHz, Hynix DDR4 16 G memory, hard disk with 300 G (solid state) plus 2 T (mechanical). The recognition performance test algorithm uses support



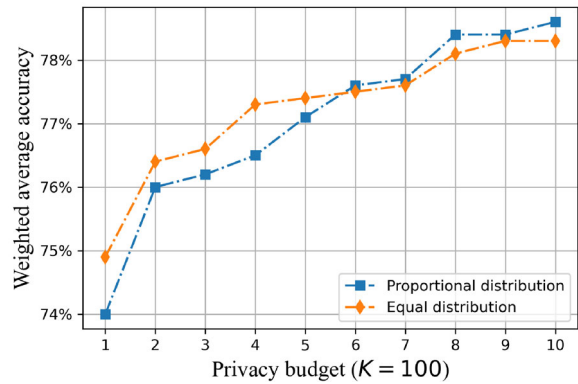
(a) Accuracy Vs. ϵ on Olivetti ($K = 50$).



(b) Accuracy Vs. ϵ on Olivetti ($K = 100$).

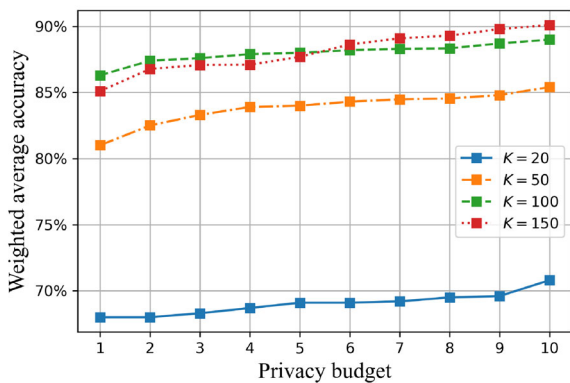


(c) Accuracy Vs. ϵ on LFW ($K = 50$).

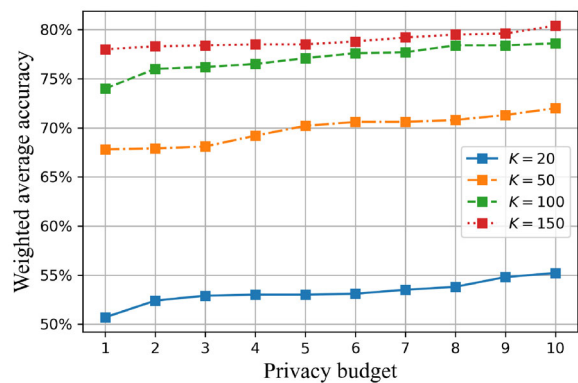


(d) Accuracy Vs. ϵ on LFW ($K = 100$).

Fig. 7 Comparison of FR performance between PEPI (privacy budget proportional distribution) and PEEP (privacy budget equal distribution) on two dataset, $K = 50, 100$



(a) PEPI performance Vs. ϵ on Olivetti.



(b) PEPI performance Vs. ϵ on LFW.

Fig. 8 The FR performance of the PEPI changes with the privacy budget ϵ when the principal component K takes four different values: 20, 40, 100 and 150

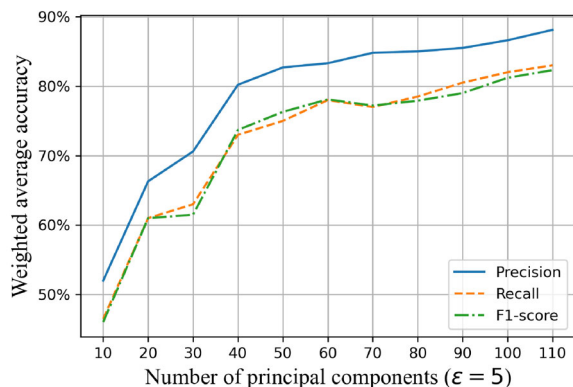
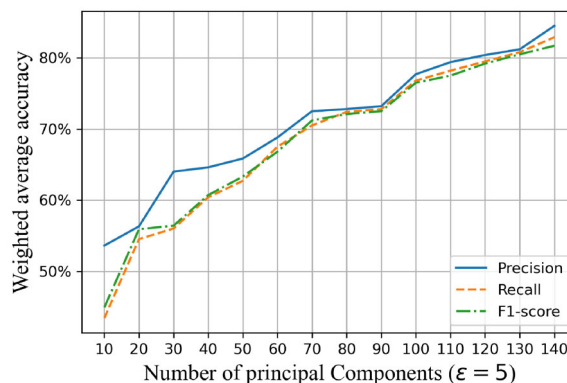
(a) PEPI performance Vs. K on Olivetti.(b) PEPI performance Vs. K on LFW.

