IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 December 2023, accepted 26 January 2024, date of publication 7 February 2024, date of current version 23 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3363494

RESEARCH ARTICLE

Research on Local Fingerprint Image Differential Privacy Protection Method Based on Clustering Algorithm and Regression Algorithm Segmentation Image

CHAO LIU, ZHAOLONG ZHI, WEINAN ZHAO, AND ZHICHENG HE
College of Communication and Electronic Engineering, Qiqihar University, Qiqihar 161000, China

Corresponding author: Chao Liu (00819@qqhru.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 42271409, in part by the Fundamental Research Funds in Heilongjiang Provincial Education Department under Grant 145109216, and in part by the Heilongjiang Province 2023 Innovation and Entrepreneurship Training Program for College Students under Grant S202310232107.

ABSTRACT Fingerprint recognition technology has been extensively employed across various sectors of society. The direct publication of fingerprint images leads to the disclosure of sensitive information. According to the fingerprint image identification process, the fingerprint image protection process is actually the fingerprint image feature point location information, quantity information, type information protection. To address this issue, this paper proposes a machine learning and differential privacy-based fingerprint image publish algorithm called DP-RKLAP. The algorithm establishes a protected process to match feature points in fingerprint images and employs a clustering algorithm for initial segmentation of the images (KLAP). Additionally, a multinomial regression algorithm is applied to preprocess the segmented image regions, constructing a regression model that accurately determines fluctuation amplitudes for precise segmentation of protected areas containing matching feature points (RKLAP). Considering the uncertainty in segmentation caused by uncertain feature point locations in fingerprint images, we introduce a dynamic allocation method (DP) for privacy budget allocation. The exponential mechanism leverages the relationship between the number of matching feature points and segmentation regions to dynamically allocate privacy budgets within the Laplace mechanism framework of differential privacy technique, thereby achieving local protection publish for fingerprint images. This reduction in sensitivity effectively mitigates noise errors during the process of privacy protection, thereby achieving a balance between privacy and usability of the fingerprint images. Experimental results confirm that our proposed method successfully achieves privacy protection during the publishing process of fingerprint images, while still maintaining high usability after protected publishing and matching verification using real-world datasets.

INDEX TERMS Clustering, regression, differential privacy, publishing fingerprint image, privacy budget allocation.

I. INTRODUCTION

The continuous development of modern information technology has led to the widespread utilization of fingerprint identification technology in various domains and products. However, this aforementioned technology presents a possibility for compromising human biometric privacy. In October 2020, the China Academy of Information and Communications Technology (CAICT), the Telecommunications Terminal Industry Association (TTIA), the Internet Society of China (ISOC), and other organizations jointly published the ''Research Report on Biometric Privacy Protection'' [1]. This report emphasized the necessity for innovative means to safeguard biometric privacy, urging vigorous enhancement in

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

fundamental theoretical research as well as active exploration and development of technical measures. In 2018, India's identification system known as Aadhaar encountered a massive database leakage incident that exposed personal information belonging to over one billion users [2]. The leaked data encompassed highly sensitive details such as fingerprints and irises. As science and technology continue to advance rapidly, ensuring privacy protection for human biometric features is becoming increasingly crucial [3]. Countries worldwide have expressed profound concerns regarding this matter by strengthening their standard systems for biometric privacy protection, establishing assessment mechanisms, and enhancing overall safeguards.

Fingerprints constitute a crucial component of human biometric features, and safeguarding the privacy of fingerprint images is imperative for information security. The protection process of fingerprint images is closely intertwined with the recognition process, wherein the matching method employed in fingerprint image recognition serves as a pivotal step in fingerprint recognition technology. The acquisition procedure of the fingerprint acquisition device projects three-dimensional fingerprints onto a two-dimensional plane [4], preprocesses the two-dimensional fingerprint image to enhance its quality [5], and subsequently extracts the unique features embedded within it. Directly publishing unprotected fingerprint images is highly likely to result in significant breaches of personal privacy. Traditional technical measures focus on preventing these images from being misappropriated [6]. However, due to the wide application of fingerprint identification systems, complete security cannot be guaranteed for all databases storing such images [7]. At the same time, publishing fingerprint images is an inevitable security verification process. Therefore, adding privacy protection during the process of publishing fingerprint images can effectively protect this sensitive information.

Most of the existing fingerprint image protection methods derive from image protection technology. Early techniques for protecting images primarily involved masking sensitive information. However, physical masking makes the images unusable. Therefore, researching data masking techniques that resist cracking has become an important focus for image protection. Among these techniques, anonymization [8], [9] and encryption [10], [11] are commonly used means of safeguarding images. Anonymization involves generalizing data to prevent accurate identification by attackers and generating multiple responses when querying databases [12], [13], [14]. One classic application of anonymization is K-anonymity technique [15]. However, it also exposes certain sensitive information that can be obtained with background knowledge gained from multiple queries. Data encryption is another method for protecting image data, including secure multiparty computation [16], homomorphic encryption [17], and other approaches. Moreover, anonymization and data encryption techniques can be compromised by background attacks. However, since fingerprint images are published for identity authentication purposes, pure anonymization or encryption techniques only guarantee single protection during the publishing process without simultaneously regulating both privacy and usability. Therefore, using differential privacy techniques that regulate the protective effect of fingerprint images represents a better approach to privacy protection. The technique of differential privacy protection [18], [19] ensures the safeguarding of sensitive information irrespective of the attacker's level of background knowledge. Meanwhile, the degree of privacy protection can be adjusted by controlling the parameter variable ε in the definition of differential privacy [20], [21]. This allows for a reasonable and adjustable planning of both privacy and usability aspects in fingerprint images while preventing excessive privacy measures from severely compromising image usability [22], [23], [24]. By adjusting the amount of noise added to fingerprint images based on sensitive information rather than overall dataset data, it avoids adding significant noise that could potentially destroy useful data in the dataset and achieves enhanced privacy protection [25], [26], [27].

Most of the existing image differential privacy techniques are primarily applied to face images for privacy protection [28], with limited research on the privacy protection of fingerprint images [29], [30]. The core principle of differential privacy technology is to introduce noise into the protected data [31], thereby perturbing the data and achieving distortion effects, ultimately ensuring data protection.

The application of differential privacy technology in protecting fingerprint images is as follows: In the literature [29], low-rank matrix factorization technology is used to decompose the two-dimensional image matrix of a fingerprint image. Perturbation noise is then introduced into the resulting low-rank matrix using differential privacy, thereby achieving privacy protection for the fingerprint image. However, this method encounters significant global sensitivity during the process due to uncertainty in the size of the fingerprint image, which subsequently leads to increased errors caused by added perturbation noise. On the other hand, in literature [30], wavelet transform is applied to process fingerprint images in the frequency domain and disturbance noise is added to the coefficient matrix obtained from wavelet decomposition for privacy protection purposes. In this approach, differential privacy's perturbation mechanism is utilized during adding noise to each data point within the wavelet transform coefficient matrix, potentially resulting in more pronounced errors caused by noise.

Face image differential privacy protection techniques are mainly realized through three methods. Firstly, there is frequency domain-based image differential privacy protection [32]. The image undergoes transformation followed by the addition of Laplace noise to achieve privacy protection. This method not only introduces noise errors from the differential privacy technique but also generates significant reconstruction errors during transformations and inverse transformations in the frequency domain. Secondly, there

are algebraic methods-based differential privacy protections for images involving matrix decomposition and compression [33]. This approach involves extracting eigenvalues from the image matrix values for protection. The proposed method incorporates both the noise error in the differential privacy technique and the reconstruction error caused by subsequent reconstruction. Additionally, a third approach involves safeguarding the 2D dataset by treating the 2D image matrix as a form of dataset [34]. This strategy maintains an amount of image data, thereby minimizing the impact of reconstruction errors on the image protection process. Consequently, only noise errors generated through differential privacy techniques persist.

The utilization of two-dimensional datasets in the protection process effectively mitigates the impact of reconstruction errors present in fingerprint images published by the protection method. However, the differential privacy protection method based on sliding window technique mentioned in literature [35] fails to address the issue of differentially private image protection from the perspective of spatial distribution characteristics inherent to the image itself. The region growing technique for protection mentioned in literature [36] excessively consumes non-essential privacy budget for safeguarding non-sensitive regions. Literature [37] mentions the effectiveness of sensitive region delineation protection in reducing privacy budget consumption. However, this method is not applicable for fingerprint images.

Protecting the sensitive region of a fingerprint image involves reducing global sensitivity by applying differential privacy techniques. In the differential privacy technique, the Laplace mechanism [20] perturbs data proportionally to global sensitivity and inversely to the size of the privacy budget. Therefore, by segmenting image data, we can modify the global sensitivity in differential privacy and consequently alter the resulting noise error. The paper proposes a local sensitivity-based method for protecting fingerprint images, as excessive global sensitivity leads to the generation of excessive noise errors. The exponential mechanism [38] images and assigns a privacy budget sequentially based on sampling probability, adding appropriate noise according to the local sensitivity with the assigned budget. Therefore, it is crucial to identify effective sensitive regions within fingerprint images for ensuring their privacy protection.

The subsequent sections encompass the primary contributions of this paper:

1) Minimizing the noise errors generated by fingerprint images using differential privacy techniques and enhancing the balance between privacy and usability when publishing protected fingerprint images, the allocation of the privacy budget is dynamically adjusted to improve the availability of the published protected fingerprint images while reducing the amount of noise introduced in the protection process.
2) The problem of reducing the significant noise error generated by the Laplace mechanism is being addressed. By leveraging the matching characteristics of fingerprint images, a combination of clustering and polynomial regression algorithms is employed to segment the feature points that match within the fingerprint image. This approach enables a localized protection process for individual regions of the image instead of globally protecting the entire fingerprint image.
3) The process of dynamically allocating privacy budget involves designing an index mechanism with a reasonable scoring function to establish the relationship between the number of matching feature points in a fingerprint image and the size of the localized image. This allows us to obtain a rational sampling order. By intelligently sampling within the local protection region, we can dynamically adjust and allocate our privacy budget accordingly, thus proposing a mechanism for dynamic allocation of privacy budget.
4) Theoretical proof demonstrates that all the algorithms proposed in this paper adhere to the definition of differential privacy. Furthermore, empirical evidence confirms that these algorithms not only satisfy the definition of differential privacy but also effectively balance the trade-off between privacy and usability in published fingerprint images through experimentation with privacy-preserving images within a real fingerprint image dataset for matching purposes.

II. BACKGROUND

A. DIFFERENTIAL PRIVACY

The concept of a neighborhood dataset (also known as a sibling dataset) is fundamental in the field of differential privacy. It refers to two datasets where only one data point differs between them. In image processing, particularly with two-dimensional grayscale image matrix data, the definition of neighboring images is based on the concept of neighboring datasets.

Definition 1 (Neighborhood Image): Given the dimensions of the original image X, which is $m \times n$, the grayscale image matrix is obtained through the normalization process denoted as $X_{m\times n}$. The processing of this matrix essentially involves manipulating each data quantity within the. Therefore, (1) representation of the image.

$$X_{m\times n} = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \tag{1}$$

Definition 2 (Differential Privacy): Given a randomized algorithm M for releasing image data, if $S \in Range(M)$ is the output range of algorithm M and any output on S from two mutually neighboring images X and X' satisfies (2), then the algorithm M satisfies ε-differential privacy.

$$\Pr[M(X) \in S] \leq \exp(\varepsilon) \times \Pr\left[M\left(X'\right) \in S\right] \tag{2}$$

Definition 3 (Global Sensitivity): The global sensitivity of query function Q, denoted as the global sensitivity can be

represented by (3), where $Q : X \to R^n$.

$$\Delta Q = \max_{X,X'} \left\| Q(X) - Q(X') \right\|_p \tag{3}$$

Definition 4 (Local Sensitivity): The local sensitivity of query function Q, denoted as (4) and (5), can be expressed when Q maps from X ($x \in X$) to R^n.

$$\Delta Q_{LS} = \max_{X,X'} \left\| Q(X) - Q(X') \right\|_p \tag{4}$$

$$\Delta \mathrm{Q_{GS}} = \max(\Delta Q_{LS}) \tag{5}$$

Theorem 1 (Laplace Mechanism): The algorithm X is defined as a randomized procedure that generates an $m \times n$ fingerprint image, where the input data is the image X and the output is denoted by X'. This algorithm satisfies (6) and ensures ε-differential privacy for algorithm M.

$$X' = X + \mathrm{Lap}(\Delta \mathrm{Q} / \varepsilon) \tag{6}$$

Theorem 2 (Exponential Mechanism): The sampling function under the exponential mechanism M selects samples from the sampling set X, where W is an element of X. The scoring function $\Delta Q(X, W)$ is established based on these samples, and Δu represents the global sensitivity of this scoring function. Therefore, the sampling process satisfies (7).

$$\Pr[M(X, \Delta Q) = W] \propto \exp\left(\frac{\varepsilon \times \Delta Q(X, W)}{2\Delta u}\right) \tag{7}$$

Property 1 (Sequence Combinatoriality): The algorithm M_i satisfies ε_i-differential privacy for a given data set X and the differential privacy algorithm respectively. Therefore, when combined, the algorithm M satisfies ε-differential privacy.

