EasyChair Preprint

№ 7152

QR-FLSB: a Personalized Location Big Data Privacy Protection Model

Baoshan Luo and Chao Yao

December 4, 2021

QR-FLSB: A Personalized Location Big Data Privacy Protection Model

Baoshan Luo
School of Information
Wuhan Vocational College of Software and Engineering
Wuhan, China
bshluo@qq.com

Chao Yao
School of Information
Wuhan Vocational College of Software and Engineering
Wuhan, China
chaoyao_wh@outlook.com

***Abstract*—With the rapid development of mobile communication and location-aware device technology, a large number of mobile intelligent terminal data will be generated every day. These data are not only large in data quantity and value, but also based on location service, so it is called location big data based on location service. In recent years, large data generated by location-based services has become a research hotspot in the industry. At the same time, people pay more and more attention to the privacy protection of big data. In view of the limitations of traditional privacy protection model based on "false location" of big location data, this paper proposes a model QR-FLSB (Quick Response-Fingerprint Location Based Services) based on fingerprint identification and two-dimensional code technology of intelligent terminals, which can better solve the privacy protection of location services to a certain extent. This experiment adopts the data from real data sets, and compares it with the location service privacy protection method of "false location". The performance of QR-FLSB model is measured by response time, robustness and privacy. The experimental results show that the scheme is not only suitable for the privacy protection of location services, but also improves the privacy protection of location services without sacrificing the quality of user location services.**

Location services; Fingerprint identification; Location privacy protection; K-anonymity technology; False position; Two-dimensional code technology

I. INTRODUCTION

With the development of science and technology, more and more intelligent life is advocated, such as intelligent city, intelligent bus and so on. For example, with the taxi software we usually used, and just tell the driver the specific location of the customer, then the driver could reach the location of the customer; and location navigation technology. These are location-based Services (LBS), which are value-added location-based Services provided by location-based service providers [1]. LBS service contains many contents, such as emergency service community, entertainment information, navigation tracking and monitoring mobile e-commerce and other location services [2]. Location services have grown in value from millions to billions in recent years. Visible location services can bring great wealth to future societies.

In order to obtain better location service, location service providers need users to provide accurate location information query requests, which can not only submit individual requirements more quickly, but also obtain better location service quality. But sometimes, once the accurate location information provided is used by hackers, it is likely to have a certain impact on users' work, life and study.

How to effectively protect user location privacy information? Gruteser M and Grunwal D et al. proposed the location k-anonymity model, whose basic idea is to replace the real location of users with an anonymous area containing k-1 users when publishing user locations, so that location service providers cannot identify a specific user from the K users [3]. K's anonymous location privacy protection method has been used in many fields (taobao shopping, etc.). Yiu M L, Jensen C S, Huang X, Lu H put forward a method of Space Twist, the user randomly selects a point near his real location as an anchor point, and then uses the anchor point instead of his real location to initiate an incremental neighbor query to the location service provider, then according to the real location of the user and the returned results, the exact query results are obtained [4]. Some researchers studied some attributes of location and proposed methods such as randomization [5], time blurring [6], and spatial blurring [6]. Li Wenhua et al. [7] based on Canonical Correlation Analysis on the basis of [8] developed a based on CCA (Canonical Correlation Analysis) of the location of the personalized path privacy protection algorithm, the algorithm of the innovation point lies in May, according to user's personal will, the location of the personal service information can be divided into sensitive or not sensitive information, and processed respectively then submitted to the location service provider. But the disadvantage of this method is that it can't define what is sensitive and what is not. At present, no method can achieve effective privacy protection. But users desperately need location service providers to have an effective way to protect their privacy. So, it's still a hot topic.

In accordance with the current development trend of smart mobile devices, private customization, this paper also adopts an improved information hiding algorithm to protect users' location service information privacy. The proposed QR-FLSB model can further improve the protection of location privacy and enable the location server to provide users with location service quality timely and efficiently. The contributions of this paper are mainly reflected in the following aspects:

- Compared with other technologies, two-dimensional code technology and fingerprint identification technology have been very mature. However, no literature has proposed to combine

the two with user location privacy protection. This paper combines these two mature technologies and applies them to the field of user location privacy protection.

