INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

PRIVACY BASED MULTIPLE LOCATION TRANSFORMATION USING ENCRYPTION FREE FRAMEWORK

Ms.P.Iswarya[1], DR.S.Padmapriya[2]

[1]PG Scholar, Department of Computer Science and Engineering,

[2]Professor and Head, Department of Computer Science and Engineering,

A.V.C College of Engineering, Mannampandal

ABSTRACT: Recent advances in positioning techniques, small devices, GIS-based services, and ubiquitous connectivity, have enabled a large variety of location-based services able to tailor services according to the location of the individual requiring the service. Location information, however, if on one side is critical for providing customized services, on the other hand, if misused, can lead to privacy breaches. Location Privacy is the serious issue where the location can be easily traced with the given system. In images there will be metadata where it contains all the image details in at. At first the feature extraction will be made using Recurrent Neural Network (RNN) thus the location feature are get known. A dummy location is done with the Pseudo random Function and the metadata location is changed. The user can access only when the access is provided to them. Here the user access can be provided by the authority who they wish to share their location. Our scheme employs an entity, termed Function Generator, to distribute the spatial transformation parameters periodically, with which the users and the LSP(location service provider) can performs the mutual transformation between a real location and a pseudo location. Without the transforming parameters, the anonymizer cannot have any knowledge about a user's real location. The main merits of our scheme include (1) no fully trusted entities are required; (2) each user can obtain accurate POIs, while preserving location privacy.

***Key terms* — Location privacy, pseudo random function, privacy preserving, RNN extraction**

I.**INTRODUCTION**

Cybercrime is the main higher level problem which been dominating over the individual security and threats to many banks, companies and governments. Large amount of organized crime security threats have been widely spread with the high trained developers for the online attacks. For hackers it seems a golden time where the many attacks and hacks occurs over multiple variations. Creating malicious software for various attacks which will get the user personnel details from the server. Hackers seem to be smarter and more creative with their malware and how they bypass authentication system is quiet tricky**.**

The main objective of this system is to make privacy for the location. A malicious entity in possession of the laptop with unconstrained access to a trusted location could access sensitive data. To propose a new attacker model, the Outsider Thief (OT), to more accurately reflects the threat of a laptop thief. The unknown attacks will be eliminated with the implemented system.

The location based privacy is the most important implementation in this system where anyone can get the location from anywhere else. Thus the implementation is mainly carried out without encryption where this is called encryption free framework is known here. Semantic security is the one of the most important requirement for any encryption schema. In that, adversary is not able to learn any partial information about original data. To handle the security issue, to propose a system of privacy-preserving image recognition with multiple locations called as dummy location, in which the server cannot uniquely determine the acknowledgment result but client clients can do so.

To begin with, client clients extricate a visual highlight from their taken photo and change it so that the server cannot extraordinarily decide the acknowledgment result. Then, the clients send the changed highlight to the server that returns a set of candidates of the acknowledgment result to the clients. The system improves the sender and the receiver where the location privacy can be added with the receiver side, sender side and the server.

II. RELATED WORKS

However, this kind of client-server image can cause a privacy issue because image recognition results are sometimes privacy-sensitive.to tackle the privacy issue, in this paper, we propose a framework of location privacy. Sun Gang Sunab summarized the Location-based social networks (LBSNs) are convenient, but users must reveal their location information to network servers to enjoy an LBSN's services. However, user location in- formation is sometimes sensitive; its disclosure can potentially cause severe privacy issues, for example, by revealing identity or health information. In this paper, we propose a *k- anonymity* -based algorithm that preserves user location information. To solve the location- privacy problem, the proposed algorithm, called the dummy-location selection algorithm, generates dummy locations that can be used to hide users' actual locations. At the same time, because users may want to search through the check-in records of their friends, we design a novel algorithm that enables a quick search either by location or by friends' social networks. We evaluate the performance of our proposed algorithm via extensive simulations. , we also provide security analysis to demonstrate that our scheme can resist internal attack, external attack and colluding attack.