B. FINGERPRINT RECOGNITION

The characteristics of biometric fingerprinting should encompass universality, ensuring that every individual possesses this biometric trait, uniqueness, guaranteeing sufficient differences in biometric traits among individuals, persistence, indicating the stability of the biometric trait over time, and collectability, enabling quantitative measurement of the biometric trait.

Fingerprint features can be classified into three levels ranging from coarse to fine-grained details [39], [40]. The first level comprises the ridge direction field and frequency map, while the second level consists of map. Lastly, the third level encompasses both inner and outer contour information of ridges. Due to widespread usage and cost considerations associated with fingerprint identification systems, current matching technologies primarily rely on [41]. Level 1 features are mainly utilized for retrieving fingerprints from databases [42]. Tertiary features offer higher accuracy for fingerprint identification and matching but require more stringent sampling requirements [43], making them suitable for scenarios demanding enhanced security and confidentiality.

The fingerprint identification system primarily encompasses fingerprint acquisition, fingerprint enhancement, feature extraction, and fingerprint matching among other aspects [44]. Fingerprint image acquisition serves as the initial step in the fingerprint recognition system, while fingerprint enhancement involves repairing the quality of the captured fingerprint image. Feature extraction plays a crucial role in automatic fingerprint recognition systems, whereas fingerprint matching constitutes the key technology within such systems. Fingerprint image matching represents the final stage of the recognition process and typically employs alignment techniques to identify corresponding points between two fingerprints. Alignment involves translating, rotating, and scaling images to achieve maximum morphological similarity before utilizing a matching criterion to compute sets of feature points for establishing correspondence between fingerprints. Current research on fingerprint recognition has yielded various methods for performing these matches.

The focus of this paper is on the process of protecting fingerprint images through the utilization of a feature point description operator, which is a widely adopted and efficient method based on point pattern matching. Figure 1 illustrates the three approaches employing point pattern matching, respectively. (a) realizes the matching process of fingerprint images by constructing the feature point description operator through the intersection points of fingerprint secondary features. (b) realizes the fingerprint image matching process by constructing the feature point description operator through the end points of the fingerprint secondary features. (c) constructs a feature point description operator through all the fingerprint secondary features to realize the fingerprint image matching process.

According to the analysis of the fingerprint image feature point description operator, the fingerprint image privacy protection process is by covering the fingerprint image feature point location information, quantity information, type information. Therefore, how to protect these sensitive information of fingerprint images while adding less disturbance noise is the main research content of this paper.

III. METHODOLOGY

The implementation of protection methods for fingerprint images must satisfy the following requirements:

1) The definition of differential privacy must be maintained throughout the entire design process of the protection method. Definition 1 and (1) demonstrate that protecting the fingerprint image involves introducing noise to its pixel points. When applying the differential privacy technique to safeguard the fingerprint image, Definition 2 and (2) indicate that as the privacy budget increases, the published fingerprint image should have a smaller error. Conversely, as the privacy budget decreases, a larger error in the published fingerprint image is acceptable.
2) In the process of fingerprint image segmentation, it is crucial to group the feature points and adopt a suitable segmentation method based on the matching characteristics of the fingerprint image. When introducing

(a) constructing the feature point description operator through the intersection points of fingerprint secondary features

(b) constructing the feature point description operator through the end points of the fingerprint secondary features

(c) constructing the feature point description operator through all the fingerprint secondary features

FIGURE 1. Different fingerprint image feature points are used to construct feature point description operators.

noise into the fingerprint image, Theorem 1 and (6) demonstrate that the magnitude of noise error depends on both global sensitivity and privacy budget. Definition 3 and (3) indicate that the computation of global sensitivity is influenced by the size of the protected image. By segmenting the image, it becomes possible to effectively reduce global sensitivity, decrease noise magnitude, and enhance usability of the fingerprint image.

3) The allocation process of the privacy budget should consider the varying importance of feature matching points in fingerprint images and their corresponding characteristics. Therefore, it is necessary to take into account the size relationship between the feature and the protected image during the allocation process. Theorem 2 and (7) demonstrate that a well-designed scoring function is essential for effectively sampling local images to reasonably allocate privacy budget. By appropriately calculating the sampling of the local region, we can determine the size of privacy budget and achieve dynamic allocation.
4) The process of incorporating privacy budget for local images, aimed at addressing the issue of high global sensitivity, can be utilized to define (4) and (5) for local sensitivity by adding perturbation noise. Property 1 demonstrates that the total amount of privacy budget remains constant throughout the fingerprint image protection process, ensuring compliance with differential privacy techniques.

A. METHODS FOR GLOBAL PROTECTION OF FINGERPRINT IMAGES

In this paper, we first propose LAP (Laplace Mechanism Publication), a differential privacy publication algorithm that employs global protection of fingerprint images. LAP directly introduces Laplace noise to perturb the global image, resulting in an output fingerprint image denoted as X'. Theorem 1 and (6) demonstrate the protection process of depicted in (8).

$$X'_{(p,q)} = X_{(p,q)} + \mathrm{Lap}\left(\frac{\Delta Q_{LAP}}{\varepsilon_{LAP}}\right) \tag{8}$$

The matrix data $\mathrm{Lap}\left(\Delta Q/\varepsilon\right)$ has the same structure as the image X matrix data. Definition 1 and (1) demonstrate that protecting the fingerprint image involves adding perturbation data to pixel values in accordance with the size of privacy budget, for a fingerprint image satisfying ε-differential privacy-preserving fingerprint image distribution method, each pixel in the image receives a privacy budget of ε for perturbed data. ΔQ represents global sensitivity, as defined in Definition 3 and (3). The magnitude of global sensitivity is determined by the amount of sensitive data present in the dataset. Thus, it is calculated as shown in (9) within the LAP algorithm.

$$\Delta Q_{LAP} = m \times n \tag{9}$$

The implementation of adding noise to the data perturbs the data in order to achieve the desired perturbation effect. Its probability density function can be mathematically expressed as (10).

$$\mathrm{Lap}\left(x/b\right) = \frac{1}{2b} \times \exp(-\frac{|x|}{b}), b = \frac{\Delta Q}{\varepsilon} \tag{10}$$

The deflation factor, denoted as b, represents the primary range of distribution for the added noise data in image protection. When safeguarding an image, it is crucial to consider that the pixel values of the protected image fall within the range of 0 to 255. Consequently, a large scaling factor can introduce significant distortion and severely compromise the usability of the image data. Therefore, it is for b to be smaller

Algorithm 1 Differential Privacy Publishes Algorithm LAP Based on Global Protection of Fingerprint Images

Input: original fingerprint image X
Output: meets ε-differential privacy global privacy-preserving fingerprint image X'
Parameters: Image size is $m \times n$, privacy budget is ε
1. Read the original image X
2. Calculate the global sensitivity ΔQ_{LAP}, $\Delta Q_{LAP} = m \times n$
3. Add Laplace noise
for p in range (m) :
for q in range (n) :
$X'_{(p,q)} = X_{(p,q)} + \mathrm{Lap}\left(\Delta Q_{LAP} / \varepsilon_{LAP}\right)$
4. Output meets ε-Differential privacy global privacy-preserving fingerprint image X'

than the maximum fluctuation in pixel values ($b \leq 256$). As such, ensuring $\varepsilon = \Delta Q/b \geq \Delta Q/256$ becomes essential when determining the size of privacy budget in LAP algorithm.

$$\varepsilon_{LAP} \geq \Delta Q_{LAP}/256 = (m \times n)/256 \tag{11}$$

The process of directly adding perturbation noise to all pixel values in the fingerprint image, known as the LAP differential privacy publish algorithm based on global protection of the fingerprint image, is implemented according to algorithm 1, considering the global sensitivity ΔQ_{LAP} and privacy budget ε_{LAP}.

The given privacy budget ε is used to protect a pair of fingerprints, each with a size of $m \times n$. To ensure privacy protection, the number of pixels in the image is first calculated to determine the global sensitivity ΔQ_{LAP} (Step 2). Then, based on this global sensitivity ΔQ_{LAP} and the privacy budget ε, perturbation noise following a Laplace distribution is added to each pixel in the fingerprint image (Step 3).

The image error generated by the LAP algorithm is calculated due to the exclusive utilization of the Laplace mechanism for data perturbation during image protection, resulting in solely noise error as indicated by (12).

$$\mathrm{Error}\left(X'\right)_{LAP} = \mathrm{LE}\left(X'_{m\times n}\right)_{LAP} \tag{12}$$

The probability density function, as illustrated in (10), is employed to compute the variance of the lace distribution for assessing the summation of noise errors' squares. The publish process of the LAP algorithm involves generating image are quantified utilizing the formula presented in (13).

$$\begin{aligned}\mathrm{Error}\left(X'\right)_{LAP} &= \mathrm{LE}\left(X'_{m\times n}\right)_{LAP} \\ &= m \times n \times \frac{2\left(\Delta Q_{LAp}\right)^2}{\varepsilon^2} \\ &= \Delta Q_{LAp} \times \frac{2\left(\Delta Q_{LAp}\right)^2}{\varepsilon^2}\end{aligned} \tag{13}$$

The above reveals that the primary determinant of image error size in the LAP algorithm is the global sensitivity of the image, denoted as ΔQ_{LAp}. Definition 3 and (3) demonstrate that the magnitude of global sensitivity is contingent upon the number of sensitive pixels present in image X. The quantity of protected sensitive pixels within image is dictated by this global sensitivity, thereby reducing ΔQ. By diminishing the extent of global sensitivity, we can minimize any potential errors arising during fingerprint image protection and enhance overall usability.

B. CLUSTERING ALGORITHM SEGMENTATION FINGERPRINT IMAGE NON-GLOBAL PROTECTION METHODS

The error is analyzed based on the LAP algorithm to propose a non-globally protected differential privacy publication algorithm, known as KLAP (K images were protected by Laplace mechanism publication), which AGNES for matching discrete randomly distributed feature points and determining the segmented image size according to the clustering result.

The description operator for matching feature points in the fingerprint matching process utilizes the relative positions and distances between these points, with the distance sequence being used to determine the description operator. The computation process of the description operator mainly relies on the distance metric between matching feature points to determine their distances, thus employing AGNES, a bottom-up clustering algorithm, as the grouping method for sample points.

The KLAP algorithm implementation segments the fingerprint image based on the AGNES clustering results to ensure the protection of positional and quantitative information of matching feature points within the cluster. Therefore, it is necessary for the segmented local image to include all matching feature points in the cluster. To determine the localized protection area, we adopt a direct and effective method by setting the maximum coordinate value of samples in the cluster as an upper limit and minimum coordinate value as a lower limit. Additionally, an adjustment amplitude is introduced to prevent leakage of sensitive information from boundary details. The specific implementation process of Algorithm KLAP is illustrated in Algorithm 2.

Assuming that the set of coordinates extracted from the fingerprint image is $point\ (x, y) = \{F_1(x_1, y_1), \cdots, F_i(x_i, y_i), \cdots, F_M(x_M, y_M)\}$ (Step 2), the fingerprint image extracted a total of M coordinates of matching feature points, take this as M. Random sample coordinates, which are clustered using the AGNES algorithm to determine the number of clusters is K and the number of samples in each cluster is M_i $(0 \leq i \leq K)$ and the number of samples in each cluster is $M = \sum_{i=0}^{i=K-1} M_i$ (Step 3). Take the clustering result M_i as the data segmentation image, according to (14) to calculate the first i critical coordinate value of the matching feature point within the cluster (Step 4).

$$\begin{aligned}\widehat{x}_{\max} &= \max\{M_i[x, :]\}, \widehat{x}_{\min} = \min\{M_i[x, :]\} \\ \widehat{y}_{\max} &= \max\{M_i[:, y]\}, \widehat{y}_{\min} = \min\{M_i[:, y]\}\end{aligned} \tag{14}$$

Algorithm 2 A Non-Globally Protected Differential Privacy Publish Algorithm KLAP Based on Clustered Segmented Fingerprint Images

Input: original image X Matching feature point coordinate set $point\ (x, y)$

Output: non-globally protected image that satisfies differential privacy X'

Parameters: Image size is $m \times n$, total privacy budget is ε, number of matching feature points is M, pixels to be protected is Q