- The QR-FLSB model proposed in this paper does not adopt a reliable third-party central server, which eliminates the performance bottleneck and the risk of being attacked in the processing of location information of the central server.
- Based on two-dimensional code technology, fingerprint technology and digital watermark, a method to protect location privacy information is designed. Although this method does not use K anonymous method, it can double protect the location privacy of users when they make queries, and at the same time, it does not need to sacrifice the service quality of users.
- The method proposed in this paper is based on the simulation data set and compares the "false location" privacy protection method to carry out sufficient experiments. Experiments show that this method has certain advantages.
- In order to achieve better robustness by hiding user location service information in fingerprint images, this paper proposes an improved LBS spatial digital watermarking algorithm.

Section 2 of this paper introduces relevant background and work. Section 3 describes that the user's location information is embedded into the fingerprint image in the form of watermark and the spatial domain transformation algorithm is adopted. Then, PDF417 (portable data file) in the two-dimensional code [11] is adopted. Each cluster of the portable data file contains the code characteristics represented by different bars and empty forms, and the fingerprint two-dimensional code is generated together with the fingerprint image. To achieve the purpose of privacy protection, the user's location privacy is hidden by the fingerprint two-dimensional code with watermark. In section 4, the advantages and disadvantages of this method are verified by the data generated by the famous simulators in the United States. Section 5 summarizes the work of this paper and looks forward to the future research on location privacy protection methods.

II. RELEVANT BACKGROUND AND WORK

A. *Fingerprint technology*

With the rapid development of information technology, smart mobile devices (such as smart phones, iPads, etc.) have been widely accepted by the public and become a tool for people to communicate with the outside world. At present, most intelligent devices use touch screen human-computer interaction design [12], which is the way of interaction, so it is easy to leave fingerprints on the screen. IPhone 5S, Samsung S5 and Xplay3S smartphones launched to the market by Apple, Samsung and Bubugao all contain fingerprint identification unlocking technology. And there are already some software about fingerprint unlocking of smart phones on the Internet, which provides a certain reality for the location privacy protection method proposed in this paper, as shown in Figure 1.

Currently, fingerprint identification technologies mainly used include optical identification, capacitive semiconductor sensor identification, biological radio frequency identification and digital optical identification [14]. This article is aimed at intelligent mobile devices (such as mobile phones, tablets, etc.) mainly using capacitive semiconductor sensors to identify the user's fingerprint.

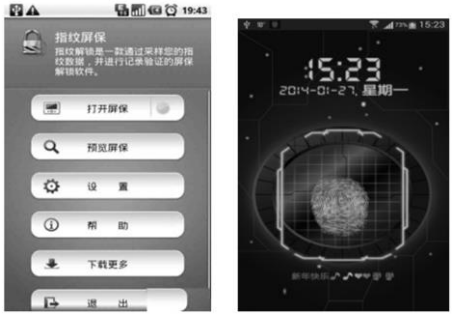

Figure 1. Fingerprint Software for Android Version 2.0 or above

B. *Two-dimensional Code*

Two-dimensional code [15-17], also known as two-dimensional bar code, is a black and white graph distributed on the plane (two-dimensional direction) according to a certain rule with a specific geometric figure, which is a key to all information and data. In modern business activities, it can be widely applied, such as: product anti-counterfeiting/traceability, advertising push, website link, data download, commodity trading, positioning/navigation, electronic certificate, vehicle management, information transfer, business card exchange, Wife sharing, etc. Two-dimensional codes have become more popular with the use of scan on smart phones.

Two-dimensional code not only has the function of anti-counterfeiting, but also has the function of confidentiality. It has certain applications in the encryption and transmission of confidential information such as business intelligence, economic intelligence, political intelligence, military intelligence and personal information. Based on these two characteristics of the two-dimensional code and the double protection of the user location service information, this paper proposes to apply the two-dimensional code technology to the location privacy protection technology.