III. PROPOSED SOLUTION

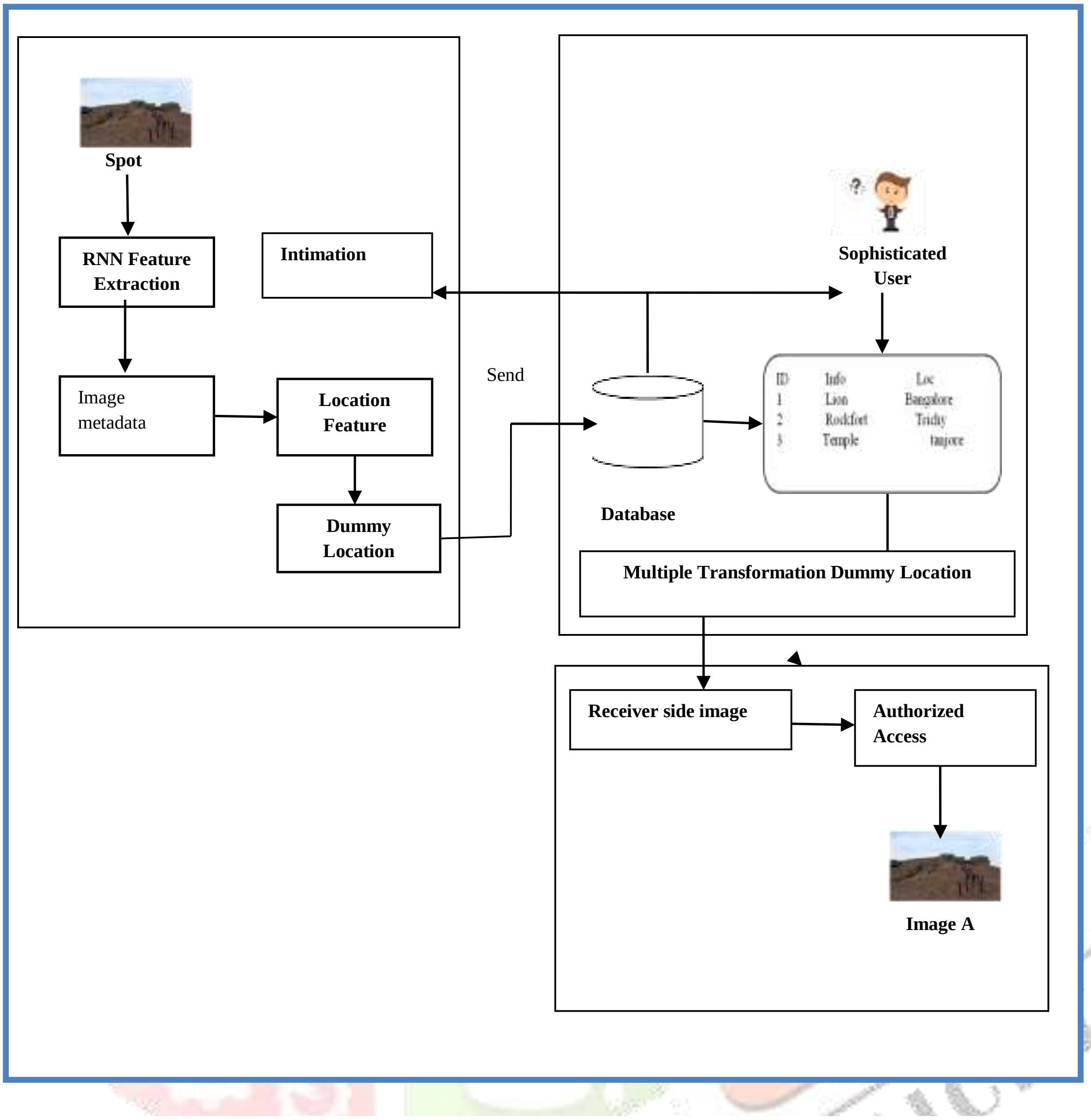
In our proposed system the image will be given with a feature based extraction system. The features are extracted with the Recurrent Neural Network where the image based locations are extracted. A dummy location is created with the Pseudo Random Function system. The location is created with the dummy location system and the unknown person authority is identified. The user can share their details with the known person where the unknown person will be stopped from accessing the details.

In this paper, users can share information, called check-in records (or check-ins), with their friends regarding a designated venue. Each check-in record contains information such as the check-in location, corresponding tips, and the check-in time. In addition, users can search through all their friends' check-ins or only those at a single specified location. Dummy location can be added with the multiple specification which are all be added and they can be used. Most recently a framework called Space Twist represented a technique for blinding an untrustworthy location server.

In this framework, the nearest neighbor is incrementally retrieved based on its incremental distance from dummy locations. However, users' habits show that check-in positions are not completely independent.