Fig. 9 The FR performance of the PEPI changes with the number of principal components K when $\epsilon = 5$

vector machine (SVM) to perform multi-class recognition of face images after PCA dimensionality reduction.

7.2.1 Performance variance with respect to ϵ

We used the weighted average of training accuracy, recall, and F1 scores to reflect the impact of different levels of privacy budget ϵ on the performance of the algorithm in two data sets, and plotted the data, as shown in Figs. 7 and 8.

Figure 7 shows the comparison between the PEPI algorithm proposed in this paper and the existing PEEP algorithm [17]. It can be seen from the figure that when the number of principal components K is constant, increasing the privacy budget improves the accuracy, because a higher privacy budget imposes less randomized disturbance on the eigenface. In addition, when $1 < \epsilon < 4$, the PEEP algorithm that allocates the privacy budget by the ratio of information can obtain a slightly higher accuracy rate than the PEPI algorithm that allocates the privacy budget based on the information ratio. When $\epsilon > 4$, as the privacy budget increases, the performance of the PEPI algorithm is closer to or even surpasses the performance of the PEEP algorithm.

Figure 8 shows the changes in the performance of the PEPI algorithm with the privacy budget when the K values are 20, 50, 100, and 150. Through comparison, we find that the number of principal components that retain the original image data after dimensionality reduction also directly affects the accuracy of the final classification. The smaller the K value, the less the proportion of original image feature information is retained, which will restrict the performance of later image analysis to a certain extent.

However, when the K value reaches a certain value (for example, 100) and the reduced image can cover more than 95% of the feature information of the original image, the

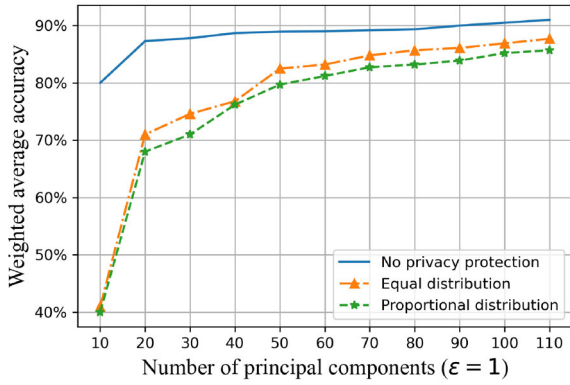
performance of the algorithm will be less affected by changes in privacy budget. There is almost no difference in the amount of information contained in $K = 150$ and $K = 100$ images for Olivetti. However, difference lies in the privacy budget allocated to each retained feature. When the total privacy budget is the same, the privacy budget allocated to each feature of $K=150$ is smaller than that of $K = 100$. The smaller the privacy budget allocated to each feature, the stronger added noise perturbation. This leads to $K = 100$ behaves better than $K = 150$ for the lower privacy budgets, as shown in Fig. 8a.

7.2.2 Performance variance with respect to K

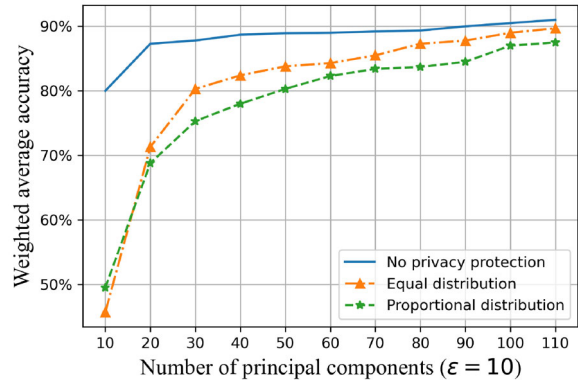
PCA retains the main feature components, and the value of the principal components K directly affects the proportion of these feature components that contain the original complete information, which in turn affects the accuracy of face recognition. We keep the privacy budget ϵ at a fixed value (for example, 0.5, 1, 5, 10, 100), only change the number of principal components K , and then compare the accuracy of face recognition in three different situations: no privacy protection, equal allocate privacy budgets and allocate privacy budgets based on the proportion of feature information.

