*Fuzzy Systems and Data Mining VI*
*A.J. Tallón-Ballesteros (Ed.)*

*doi:10.3233/FAIA200745*

# Differential Privacy Trajectory Data Protection Algorithm Based on Polar Coordinate Transformation

Zhenzhen ZHANG, Jianping CAI, Lan SUN, Yongyi GUO, Yubing QIU, Yingjie WU[1]
*College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China*

**Abstract.** Differential privacy technology has been widely used in the issue of trajectory data release. Improving the availability of data release under the premise of ensuring privacy and security is one of its basic research goals. At present, most trajectory data release methods use a rectangular coordinate system to represent location information. Research has shown that the availability of published data cannot be optimized through the rectangular coordinate system. In order to improve the effect of trajectory data release, this paper proposes a differential privacy trajectory data protection algorithm based on polar coordinates. First, the stay point detection method is used to find frequent stay points in the trajectory and the key location points related to personal privacy are detected by the type of location points. Then, this paper converts the rectangular coordinate system representation of the key position points to the polar coordinate system representation, and implement differential privacy trajectory data release by adding noise to the key position points represented by the polar coordinates. Experiments show that the algorithm proposed in this paper effectively improves the usability of trajectory data on real data sets.

**Keywords.** Trajectory data protection, Differential privacy, Polar coordinates, Position type

## 1. Introduction

In recent years, with the development of smartphones and the popularization of location-based services (LBS), the location information continuously uploaded by mobile objects has formed trajectory big data. The release of trajectory data enables people to analyze and mine it, and provide strong support for government departments in urban planning and commercial organizations in decision-making. However, if these trajectory data is directly released without protection, malicious attack reasoning will pose a serious threat to individual privacy. For example, Strava [1], a popular movement in Europe and the United States in 2017, released a "heat map" of user activities in the world, and netizens unearthed the location of military bases, training time, home addresses and real identities of individual users. Therefore, protecting the privacy of user identity while taking into account the high availability of data and

[1] Corresponding Author: Yingjie WU, College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China; E-mail: yjwu@fzu.edu.cn.

achieving the secure release of trajectory data has become the core content of current trajectory data release research.

Nowadays, more and more people pay attention to privacy data protection, and some researchers [2-3] have conducted in-depth studies on privacy date protection in many fields. To realize an effective personal privacy protection scheme in the process of data release, in 2006 Dwork [4] and others proposed a differential privacy protection model, which is currently recognized as a model for strict privacy protection, mainly through the original data, original data add appropriate noise to the conversion or statistical results to achieve privacy protection. Compared with other trajectory protection methods such as suppression [5], it theoretically guarantees that no matter what background knowledge the attacker has, any record in the original database cannot be identified [6].

Differential privacy protection was originally applied in the field of statistical database security, aiming to protect the private information of individuals in the database when statistical information is released. In 2012, Chen et al. [7] proposed the use of differential privacy to protect trajectory data. By adding Laplace noise to the location data to ensure that the mining results meet the differential privacy requirements, the trajectory privacy protection of transportation information can be realized. The differential privacy mechanism has since been used for trajectory privacy protection. Subsequently, many researchers researched this field and achieved a series of results. The PriLocation [8] algorithm consists of three operations: location clustering, weight interference, and location selection. Since the number of clusters is much smaller than the number of locations, the number of times of adding noise is drastically reduced, thereby reducing the amount of noise. Literature [9] believes that the generated random and unbounded noise cannot completely realize differential privacy, so it proposes a bounded noise generation algorithm and a trajectory merging algorithm, which effectively improves the efficiency of privacy protection. Literature [10] proposed a method of dividing the trajectory into shorter new trajectories, which is suitable for processing longer trajectory data. Literature [11] divides the entire plane location area into several hexagons, and at the same time geographic indistinguishability technology is used to reduce the loss of privacy budget by publishing the location of the centroid of each hexagon.