Advantages:

- The leakage of location is identified.
- Privacy to the location is enhanced in this secured system.
- The user privacy is achieved with the implemented form based system.
- This enhances the location privacy of the user while taking or uploading photo.
- The user only can know the location but not the third party.



ID	Info	Loc
1	Lion	Bangalore
2	Rockfort	Trichy
3	Temple	tanjore

Fig 3.1 System architecture of the location privacy with multiple dummy locations

IV. IMPLEMENTATION

The image transfer module will upload the image with the user uploaded system to the receiver**.** The user will upload the image where the user will share the image with user specified location**.** Before the image to be uploaded the user location privacy should be achieved. The receiver will be waited for the image to be uploaded by the user. More traditionally, peer-to-peer LBS refer to the way sharing information is traversed over the network. For example, the P2P k-anonymity algorithm has several steps: select a central peer who will act as an agent for the group, next, the central peer will discover other k-1 different peers via single-hop or multi-hop to compose the group and finally find a cloaked region covering all locations that every peer may arrive. In our article we are using “peer-to-peer” term at the first hand for highlighting the target party for the location sharing request. It is “another peer” directly, rather than the central server (data store). In terms of patterns for LBS this approach targets at the first hand such tasks as ‘Friend finder’ and the similar. In other words it is anything that could be linked to location monitoring.

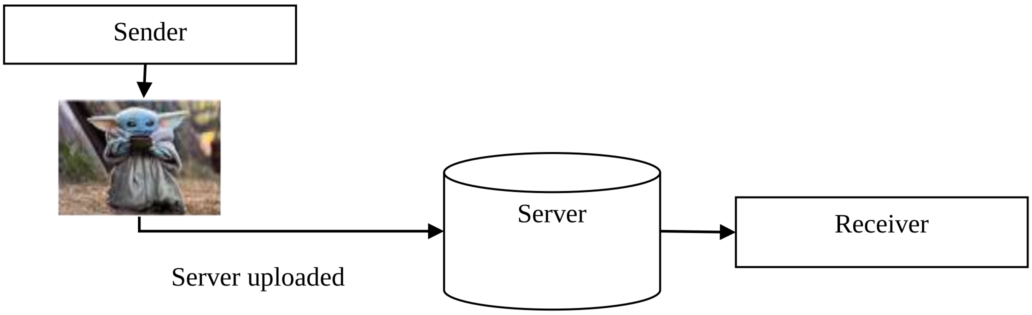


Fig 4.1 Block diagram of image transferring

Metadata extraction is the retrieval of any embedded metadata that may be present in a given file. There are a few ways to retrieve geo-location data from images; the easiest is to use a recurrent neural network based feature extraction system is the one where the user will extract the features of the images. The feature extraction system will be given by the user analysis and the Meta data from the user. The user will get an analysis of the user location extraction from the system and the location features are getting changed. In Meta data extraction module multiple features are extracted in a single image. Extracting preservation metadata is a two-stage process. In the first phase each incoming file is processed by the adapters until one of the adapters recognizes the file type. That adapter extracts data from the header fields of the file and generates an image.

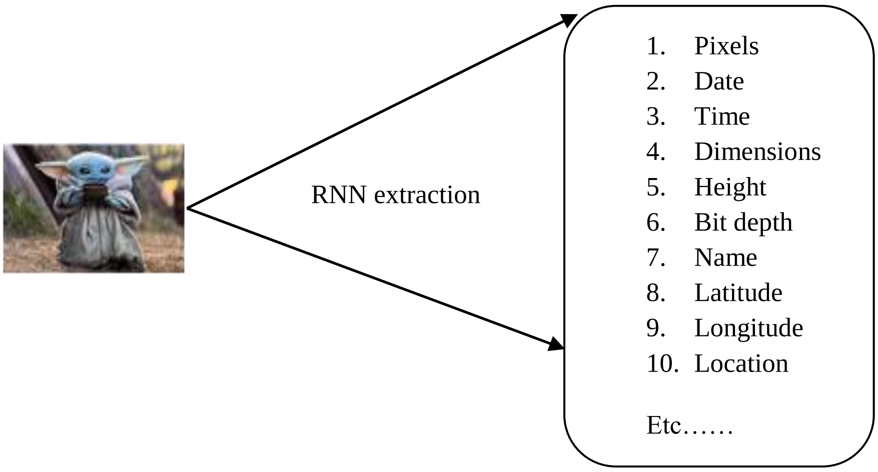


Fig 4.2 Block Diagram of the Meta data extraction

The extracted features are placed with a dummy location system. The dummy location is given with the system where the user locations are getting viewed with the dummy location identification. The location systems are getting known with the system and the dummy location are getting stored in the system. Dummy pictures are "mock" pictures containing text that may later be replaced by a real image. The text in the dummy images can for example contain information about where the original image is stored. At a later z2swzaRstage multiple locations can be used to merge the text in the dummy image with the real image file. Multiple random functions can be added so that multiple trained locations will be added for a single image.