Figure 9 shows that the face recognition performance of the PEPI algorithm changes with the principal component when $\epsilon = 5$ through three indicators of weighted average accuracy: precision, recall, and F1-score. As shown in the figure, when the privacy budget is constant, the overall trend of the accuracy is significantly improved with the increase of the value of the principal component. However, when K reaches a certain size, the increase in accuracy will tend to be flat.

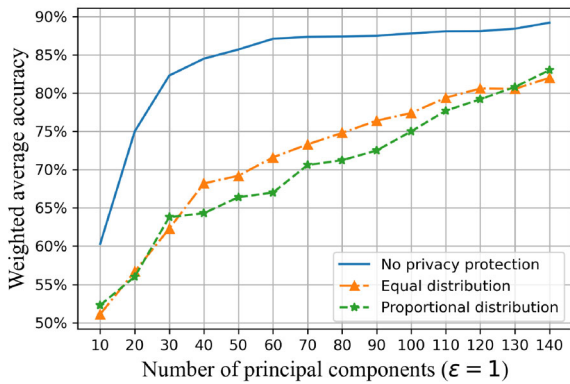
Figure 10 shows the classification accuracy on the data set processed by the PEPI algorithm when $\epsilon = 1, 10$, and



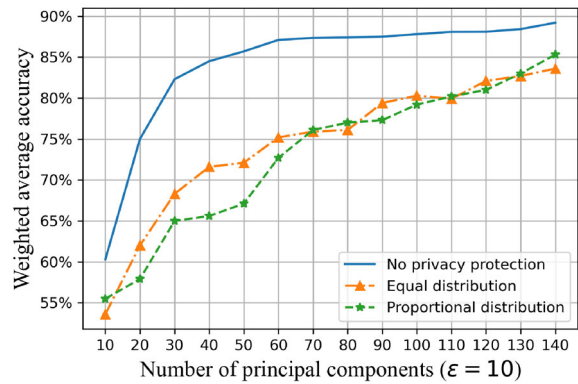
(a) Accuracy Vs. K on Olivetti ($\epsilon = 1$).



(b) Accuracy Vs. K on Olivetti ($\epsilon = 10$).

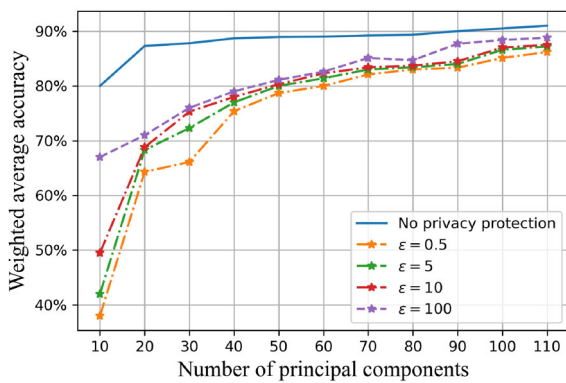


(c) Accuracy Vs. K on LFW ($\epsilon = 1$).

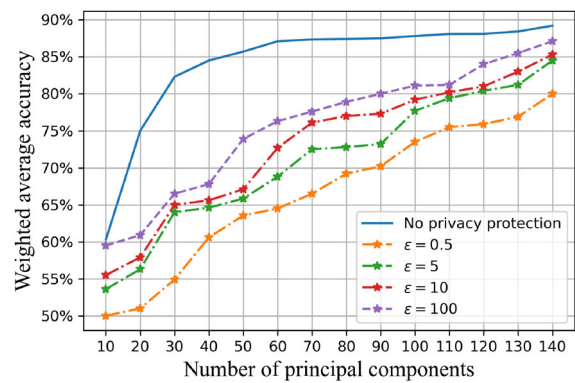


(d) Accuracy Vs. K on LFW ($\epsilon = 10$).

Fig. 10 Comparison of the accuracy of FR in three different situations: no privacy protection, PEPI (privacy budget proportional distribution) and PEEP (privacy budget equal distribution)



(a) Accuracy Vs. K on Olivetti (different ϵ).



(b) Accuracy Vs. K on LFW (different ϵ).