1. Read the original image X and convert to grayscale image matrix $X_{m\times n}$
2. Create all-zero matrix $Y_{m\times n}$, read the set of coordinates of matching feature points $point\ (x, y)$ and mark $Y\ (x, y) = 255$
3. The matching feature points are clustered using the hierarchical clustering algorithm AGNES, and the clustering result is M_i, $M = \sum_{i=0}^{i=K-1} M_i$
4. Clustering results to identify localized protected areas
   4.1. Select from the clustering result M_i and labeling
   4.2. The coordinates of matching feature points in the cluster extract the number of pixels to be protected
   4.2.1. Determination of localized protection area boundaries
   Calculation of the adjustment
   $dist\_x = \min\{dist\ (x_m, x_n)\ , x_m \in M_i, x_n \in M_i\}$
   $dist\_y = \min\{dist\ (y_m, y_n)\ , y_m \in M_i, y_n \in M_i\}$
   Calculation of area boundaries
   $x_{\max} = \max\{M_i\,[x, :]\} + dist\_x$
   $x_{\min} = \min\{M_i\,[x, :]\} - dist\_x$
   $y_{\max} = \max\{M_i\,[:, y]\} + dist\_y$
   $y_{\min} = \min\{M_i\,[:, y]\} - dist\_y$
   4.2.2. Marking pixels to be protected
   for x in range $(x_{\max} - x_{\min} + 1)$:
   for y in range $(y_{\max} - y_{\min} + 1)$:
   $Y\ (x + x_{\min}, y + y_{\min}) = 255$
   $Q_i = Q_i + 1$
   4.2.3. Skip to step 4.1 and re-select the M_i until all the M_i are labeled
   4.3. Calculate the total number of pixels to be protected Q, $Q = \sum_{i=0}^{i=K-1} Q_i$
   for x in range (m) :
   for y in range (n) :
   if $(Y\ (x, y) == 255)$:
   $Q = Q + 1$
5. Calculate the global sensitivity ΔQ, $\Delta Q = Q$
6. Add Laplace noise
   for p in range (m) :
   for q in range (n) :
   if $(Y\ (p, q) == 255)$:
   $X'_{(p,q)} = X_{(p,q)} + \mathrm{Lap}\left(\Delta Q_{KLAP} / \varepsilon_{KLAP}\right)$
7. Output non-globally protected images that satisfy differential privacy X'

The region boundary should not be directly determined by the critical coordinate value of the matching feature point, as it may inadvertently disclose privacy information. Instead, consider incorporating a certain adjustment amplitude to the critical coordinate value of the matching feature point. This adjustment amplitude be calculated as the minimum coordinate interval between the matching feature points, and (15) provides a method for its calculation.

$$\begin{aligned} dist\_x &= \min\{dist\ (x_m, x_n)\ , x_m \in M_i, x_n \in M_i\} \\ dist\_y &= \min\{dist\ (y_m, y_n)\ , y_m \in M_i, y_n \in M_i\} \end{aligned} \tag{15}$$

The critical coordinate values of the matched feature points are adjusted by incorporating the adjustment magnitude, and subsequently, the region boundary is computed using (16).

$$\begin{aligned} x_{\max} &= \max\{M_i\,[x, :]\} + dist\_x \\ x_{\min} &= \min\{M_i\,[x, :]\} - dist\_x \\ y_{\max} &= \max\{M_i\,[:, y]\} + dist\_y \\ y_{\min} &= \min\{M_i\,[:, y]\} - dist\_y \end{aligned} \tag{16}$$

The localized image of the segmented image is determined by $x_{\max}, x_{\min}, y_{\max}$ and $y_{\min}$ as the boundaries of the rectangular region. The (17) represents the side lengths of the segmented image.

$$\begin{aligned} \Delta x &= x_{\max} - x_{\min} + 1 \\ \Delta y &= y_{\max} - y_{\min} + 1 \end{aligned} \tag{17}$$

The number of pixels to be protected in the determined local area is calculated as (18) based on the clustering result M_i.

$$Q_i = \Delta x \times \Delta y \tag{18}$$

Similarly, the quantity of pixels to be safeguarded within the local region determined by all matching feature point information is as Q. Definition 3 and (3) demonstrate that the magnitude of global sensitivity is linked to the volume of data in the protection dataset. Moreover, due to the occurrence of overlapping issues in determining the upper and lower boundaries of segmented graphics, there is no need for repetitive calculation when determining the number of protections. Consequently, (19) accurately represents the size of global sensitivity.

$$\Delta Q_{KLAP} = Q \le \sum_{i=0}^{i=K-1} Q_i \tag{19}$$

Based on the analysis of Laplace distribution probability density function calculation, it is necessary to establish a minimum lower limit for privacy budget in order to avoid significant image data during fingerprint image privacy protection. Therefore, the amount of privacy budget required by the KLAP algorithm must satisfy the relationship shown in (20).

$$\varepsilon_{KLAP} \ge \frac{\Delta Q_{KLAP}}{256} \tag{20}$$

Based on Theorem 1 and (6), it can be observed that the process of adding privacy protection to fingerprint image X involves introducing perturbation noise to each pixel in the

image, while (21) represents the safeguarding of the fingerprint image through Laplace mechanism.

$$X'_{(p,q)} = X_{(p,q)} + \mathrm{Lap}\left(\Delta Q_{LAP}/\varepsilon_{LAP}\right) \tag{21}$$

The image error generated during the protection process of the KLAP algorithm for fingerprint image X is solely attributed to the utilization of Laplace mechanism. Therefore, only noise error exists, which satisfies (22).

$$\mathrm{Error}\left(X'\right)_{KLAP} = \mathrm{LE}\left(X'_{m\times n}\right)_{KLAP} \tag{22}$$

The process of calculating the sum of squared errors in (13) for global protection can also be the calculation of non-global protection, namely, the sum of squared errors for all pixels with added noise. The process of calculating the sum of lace mechanism is given by (23).

$$\begin{aligned}
\mathrm{LE}\left(X'_{m\times n}\right) &= E\left(\sum_{p=1}^{m}\sum_{q=1}^{n}\left(X'_{(p,q)} - X_{(p,q)}\right)^2\right) \\
&= E\left(\sum_{i=0}^{K-1}\sum_{x=x_{\min}}^{x_{\max}}\sum_{y=y_{\min}}^{y_{\max}}\left(X'_{(x,y)} - X_{(x,y)}\right)^2\right) \\
&= E\left(\sum_{i=0}^{K-1}\sum_{x=x_{\min}}^{x_{\max}}\sum_{y=y_{\min}}^{y_{\max}}\left(LAP\left(\frac{\Delta Q}{\varepsilon}\right)\right)^2\right) \\
&= E\left(\sum_{i=0}^{K-1}\sum_{x=x_{\min}}^{x_{\max}}\sum_{y=y_{\min}}^{y_{\max}} Error\left(LAP\left(\frac{\Delta Q}{\varepsilon}\right)\right)\right) \\
&= \sum_{i=0}^{K-1}\left(Q_i \times \frac{2\left(\Delta Q\right)^2}{\varepsilon^2}\right) \le Q \times \frac{2\left(\Delta Q\right)^2}{\varepsilon^2} \\
&= \Delta Q \times \frac{2\left(\Delta Q\right)^2}{\varepsilon^2}
\end{aligned} \tag{23}$$

The inclusion of the sum of squared errors from the Laplace mechanism in (22) provides a measure for image error magnitude of the KLAP algorithm, as shown in (24).

$$\begin{aligned}
\mathrm{Error}\left(X'\right)_{KLAP} &= \mathrm{LE}\left(X'_{m\times n}\right)_{KLAP} \\
&= \Delta Q_{KLAP} \times \frac{2\left(\Delta Q_{KLAP}\right)^2}{\varepsilon^2_{KLAP}}
\end{aligned} \tag{24}$$

According to the image error calculation of KLAP algorithm, it can be seen that the reduction of the size of the number of pixels to be protected by using local segmentation method can effectively reduce the size of the amount of noise in the process of publishing image, while the privacy budget remains unchanged. Therefore, Algorithm KLAP is better than Algorithm LAP in terms of fingerprint image X protection effect is better than Algorithm LAP.

C. EGRESSION ALGORITHM SEGMENTATION FINGERPRINT IMAGE NON-GLOBAL PROTECTION METHODS

The KLAP algorithm utilizes the AGNES algorithm to cluster the matching feature points of the fingerprint image, and based on the clustering result, segments the localized privacy protected image. However, there is still a significant amount of protection wastage in the determined local image, thus further segmentation of the local protected image can be conducted. In this section, we propose a non-globally protected divided privacy publication algorithm for fingerprint images based on clustering and local polynomial regression RKLAP (Regression method divided K images were protected by Laplace mechanism publication).

The samples of matched feature points were assigned labels within the cluster using polynomial regression after clustering. Additionally, the residual values between each sample point and the regression model were calculated. The line region of the myopic regression model was determined by considering the maximum residuals as the main flux samples within the cluster. However, when applying polynomial regression to construct a regression model for matching feature points within clusters, an overfitting state may result in excessively small, thereby revealing precise information about both the location and number of matching feature points within clusters.

The RKLAP algorithm utilizes two main methods to address the overfitting problem in local segmentation of sample regions within a cluster. Firstly, increasing the number of matching feature points in the cluster allows for higher dimensions in the polynomial regression model, resulting in improved fitting effect. However, also leads to an increase in maximum residuals between the samples and the regression model as more sample points are included. Secondly, reducing the number of regressions helps decrease the dimensionality of polynomial regression and subsequently reduces the degree of fit between samples and regression models, thereby increasing maximum residual variance. It is important to note that a larger value of residual difference does not necessarily indicate better performance. Instead, it signifies larger splits by the regression model on local regions. Therefore, setting an optimal threshold for residual difference is necessary during implementation as outlined in Algorithm III-C.

The KLAP algorithm clusters the matched feature points extracted from the fingerprint image and determines the result in terms of clusters M_i. The local image of the segmented image is determined based on $x_{\max}$, $x_{\min}$, $y_{\max}$ and $y_{\min}$ as the boundaries of the rectangular region. Subsequently, polynomial regression prediction is performed on the cluster samples within the local region determined by clustering results to obtain the regression model $h'(x)$. The minimum distance between matching feature points within a cluster is calculated according to (25).

$$Loss = \min dist\left(x_m, x_n\right) \tag{25}$$

The optimal residuals for predicting polynomial regression are determined by taking the minimum distance of matched feature points within a cluster *Loss*. The construction of the polynomial regression model involves matching feature points within clusters, and ultimately obtaining a polyno-

Algorithm 3 Clustering and Polynomial Regression Based Differential Privacy Publish Algorithm RKLAP for Non-Global Protection of Fingerprint Images

Input: Original image X Matching feature point coordinate set *point* (x, y)
Output: Non-globally protected image that satisfies differential privacy X'
Parameters: Image size is $m \times n$, total privacy budget is ε, number of matching feature points is M, pixels to be protected is Q
1. Read the original image X and convert to grayscale image matrix $X_{m\times n}$
2. Create all-zero matrix $Y_{m\times n}$, read the set of coordinates of matching feature points *point* (x, y) and mark $Y(x, y) = 255$
3. According to Algorithm 2, the coordinates of the matching feature points are clustered, and the clustering result is used to partition the protection area.
  3.1. Cauterization results $M_i, M = \sum_{i=0}^{i=K-1} M_i$
  3.2. Segmentation of the boundaries of protected areas
  Calculation of the adjustment
    $dist\_x = \min\{dist(x_m, x_n), x_m \in M_i, x_n \in M_i\}$
    $dist\_y = \min\{dist(y_m, y_n), y_m \in M_i, y_n \in M_i\}$
  Calculation of area boundaries
    $x_{\max} = \max\{M_i[x, :]\} + dist\_x$
    $x_{\min} = \min\{M_i[x, :]\} - dist\_x$
    $y_{\max} = \max\{M_i[:, y]\} + dist\_y$
    $y_{\min} = \min\{M_i[:, y]\} - dist\_y$
4. regression algorithm for further segmentation of the local segmentation region
  4.1. select from the clustering result M_i and labeling
  4.2. Calculate the minimum sample distance within a cluster as the optimal residuals
    $Loss = \min dist(x_m, x_n)$
  4.3. Optimal residual judgment predicts polynomial regression models $h'(x)$, find the actual regression model $h(x)$
  4.4. Calculate the actual regression model $h(x)$
  maximum residual
    $dist\_\max = \max \|h(x) - x\|_1$
  minimum residual
    $dist\_\min = \min \|h(x) - x\|_1$
  amplitude of fluctuations
    $dist = dist\_\max + dist\_\min$
  4.5. *dist* is the fluctuation amplitude and $h(x)$ is the regression model, segment the protected area image
  4.5.1. In $x_{\max}$ to $x_{\min}$ select successive coordinate values on the x
  4.5.2. Determine the pixel coordinate values within the fluctuation amplitude y,
    $(h(x) - dist) \le y \le (h(x) + dist)$
  4.5.3. determine whether the fluctuating pixels are within the protected area segmented by the KLAP algorithm, and mark
    if $(y_{\min} \le y \le y_{\max})$:
      $Y(x, y) = 255$
      $Q_i = Q_i + 1$
  4.5.4. Skip to step 4.1 and re-select the M_i until all the M_i are labeled
  4.6, Calculate the total number of pixels to be protected
    $Q, Q \le \sum_{i=0}^{i=K-1} Q_i$
    for x in range (m) :
      for y in range (n) :
        if $(Y(x, y) == 255)$:
          $Q = Q + 1$
5. Calculate the global sensitivity based on the number of pixels to be protected ΔQ, $\Delta Q = Q$
6. Add Laplace noise
    for p in range (m) :
      for q in range (n) :
        if $(Y(p, q) == 255)$:
          $X'_{(p,q)} = X_{(p,q)} + \mathrm{Lap}\left(\Delta Q_{RKLAP} / \varepsilon_{RKLAP}\right)$
7. Non-globally protected images that satisfy differential privacy X'

mial regression model where the maximum residuals of a strip of samples are closest to the optimal residuals x. The equation (26) represents the calculation for actual maximum residuals.