When protecting the trajectory data set, the existing trajectory data protection algorithms directly add noise to the longitude and latitude of the position indicated in the rectangular coordinate system. And most of them are only based on the distance measurement to identify the location, which is difficult to distinguish a certain location belongs to what type of building. Though personal privacy is protected, the availability of data is low [12]. At the same time, during the privacy protection of trajectory data, if all trajectory data sets are directly disturbed to protect personal privacy, serious loss of data information will become unusable. Therefore, finding key location points in the trajectory data set that will leak personal privacy is a major problem at present. And Literature [13] proposed a method to protect important location points of the trajectory based on the k-anonymity model. It innovatively models and process semantic trajectories which greatly improve data availability. But the k-anonymity model cannot provide an effective and strict method to prove its level of privacy protection. In order to solve the above problems, Baidu Map Application Programming Interface (API) technology is utilized to mine the Point of Information (POI) of frequently staying points to obtain the types of location points, thereby determining the key location points for protection and subsequent experiments prove that the rectangular coordinate representation of longitude and latitude is converted into extremes. Coordinate representation and differential privacy protection can greatly improve the availability of trajectory data.

In summary, this paper has made the following innovations.

- In order to provide stronger support for government departments in urban planning and decision-making by commercial institutions, Baidu Map API technology is utilized to get the POI of the location point to obtain the location type. Then according to whether the location type leak privacy, the location points are divided into key location points and non-critical locations, and key location points which are easy to reveal personal privacy are protected. Make the protected data more realistic.
- This paper innovatively proposes that converting the rectangular coordinate representation of the private location point into polar coordinate representation. Then the differential privacy protection mechanism is used to protect the polar coordinate of the sensitive location point. Experiments on the real data set prove that the data conversion can greatly improve the availability of data.

## 2. Basic Knowledge and Definitions

The differential privacy protection model is currently recognized as a model that provides strict privacy protection. It mainly implements privacy protection by adding appropriate noise to the original data, the conversion of the original data, or the statistical results.

**Definition 1** ($\varepsilon$ - Differential Privacy [4]) Given data sets $D_1$ and $D_2$ that differ by only one record, i.e. $|D_1 \Delta D_2 \leq 1|$ .Given a privacy algorithm $A$ , $Rang(A)$ is the range of $A$ . If the output result $O(O \in Rang(A))$ of algorithm $A$ on data set $D_1$ and $D_2$ satisfies Eq. (1), then $A$ satisfies $\varepsilon$ - differential privacy.

$$\Pr[A(D_1) = O] \leq e^{\varepsilon} \times \Pr[A(D_2) = O] \tag{1}$$

Privacy budget parameter $\varepsilon$ represents the degree of privacy protection. The smaller the $\varepsilon$ value, the higher the degree of privacy protection and the greater the noise added. And the Laplacian mechanism [14] is a commonly used noise adding mechanism, which realizes differential privacy by adding a noise value satisfying the Laplacian distribution to the query result.

**Definition 2** (Trajectory Data Set [15]) A trajectory is a chronological sequence of the position information of a moving object. A trajectory can be expressed as $T = \{(x_1, y_1, t_1), (x_2, y_2, t_2), ..., (x_n, y_n, t_n)\}$ , where $(x_i, y_i, t_i)$ represents the user's position point at time $t_i$, $x_i$ represents latitude, and $y_i$ represents longitude. $T[i]$ represents the i-th element of the trajectory $T$ , $|T| = n$ represents the length of the trajectory $T$ .The trajectory data set is a set of multiple trajectories.

In order to realize the safe release of the trajectory data set, literature [16] uses the definition of differential privacy to propose a Geo-indistinguishability model (Geo-Indistinguishability). Based on the reality of location privacy protection, this model believes that small changes in the user's location should have little impact on the query results, but when the user's location changes greatly, the query results can have large changes, so it can be based on the degree of user location changes. Set the corresponding privacy protection level.