C. *Digital Watermarking*

QR-FLSB model hides user's location service information in fingerprint image, which is actually a digital watermarking method. Digital watermarking is an effective way to protect information security, realize anti-counterfeiting traceability and copyright protection. It is an important branch and research direction in the field of information hiding technology. The digital watermarking algorithm involved in this paper is based on Android platform to transform fingerprint image in spatial domain and hide user location service information.

In view of the advantages of the two-dimensional code technology, fingerprint identification technology and digital watermarking technology mentioned above, this paper proposes a location privacy protection model QR-FLSB based on the combination of their advantages.

III. QR-FLSB LOCATION PRIVACY PROTECTION MODEL

With the rapid development of science and technology, the access capabilities and computational processing capabilities of the mobile devices used by users have been greatly improved. It is feasible to add a small computing module to the existing fingerprint-unlocked mobile client system. In this paper, a QR-FLSB model is proposed, which is composed of mobile user client and location server. Next, the detailed process of QR-FLSB algorithm will be described in detail.

A. Relevant Concepts

Definition 1: The location query information M issued by user U is expressed in the specific form of M, the specific expression of M is (1), which represents the IP address used by the user when he sends the query information.

$$M = \left\{ \mathrm{U}_{\mathrm{ip}}, L, V, C, U_f \right\} \tag{1}$$

U_f represents the user's fingerprint stored in the smart device to unlock; L= (x,y,t) represents the user's location when the query information is sent out; x,y and t represent the longitude, latitude and time respectively when the location information is sent out; V represents the moving speed when the user issues the query; C represents the specific content of the query issued by the user. Parameters, L and V can be obtained by the user using the smart-phone client, and parameter C is determined by what location service the user needs to obtain.

Definition 2: QoS of quality of service

According to SERVQUAL theory [20], the evaluation formula of location-based service quality model is as follows:

$$QoS(u) = \sum_{i=1}^{5} w_i (P_i - E_i) \quad , \sum_{i=1}^{5} w_i = 1, 0 \le P_i \le 1 (1 \le i \le 5) \tag{2}$$

In the format, weight and value range of each parameter are [0,1]. Variable P_1 represents privacy of user service quality PA(u), variable P_2 represents reliability of user service quality, P_3 represents response time of user service quality, P_4 represents assurance of user service quality and P_5 represents empathy of user service quality. P_1 and P_3 are calculated by the system, P_2, P_4 and P_5 are evaluated by the user. Variable E_i represents the expectations of each feature of the user, with an initial default of 1. Variable w_i represents the weight of each location service measurement, with an initial default of 0.2.

B. Basic Ideas of QR-FLSB Model

User U uses a smart phone (for devices with fingerprint unlocking), and the smart device obtains the user's fingerprint and stores it in the device to identify the user. When user U needs to obtain location service and send out service information C, information C is not sent directly to location server, but through the processing module of user terminal, fingerprint image F uses spatial transformation to change the lowest bit of fingerprint image pixels, hides information C in fingerprint image F in the form of watermarking, and then gets processed. Then the processed fingerprint image (pseudo-fingerprint) is compressed into a data template format (This format is 1/3 of the capacity of a normal graphics format). Then the pseudo-fingerprint image is generated into the corresponding two-dimensional code. At last, the mobile client sends the corresponding two-dimensional code to the location server. The location server receives the two-dimensional code sent by the user, carries on the reverse operation, extracts the location service information C sent by the user, and actively responds to the user U's location service query request. The overall structure of the QR-FLSB model is shown in Figure 2.