Fig. 11 The FR performance varies with the number of principal components K under different values of ϵ . Here is a comparison of the difference in performance when the privacy budget ϵ takes four different values: 0.5, 5, 10, and 100

Table 1 Security comparison of related privacy-preserving FR schemes

References	Methods	Eigenface	Defensible attack			
			Data poisoning	Differential	Man-in-the-middle	Tamper
Erkin et al. [13]	PH cryptosystem	Non-privacy	✓			
Sadehi et al. [18]	PH cryptosystem	Non-privacy	✓			✓
Xiang et al. [14]	FH cryptosystem	Non-privacy	✓		✓	
Chamikara et al. [17]	LDP	Privacy		✓	✓	
The proposed	LDP, authentication	Privacy	✓	✓	✓	✓

compares it with the two cases: no disturbance and PEEP. As shown in the figure, when the value of K increases from 10 to 20, the performance improves rapidly. After K increases to 20, the performance gradually improves. This is because the first 20–40 principal components represent the most important features of the original face image. Although the performance improvement is not too obvious when K is a value after 40, the overall performance is improved, which also shows that the more principal components retained, the better the performance.

In addition, we also compared the changes of face recognition performance with principal components under different ϵ values (three conventional values: 0.5, 5, 10, and an extreme value: 100), as shown in Fig. 11. It can be seen that the larger the privacy budget and the number of principal components, the better the performance.

7.3 Security comparison

Table 1 shows the security comparison of related privacy-preserving face recognition schemes. The commonality of each scheme is that face recognition is processed in the cloud. The difference lies in the privacy protection method and whether the eigenface is private for the cloud server. Outsourcing can reduce the computational complexity for face image owners and authenticated users. Since eigenfaces still contain some private information, privacy needs to be protected before outsourcing. In [13, 14, 18], a homomorphic cryptosystem is utilized to protect the privacy of faces. The projections of the three schemes are all processed in the cloud, but none of the eigenfaces are private to the cloud server. Camara et al. [17] uses LDP technology to achieve eigenface perturbation, however, data poisoning attacks and tampering attacks by malicious users are not addressed.

8 Conclusions

We propose a user privacy protection scheme suitable for FR application scenarios based on EC. This framework takes into account the privacy protection issues during the

entire cycle from collection to recognition of face images. A new mechanism of PEPI using the characteristics of LDP is proposed, which combines the proportion of principal component feature information to perform data disturbance to realize the privacy protection of FR users.

Our scheme does not require a trusted third party. The edge center uses localized processing methods to apply randomization before the image reaches the untrusted server. In addition, adjusting the privacy budget parameters according to the proportion of principal component feature information can achieve the maximum balance of privacy protection and data utility compared with existing solutions. Of course, there are still some issues worthy of further research in the future, such as improving the security of the key exchange process, edge-based processing with private multi-dimensional classification information and heterogeneous data.

Author contributions All authors contributed to the study conception and design. YX designed the scheme, performed the experiment and wrote the paper. PL designed the experiment. NN, BBG and DT provided amendments and comments on the scheme and the experiment. JZ reviewed the paper.

Funding This work is sponsored by the National Natural Science Foundation of P. R. China (Grant Nos. 61872196, 61872194, 61902196, 62102194 and 62102196), Six Talent Peaks Project in Jiangsu Province (Grant No. RJFW111), Graduate Research and Innovation Projects of Jiangsu Province (Grant Nos. KYCX19_0909, KYCX19_0911, KYCX20_0759, KYCX21_0787, KYCX21_0788, KYCX21_0799, KYCX22_1019 and KYCX22_1027), Natural Science Research Project in Colleges and Universities of Jiangsu Province (Grant No. 21KJB510020).

Data availability The data and material that support the findings of this study are available from the corresponding author upon reasonable request.

Code availability The code of this study are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors declare that they have no conflicts of interest.

Ethical approval This material has not being published in whole or in part elsewhere.