**Definition 3** (Geo-Indistinguishability [16]) Suppose that $X$ represents the set of possible locations for users and $Z$ represents the set of possible locations for publishing, $d(\cdot,\cdot)$ is the Euclidean distance, For any two positions $x_{1,} x_2 \in X$, $z \in Z$ and $d(x_1, x_2) \leq r$, if the algorithm $K$ satisfies Eq. (2), it is said that $K$ satisfies $\varepsilon$ -inseparable region within the radius $r$.

$$\Pr[K(x_1) = z] \leq \exp(\varepsilon \cdot d(x_1, x_2)) \cdot \Pr[K(x_2) = z] \tag{2}$$

The parameter $\varepsilon$ represents the privacy protection level per unit distance. Geo-Indistinguishability can be achieved by adding two-dimensional Laplace noise to the user's real location. The geographical indistinguishability model proposes a practical mechanism for the application of differential privacy in location privacy protection, which becomes the basis of some follow-up studies.

Literature [17] proposes that if Geo-Indistinguishability is independently applied to each location, the amount of noise generated will be unacceptable. Since certain behavior patterns and habits of users can be obtained by digging the location points or areas where the user stays for a long time, these location points and areas are protected.

**Definition 4** (Stop point detection [18]) A cluster whose distance is less than a certain threshold and whose time difference is greater than a certain threshold is regarded as a stopping area. If the requirement of Eq.(3) is satisfied, the trace sequence from $(x_i, y_i, t_i)$ to $(x_j, y_j, t_j)$ is the stay region. The average position point of latitude and longitude of the trajectory sequence of the stop area is the stop point.

$$\begin{aligned} &Dis\tan ce((x_i, y_i),(x_j, y_j)) \leq \Delta S \\ &\cap Dis\tan ce((x_i, y_i),(x_{j+1}, y_{j+1})) \succ \Delta S \cap t_j - t_i \geq \Delta T \end{aligned} \tag{3}$$

Because Dynamic Time Warping (DTW) distance allows time series to be scaled locally to minimize the distance between two sequences, it can better match the characteristics of time series, which makes it widely adopted [19]. Therefore, this paper adopts DTW distance to measure data availability.

**Definition 5** (Dynamic Time Warping (DTW) distance [20]) Suppose there are two tracks $A = \{(x_1, y_1, t_1),(x_2, y_2, t_2),\ldots,(x_n, y_n, t_n)\}$ and $B = \{(x_1, y_1, t_1),(x_2, y_2, t_2),\ldots,(x_m, y_m, t_m)\}$, is the DTW distance between two trajectories as follows:

$$\begin{aligned} &DTW(A,B) = dist(A_1, B_1) + \\ &\min(DTW(\mathrm{Re}\,st(A),B), DTW(A,\mathrm{Re}\,st(B)), DTW(\mathrm{Re}\,st(A),\mathrm{Re}\,st(B)) \end{aligned} \tag{4}$$

where $dist(A_1, B_1) = |A_1 - B_1|$, $Rest(T)$ is the child track after the first position point of the track is removed.

## 3. Differential Privacy Trajectory Data Protection Algorithm Based on Polar Coordinate Transformation

To achieve the high availability of the trajectory data set, and security, this paper proposes a differential privacy trajectory data protection algorithm based on polar coordinate transformation, the algorithm includes two steps. First step, find frequent stops, and then Baidu Map API technology is used to get the POI for the position type, so as to determine the key location points which easily leak privacy. Second step, Transform the rectangular coordinate system representation of the privacy position points into the polar coordinate system representation. Then, using the differential privacy protection mechanism to add noise to the key location points in the polar coordinate representation. Finally generate the trajectory data after user privacy protection. Each of these processes is described below.

### *3.1. Find Key Location Points*

When the privacy of trajectory data is protected, if all the position points are directly protected by noise, the data will become unusable. Moreover, not all points can reveal personal privacy, so it is a big problem to find the key points in the trajectory data set that can reveal personal privacy.