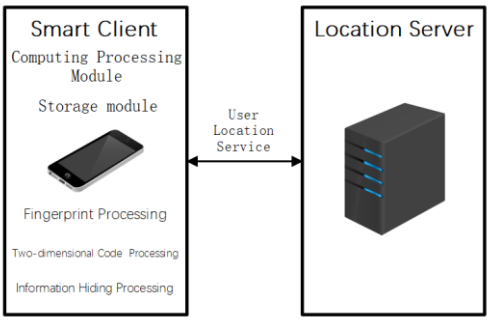

Figure 2. Overall Structure Diagram of QR-FLSB Model

As can be seen from Figure 2, the smart client consists of computing processing module and storage module, as well as fingerprint processing, two-dimensional code processing and information hiding processing module. However, at present, only a small number of mobile phones contain fingerprint processing and two-dimensional code processing module, and few terminals contain information hiding processing module. Therefore, it is necessary to add an information privacy computing and processing module on the client side and the location server side. This helps to improve the security of user location privacy protection and the quality of user experience.

C. LSB Algorithm

QR-FLSB model hides user position request information in fingerprint image in the form of watermarking. Because the current digital watermarking algorithms generally use frequency domain [19] and spatial domain [20] methods to ensure the robustness of the algorithm. Spatial domain algorithm has the advantages of simple implementation and low time complexity without image transformation. Frequency domain algorithm does not directly modify the pixel value of the image, but first transforms the image, and then embeds the watermarking in the transform domain. The frequency domain algorithm essentially distributes the watermarking information to every pixel of the carrier image, which makes the frequency domain algorithm more robust. Although the frequency domain algorithm has strong robustness, the capacity and transmission capacity of the smart terminal itself are limited, and the high time complexity makes it unsuitable to promote it on Android or Apple platforms such as smartphones or tablets [21].

In this paper, the LSB (Least Significant Bits) algorithm [22] is used to combine user location request information with user Fingerprint.

Step 1, calculate the maximum hidden amount of private data of the carrier fingerprint image.

Step 2, convert private data into a bitstream.

Step 3, each bit information in the bit stream is replaced by the lowest significant bit of the corresponding carrier pixel. After the replacement is completed, image1 with watermarking is obtained. It can be expressed by (3).

$$M_{i,j} = \begin{cases} X_{i,j} + W_{i,j}, & X_{i,j} \text{ is even number.} \\ X_{i,j} + W_{i,j} - 1, & X_{i,j} \text{ is odd number.} \end{cases} \quad (3)$$

$X_{i,j}$ is the original image pixel value of column J in row I. $W_{i,j}$ is embedded binary privacy information. Actually, the lowest effective bit of the carrier image pixel is zeroed out in (3), and then the binary privacy information is added to the embedding.

Step 4, the median filter is used to remove noise from image1, resulting in image2. That is to say, the combination of location request information and user`s Fingerprint is completed, so that the user's location request information is hidden in the fingerprint image in the form of watermarking [23].

D. Fingerprint Two-dimensional Code Algorithms

PDF417 bar code in the two-dimensional code selected in this paper, each PDF417 bar code is composed of 3 ~ 90 lines, each line is composed of the beginning character, the left line indicator, 1 ~ 30 symbol characters, the right line indicator, and the termination character. Where, the character set in PDF417 consists of 3 clusters (0, 3, 6 clusters respectively), each cluster contains all 929 code words represented by different bars and empty forms, and the serial Numbers correspond to 0 ~ 928[28]. According to (4), the cluster number of a row is selected to determine.

$$\text{Cluster number} = (\text{Line number mod3}) * 3 \quad (4)$$

Feature extraction was carried out for the image2 image in section 3.3, and the extracted feature values were encoded to generate PDF417 two-dimensional code. Experimental results are shown in figure 3.

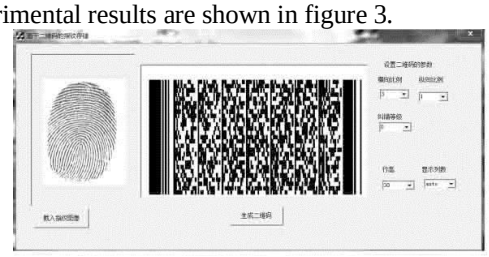

Figure 3. Generating fingerprint two-dimensional code

E. Algorithm Description

Algorithm 1. The improved LSB algorithm and fingerprint image are used to generate fingerprint two-dimensional code to hide user's location service information.