- The multiple dummy location are added with the real location.
- Here the location can be changed as h1,ht-1,hl with the newly added dataset from v1,…..vn.
- These data changing can be made with the Recurrent Neural Network.

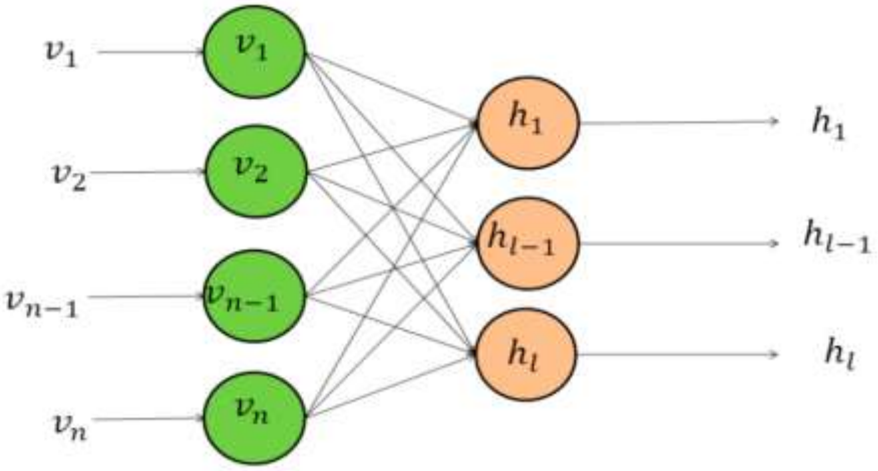


Fig 4.3 Recurrent Neural Network system to create multiple locations trained systems

In server upload technique the user will upload the data to the server. The image now stored will be with the dummy location system. The dummy location which is produced with the efficient RNN based processing system. The locations which are all given with the system analyzing that the server location get protected. Thus the location privacy is created where the server stores the transform feature in it. The transformed feature gets stored in the server. The location of the user gets protected without the encryption process. The web server will very quickly find an image file and send it to a visitor. Sending files to visitors is the main job of a web server. There are sometimes good reasons to store images in a database but there aren't too many users.

The privacy preserving system is added to preserve the location data with the user assistant. The user will make sure that the known user will make a access to the location and view the exact location of the user. The data can be preserved by using the Privacy Preserving CBIR. Here the data get protected with the secured services of the unknown person. Novel image privacy is enhanced to protect the image from the unknown user. The location will be extracted stored in the database with the secured dummy location.

$$T\ rp(Q, rk) \leftarrow PPcbir(Q, rk, ik)$$

Here the trapdoor attack is overcome with the dummy location and original location for the known user. The location privacy is mainly achieved without encryption format.

The third party intimation system can be made with the higher user security. If the unknown user tries to get the image then the third party will be intimated to the user where they will find difficult to access the image and location. The third party access will be notified with an IP address, Mac address, latitude and Longitude. An image distributor has given sensitive location to the trusted third parties (agents).

If some location are leaked and found in an unauthorized place. The distributor must analyze that the leaked data came from (where) one or more agents. To propose data allocation strategies to improve the probability of identifying leakages of locations and also add" fake object" to further improve our chances of detecting leakage and identifying the guilty party.

Two main algorithm implementation here is Recurrent neural Network and the Pseudo random function..

RECURRENT NEURAL NETWORK

A recurrent neural network (RNN) is a class of artificial neural networks where connections between nodes form a directed graph along a temporal sequence. This allows it to exhibit temporal dynamic behavior. Derived from feedforward neural networks, RNNs can use their internal state (memory) to process variable length sequences of inputs. This makes them applicable to tasks such as unsegmented, connected handwriting recognition or speech recognition.