$$dist\_\max = \max \| h(x) - x \|_1 \tag{26}$$

The equation (27) is the actual minimum residual calculation.

$$dist\_\min = \min \| h(x) - x \|_1 \tag{27}$$

The maximum residual, when used as the fluctuation amplitude, can encompass all the coordinates of the matching feature points within the protected local area image. However, there may still be some matching feature points that appear at the boundary position. To effectively prevent information leakage of these matching feature points, an adjustment amplitude is added to the boundary by considering $dist\_\max$ as the boundary and *dist* as the adjustment amplitude. This approach calculates the fluctuation amplitude of the regression model using (28).

$$dist = dist\_\max + dist\_\min \tag{28}$$

The regression model is applied sequentially from $x_{\max}$ to $x_{\min}$, selecting coordinate values on x and calculating the corresponding value of y. The equation (29) demonstrates the calculation of pixel coordinate value y when the amplitude of fluctuation is considered as a parameter in the regression model.

$$y = h(x) + \Delta y, (-dist \le \Delta y \le dist) \tag{29}$$

The objective is to ascertain whether the fluctuating pixel (x, y) falls within the predetermined rectangular segmentation area that satisfies (30).

$$x_{\min} \le x \le x_{\max}, y_{\min} \le y \le y_{\max} \tag{30}$$

If the pixel falls within the rectangular area segmented by the KLAP algorithm, it is designated as a protected pixel and its count is recorded as $Q_i = Q_i + 1$ this protected area is not labeled. After constructing regression models for, excluding overlapping regions, the total labeled pixels to be protected (Q) is calculated. The count of pixels to be protected (Q_i) is calculated for all labeled pixels $Q \le \sum_{i=0}^{i=K-1} Q_i$.

The definition of 3 and (3) demonstrate that the computation of the global sensitivity in the RKLAP algorithm is determined according to (31).

$$\Delta Q_{RKLAP} = Q \tag{31}$$

The privacy protection of fingerprint images necessitates the establishment of a minimum lower limit on the privacy budget in order to prevent significant distortions in image data. Therefore, it is imperative for the amount of privacy budget in the RKLAP algorithm to satisfy the relationship depicted in (32).

$$\varepsilon_{RKLAP} \ge \frac{\Delta Q_{RKLAP}}{256} \tag{32}$$

Theorem 1 and (6) demonstrate that, in the case of a fingerprint image X, the process of incorporating privacy protection entails introducing perturbation noise to each pixel within the furthermore, (33) illustrates the procedure for safeguarding the fingerprint image through utilization of the Laplace mechanism.

$$X'_{(p,q)} = X_{(p,q)} + \mathrm{Lap}\left(\Delta Q_{RKLAP} / \varepsilon_{RKLAP}\right) \tag{33}$$

The image error generated during the protection process of fingerprint image X using the RKLAP algorithm is solely attributed to the noise introduced by the Laplace mechanism. In other words, the equation (34) holds true.

$$\mathrm{Error}\left(X'\right)_{RKLAP} = \mathrm{LE}\left(X'_{m\times n}\right)_{RKLAP} \tag{34}$$

The computation of the error sum of squares can be obtained by combining (13) and it into (34) provides the magnitude of image error generated by the RKLAP algorithm as expressed in (35).

$$\begin{aligned}\mathrm{Error}\left(X'\right)_{RKLAP} &= \mathrm{LE}\left(X'_{m\times n}\right)_{RKLAP} \\ &= \Delta Q_{RKLAP} \times \frac{2\left(\Delta Q_{RKLAP}\right)^2}{\varepsilon^2_{RKLAP}}\end{aligned} \tag{35}$$

The algorithms LAP, KLAP, and RKLAP are applied to the fingerprint image X. The error satisfies the relationship stated in (36).

$$\mathrm{Error}\left(X'\right)_{RKLAP} \le \mathrm{Error}\left(X'\right)_{KLAP} \le \mathrm{Error}\left(X'\right)_{LAP} \tag{36}$$

Therefore, when considering the same fingerprint image and maintaining the privacy protection of location and number of fingerprint matching feature points, algorithm RKLAP demonstrates superior privacy preservation compared to algorithms KLAP and LAP under an equal privacy budget. Additionally, algorithm KLAP outperforms algorithm LAP in terms of privacy preservation. Simultaneously, the availability of fingerprint images protected by algorithm RKLAP is highest, followed by algorithm KLAP, while algorithm LAP exhibits the lowest availability.

D. DYNAMIC BUDGET FINGERPRINT IMAGE NON-GLOBAL PROTECTION METHODS

The aforementioned three algorithms incorporate Laplace noise protection into the global sensitivity of fingerprint data. However, due to the high global sensitivity, a significant amount of perturbation noise is added, resulting in distortion of a large number of image data. To address this issue, we employ the local sensitivity approach defined in Definition 4 and (4) (5) to add perturbation protection specifically for fingerprint images. Nevertheless, it is crucial to select the order of adding perturbation noise reasonably as it greatly impacts the outcome of image protection.

The work of fingerprint matching can be analyzed to design a rational allocation mechanism for privacy budget, prioritizing the protection of regions with denser distribution of fingerprint matching feature points and allocating more privacy budget accordingly. Conversely, regions with sparse distribution of fingerprint matching feature points indicate the presence of outlier matching feature points in the local region, limiting their utilization in fingerprint matching work and resulting in a later order and less allocation of privacy budget during the protection process. This reasonable mechanism for allocating privacy budget can effectively enhance the recognition rate and usability of fingerprint images.

Therefore, in the context of privacy protection for fingerprint images, it is crucial to strategically determine the order of perturbation noise addition to the segmented region image. This approach aims to enhance both the usability and recognition rate of fingerprints, a quantitative analysis is conducted to establish a correlation between the number of pixels in the segmented region image and the count of matching feature points. Furthermore, a density relationship for measuring matching feature point density within the protected segment is defined. A scoring function based on this density relationship is devised as an index mechanism, enabling effective sampling of local regions. The allocation of privacy budget size dynamically adjusts according to factors such as feature point count and regional size within these sampled areas. This comprehensive process, referred to as DP (Dynamic Protection mechanism), follows Algorithm 4 for specific implementation.

Firstly, the data results obtained from the RKLAP algorithm are collected. The clustering outcomes of the AGNES algorithm are denoted as M_i, with $M = \sum_{i=0}^{i=K-1} M_i$. Polynomial regression algorithm is utilized for of image regions, and the pixel amount in each region is represented by Q_i, with $Q \le \sum_{i=0}^{i=K-1} Q_i$. The degree of protection for a single protected pixel against matching feature points is defined as I_i. An increase in I_i leads to an increase in ρ, while a decrease in I_i results in a decrease in ρ. The calculation method is illustrated by (37).

$$I_i = M_i / Q_i \tag{37}$$

The metric for measuring the density of matching feature points is defined through Theorem 2 and (7), and a suitable scoring function is designed based on this metric to determine the sampling probability. Specifically, higher densities of feature points correspond to, while lower densities lead to smaller one's privacy definition, we can use these densities to establish a reasonable sampling order for regions in fingerprint images that require protection, thereby facilitating dynamic allocation of privacy budgets.

The allocation of the privacy budget is dynamically determined based on the number of pixels in the local region, and a method for allocating the privacy budget according to the pixel count in the local region is considered. By calculating the remaining number of pixels to be protected, denoted as Q^{left}_{j-1} in (38), and determining the remaining privacy budget allocation, denoted as ε^{left}_{j-1} in (39), we can illustrate the dynamic distribution process of privacy budget using (40) to (44).

$$Q^{left}_{j-1} = Q^{left}_{j-2} - Q_{j-1}, Q^{left}_0 = Q, \quad Q^{left}_K = 0 \tag{38}$$

Algorithm 4 Exponential Mechanism Sampling Probability Designing a More Rational Privacy Budget Allocation Mechanism DP

Inputs: cluster result M_{i}, local area pixel amount Q_{i} Privacy budget $\varepsilon = \varepsilon_1 + \varepsilon_2$

Output: size of the local image allocation privacy budget is ε_i

Parameters: number of matching feature points M, pixels to be protected Q, original image X

1. Read the clustering results of the AGNES algorithm M_i, $M = \sum_{i=0}^{i=K-1} M_i$
2. Polynomial regression algorithm for local segmentation of images with local region pixel volume Q_i, $Q \leq \sum_{i=0}^{i=K-1} Q_i$
3. Calculate the degree of protection of a single protected pixel against matching feature points I_i, $I_i = M_i \big/ Q_i$
4. Taking I_i as the input to the exponential mechanism, design the scoring function $\Delta Q(X, I)$ for the exponential mechanism
5. The scoring function of the exponential mechanism calculates the sampling probability for each localized region $P_i \propto \exp\left[\frac{\varepsilon_1 \times \Delta Q(X, I_i)}{2\Delta u}\right]$
6. Sampling probability for localized images with privacy budget allocation process ordering $P_j = \max\{P_1, P_2, P_3, \cdots, P_i, \cdots, P_{K-1}\}$
7. Allocation of the privacy budget
   7.1. Sampling probability to select local images $P_j \rightarrow Q_j$
   7.2. Calculate the remaining number of pixels to be protected Q_{j-1}^{left}
   $Q_{j-1}^{left} = Q_{j-2}^{left} - Q_{j-1}, Q_0^{left} = Q, Q_K^{left} = 0$
   7.3. Residual privacy budget allocation ε_{j-1}^{left}
   $\varepsilon_{j-1}^{left} = \varepsilon_{j-2}^{left} - \varepsilon_{j-1}, \varepsilon_0^{left} = \varepsilon, \varepsilon_K^{left} = 0$
   7.4. Local Area Pixel Amount Q_j and the number of remaining pixels to be protected Q_{j-1}^{left} The privacy budget is allocated in relation to the
   7.4.1. If $Q_j \leq \frac{1}{4} Q_{j-1}^{left}$ then $\varepsilon_j = \frac{2Q_j}{Q_{j-1}^{left}} \times \varepsilon_{j-1}^{left}$
   7.4.2. If $\frac{1}{4} Q_{j-1}^{left} \leq Q_j \leq \frac{1}{2} Q_{j-1}^{left}$ then $\varepsilon_j = \frac{1}{2} \times \varepsilon_{j-1}^{left}$
   7.4.3. If $\frac{1}{2} Q_{j-1}^{left} \leq Q_j$ then $\varepsilon_j = \frac{Q_j}{Q_{j-1}^{left}} \times \varepsilon_{j-1}^{left}$
   7.5. Repeat the sampling of localized images, skipping step 7.1, until all localized images are assigned privacy budgets
8. Output localized images to assign the size of the privacy budget ε_i, $\varepsilon_2 = \sum_{i=0}^{i=K-1} \varepsilon_i$

$$\varepsilon_{j-1}^{left} = \varepsilon_{j-2}^{left} - \varepsilon_{j-1}, \varepsilon_0^{left} = \varepsilon, \varepsilon_K^{left} = 0 \tag{39}$$

If $Q_j \leq \frac{1}{4} Q_{j-1}^{left}$, holds true

$$\varepsilon_j = \frac{2Q_j}{Q_{j-1}^{left}} \times \varepsilon_{j-1}^{left} \tag{40}$$

If $\frac{1}{4} Q_{j-1}^{left} \leq Q_j \leq \frac{1}{2} Q_{j-1}^{left}$, holds true

$$\varepsilon_j = \frac{1}{2} \times \varepsilon_{j-1}^{left} \tag{41}$$

If $\frac{1}{2} Q_{j-1}^{left} \leq Q_j$, holds true

$$\varepsilon_j = \frac{Q_j}{Q_{j-1}^{left}} \times \varepsilon_{j-1}^{left} \tag{42}$$

Calculation Q_j^{left} with ε_j^{left}

$$Q_j^{left} = Q_{j-1}^{left} - Q_j \tag{43}$$

$$\varepsilon_j^{left} = \varepsilon_{j-1}^{left} - \varepsilon_j \tag{44}$$

The privacy budget allocation mechanism DP involves counting the allocations of the privacy budget. Let ω represent the allocation coefficient for each individual allocation of the privacy budget.

When $Q_j \leq \frac{1}{4} Q_{j-1}^{left}$, $\omega = \frac{2Q_j}{Q_{j-1}^{left}}$,
when $\frac{1}{4} Q_{j-1}^{left} < Q_j \leq \frac{1}{2} Q_{j-1}^{left}$, $\omega = \frac{1}{2}$,
when $\frac{1}{2} Q_{j-1}^{left} \leq Q_j$, $\omega = \frac{Q_j}{Q_{j-1}^{left}}$.