Research involving human and/or animal participants This study does not involve human participants and/or animal research, which is used for non-life science journals.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Ren, P., Xiao, Y., Chang, X., Huang, P.-Y., Li, Z., Chen, X., Wang, X.: A comprehensive survey of neural architecture search: challenges and solutions. *ACM Comput. Surv.* **54**(4), 1–34 (2021)
- Fan, T., Xu, J.: Image classification of crop diseases and pests based on deep learning and fuzzy system. *Int. J. Data Wareh. Min.* **16**(2), 34–47 (2020)
- Ali, M.U., Ahmed, S., Ferzund, J., Mehmood, A., Rehman, A.: Using PCA and factor analysis for dimensionality reduction of bio-informatics data. *Int. J. Adv. Comput. Sci. Appl.* **08**(5), 415–426 (2017)
- Alsmirat, M.A., Al-Alem, F., Al-Ayyoub, M., Jararweh, Y., Gupta, B.: Impact of digital fingerprint image quality on the fingerprint recognition accuracy. *Multimed. Tools Appl.* **78**(3), 3649–3688 (2019)
- Mousavi, M., Rezazadeh, J., Sianaki, O.A.: Machine learning applications for fog computing in IoT: a survey. *Int. J. Web Grid Serv.* **17**(4), 293–320 (2021)
- Zhu, M., Meng, S., Li, J., Yan, S.: Mobile service selection in edge and cloud computing environment with grey wolf algorithm. *Int. J. Web Grid Serv.* **18**(3), 229–249 (2022)
- Li, S., Qin, D., Wu, X., Li, J., Li, B., Han, W.: False alert detection based on deep learning and machine learning. *Int. J. Semant. Web Inf. Syst.* **18**(1), 1–21 (2022)
- Bowyer, K.W.: Face recognition technology: security versus privacy. *IEEE Technol. Soc. Mag.* **23**(1), 9–19 (2004)
- Aamir, H.: San Francisco becomes the first us city to ban facial recognition by government agencies. <https://www.techspot.com/news/80088-san-francisco-becomes-first-us-city-ban-facial.html> (2019)
- Mohassel, P., Zhang, Y.: Secureml: a system for scalable privacy-preserving machine learning. In: *Security and Privacy*, pp. 19–38 (2017)
- Salem, M., Taheri, S., Yuan, J.S.: Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system. *Computers* **8**(1), 3 (2018)
- Xiong, X., Fei, C., Huang, P., Tian, M., Hu, X., Badong, C., Qin, J.: Frequent itemsets mining with differential privacy over large-scale data. *IEEE Access* **6**, 28877–28889 (2018)
- Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Toft, T.: Privacy-preserving face recognition. In: *Privacy Enhancing Technologies, International Symposium, Pets, Seattle, August*, pp. 235–253 (2009)
- Xiang, C., Tang, C., Cai, Y., Xu, Q.: Privacy-preserving face recognition with outsourced computation. *Soft Comput.* **20**(9), 3735–3744 (2016)
- Lu, W., Varna, A.L., Min, W.: Security analysis for privacy preserving search of multimedia. In: *IEEE International Conference on Image Processing*, pp. 2093–2096 (2010)
- Zhang, X., Fu, C., Meng, X.: Facial image publication with differential privacy. *J. Image Graph.* **23**(9), 1305–1315 (2018)
- Chamikara, M., Bertok, P., Khalil, I., Liu, D., Camtepe, S.: Privacy preserving face recognition utilizing differential privacy. *Comput. Secur.* **97**, 101951 (2020)
- Sadeghi, A.-R., Schneider, T., Wehrenberg, I.: Efficient privacy-preserving face recognition. In: *International Conference on Information Security and Cryptology*, pp. 229–244 (2009)
- Haghighat, M., Zonouz, S., Abdel-Mottaleb, M.: CloudID: trustworthy cloud-based and cross-enterprise biometric identification. *Expert Syst. Appl.* **42**(21), 7905–7916 (2015)
- Cai, Y., Tang, C.: Securely outsourced face recognition under federated cloud environment. In: *2016 15th International Symposium on Parallel and Distributed Computing (ISPDC)* (2016)
- Ma, Y., Wu, L., Gu, X., He, J., Yang, Z.: A secure face-verification scheme based on homomorphic encryption and deep neural networks. *IEEE Access* **5**, 16532–16538 (2017)
- Ma, Z., Liu, Y., Liu, X., Ma, J., Ren, K.: Lightweight privacy-preserving ensemble classification for face recognition. *IEEE Internet Things J.* **6**(3), 5778–5790 (2019)
- Terhorst, P., Riehl, K., Damer, N., Rot, P., Kuijper, A.: PE-MIU: a training-free privacy-enhancing face recognition approach based on minimum information units. *IEEE Access* **8**, 93635–93647 (2020)
- Newton, E.M., Sweeney, L., Malin, B.: Preserving privacy by de-identifying face images. *IEEE Trans. Knowl. Data Eng.* **17**(2), 232–243 (2005)
- Bhattacharai, B., Mignon, A., Jurie, F., Furon, T.: Puzzling face verification algorithms for privacy protection. In: *International Workshop on Information Forensics and Security* (2014)
- Letournel, G., Bugeau, A., Ta, V.-T., Domenger, J.-P.: Face de-identification with expressions preservation. In: *2015 IEEE International Conference on Image Processing (ICIP)*, pp. 4366–4370. IEEE (2015)
- Sun, Z., Meng, L., Ariyaeeinia, A.: Distinguishable de-identified faces. In: *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, vol. 4, pp. 1–6. IEEE (2015)
- Meden, B., Malli, R.C., Fabijan, S., Ekenel, H.K., Štruc, V., Peer, P.: Face deidentification with generative deep neural networks. *IET Signal Process.* **11**(9), 1046–1054 (2017)
- Sun, Q., Ma, L., Oh, S.J., Van Gool, L., Schiele, B., Fritz, M.: Natural and effective obfuscation by head inpainting. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 5050–5059 (2018)
- Othman, A., Ross, A.: *Privacy of Facial Soft Biometrics: Suppressing Gender But Retaining Identity*. Springer, Cham (2014)
- Guo, R., Qi, H.: Facial feature parsing and landmark detection via low-rank matrix decomposition. In: *2015 IEEE International Conference on Image Processing (ICIP)*, pp. 3773–3777 (2015)
- Fan, L.: Image pixelization with differential privacy. In: *IFIP Conference on Data and Applications Security and Privacy* (2018)
- Croft, W.L., Sack, J.-R., Shi, W.: Differentially private obfuscation of facial images. In: *International Cross-Domain Conference for Machine Learning and Knowledge Extraction*, pp. 229–249. Springer (2019)