The term "recurrent neural network" is used indiscriminately to refer to two broad classes of networks with a similar general structure, where one is finite impulse and the other is infinite impulse. Both classes of networks exhibit temporal dynamic behavior. A finite impulse recurrent network is a directed acyclic graph that can be unrolled and replaced with a strictly feed forward neural network, while an infinite impulse recurrent network is a directed cyclic graph that cannot be unrolled.

Both finite impulse and infinite impulse recurrent networks can have additional stored states, and the storage can be under direct control by the neural network.

The storage can also be replaced by another network or graph, if that incorporates time delays or has feedback loops. Such controlled states are referred to as gated state or gated memory, and are part of long short-term memory networks (LSTMs) and gated recurrent units. This is also called Feedback Neural Network.

The idea behind RNNs is to make use of sequential information. In a traditional neural network we assume that all inputs (and outputs) are independent of each other. But for many tasks that's a very bad idea. If you want to predict the next word in a sentence you better know which words came before it. RNNs are called recurrent because they perform the same task for every element of a sequence, with the output being depended on the previous computations. Another way to think about RNNs is that they have a "memory" which captures information about what has been calculated so far. In theory RNNs can make use of information in arbitrarily long sequences, but in practice they are limited to looking back only a few steps (more on this later). Here is what a typical RNN looks like:

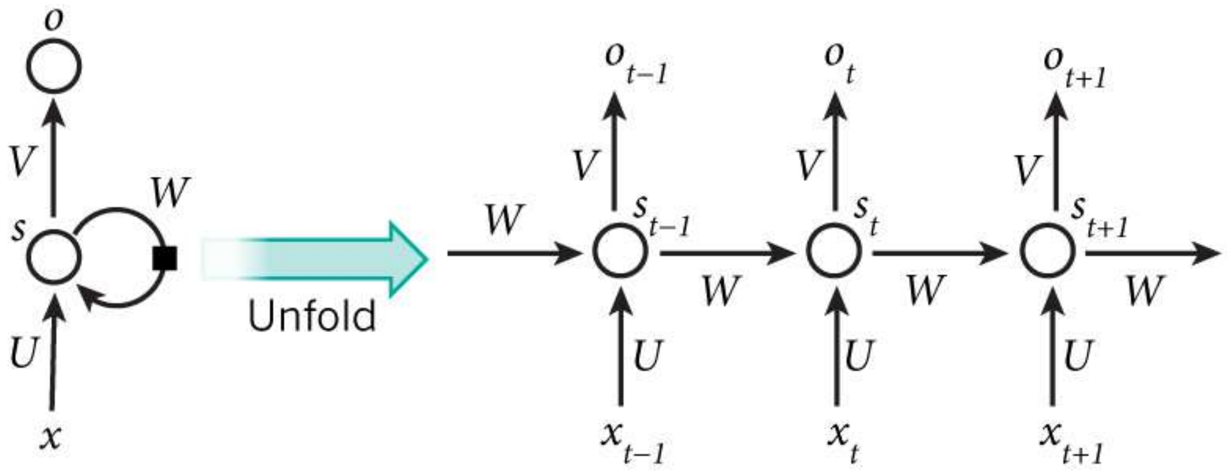


Fig 4.4 RNN based feature extraction from the images

The above diagram shows a RNN being unrolled (or unfolded) into a full network. By unrolling we simply mean that we write out the network for the complete sequence. For example, if the sequence we care about is a sentence of 5 words, the network would be unrolled into a 5-layer neural network, one layer for each word. The formulas that govern the computation happening in a RNN are as follows:

- x_t is the input at time step t. For example, x_1 could be a one-hot vector corresponding to the second word of a sentence.
- s_t is the hidden state at time step t. It's the "memory" of the network. s_t is calculated based on the previous hidden state and the input at the current step: $s_t = f(Ux_t + Ws_{t-1})$. The function f usually is nonlinearity such as tanh or ReLU. s_{-1}, which is required to calculate the first hidden state, is typically initialized to all zeroes.
- o_t is the output at step t. For example, if we wanted to predict the next word in a sentence it would be a vector of probabilities across our vocabulary. $o_t = \mathrm{softmax}(Vs_t)$.