1. $\varepsilon_1 = \omega_1 \times \varepsilon$	$\varepsilon_1^{left} = \varepsilon - \varepsilon_1$
2. $\varepsilon_2 = \omega_2 \times \varepsilon_1^{left}$	$\varepsilon_2^{left} = \varepsilon_1^{left} - \varepsilon_2$
3. $\varepsilon_3 = \omega_3 \times \varepsilon_2^{left}$	$\varepsilon_3^{left} = \varepsilon_2^{left} - \varepsilon_3$
4. $\varepsilon_4 = \omega_4 \times \varepsilon_3^{left}$	$\varepsilon_4^{left} = \varepsilon_3^{left} - \varepsilon_4$
...	...
...	...
K-1. $\varepsilon_{K-1} = \omega_{K-1} \times \varepsilon_{K-2}^{left}$	$\varepsilon_{K-1}^{left} = \varepsilon_{K-2}^{left} - \varepsilon_{K-1}$
K. $\varepsilon_K = \varepsilon_{K-1}^{left}$	$\varepsilon_K^{left} = \varepsilon_{K-1}^{left} - \varepsilon_K = 0$

The magnitude of local sensitivity in the process of protecting fingerprint images through dynamic privacy budget corresponds to the density of the distribution of matching feature points, thereby enhancing the rationality of calculating local sensitivity when introducing perturbation noise to fingerprint images using Laplace mechanism. Definition 4 and (4) (5) demonstrate that the exponential mechanism computes the allocated privacy budget based on the calculation of local sensitivity for extracting local images.

The allocation process of the privacy budget in the DP mechanism is analyzed when the initial privacy budget is $\varepsilon = \varepsilon_1 + \varepsilon_2$. Given that the exponential mechanism satisfies ε_1-differential privacy, and since $\varepsilon_2 = \sum_{i=0}^{i=K-1} \varepsilon_i$ according to property 1, it follows that the allocation process of the privacy budget satisfies sequential composability. In other words, the allocation process of the privacy budget ensures ε_2-differential privacy, thereby satisfying sequence composability for the DP-based allocation mechanism of the privacy budget and ensuring overall ε-differential privacy.

The DP allocation mechanism for privacy budget is utilized to introduce Laplace perturbation noise into the segmented local images, enabling dynamic allocation of privacy budget

to these images. This approach, known as the DP-RKLAP (Dynamic Protection Regression method with K-image division protected by Laplace mechanism) algorithm, implements a specific process outlined in Algorithm 5.

IV. EXPERIMENT AND RESULT ANALYSIS

The image provided in Figure 2 serves as an illustrative example. The selected image 102-7 from dataset DB2 in the public fingerprint image database FVC2004, with an image size of $m \times n = 256 \times 393$, exhibits a total of 25 matching feature points. Considering clustering requirements $M_i > 4$ as per (11)(32), it is necessary to calculate the privacy budget size satisfying $\varepsilon \geq (m \times n)/256$ Consequently, when comparing the level of protection for fingerprint images under different privacy budgets, we consider the privacy budget sizes as follows: $\varepsilon_1 = (mn)/256$, $\varepsilon_2 = 2 \times (mn)/256$, $\varepsilon_3 = 3 \times (mn)/256$, $\varepsilon_4 = 4 \times (mn)/256$, $\varepsilon_5 = 5 \times (mn)/256$.

By comparing the computations in the privacy budget allocation mechanism for protecting fingerprint images, we divide the privacy budget into two parts: $\varepsilon = \varepsilon_1 + \varepsilon_2$. ε_1 is allocated to the index mechanism, while ε_2 is assigned to the Laplace mechanism. In practical applications, it has been observed that a value less than 1 is sufficient for achieving the desired protection effect with respect to $\varepsilon 1$ in the exponential mechanism. On the other hand, when safeguarding an image, it should satisfy $\varepsilon_2 = \Delta Q/b \geq \Delta Q/256$. Hence, a larger value of ε_2 is required. Consequently, when protecting fingerprint images, allocating a significantly larger portion of the privacy budget to ε_2 compared to ε_1 ensures that during error calculations associated with fingerprint images, we have approximately equal values of ε and ε_2.

A. SEGMENTATION OF IMAGES FOR PROTECTED EXPERIMENTS

The algorithms, namely Algorithm LAP, Algorithm KLAP, and Algorithm RKLAP, continuously reduce the number of pixels to be protected in order to decrease the global sensitivity and enhance the protection.

Experimental labeling on the protected regions of these algorithms resulted in respective protected regions: $Q_{LAP} = m \times n = 100608$, $Q_{KLAP} = 43488$, $Q_{RKLAP} = 14014$ as depicted in Figure 3 is made between the protected regions of each algorithm along with an evaluation of their corresponding global sensitivities. (a) represents the image protection region when the perturbation noise is added to the global image using the LAP algorithm. (b) represents the image protection region obtained by clustering and segmenting the feature points in the fingerprint image using the KLAP algorithm. (c) represents the protected area of the image obtained after the clustering segmented image is further segmented by the polynomial regression algorithm using the RKLAP algorithm. The final algorithm DP-RKLAP of this paper uses the RKLAP algorithm to segment the image protection area with the smallest protection sensitive area for protection.

Algorithm 5 A Non-Globally Protected Differential Privacy Publish Algorithm Based on An Exponential Mechanism for Allocating Privacy Budget DP-RKLAP

Input: Original image X matching feature point coordinate set *point* (x, y)

Output: Non-globally protected image that satisfies differential privacy X'

Parameters: Image size is $m \times n$, total privacy budget is $\varepsilon = \varepsilon_1 + \varepsilon_2$, number of matching feature points is M, pixels to be protected is Q

1. Read the original image X and convert to grayscale image matrix $X_{m\times n}$
2. Creating an all-zero matrix $Y_{m\times n}$, $Z_{m\times n}$ Read the set of coordinates of matching feature points *point* (x, y) and mark $Y(x, y) = 255$
3. According to Algorithm III-C, the coordinates of the matched feature points are clustered to split the local protection region.
   - 3.1. The results of cluster analysis are, M_i $M = \sum_{i=0}^{i=K-1} M_i$
   - 3.2. Segmentation of localized protected area boundaries
     $x_{\max} = \max\{M_i[x, :]\} + dist\_x$
     $x_{\min} = \min\{M_i[x, :]\} - dist\_x$
     $y_{\max} = \max\{M_i[:, y]\} + dist\_y$
     $y_{\min} = \min\{M_i[:, y]\} - dist\_y$
   - 3.3. Segmenting the amount of local image pixels Q_i, $Q \leq \sum_{i=0}^{i=K-1} Q_i$
4. According to Algorithm 4, a privacy budget is assigned to the localized image.
   - 4.1. the exponential mechanism satisfies ε_1-differential privacy
   - 4.2. The Laplace mechanism satisfies ε_2-differential privacy
   - 4.3. assign privacy budgets to localized images ε_1, $\varepsilon_2 = \sum_{i=1}^{i=K} \varepsilon_i$.
5. Adding Disturbance Noise
   - 5.1. Selecting local images in sequence P_j
   - 5.2. Getting the number of pixels in the current local image $P_j \rightarrow Q_j$
   - 5.3. Calculate the current local sensitivity $\Delta Q^j_{GS} = Q_j$
   - 5.4. Getting the privacy budget of the current local image $P_j \rightarrow \varepsilon_j$
   - 5.5. To mark pixels $Z(x, y)$ add noise
     for p in range(m) :
     for q in range(n) :
     if $(Z(p, q) == 255)$:
     $X'_{(p,q)} = X_{(p,q)} + Lap(\Delta Q^j_{GS}/\varepsilon_j)$
   - 5.6. Re-select the local image, skip to step 5.1, until all local images are added to the protection
6. Output a locally protected image that satisfies differential privacy X'

According to Definition 3, the size of global sensitivity is determined by the volume of data in the dataset. In the con-

FIGURE 2. Example image.

TABLE 1. Performance comparison of different algorithms for image segmentation.

algorithm	size of image	Amount of protected pixels	Global sensitivity	Proportion of protected pixels
LAP	256×393	100608	100608	100%
KLAP	256×393	43488	43488	43.23%
RKLAP	256×393	14014	14014	13.93%
DP-RKLAP	256×393	14014	14014	13.93%

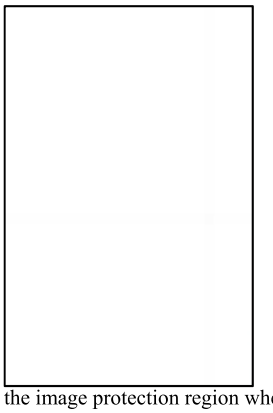
text of protecting fingerprint images, the global sensitivity is equivalent to number of pixels in the protected area, denoted as $\Delta Q = Q$. For LAP algorithm, $\Delta Q_{LAP} = Q_{LAP} = 100608$, for KLAP algorithm, $\Delta Q_{KLAP} = Q_{KLAP} = 43488$, and for RKLAP algorithm, $\Delta Q_{RKLAP} = Q_{RKLAP} = 14014$. By substate into (15), (24), and (35), we can verify the analytical results presented in (36).

Table 1 shows the comparison of the size of the local image to be protected produced by different algorithms for different degrees of fingerprint image segmentation. From the data in the above table, it can be seen that the global sensitivity of RKLAP algorithm and DP-RKLAP algorithm is significantly reduced after different degrees of image segmentation.

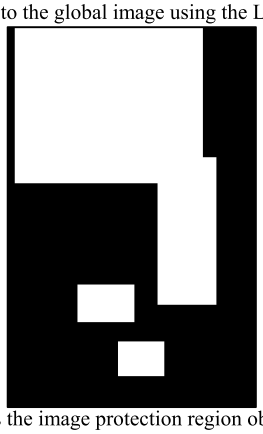
B. EXPERIMENTS WITH PRIVACY BUDGET ALLOCATION MECHANISMS

The privacy budget allocation mechanism DP involves two protection mechanisms, namely the exponential mechanism and the Laplace mechanism. In the exponential mechanism, the scoring function determines the degree of protected pixel against matching feature points, and different privacy budgets are compared based on the size of the sampling probability. In the Laplace mechanism, the size of the privacy budget is allocated based on the relationship between the number of pixels in a segmented image and its total number of This ensures that local images with denser distributions of matching feature points receive relatively larger privacy budgets, while those with sparser distributions receive relatively smaller ones. Table 2 presents specific data after image segmentation.

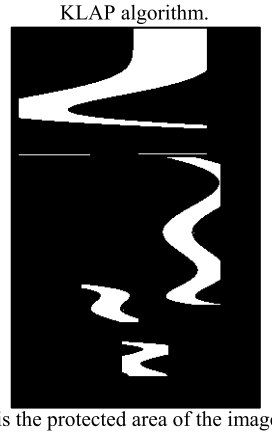
The privacy budget allocation mechanism initially extracts the segmented image data from the RKLAP algorithm to obtain clustering results M_i, where $M = \sum_{i=0}^{i=K-1} M_i$. Then, it determines the number of pixels in the local region of



(a) The white area is the image protection region when the perturbation noise is added to the global image using the LAP algorithm.



(b) The white area is the image protection region obtained by clustering and segmenting the feature points in the fingerprint image using the KLAP algorithm.



(c) The white area is the protected area of the image obtained after the clustering segmented image is further segmented by the polynomial regression algorithm using the RKLAP algorithm.

FIGURE 3. Comparison of protection areas of publishing algorithms.

TABLE 2. Localized image data extraction.

Image Number	0	1	2	3
Matching Feature Points	4	7	7	7
Protecting Pixels	8146	1110	3679	1076
unit pixel	2036.5	158.6	525.6	153.7
Level of protection	4.91×10^{-4}	6.31×10^{-3}	1.90×10^{-3}	6.51×10^{-3}

TABLE 3. DP mechanism privacy budget allocation.

Image Number	3	1	2	0
Protecting Pixels	1076	1110	3679	8146
remaining pixels	12935	11825	8146	0
Allocation of epsilon ratios	15.36%	14.53%	35.06%	35.05%
Remaining epsilon ratio	84.64%	70.11%	35.05%	0

the image through polynomial regression algorithm as Q_i with $Q \leq \sum_{i=0}^{i=K-1} Q_i$. Subsequently, it calculates the unit pixel required to protect a single matching feature point as $O_i = Q_i/M_i$ and evaluates the degree of protection provided by a single protected pixel for a matching feature point as $I_i = M_i/Q_i$.

Figure 4 illustrates a comparison of the sampling probabilities generated by the exponential mechanism across different privacy budgets.

The sampling probability is calculated under various privacy budgets, revealing that the sampling probability changes as the privacy budget increases. For local images with a higher level of protection for matching feature points input by the scoring function, the sampling probability gradually increases with an increasing privacy budget. Conversely, for local images with a lower degree of protection for matching feature points input by the scoring function, the sampling probability gradually decreases as the privacy budget continues to rise.

The privacy budget for each sampled image is allocated based on the pixel size, and the current remaining number of unprotected pixels and the amount of allocated privacy budget are calculated. During the allocation process, the size of the privacy budget is reasonably distributed according to the pixel count of each sampled image, ensuring that each allocation is proportional to the image size without excessively consuming privacy budget The specific allocation process for privacy budget is illustrated in Table 3.