34. Croft, W.L., Sack, J.-R., Shi, W.: Obfuscation of images via differential privacy: from facial images to general images. *Peer-to-Peer Netw. Appl.* **14**(3), 1705–1733 (2021)
35. Liu, C., Yang, J., Zhao, W., Zhang, Y., Mu, C.: Face image publication based on differential privacy. *Wirel. Commun. Mob. Comput.* **2021**(9), 1–20 (2021)
36. Qing-Qing, Y.E., Meng, X.F., Zhu, M.J., Huo, Z., Information, S.O.: Survey on local differential privacy. *J. Softw.* **29**(7), 1981–2005 (2018)
37. Zhu, K., Van Hentenryck, P., Fioretto, F.: Bias and variance of post-processing in differential privacy. In: *Proceedings of the AAAI Conference on Artificial Intelligence* (2021)
38. Chang, X., Nie, F., Wang, S., Yang, Y., Zhou, X., Zhang, C.: Compound rank- k projections for bilinear analysis. *IEEE Trans. Neural Netw. Learn. Syst.* **27**(7), 1502–1513 (2015)
39. Feng, W., Zhao, Y., Deng, J.: Application of SVM based on principal component analysis to credit risk assessment in commercial banks. In: *2009 WRI Global Congress on Intelligent Systems*, vol. 4, pp. 49–52. IEEE (2009)
40. Zhu, T., Gang, L., Zhou, W., Yu, P.S.: Differentially private data publishing and analysis: a survey. *IEEE Trans. Knowl. Data Eng.* **29**(8), 1619–1638 (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

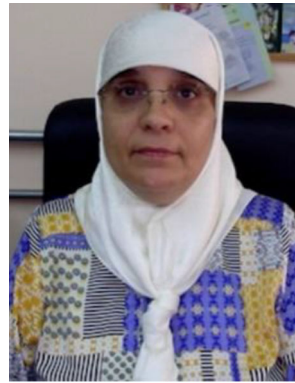


Yun Xie is currently a PhD student in the School of Computer Science, Nanjing University of Posts and Telecommunications, and her research interests are cloud computing, distributed learning, and privacy protection.



Peng Li received the Ph.D. degree in computer science and technology from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2013. He is currently a Professor and Master Supervisor with the School of Computer Science, Software and Cyberspace Security, Nanjing University of Posts and Telecommunications. He has presided over ten national, provincial and ministerial projects. His main research interests

include computer communication networks, wireless sensor networks, and information security. He is a member of the CCF, the IEEE and the IEEE Communications Society.