- Select the fingerprint image F1 which opened mobile phone most recently.
- F2←F1 Convert to binary.
- Initialize the user's location query service C (convert to binary).
- when length(C) < the total number of pixels of F2.
- For F3←low (F2, C); //Replace the lowest pixel of F2 with C successively to get F3; When the substitution is complete, the lowest place of the next pixel is replaced by "#".
- Convert F3 to decimal F4.
- Generate fingerprint two-dimensional code Q according to special two-dimensional code protocol and fingerprint image F4.

Algorithm 2. Get location service.

- Smart phone Client Sends Q to Location Server.
- The server side obtains fingerprint image F4 according to the two-dimensional code protocol.
- Extract the user's location service information C according to the watermark extraction method.
- Feedback location service to customer according to C.

1) The analyses of the degree of privacy preserving and service quality: QR-FLBS model guarantees the privacy of the algorithm from two aspects. Two protocols are established between client and location server: one is blind watermarking embedding and extraction protocol; the other is two-dimensional code encryption and decryption protocol. And the protocol is generated by agreement between the location server and the client. Even if the attacker intercepts the data packet sent by the client or location server, because the attacker does not know the decryption algorithm of the two-dimensional code, it is very difficult for the attacker without certain knowledge background to unlock the data packet easily. Even if the data packet is unlocked, it will only get the fingerprint image with blind watermarking, even if the user's fingerprint is obtained, nor can the attacker quickly infer who the user is. Then the user's information is not of great value to the attacker. If the attacker knows the user's identity and gets the user's fingerprint, it may cause some harm to the user, but this situation is small after all.

2) Complexity analysis of the algorithm: As the computing power of intelligent mobile client is limited, its location privacy protection algorithm should not be too complex. In QR-FLBS model, the carrier fingerprint image of location service request information needs to be processed., and two-dimensional code decryption and encryption protocol is used. The time complexity of client algorithm is O(n), n is the size of the request information sent by the user. Generally, the amount of information sent by the user is relatively small. The spatial complexity of the algorithm is O(k), K is the storage space of fingerprint two-dimensional code. Nowadays, many smart-phones, such as Apple 5S, can store five fingerprints, and the mobile phone has its own two-dimensional code reading software. The required space will not seriously affect the operation speed of the client.

IV. EXPERIMENT

A. Experimental Environment

The experiment is implemented with C++ and runs on the Windows 7 platform of Intel Pentium CPU 2020M 2.4

GHz processor and 4 GHz memory. The experiment uses the famous network-based Generator of Moving Objects simulator [24] and traffic network data [25] of Oldenburg urban area, and adds user fingerprint information to the database table and generates fingerprint two-dimensional code. To simulate the degree of user privacy protection when users use network queries. The scene parameters for the simulation experiment are shown in Table 1.

TABLE I. SIMULATED EXPERIMENTAL SCENE PARAMETER TABLE

Name of parameter	*Parameter values*
Q (Location query request issued by user)	1⩽Q⩽100
Number of initialized mobile terminals	10
F (Characteristic values of unlocked fingerprints recently used by users)	100⩽F⩽200

B. *The Experiment Content*

- The influence of the size of query information Q sent by users on QR-FLSB model and K anonymous "pseudo-location" model is analyzed and compared.
- Determine whether the QR-FLSB model and K anonymous "false location" model are used in an area to analyze the privacy security of users when the number of users changes respectively

C. *Experimental Analysis*

In the control of experimental environment, traffic network data in Oldenburg city are selected and intelligent terminals are used to send queries to the location server through terminals containing QR-FLSB model to collect experimental data. Then, the selected network data will use K anonymous "false location" model in a certain range to send queries to the location service, collect experimental data, and analyze the data. The simulation diagrams in figure 4 and figure 5 are obtained.