The allocation consumption process of the privacy budget under different allocation mechanisms is depicted in Figure 5. In the experiments, the DP mechanism proposed in this paper is compared with traditional methods including Taylor expansion, bisection, special rank, and p-rank (from left to right). Data comparison reveals that the traditional allocation mechanism rapidly dates the privacy budget as allocations increase linearly. Conversely, the DP mechanism's allocation is based on the data volume of protected images, allowing for a reasonable distribution of privacy budget according to each sampling's data size. Therefore, our proposed DP-based privacy budget allocation mechanism outperforms traditional approaches when allocating fingerprint image privacy budgets.

C. SIMULATION EXPERIMENTS

In this section of the experiment, the example images are protected under different privacy budget conditions using various algorithms fingerprint images.

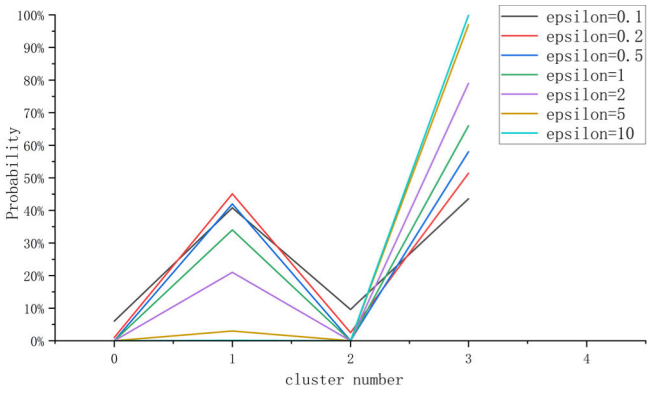


FIGURE 4. The sampling probabilities generated by the exponential mechanism across different privacy budgets.

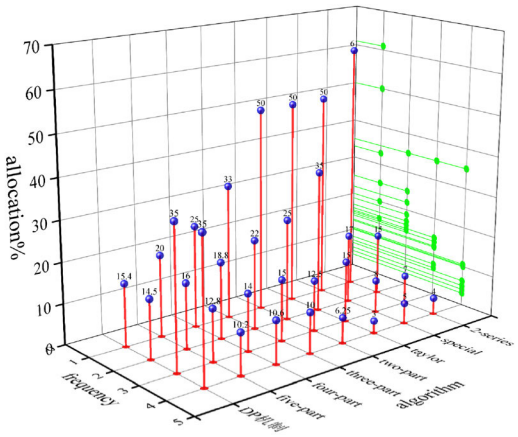


FIGURE 5. Privacy budget allocation under different mechanisms.

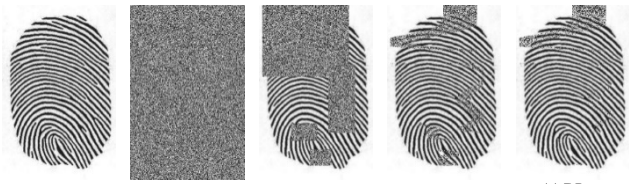


FIGURE 6. Comparison of publishing fingerprint images for different algorithms when privacy budget consumption is ε_1.

The publishing images are illustrated in Figure 6 to Figure 10, with each image corresponding to a specific value of the privacy budget denoted as $\varepsilon_1 = (mn)/256$, $\varepsilon_2 = 2\times(mn)/256$, $\varepsilon_3 = 3\times(mn)/256$, $\varepsilon_4 = 4\times(mn)/256$, $\varepsilon_5 = 5\times(mn)/256$.

After analyzing the aforementioned experimental results, it becomes evident that the fingerprint contours of publishing fingerprint images gradually become more distinct under the same privacy budget. Similarly, the contours of publishing fingerprint images by the same algorithms under privacy budgets also exhibit a gradual increase in clarity. Consequently, it can be concluded that this aligns with the definition of differential privacy protection. Moreover, it is observed that

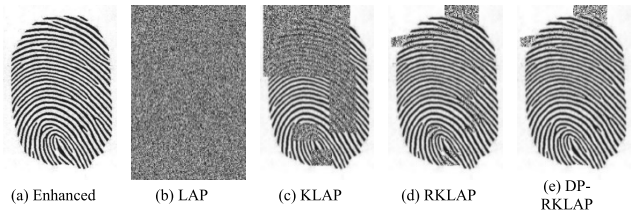


FIGURE 7. Comparison of publishing fingerprint images for different algorithms when privacy budget consumption is ε_2.

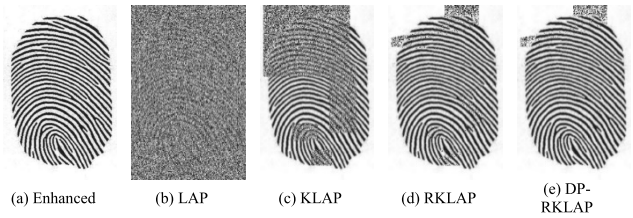


FIGURE 8. Comparison of publishing fingerprint images for different algorithms when privacy budget consumption is ε_3.

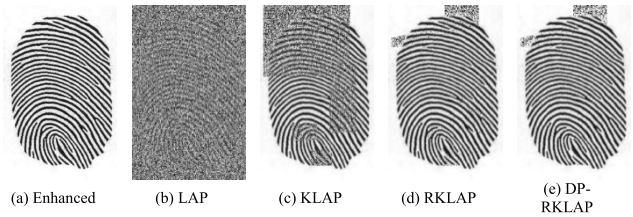


FIGURE 9. Comparison of publishing fingerprint images for different algorithms when privacy budget consumption is ε_4.

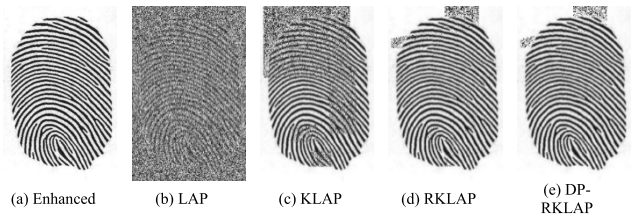


FIGURE 10. Comparison of publishing fingerprint images for different algorithms when privacy budget consumption is ε_5.

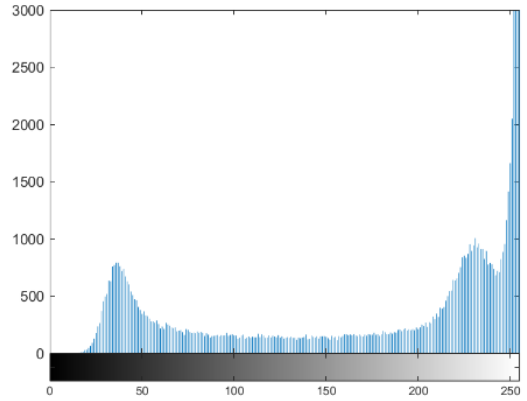


FIGURE 11. Distribution of pixel values in the original image.

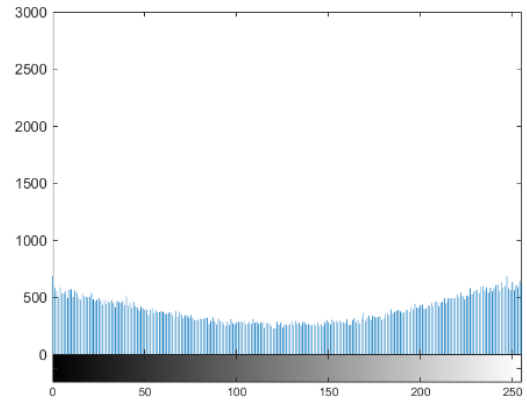


FIGURE 12. Distribution of pixel values of publishing images by LAP algorithm.

as the privacy budget increases, there is an enhancement in usability but a decrease in privacy for publishing fingerprint images by the same algorithm. Conversely, as the privacy budget decreases, there is reduction in privacy for these images. Notably, among all these observations, it can be stated that DP-RKLAP fingerprint image demonstrates superior usability when published under identical privacy budgets.

The usability of fingerprint image protection can also be assessed by analyzing the distribution of different pixel values in the 2D fingerprint image data. Figure 11 to Figure 15 compare the pixel value distributions of fingerprint images generated by various all with an identical privacy budget.

The results of the aforementioned experiments are analyzed based on the distribution of pixel values in fingerprint images obtained using different publishing algorithms, specifically at $\varepsilon_1 = (mn)/256$ for comparison purposes. The pixel LAP publishing image (Figure12) differs significantly from that of the original image (Figure11), while the KLAP publishing image (Figure13) exhibits a closer resemblance. Moreover, both RKLAP publishing image (Figure14) and DP-RKLAP publishing image (Figure15) demonstrate virtually identical pixel value distributions as compared to the original image (Figure11). Experimental evidence confirms that the error relationship between LAP, KLAP, and RKLAP algorithms and their respective original images aligns with (36). Additionally, due to privacy budget allocation within DP mechanism, algorithm RKLA pixel value distribution closely resembles that of DP-RKLAP published image, thereby enhancing protection availability and privacy preservation for local images.

The published images under different algorithms with varying privacy budgets are subjected to matching feature point recognition. The experimental results, depicted in Figure 16, demonstrate the rates of matching feature point recognition between the published and original images for privacy budgets $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5$ (from right to left). Additionally, the rates of matching feature point recognition

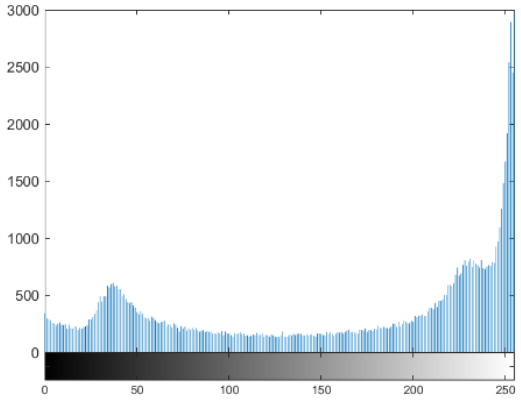


FIGURE 13. Distribution of pixel values of publishing images by KLAP algorithm.

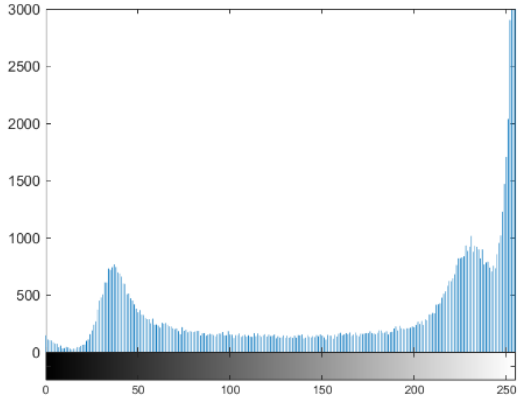


FIGURE 14. Distribution of pixel values of publishing images by RKLAP algorithm.

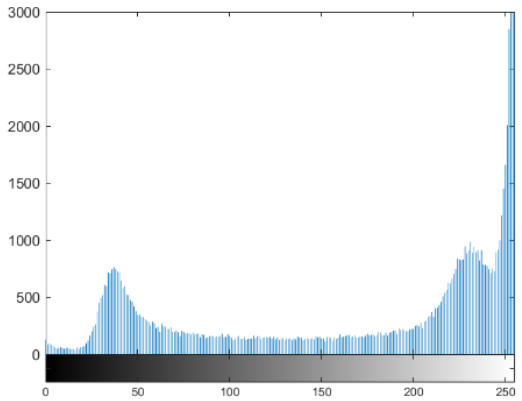


FIGURE 15. Distribution of pixel values of publishing images by DP-RKLAP algorithm.

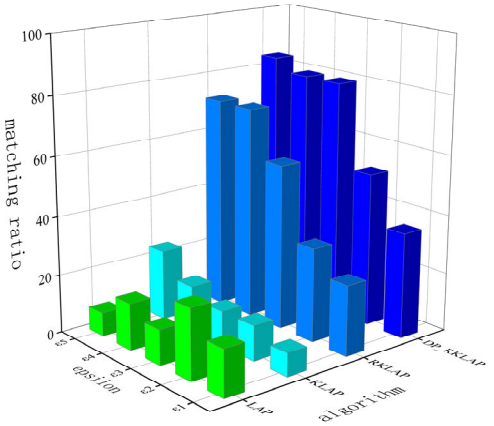


FIGURE 16. Different algorithms with varying privacy budgets are subjected to matching feature point recognition.

between the published and original images are evaluated for algorithms LAP, KLAP, RKLAP, and DP-RKLAP (from left to right).

The experiment clearly demonstrates that the LAP algorithm exhibits unstable image recognition rates due to significant data distortion, resulting in a smaller impact of privacy budget changes on the recognition rate. In contrast, the KLAP algorithm shows a synchronous increase in both published and original image recognition rates with an increased privacy budget, although the overall recognition rate remains low. On the other hand, the RKLAP algorithm gradually improves its publication and original image recognition rates as the privacy budget increases, leading to a higher overall recognition rate. Similarly, for the DP-RKLAP algorithm, increasing the privacy budget results in gradual improvements in both published and original image recognition rates, ultimately leading to a higher overall recognition rate.