Nadia Nedjah graduated in 1987 in Systems Engineering and Computation and in 1990 obtained an M.Sc. degree also in Systems Engineering and Computation. Both degree were obtained from University of Annaba, Algeria. Since 1997 she holds a Ph.D. degree from University of Manchester—Institute of Science and Technology, UK. She joined the Department of Electronics Engineering and Telecommunications of the Engineering Faculty of the State University of Rio de Janeiro as an Associate Professor. Between 2009 and 2013, she was the head of the Intelligent System research area in the Electronics Engineering Post-graduate program of the State University of Rio de Janeiro, Brazil. She is the founder and the Editor-in-Chief of the International Journals of High Performance System Architecture and of Innovative Computing Applications, both published by Inderscience, UK. She published three authored books about Functional and Re-writing Languages, Hardware/Software Co-design for Systems Acceleration and Hardware for soft Computing vs. Soft Computing for Hardware. She (co-)guest edited more than 20 special issues for high impact journals and more than 45 organized books on computational intelligence related topics, such as Evolvable Machines, Genetic Systems Programming, Evolutionary Machine Design: Methodologies and Applications and Real-World Multi-Objective System Engineering. She (co-)authored more than 120 journal papers and more than 200 conference papers. She is Associate Editor of more than 10 international journals, such as the Francis & Taylor's International Journal of Electronics, Elsevier's Integration, The VLSI Journal and Microprocessors and Microsystems and IET's Computer & Digital Techniques. She organized several major conferences related to computational intelligence, such as the 7th edition of Intelligent Systems Design and Application and the 5th edition of Hybrid Intelligent Systems. She also was one of the founder of the International Conference on Adaptive and Intelligent Systems. (More details can be found at her homepage: <http://www.eng.uerj.br/~nadia/english.html>.)



Brij B. Gupta is working as Director of International Center for AI and Cyber Security Research, Incubation and Innovations, and Full Professor with the Department of Computer Science and Information Engineering (CSIE), Asia University, Taiwan. In more than 17 years of his professional experience, he published over 470 papers in journals/conferences including 30 books and 10 Patents with over 17000 citations. He has received numerous national and international awards including Canadian Commonwealth Scholarship (2009), Faculty Research Fellowship Award (2017), MeitY, GoI, IEEE GCCE outstanding and WIE paper awards and Best Faculty Award (2018 & 2019), NIT KKR, respectively. He is also selected in the 2022, 2021 and 2020 Stanford University's ranking of the world's top 2% scientists. He is also a visiting/adjunct professor with several universities worldwide. He is also an IEEE Senior Member (2017) and also selected as 2021 Distinguished Lecturer in IEEE CTSoc. Dr Gupta is also serving as Member-in-

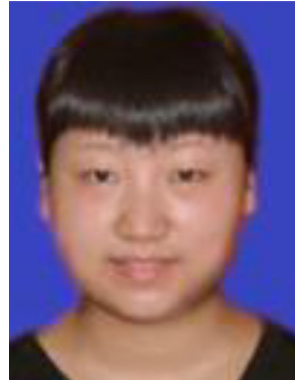
Large, Board of Governors, IEEE Consumer Technology Society (2022–2024). Prof Gupta is also leading IJSWIS, IJSSCI, STE and IJCAC as Editor-in-Chief. Moreover, he is also serving as lead-editor of a Book Series with CRC and IET press. He also served as TPC members in more than 150 international conferences also serving as Associate/Guest Editor of various journals and transactions. His research interests include information security, Cyber physical systems, cloud computing, blockchain technologies, intrusion detection, AI, social media and networking.



David Taniar received his MSc and PhD in Computer Science, from Swinburne University of Technology and Victoria University, respectively. His research is in the area of Big Data Management, covering the 3Vs of Big Data (Volume, Variety, and Velocity). In Big Data Volume, he works on parallel databases, in which he has published a book in this topic (High Performance Parallel Database Processing, Wiley 2008). In Big Data Variety, he

works on various data structures for data warehousing, especially for

non-relational data. And in Big Data Velocity, he works on IoT data processing, where he has completed IoT projects for manufacturing, railway, environment and ecology, utility, and healthcare. He has published more than 150 journal papers in various areas of data management. He is the Founding Editor-in-Chief of two SCI-E journals (Data Warehousing and Mining, and Web and Grid Services). He is currently an Associate Professor at Monash University, Australia.



Jindan Zhang now is an associate professor in Xianyang Vocational Technical College and obtained her PhD from Xidian University, her main research interests include public key cryptography and cloud security. She has published about 20 papers in the field of information security including IEEE transaction journals.