### *3.1.1. Frequent Stop Points Detection*

Literature [21] points out that users' frequent stop points are the easiest to infer personal privacy information. If the occurrence times of a stop location point are greater than the frequency threshold $\Delta Q$, the stop point is a frequent stop point. And Literature [17] adds noise to the frequent stop points of the trajectory to achieve personal privacy protection, and the experimental results showed that the availability of data was greatly improved. Therefore, based on this work, this paper further improves the availability of data. This process is mainly to find the frequent stop points in the user's trajectory data set. The key is to calculate the trajectory set whose stay time is greater than a certain time threshold, but whose distance is limited within a certain distance threshold, and then traverse to find the stop points whose occurrence frequency is greater than the frequency threshold, which are frequent stop points. In this paper, the time threshold and distance threshold of the stop point refers to the stop point analysis of Baidu Map API, and the time threshold is set as 10 minutes, the distance threshold is 20m. And the frequency threshold $\Delta Q$ is analyzed in the experimental part.

### *3.1.2. Identify Key Location Points*

Baidu Map API technology is a set of application interfaces based on Baidu Map service which is provided for developers for free. It provides a basic map display, reverses geocoding services, and other functions. The reverse geocoding service can provide the POI for the corresponding location based on the longitude and latitude of the requested location point, where the POI contains the type of the location point. A partial display of Baidu Map as shown in Figure 1. For each location, in addition to the name information, there are icons of the type to which the location belongs, such as Brownings Grove Park belongs to the type of tourist attractions in Figure 1.

**Figure 1.** A Part of Baidu Map.

Literature [22] found that by disturbing the location points in the continuous positions, the user's trajectory privacy can also be obtained by restricting the attacker's association. Therefore, it is important to select key location points in the trajectory data set that is likely to leak user privacy.

In order to make the track data released safely can better provide strong support for the urban planning of government departments and the decision-making of commercial organizations. Baidu Map API technology is used to connect the trajectory with reality, and requests the types of frequent stop points from Baidu Map API. The types are set as non-key location points according to whether the location points are public entertainment and not easy to reveal personal privacy. In this paper, shopping, tourist attractions and life services are set as non-key location points. And the other point types that leak personal privacy are set as the key location points, then protect these points. This paper roughly classifies whether the location is critical, and a follow-up investigation is needed to determine whether the point type is a key point type that is prone to divulging personal privacy.

The process begins by setting the appropriate API's Uniform Resource Location (URL) with the latitude and longitude of frequent stop points. Then, a request is sent to the Baidu Map API, and the POI of the location point represented by the Extensible Markup Language (XML) file is returned, and the location type is extracted by using the regular expression. Finally, determining if the type of point contains the name of the above key point types. If yes, setting the point as the key location point which is saved to the critical location point set $G = \{(x_1, y_1), (x_2, y_2), ..., (x_m, y_m)\}$ for privacy protection in the next step.

### 3.2. Add Noise to Key Location Points Based on Polar Coordinate

If the key location points that are likely to leak personal privacy are published without personal privacy protection, it may damage personal reputation, property, physical and mental health or discriminatory treatment [23]. Because Geo-indistinguishability can be achieved by adding two-dimensional Laplace noise to a user's real location. Therefore, for the attacker cannot obtain personal sensitive information from the published trajectory information, traditional differential privacy trajectory data protection algorithms directly noise the longitude and latitude which expressed by the rectangular coordinate system. In this paper, the rectangular coordinate representation of latitude and longitude is creatively converted into polar coordinate representation, and then noise protection is carried out. After data transformation, the position points in spatial coordinates can be expressed in the same way, but the availability of data can be greatly improved.

The process starts with the data transformation of the set of key location points obtained in the previous step $G=\{(x_1,y_1),(x_2,y_2),...,(x_m,y_m)\}$, convert the rectangular coordinate system representation of latitude and longitude of each location point to polar coordinate system representation $JG=\{(\rho_1,\theta_1),(\rho_2,\theta_2),...,(\rho_m,\theta_m)\}$ .Then $2m$ random noises obeying Laplace distribution are generated, and the noises were successively added to the polar coordinates $\rho_i$ and $\theta_i$ in the JG data set. Finally, the polar coordinate system is converted back to the longitude and latitude coordinate system, and the original position points are replaced. The algorithm steps are shown in algorithm 1.