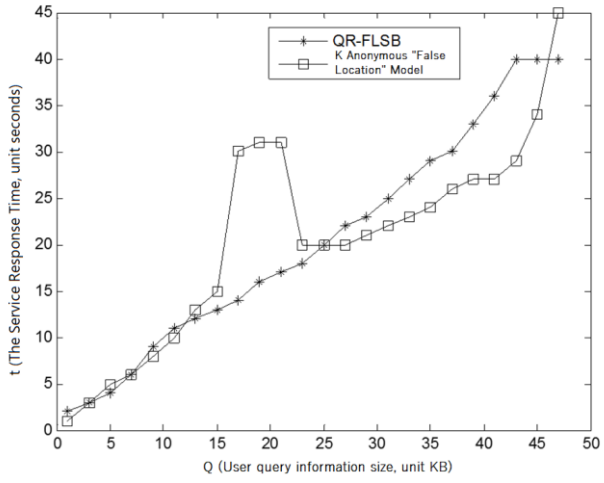

Figure 4. The relationship between t (the service response time) and Q (user query information size)

As can be seen from figure 4, the vertical coordinate is the time t required by the query service, and the horizontal coordinate is the query information of the user, or the size of Q. The greater the Q, the longer the time QR-FLSB model needs. When reach a certain extent, QR-FLSB model tends to saturation, depending on the user's query information matching, if user's fingerprint is found to be the same, there is no need for a second decoding algorithm, just call the most recent fingerprint two-dimensional code decoding algorithm of the user in the cache, so comparing with the "false location" algorithm, the QR-FLSB model is not as good as the "false location" method in time complexity. It can be seen that QR-FLSB model spends more time on two-dimensional code decoding and fingerprint identification than "false position" in the actual operation. However, similarly, when Q is larger, that is, when there are a large number of users in an area, it is difficult to select false location points, so it will be more difficult to find K anonymous "false location points" than Q value is relatively small, and the processing time consumed will be longer. It can be seen from figure 4 that the false position model and the QR-FLSB model keep the same general trend. According to the experimental results, the time-consuming complexity of the QR-FLSB model is larger than that of the false position model, although no substantial improvement has been made. However, the security of QR-FLSB model is higher than that of "false position" algorithm. Specific experimental results are shown in figure 5.

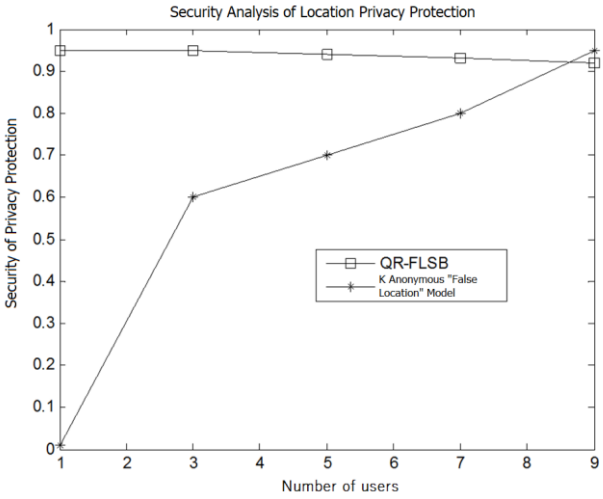

Figure 5. The relationship between the number of users and the degree of privacy protection

As can be seen from figure 5, when the number of users increases to a certain limit, the privacy protection security of the "false location" algorithm (i.e., the privacy protection degree) gradually increases, and eventually decreases, and then tends to saturation. This is mainly because when the number of users in the fixed anonymous area increases, the available "false location" points will gradually decrease, and the privacy security of users will gradually weaken. The service quality provided by it will gradually deteriorate from high quality, but it can effectively provide security for user location privacy service within a certain range. At the same time, the security of the QR-FLSB model is relatively high and relatively stable compared with the "false location" algorithm, because the QR-FLSB model is for one machine and one person, and it contains the double protection mentioned in this paper, so compared with the "false location" algorithm, the privacy protection of users is still better.