D. ANALYSIS OF RESULTS

The algorithm's feasibility was initially assessed by validating it with the fingerprint dataset DS, comprising 432 fingerprint images collected from nine individuals (six fingerprints per individual) and eight different angles of each fingerprint.

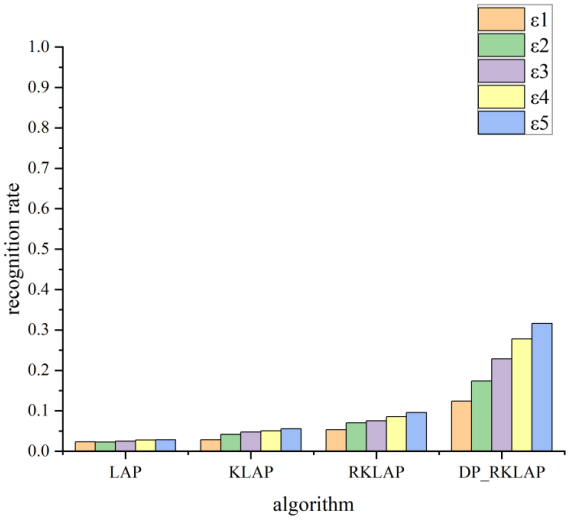


FIGURE 17. Average recognition rate in the experimental dataset DS.

Then 800 fingerprint image from DB2 in the public fingerprint database FVC2004 standard database are used for validation [45].

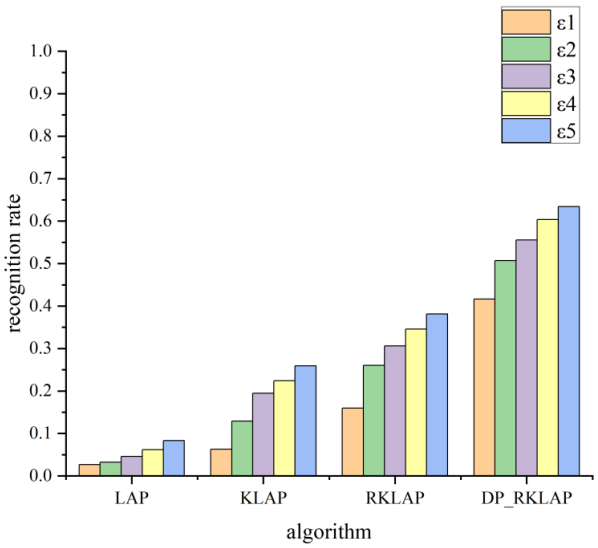


FIGURE 18. Average recognition rate in the experimental dataset FVC2004.

The experimental environment is Intel® Core i5-9300H CPU @ 2.40 GHz, 32G RAM, GTX 21080TI GPU, Windows 11 operating system, PyCharm Community Edition 2023.2.

When incorporating protection measures for fingerprints using the fingerprint dataset DS and the FVC2004 standard dataset, the fingerprints are partitioned into a training set and protected fingerprint images are then matched with the images in the fingerprint library. During the of protecting fingerprint images, a minimum cluster size of 5 samples is set ($M_i > 4$). For privacy budget considerations, we respectively take $\varepsilon_1 = (mn)/256, \varepsilon_2 = 2 \times (mn)/256, \varepsilon_3 = 3 \times (mn)/256, \varepsilon_4 = 4 \times (mn)/256, \varepsilon_5 = 5 \times (mn)/256$. We of each algorithm on the publishing protected images and present their average recognition rates in Figure 17 for experimental dataset DS and Figure 18 for experimental dataset FVC2004.

The validation on the experimental dataset reveals that LAP, a differential privacy publishing algorithm based on global protection of fingerprint images, exhibits a low recognition rate for privacy-protected fingerprint images. This significantly diminishes the usability of fingerprint images while aiming to enhance their privacy. KLAP, another differential privacy publishing algorithm based on clustering segmented fingerprint images with non-global protection, demonstrates a slight improvement in the recognition rate of privacy-preserving fingerprint images. However, this improvement is not substantial. On the other hand, RKLAP, a non-globally protected differential privacy publishing algorithm for fingerprint images based on clustering and local polynomial regression, shows consistent progress in terms of recognition rate compared to both LAP and KLAP algorithms. Although there is still room for enhancement as the recognition rate remains low and some errors persist during the process of fingerprint matching. Conversely,

TABLE 4. DS & matching rate.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	2.32%	2.86%	5.35%	12.40%
ε=2	2.30%	4.18%	7.00%	17.36%
ε=3	2.49%	4.79%	7.51%	22.89%
ε=4	2.81%	5.06%	8.57%	27.81%
ε=5	2.84%	5.56%	9.58%	31.66%

TABLE 5. DS & matching accuracy.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	83.81%	90.26%	93.03%	97.70%
ε=2	86.34%	90.77%	94.16%	98.75%
ε=3	87.08%	92.03%	94.79%	99.30%
ε=4	85.38%	92.00%	96.30%	99.50%
ε=5	85.66%	91.78%	96.14%	99.91%

TABLE 6. DS & matching score.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	1.84%	2.60%	5.09%	12.27%
ε=2	1.91%	3.87%	6.74%	17.26%
ε=3	2.09%	4.52%	7.30%	22.82%
ε=4	2.36%	4.75%	8.41%	27.76%
ε=5	2.40%	5.26%	9.41%	31.64%

TABLE 7. DS & recall rate.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	24.89%	28.10%	34.90%	44.10%
ε=2	25.17%	31.59%	37.61%	49.11%
ε=3	25.48%	32.45%	37.99%	53.96%
ε=4	26.54%	32.81%	39.09%	57.90%
ε=5	25.94%	33.27%	40.70%	59.99%

DP-RKLAP - a differential privacy publishing algorithm utilizing an index mechanism for reasonable allocation of privacy budget under non-global protection - displays higher effectiveness in matching dense regions of feature points due to its rational allocation of privacy budget using DP mechanism. Consequently, it greatly enhances the recognition rate during matching processes and significantly improves identification accuracy compared to the previous three algorithms.

Table 4 and Table 5 show the evaluation metrics of the assumed matching rate of different algorithms on two datasets under different privacy budget conditions, respectively. Table 6 and Table 7 show the evaluation metrics of matching accuracy of different algorithms on two datasets under different privacy budget conditions, respectively. Table 8 and Table 9 demonstrate the evaluation metrics of matching scores of different algorithms on two datasets under different privacy budget conditions, respectively. Table 10 and Table 11 show the recall evaluation metrics of different algorithms on two datasets under different privacy budget conditions, respectively.

By analyzing the above experimental data, according to the definition of differential privacy, as the privacy budget continues to increase, the amount of added disturbance

TABLE 8. FVC2004 & matching rate.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	10.32%	13.02%	18.33%	62.65%
ε=2	11.82%	14.71%	33.01%	79.30%
ε=3	16.45%	18.33%	41.85%	81.37%
ε=4	17.10%	19.00%	51.65%	85.98%
ε=5	17.87%	25.46%	55.23%	91.46%

TABLE 9. FVC2004 & matching accuracy.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	65.97%	66.10%	76.93%	99.29%
ε=2	69.33%	72.44%	92.59%	99.55%
ε=3	56.47%	73.48%	96.67%	100.00%
ε=4	64.56%	95.30%	94.56%	99.59%
ε=5	66.36%	92.06%	98.01%	100.00%

TABLE 10. FVC2004 & matching score.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	6.24%	8.26%	14.31%	62.17%
ε=2	7.44%	10.14%	30.88%	78.98%
ε=3	9.24%	14.27%	40.67%	81.37%
ε=4	10.88%	18.18%	49.08%	85.65%
ε=5	11.83%	23.79%	54.21%	91.46%

TABLE 11. FVC2004 & recall rate.

epsilon	LAP	KLAP	RKLAP	DP-RKLAP
ε=1	15.69%	17.00%	29.43%	83.17%
ε=2	17.03%	19.94%	52.39%	93.25%
ε=3	20.68%	28.37%	61.61%	93.33%
ε=4	21.48%	36.23%	70.69%	95.47%
ε=5	24.26%	43.72%	73.23%	97.62%

noise continues to decrease, so the size of the privacy budget is inversely proportional to the added disturbance noise. According to the above tabular data, as the privacy budget continues to increase, the size of matching rate, matching score and recall rate increases, and the size of matching rate, matching score and recall rate is inversely proportional to the added disturbance noise. Therefore, the matching rate, matching score and recall are strongly correlated with the perturbation noise. Meanwhile, with the change of privacy budget, the change trend of matching accuracy is not obvious. Therefore, the matching accuracy has a weak correlation with the disturbance noise. This finding is consistent with theoretical evidence.

Through the above performance experimental analysis, under the same privacy budget condition, DP-RKLAP algorithm has higher matching rate, matching score, recall rate and matching precision rate. This is the same as the conclusion obtained in the theoretical proof stage. DP-RKLAP reduces the amount of added disturbance noise as much as possible by reducing the global sensitivity and dynamically allocating the privacy budget, so as to improve the availability of published images. Therefore, the algorithm performance of algorithm DP-RKLAP is higher than other algorithms.

E. RESEARCH AND DEVELOPMENT

In this paper, we mainly study the method of applying differential privacy technology to protect fingerprint images. According to the recognition characteristics of biological images, the recognition feature points of fingerprint images are discrete, which are different from face images. Therefore, the local image protection method suitable for fingerprint images needs to protect the position information, quantity information and type information of fingerprint image feature points.

According to the discrete characteristics of fingerprint image feature points, this paper uses clustering algorithm and regression algorithm to segment the fingerprint image, and according to the size of the segmented image, the exponential mechanism of differential privacy technology is used to complete the dynamic allocation process of privacy budget to allocate the privacy budget reasonably. It lays the foundation for differential privacy technology in the protection of fingerprint images.

However, since the protection process of fingerprint images is related to the size of the image, different amounts of disturbance noise will be generated for different sizes of fingerprint images under the same privacy budget. As the image size increases, the generated disturbance noise will also continuously increase. Therefore, how to reduce the disturbance noise generated by larger size images will be another research direction of related research.

V. CONCLUSION

The paper proposes a fingerprint image publishing algorithm, DP-RKLAP, based on machine learning and differential privacy techniques to address the issue of privacy leakage in the fingerprint image publishing process. This algorithm dynamically allocates the privacy budget while reducing the amount protection, thereby enhancing the usability of publishing fingerprint images. By leveraging clustering and polynomial regression algorithms, KLAP and RKLAP algorithms segment matching feature points in fingerprint images to achieve global protection through local image protection. Furthermore, this approach solves the problem of excessive noise generated by the Lap mechanism by employing a dynamic allocation mechanism for privacy budget DP. A reasonable sampling order is obtained through designing an appropriate scoring function for index mechanisms and considering factors such as the number of matching feature points in a fingerprint image, size of local images, and size of privacy budget.

The paper proposes that all algorithms should adhere to the definition of differential privacy. During the theoretical proof, the error in the publishing image is calculated and compared with the errors produced by four algorithms: LAP, KLAP, RKLAP, and DP-RKLAP. This analysis aims to evaluate the image error under global sensitivity calculation using (39). Results show that the RKLAP algorithm produces the smallest image error while LAP algorithm yields the

largest one. Regarding error analysis under local sensitivity calculation, fingerprint images publishing by DP-RKLAP algorithm outperform those publishing by RKLAP algorithm. In the experimental stage, example image experiments are conducted under different privacy budget conditions and various algorithm settings to validate their usability relationship. The results obtained from these experiments align with theoretical proofs. Additionally, a large number of fingerprint image datasets confirm high matching feature point recognition rates.

By using the image matching evaluation index to identify and match the protected image, the performance of the algorithm proposed in this paper is analyzed. In this paper, four evaluation metrics, matching rate, matching score, recall and matching accuracy, are mainly used for analysis. After a large number of experiments, with the minimum privacy budget, the final algorithm proposed in this paper has the matching rate higher than 12.40%, the matching accuracy higher than 97.70%, the matching score higher than 12.27%, and the recall rate higher than 64.10% on the self-built data set DS. Compared with the Laplace mechanism, the matching rate is increased by 10.08%, the matching accuracy is increased by 13.89%, the matching score is increased by 10.43%, and the recall rate is increased by 19.22%. On the public data set FVC2004, the matching rate is higher than 62.65%, the matching accuracy is higher than 99.29%, the matching score is higher than 62.17%, and the recall rate is higher than 83.17%. Compared with the Laplace mechanism, the matching rate is increased by 52.33%, the matching accuracy is increased by 33.32%, the matching score is increased by 55.93%, and the recall rate is increased by 67.48%.