**Algorithm 1** Data conversion and add noise

**Input:** Key location points set $G=\{(x_1,y_1),(x_2,y_2),...,(x_m,y_m)\}$;

**Output:** $PG=\{(x_1^{'},y_1^{'}),(x_2^{'},y_2^{'}),...,(x_m^{'},y_m^{'})\}$ as the points set after differential privacy protection;

```
Converts the set G to a polar representation $JG=\{(\rho_1,\theta_1),(\rho_2,\theta_2),...,(\rho_m,\theta_m)\}$;
Generate $Lap(1/\varepsilon)$ noise sets $L=\{(z\rho_1,z\theta_1),(z\rho_2,z\theta_2),...,(z\rho_m,z\theta_m)\}$;
For $S$ in $JG$
    $\rho_i=\rho_i+z\rho_i$; $\theta_i=\theta_i+z\theta_i$;
End for;
Converts a $JG$ set to a set $PG$ represented by rectangular coordinates
```

In order to verify that the conversion of the rectangular coordinate system representation of the location point to the polar coordinate representation can improve the usability of the data, the frequent stay points with and without data conversion are compared and analyzed. Figure 2 randomly selects all trajectory data sets of three users in a year as examples, but the complete experimental results are consistent with the distribution of the sample trajectory results. Among them, the PC method represents the method of adding noise to the position indicated by the polar coordinate system which use a five-pointed star to mark the point; RC represents the method of adding noise to the position expressed by the rectangular coordinate system which use a triangle to mark the point. Different users are represented by different colors. It can be seen from Figure 2 that for each user, the PC method has less distortion than the IR method. And when the value of ε is smaller which represent the degree of privacy protection is higher, the less distortion of the PC method than the IR method becomes more obvious. It is verified that data conversion can greatly improve the usability of trajectory data.

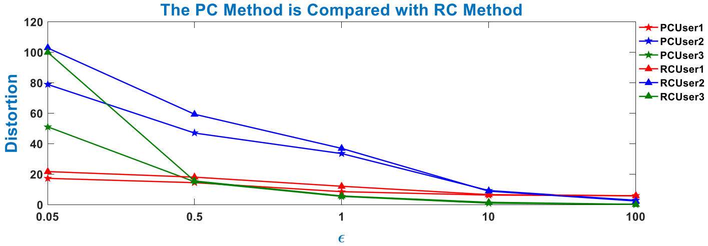

**Figure 2.** The PC Method is Compared with RC Method.

## 4. Experimental Analysis

For fair comparisons, all experiments are implements on MATLAB and GeoLife GPS Trajectories [24-26] dataset provided by Microsoft Research Asia. The dataset was completed by 182 users in more than 5 years. There are 17621 trajectories, each represented by a series of timestamps points, and each timestamps point contains latitude, longitude, and time information. Most of the data is created every 1 to 5 seconds or every 5 to 10 meters in Beijing, China. Since the location points of the trajectory data set are collected intensively, this article reads the original trajectory data every 5 minutes to simplify the data set.

### *4.1. Evaluation Criteria*

In the data release research for trajectory privacy protection, data utility and privacy protection degree are two main evaluation indicators.

- **Data utility.** Since DTW distance [16] allows time series to be locally scaled to minimize the distance between the two series, it can better match the characteristics of the time series, which makes it widely adopted. Therefore, this paper uses DTW to determine the deviation from the original trajectory and measure the utility of the data. The DTW distance represents the degree of distortion after trajectory data protection. The smaller the trajectory distortion, the greater the similarity to the original trajectory, and the higher the availability of processed data. The greater the trajectory distortion, the smaller the similarity to the original trajectory, and the lower the availability of processed data.
- **Degree of privacy protection.** According to the definition of differential privacy, the privacy budget parameter $\varepsilon$ represents the degree of privacy protection. The smaller the ε value, the greater the noise added to the original trajectory and the higher the degree of privacy protection; the larger the $\varepsilon$ value, the smaller the noise added to the original trajectory. The lower the degree of privacy protection.