V. CONCLUSIONS AND PROSPECTS

The QR-FLSB method proposed in this paper not only applies the digital watermark technology to the protection of location privacy, but also combines the two-dimensional code technology, so that the user location service information is double protected. Traditional location privacy protection methods mostly adopt a reliable third party, and use false location to query in the anonymous area of K anonymity. False location will sacrifice the quality of service for the security of privacy protection to some extent. QR-FLSB model, however, does not sacrifice the quality of location service and has high security compared with "false location" algorithm. The QR-FLSB model effectively utilizes the existing technologies in the smart client to avoid the waste of resources. This paper simulates the implementation of the QR-FLSB scheme, but the fingerprint in this scheme is the privacy part of the user. Although it is protected by a layer, it is obtained by an attacker with certain background knowledge, who may steal the user's fingerprint to do something harmful to the user. Moreover, this model is affected by the size of user query information. The improvement of time complexity of QR-FLSB model needs to be studied continuously from the comparative analysis of experiments. The improvement of time complexity of QR-FLSB model needs to be studied continuously from the comparative analysis of experiments. In the future, the research work can not only protect users' location privacy information effectively, but also protect users' other privacy from being exposed, and whether there are other better algorithms to ensure that users experience a more efficient and secure method of location privacy protection, and to secure the privacy of location services.

REFERENCES

[1] Mokbel, M.F., "Privacy in Location-Based Services: State-of-the-Art and Research Directions", Proc. International Conference on Mobile Data Management (MDM. 07) .Mannheim, Germany, 2007, pp. 228, doi: 10.1109/MDM.2007.45.

[2] LIN Xin1, LI Shan-Ping and YANG Zhao-Hui, "Attacking Algorithms Against Continuous Queries in LBS and Anonymity Measurement" (In Chinese), Journal of Software, vol 20(4), 2009, pp. 1058-1068, doi: 10.3724/SP.J.1001.2009.03428.

[3] Gruteser M and Grunwal D, "Anonymous usage of location based services through spatial and temporal cloaking Proceedings of the International Conference on Mobile Systems, Applications, and Services" (MobiSys 03). New York, USA, 2003, pp. 163–168.

[4] Man Lung Yiu, Jensen, C.S., Xuegang Huang and Hua Lu, "SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services", Proc. IEEE International Conference on Data Engineering (ICDE 08). Cancun, Mexico, 2008, pp. 366–375, doi: 10.1109/ICDE.2008.4497445.

[5] ZHANG Hai-tao, HUANG Hui-hui, XU Liang and GAO Sha-sha, "Research advances on privacy-preserving data mining" (In Chinese), Application Research of Computers vol 30(12), 2013, pp. 3529-3535, doi: 10.3969/j.issn.1001-3695.2013.12.003.

[6] WANG Lu and MENG Xiao-Feng, "Location Privacy Preservation in Big Data Era: A Survey" (In Chinese), Journal of Software, vol 25(4), 2014, pp. 693-712, doi: 10.13328/j.cnki.jos.004551.

[7] LI Wen-ping, YANG Jing, ZHANG Jian-pei and YIN Gui-sheng, "LI Wen-ping YANG Jing ZHANG Jian-pei YIN Gui-sheng" (In Chinese), Journal of Jilin University (Engineering and Technology Edition), vol 45(02), 2015, pp. 630-638, doi: 10.13229/j.cnki.jdxbgxb201502044.

[8] Huang Yi, Huo Zheng and Meng Xiaofeng, "CoPrivacy:A Collaborative Location Privacy-Preserving Method without Cloaking Region" (In Chinese), Chinese Journal of Computers, vol 34(10), 2011, pp. 1976-1985, doi: 10.3724/SP.J.1016.2011.01976.