REFERENCES

[1] (Oct. 2020). *Biometric Privacy Protection Research Report. China Information and Communication Academy, Telecommunication Terminal Industry Association, Internet Society of China*. Accessed: Jul. 19, 2023. [Online]. Available: http://www.caict.ac.cn/kxyj/qwfb/ztbg/202010/P020201028364732231494.pdf

[2] V. Gopichandran, P. Ganeshkumar, S. Dash, and A. Ramasamy, "Ethical challenges of digital health technologies: Aadhaar, India," *Bull. World Health Org.*, vol. 98, no. 4, pp. 277–281, Apr. 2020, doi: 10.2471/blt.19.237123.

[3] C. Militello, V. Conti, S. Vitabile, and F. Sorbello, "Embedded access points for trusted data and resources access in HPC systems," *J. Supercomput.*, vol. 55, no. 1, pp. 4–27, Jan. 2011.

[4] Z. Cui, J. Feng, and J. Zhou, "Monocular 3D fingerprint reconstruction and unwarping," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 7, pp. 8679–8695, Jul. 2023, doi: 10.1109/TPAMI.2022.3233898.

[5] R. Richter, C. Gottschlich, L. Mentch, D. H. Thai, and S. F. Huckemann, "Smudge noise for quality estimation of fingerprints and its validation," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 1963–1974, Aug. 2019, doi: 10.1109/TIFS.2018.2889258.

[6] V. S. Baghel, S. Prakash, and I. Agrawal, "An enhanced fuzzy vault to secure the fingerprint templates," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 33055–33073, Sep. 2021, doi: 10.1007/s11042-021-11325-w.

[7] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2D fingerprint recognition," *EURASIP J. Image Video Process.*, vol. 2021, no. 1, pp. 1–28, Dec. 2021, doi: 10.1186/s13640-021-00548-4.

[8] Y. Wen, B. Liu, M. Ding, R. Xie, and L. Song, "IdentityDP: Differential private identification protection for face images," *Neurocomputing*, vol. 501, pp. 197–211, Aug. 2022, doi: 10.1016/j.neucom.2022.06.039.

[9] Z. Kuang, L. Teng, X. He, J. Ding, Y. Nakashima, and N. Babaguchi, "Anonymous identity sampling and reusable synthesis for face camouflage," *J. Electron. Imag.*, vol. 31, no. 2, Mar. 2022, Art. no. 023011, doi: 10.1117/1.jei.31.2.023011.

[10] L. Bastian, T. D. Wang, T. Czempiel, B. Busam, and N. Navab, "DisguisOR: Holistic face anonymization for the operating room," *Int. J. Comput. Assist. Radiol. Surg.*, vol. 18, no. 7, pp. 1209–1215, May 2023, doi: 10.1007/s11548-023-02939-6.

[11] C. Kim, "Separable reversible data hiding in encrypted AMBTC images using Hamming code," *Appl. Sci.*, vol. 12, no. 16, p. 8225, Aug. 2022, doi: 10.3390/app12168225.

[12] U. Sopaoglu and O. Abul, "Classification utility aware data stream anonymization," *Appl. Soft Comput.*, vol. 110, Oct. 2021, Art. no. 107743, doi: 10.1016/j.asoc.2021.107743.

[13] E. D. Cannas, S. Mandelli, P. Bestagini, S. Tubaro, and E. J. Delp, "Deep image prior amplitude SAR image anonymization," *Remote Sens.*, vol. 15, no. 15, p. 3750, Jul. 2023, doi: 10.3390/rs15153750.

[14] C.-H. Yang, C.-Y. Weng, and J.-Y. Chen, "High-fidelity reversible data hiding in encrypted image based on difference-preserving encryption," *Soft Comput.*, vol. 26, no. 4, pp. 1727–1742, Feb. 2022, doi: 10.1007/s00500-022-06745-1.

[15] F. Song, T. Ma, Y. Tian, and M. Al-Rodhaan, "A new method of privacy protection: Random k-Anonymous," *IEEE Access*, vol. 7, pp. 75434–75445, 2019, doi: 10.1109/ACCESS.2019.2919165.

[16] G. Xu, G. Li, S. Guo, T. Zhang, and H. Li, "Secure decentralized image classification with multiparty homomorphic encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 7, pp. 3185–3198, Jul. 2023, doi: 10.1109/TCSVT.2023.3234278.

[17] J. Liu, K. Zhao, and R. Zhang, "A fully reversible data hiding scheme in encrypted images based on homomorphic encryption and pixel prediction," *Circuits, Syst., Signal Process.*, vol. 39, no. 7, pp. 3532–3552, Jul. 2020, doi: 10.1007/s00034-019-01321-9.

[18] C. Dwork, "Differential privacy," in *Proc. Int. Colloq. Automata, Lang., Program.* Berlin, Germany: Springer, Jul. 2006, pp. 1–12, doi: 10.1007/11787006_1.

[19] S. Guo, T. Zhang, G. Xu, H. Yu, T. Xiang, and Y. Liu, "Topology-aware differential privacy for decentralized image classification," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 6, pp. 4016–4027, Jun. 2022, doi: 10.1109/TCSVT.2021.3105723.

[20] Y. Kong, Y. Qian, F. Tan, L. Bai, J. Shao, T. Ma, and S. N. Tereshchenko, "CVDP k-means clustering algorithm for differential privacy based on coefficient of variation," *J. Intell. Fuzzy Syst.*, vol. 43, no. 5, pp. 6027–6045, Sep. 2022, doi: 10.3233/jifs-213564.

[21] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Trans. Signal Process.*, vol. 68, pp. 4069–4082, 2020, doi: 10.1109/TSP.2020.3006760.

[22] F. Kato, Y. Cao, and M. Yoshikawa, "Preventing manipulation attack in local differential privacy using verifiable randomization mechanism," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*. Cham, Switzerland: Springer, 2021, pp. 43–60, doi: 10.1007/978-3-030-81242-3_3.

[23] C. M. Bowen and J. Snoke, "Comparative study of differentially private synthetic data algorithms from the NIST PSCR differential privacy synthetic data challenge," 2019, *arXiv:1911.12704*.

[24] M. Kroll, "On density estimation at a fixed point under local differential privacy," *Electron. J. Statist.*, vol. 15, no. 1, pp. 1783–1813, Jun. 2023, doi: 10.1214/21-EJS1830.

[25] Z. Shen, Z. Xia, and P. Yu, "PLDP: Personalized local differential privacy for multidimensional data aggregation," *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Jan. 2021, doi: 10.1155/2021/6684179.

[26] M. Aissaoui, "Proportional differential privacy (PDP): A new approach for differentially private histogram release based on buckets densities," in *Proc. 9th IFIP Int. Conf. Perform. Eval. Model. Wireless Netw. (PEMWN)*, Dec. 2020, pp. 1–7, doi: 10.23919/PEMWN50727.2020.9293079.

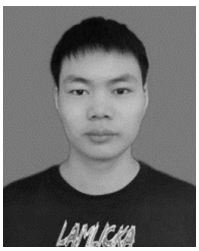
[27] S. Zhang, W. Ni, and N. Fu, "Community preserved social graph publishing with node differential privacy," in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, Nov. 2020, pp. 1400–1405, doi: 10.1109/ICDM50108.2020.00184.

[28] C. Liu, J. Yang, X. Zhang, Y. Zhang, W. Zhao, F. Miao, and Y. Shao, "Local privacy protection for sensitive areas in multiface images," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–15, Mar. 2022, doi: 10.1155/2022/5919522.

[29] T. Wang, Z. Zheng, A. K. Bashir, A. Jolfaei, and Y. Xu, "FinPrivacy: A privacy-preserving mechanism for fingerprint identification," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–15, Aug. 2021, doi: 10.1145/3387130.

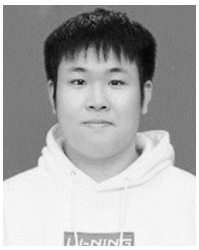
[30] X. Xiao, G. Wang, and J. Gehrke, "Differential privacy via wavelet transforms," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 8, pp. 1200–1214, Aug. 2011, doi: 10.1109/TKDE.2010.247.
[31] S. Zhang, L. Liu, Z. Chen, and H. Zhong, "Probabilistic matrix factorization with personalized differential privacy," *Knowl.-Based Syst.*, vol. 183, Nov. 2019, Art. no. 104864, doi: 10.1016/j.knosys.2019.07.035.
[32] X. Zhang, C. Fu, and X. Meng, "The differential privacy preservation for face image publishing," *Chin. J. Image Graph.*, vol. 9, pp. 1305–1315, May 2018, doi: 10.11834/jig.170647.
[33] X. Zhang, C. Fu, and X. Meng, "Combining matrix decomposition and the differential privacy for face image publishing," *Chin. J. Image Graph.*, vol. 25, pp. 655–668, Sep. 2020, doi: 10.11834/jig.190308.
[34] C. Liu, J. Yang, and J. Wu, "Web intrusion detection system combined with feature analysis and SVM optimization," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–9, Dec. 2020, doi: 10.1186/s13638-019-1591-1.
[35] C. Liu, J. Yang, W. Zhao, Y. Zhang, J. Li, and C. Mu, "Face image publication based on differential privacy," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–20, Jan. 2021, doi: 10.1155/2021/6680701.
[36] C. Liu, J. Yang, W. Zhao, Y. Zhang, C. Shi, F. Miao, and J. Zhang, "Differential privacy protection of face images based on region growing," *Traitement Signal*, vol. 38, no. 5, pp. 1385–1401, Oct. 2021, doi: 10.18280/ts.380514.
[37] C. Liu, J. Yang, Y. Zhang, X. Zhang, W. Zhao, F. Miao, and Y. Shao, "Non-global privacy protection facing sensitive areas in face images," *Traitement Signal*, vol. 38, no. 6, pp. 1677–1687, Dec. 2021, doi: 10.18280/ts.380611.
[38] H. Xu, Z. Cai, and W. Li, "Privacy-preserving mechanisms for multi-label image recognition," *ACM Trans. Knowl. Discovery Data*, vol. 16, no. 4, pp. 1–21, Aug. 2022, doi: 10.1145/3491231.
[39] S. S. Hameed, I. T. Ahmed, and O. M. A. Okashi, "Real and altered fingerprint classification based on various features and classifiers," *Comput., Mater. Continua*, vol. 74, no. 1, pp. 327–340, 2023, doi: 10.32604/cmc.2023.031622.
[40] M. Min, L. Xiao, J. Ding, H. Zhang, S. Li, M. Pan, and Z. Han, "3D geo-indistinguishability for indoor location-based services," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 4682–4694, Jul. 2022, doi: 10.1109/TWC.2021.3132464.
[41] D. Arivalagan, K. B. Began, S. E. P. Pushpa, and K. Rajendran, "A novel intelligent 12-layer convolutional neural network model for gender classification using fingerprint images," *J. Intell. Fuzzy Syst.*, vol. 45, no. 2, pp. 2685–2706, Aug. 2023, doi: 10.3233/jifs-224284.
[42] S. Zhao, D. Ge, J. Zhao, and W. Xiang, "Fingerprint pre-processing and feature engineering to enhance agricultural products categorization," *Future Gener. Comput. Syst.*, vol. 125, pp. 944–948, Dec. 2021, doi: 10.1016/j.future.2021.07.005.
[43] Q. Pang, Y. Xu, F. Chen, G. Lu, and D. Zhang, "Hierarchical pore-based high-resolution fingerprint indexing," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–13, 2022, doi: 10.1109/TIM.2022.3146944.
[44] A. S. Shinde and V. Bendre, "An embedded fingerprint authentication system," in *Proc. Int. Conf. Comput. Commun. Control Autom.*, Feb. 2015, pp. 205–208, doi: 10.1109/ICCUBEA.2015.45.
[45] (2004). *Fingerprint Verification Competition*. [Online]. Available: http://bias.csr.unibo.it/fvc2004/

CHAO LIU was born in Qiqihar, Heilongjiang, China, in 1982. He received the Ph.D. degree in computer science and technology from Harbin Engineering University, Harbin, Heilongjiang, in 2020. He is currently a Professor with the School of Communication and Electronic Engineering, Qiqihar University, where his main research interests include artificial intelligence, privacy protection, and image recognition.



ZHAOLONG ZHI was born in Zhoukou, Henan, China, in 2000. He received the B.S. degree in electronic information engineering from the Anyang Institute of Technology, Anyang, Henan, in 2022. He is currently pursuing the M.S. degree in information and communication systems, with a major focus on research on the protection of private images that contain human biometrics with Qiqihar University, Qiqihar, Heilongjiang, China.

WEINAN ZHAO was born in Daqing, Heilongjiang, China, in 1984. She received the master's degree in international accounting and strategic consulting from the University of Reading, U.K., in 2009. She is currently a Lecturer with the School of Economics and Management, Qiqihar University, where she focuses her research on issues related to economic data forecasting and privacy protection.



ZHICHENG HE was born in Jingdezhen, Jiangxi, China, in 2003. He is currently pursuing the Bachelor of Engineering degree in artificial intelligence with Qiqihar University, Qiqihar, Heilongjiang, China, focusing on research on the protection of human biometric privacy images.