### *4.2. Parameter Analysis*

In summary, this paper has two parameters, the frequency threshold $\Delta Q$ of the stay point and the privacy protection degree $\varepsilon$ of the differential privacy protection mechanism. This section analyzes and discusses the different values of $\Delta Q$ and $\varepsilon$ for studying the influence of the setting of these two parameters on the performance of the algorithm.

In this paper, the stay points where a certain stay point appears more than the frequency threshold $\Delta Q$ are called frequent stay points. Considering the accuracy of the actual latitude and longitude which have six decimal places, and the stay points are obtained as the average of multiple points, so when searching frequent stay point, this paper set the actual tolerance of 1 meter. Figure 3 randomly selects all trajectory data sets of 5 users in a year for display, and analyzes the influence of different frequency threshold $\Delta Q$ on distortion when $\varepsilon = 0.5$. Different colors indicate different users, the abscissa indicates the frequency threshold $\Delta Q$, and the ordinate indicates the distortion represented by the DTW distance. It can be seen from Figure 3 that as the frequency threshold $\Delta Q$ increases, the distortion shows a downward trend. The reason is that the greater the frequency threshold $\Delta Q$, the stricter the conditions for forming key location points which making fewer key location points. So that the disturbance location points become less when adding noise which leads to the less distortion. And due to the randomness of noise, some data fluctuate slightly in a certain interval.

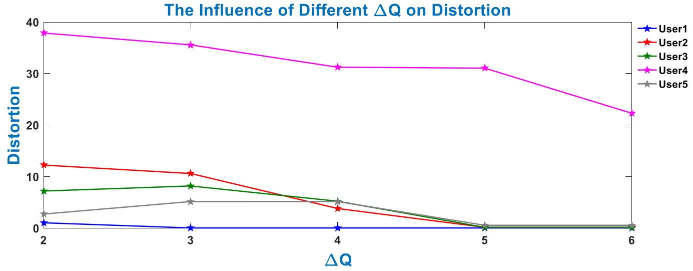

**Figure 3.** The Influence of Different $\Delta Q$ on Distortion.

Figure 4 also randomly selects all trajectory data sets of 5 users in a year for display, and analyzes the influence of different privacy protection degrees $\varepsilon$ on distortion when $\Delta Q = 2$. Among them, different colors represent different users, the abscissa represents the frequency threshold $\Delta Q$, and the ordinate represents the distortion represented by the DTW distance. It can be seen from Figure 4 that as the degree of privacy protection $\varepsilon$ increases, the distortion degree shows a downward trend. This is because of the larger the $\varepsilon$ value, the lower the degree of privacy protection, the smaller the added noise, and the smaller the distortion. Due to the randomness of noise, some data fluctuate slightly in a certain interval.

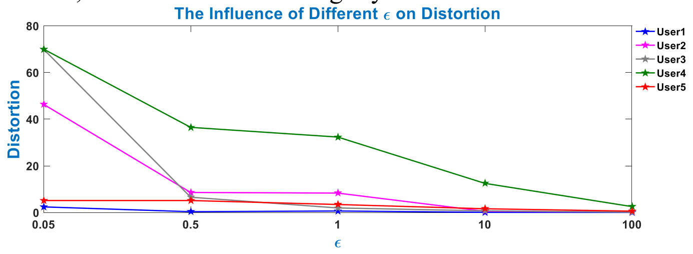

**Figure 4.** The Influence of Different $\varepsilon$ on Distortion.

### 4.3. Experimental Comparison and Analysis

In 2019, literature [17] proposed the Interest Region (IR) method which is the frontier method in this direction. And it also protects the sensitive location points of the trajectory based differential privacy technology. So the IR method is used as a baseline method to demonstrate the effectiveness of the proposed method in this paper. In this section, this paper compares and analyzes the PT algorithm which is proposed in this paper and IR algorithms. This experiment use real data sets and set $\Delta Q = 2$. Figure 5 randomly selects all trajectory data sets of three users in one year for example, but the complete experimental results are consistent with the distribution of the sample trajectory results. The algorithm PT algorithm uses five-pointed stars for punctuation;