[9] Shen Chaoyang, "Analysis and Suggestions on Mobile Two-Dimensional Code Service" (In Chinese), Mobile Communications, vol Z1, 2008, pp. 137-141, doi: 10.3969/j.issn.1006-1010.2008.03.032

[10] Zhang Xianquan, Tang Ying and Guo Mingming, "An Improved Quick Thinning Algorithm for Fingerprint Image" (In Chinese), Journal of Guangxi Academy of Sciences, vol 04, 2006, pp. 237-239, doi: 10.13657/j.cnki.gxkxyxb.2006.04.003.

[11] Zhang Duo and Wang Yaoqiu, "Bar Code Technology and Electronic Data Exchange" (In Chinese), China Railway Publishing House, 2012.

[12] Lu Qunxia, Xiong Xinfu and Zhang Qiliang, "Design on computer human interaction of product interface" (In Chinese), Packaging Engineering, vol 05, 2005, pp. 163-164, doi: 10.3969/j.issn.1001-3563.2005.05.060.

[13] ZHAN Xiao-si, MENG Xiang-xu and YIN Yi-long, "Algorithm based on texture character analysis for fingerprint image segmentation" (In Chinese), Computer Engineering and Applications, vol 44(21), 2008, pp. 162-165, doi: 10.3778/j.issn.1002-8331.2008.21.045.

[14] Jain, A. and Lin Hong, "On-line fingerprint verification", Proc. 13th International Conference on Pattern Recognition, Vienna, Austria, vol 19(4), 1997, doi: 10.1109/ICPR.1996.547016.

[15] Yang Jun and Yang Yan, "The Study and Application of the Two-dimensional Code" (In Chinese), Applied Science and Technology, vol 11, 2002, pp. 11-13, doi: 10.3969/j.issn.1009-671X.2002.11.004.

[16] Pan Jicai, "Analysis of Two-Dimensional Bar Code Technology and Its Application" (In Chinese), Market Modernization, vol 09, 2009, pp. 118-120, doi: 10.3969/j.issn.1006-3102.2009.09.078.

[17] Wang Wenhao, Zhang Yahong, Zhu Quanyin and Shan Jinsong, "Image Recognition in 2-D Bar Code Based on QR Code" (In Chinese), Computer Technology and Development, vol 10, 2009, pp.123-126, doi : 10.3969/j.issn.1673-629X.2009.10.034.

[18] Wu Jinhai and Lin Fuzong, "Image Authentication Based on Digital Watermarking" (In Chinese), Chinese Journal of Computers, vol 09, 2004, pp. 1153-1161, doi: 10.3321/j.issn:0254-4164.2004.09.001.

[19] Chen Chunning and Wang Tingjie, "Image contrast enhancement by homomorphic filtering in frequency field" (In Chinese), Microcomputer Information, vol 06, 2007, pp. 264-266, doi: 10.3969/j.issn.1008-0570.2007.06.108.

[20] Su Qingtang, Niu Yugang and Liu Xianxi, "Image watermarking algorithm based on DC components implementing in spatial domain" (In Chinese), Application Research of Computers, vol 04, 2012, pp., doi: 10.3969/j.issn.1001-3695.2012.04.067.

[21] Zhou Jun, "Discussion on the Implementation of Digital Watermark in Android" (In Chinese), Electronic Technology, vol 11, 2011, pp. 17+9, doi: 10.3969/j.issn.1000-0755.2011.11.009.

[22] Fu Desheng and Liu Tong, "An Improved Information Hiding Algorithm Based on LSB" (In Chinese), Value Engineering, vol 30(06), 2011, pp. 108-109, doi: 10.3969/j.issn.1006-4311.2011.06.093.

[23] SHEN Hong and CHEN Bo, "From single watermark to dual watermark: A new approach for image watermarking", Computers and Electrical Engineering, vol 38, 2012, pp. 1310-1324, doi: 10.1016/j.compeleceng.2011.11.012.

[24] Sythoff J, Morrison J. Location-Based services. 2011. URL: http://www.pyramidresearch.com/store/Report-Location-Based-Services.htm

[25] URL: http://iapg.jade-hs.de/personen/brinkhoff/generator/