the IR algorithm uses circular punctuation. Different users are represented by different colors. It can be seen from Figure 5 that for each user, the PT algorithm which is proposed in this paper has less distortion than the IR algorithm. And when the value $\varepsilon$ is smaller which means the degree of privacy protection is higher, the less distortion of the PT algorithm than the IR algorithm becomes more obvious. It is verified that the algorithm in this paper can greatly improve the usability of trajectory data in the process of safely publishing trajectory data.

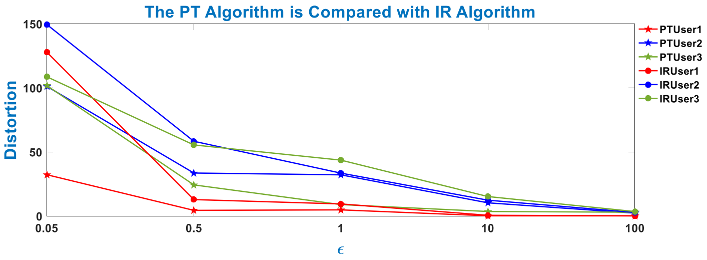

**Figure 5.** The PT Algorithm is Compared with IR Algorithm.

## 5. Conclusion

For the release of the trajectory data set, this paper connects the position with reality, and proposes a differential privacy trajectory data protection algorithm based on polar coordinate conversion. The algorithm uses Baidu Map API technology to obtain POI which contain point types. Then determining key location points that are likely to leak personal privacy, thereby provide stronger support for government departments in urban planning and commercial organizations in decision-making. Besides, the rectangular coordinate system representation of the key location points is converted to the polar coordinate system representation, and then the differential privacy protection mechanism is used to protect the key location points represented by the polar coordinate system. Experiments show that this data conversion greatly improves the availability of data. However, the trajectory also contains a lot of other real information, such as speed, transportation, etc. Combining this real information to set different privacy protection levels can make the protected data more realistic and improve the usability of the data. Therefore, how to use other realistic information to achieve better trajectory data privacy protection and release is the next research direction.

## References

[1] Lu YL. An American fitness APP leaked information about military bases, 2018. https://www.guancha.cn/america/2018_01_29_445035_s.shtml

[2] D.Chandramohan, Rajaguru.D, Vengattaram.T, Dhavachelvan.P, "A COORDINATOR ‐ SPECIFIC PRIVACY ‐ PRESERVING MODEL FOR E ‐ HEALTH MONITORING USING ARTIFICIAL BEE COLONY APPROACH", Security and Privacy. (2018). https://doi.org/10.1002/spy2.32.

[3] Chandramohan.D, Vengattaraman.T, Rajaguru.D, Baskaran.R and Dhavachelvan.P, "EMPPC-An Evolutionary Model Based Privacy Preserving Technique for Cloud Digital Data Storage Service", 3rd IEEE International Advance Computing Conference, INDIA, 2013, 6, pp.89-95. ISBN: 978-1-4673-4528.

[4] Dwork C. Differential privacy. Proceedings of the 33rd international conference on Automata, Languages and Programming - Volume Part II. Springer, Berlin, Heidelberg, 2006. 26(2):1-12.

[5] Komishani EG, Abadi M, Deldar F. PPTD: Preserving personalized privacy in trajectory data publishing by sensitive attribute generalization and trajectory local suppression. Knowledge-Based Systems, 2016, 94(Feb.15):43–59.

[6] Zhang XJ, Meng XF. Differential privacy in data publication and analysis. Chinese Journal of Computers, 2014(4):927-949.

[7] Chen R, et al. Differentially private transit data publication: a case study on the montreal transportation system. Proceedings of the18th ACM SIGKDD international conference on Knowledge discovery and data mining, Beijing, China, August 12-16.New York, NY, USA: ACM, 2012: 213-221.

[8] Xiong P, Zhu TQ, Pan L, et al. Privacy preserving in location data release: A differential privacy approach. In: Pham DN and Park SB, Eds, PRICAI 2014: Trends in Artificial Intelligence, Springer, Berlin, 183-195.

[9] Li M, Zhu L, Zhang Z, et al. Achieving differential privacy of trajectory data publishing in participatory sensing. Information Sciences, 2017, s 400–401:1-13.

[10] Terrovitis M, Poulis G, Mamoulis N, et al. Local suppression and splitting techniques for privacy preserving publication of trajectories. IEEE Transactions on Knowledge and Data Engineering, 2017, 29(7):1466-1479.

[11] Hua JY, Tong W, Xu FY. A geo-Indistinguishable location perturbation mechanism for location-based services supporting frequent queries. IEEE Transactions on Information Forensics and Security, 2017:1-1.

[12] Wang B, Zhang L, Zhang GY. A gradual sensitive indistinguishable based location privacy protection scheme. Journal of Computer Research and Development, 2020, 57(3):616-630.

[13] Tan R , Tao Y , Si W , et al. Privacy preserving semantic trajectory data publishing for mobile location-based services[J]. Wireless Networks, 2019(1).

[14] Dwork C, Mcsherry F, Nissim K, et al. Calibrating noise to sensitivity in private data analysis. Proceedings of theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2006:265-284.

[15] Huo Z, Meng X F. A survey of trajectory privacy-preserving techniques. Chinese Journal of Computers, 2011, 34(10):1820-1830.

[16] Miguel E. Andrés NE. Bordenabe CK. Geo-Indistinguishability: Differential privacy for location-based systems. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, 4-8 November 2013, 901-914.

[17] Lan W, Lin Y, Bao LY, et al. A Trajectory-differential privacy-protection method with interest region. Journal of Frontiers of Computer Science and Technology,2020,14(1):59-72.

[18] Fu ZL, Tian ZS, Xu YQ, et al. A two-step clustering approach to extract locations from individual GPS trajectory data. ISPRS International Journal of Geo-Information, 2016, 5 (10):166.

[19] Liu Y , Chen J, Wu S , et al. Incremental fuzzy C me-doids clustering of time series data using dynamic time warping distance. PLoS ONE, 2018, 13(5):1-25.

[20] Sharma A, Sundaram S. On the exploration of Information from the DTW cost matrix for online signature verification. IEEE Transactions on Cybernetics, 2017, 48(2):611-624.

[21] Feng DG, Zhang M, Ye YT. Research on differentially private trajectory data publishing. Journal of Electronics & Information Technology, 2020, 042(001):74-88.

[22] Fei F, Li S, Dai H, et al. A K-anonymity based schema for location privacy preservation. IEEE Transactions on Sustainable Computing, 2019, 4(2): 156-167.

[23] Research report on Personal Information Protection of Internet + Industry. China Academy of Information and Communications Technology, 2020. http://www.caict.ac.cn/kxyj/qwfb/bps/202003/t20200301_275474.htm

[24] Zheng Y, Zhang LZ, Xie X, et al. Mining interesting locations and travel sequences from GPS trajectories. Proceedings of International conference on World Wild Web (WWW 2009), Madrid Spain. ACM Press, 2009: 791-800.

[25] Zheng Y, Li QN, Chen YK, et al. Understanding mobility based on GPS data. Proceedings of ACM conference on Ubiquitous Computing (UbiComp 2008), Seoul, Korea. ACM Press: 312-321.

[26] Zheng Y, Xie Y, Ma WY. GeoLife: A collaborative social networking service among user, location and trajectory. IEEE Data Engineering Bulletin. 2010, 33, 2, pp. 32-40.