Together with convolutional Neural Networks, RNNs have been used as part of a model to generate descriptions for unlabeled images. It's quite amazing how well this seems to work. The combined model even aligns the generated words with features found in the images. Training a RNN is similar to training a traditional Neural Network. Because the parameters are shared by all time steps in the network, the gradient at each output depends not only on the calculations of the current time step, but also the previous time steps. For example, in order to calculate the gradient at $t = 4$ we would need to back propagate 3 steps and sum up the gradients. From the extracted features the RNN system mainly gets the location features which are called latitude and longitude**.** The latitude and the longitude values can be added with the trained location datasets randomly**.** Here the location can be matched with the multiple functions with the hidden state vector**.** The Classified locations with different latitude values and longitude values are captured and analyzed**.** Each classification are made and analyzed to be stored in the database.

PSEUDO RANDOM FUNCTION

A pseudorandom function is a deterministic function of a key and an input that is indistinguishable from a truly random function of the input. More precisely, let s be a security parameter, let K be a key of length s bits, and let f (K,x) be a function on keys K and inputs x.

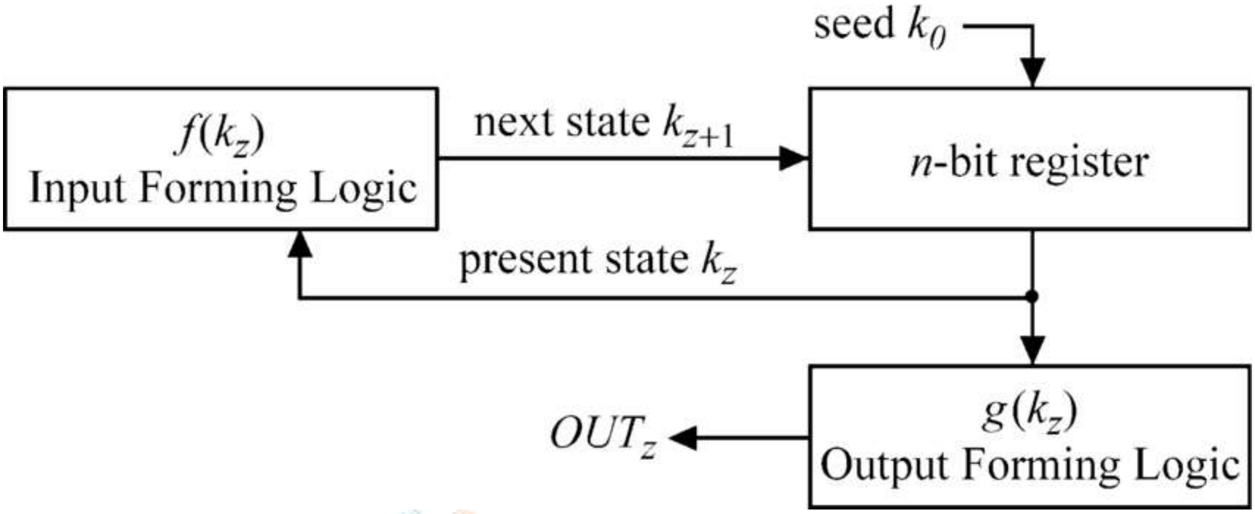


Fig 4.5 Pseudo random function with multiple dummy location generation with a output forming logic is done

A pseudorandom function is a deterministic function of a key and an input that is indistinguishable from a truly random function of the input. More precisely, let s be a security parameter, let K be a key of length s bits, and let f (K,x) be a function on keys K and inputs x. Then f is a pseudorandom functions if:

- f can be computed in polynomial time in s; and
- If K is random, then f cannot be distinguished from a random function in polynomial time.

In this context, “distinguish ability” refers to the ability of an algorithm to tell whether a function is not truly random. Let g be a truly random function of x with the same output length as f. Suppose a polynomial-time algorithm A is given access to a “oracle” which, on input x, either consistently returns f (K, x), or consistently returns g(x). After some (polynomial) number of accesses to the oracle, the algorithm outputs a guess, b, as to whether the oracle is f or g. Let ε be A's advantage, i.e., the difference in probabilities.

The following construction [NR’95] can be evaluated efficiently in parallel. The seed is [a1,0,a1,1,...,an,0,an,1∈{0,1}s][a1,0,a1,1,...,an,0,an,1∈{0,1}s]. Then to compute FNR(x1...xn)FNR(x1...xn), start with a1,x1a2,x2...an,xna1,x1a2,x2...an,xn, and squish pairs of strings together using S:{0,1}s×{0,1}s→{0,1}sS:{0,1}s×{0,1}s→{0,1}s. Then take the n/2n/2 outputs and squish them in pairs again. Then repeat the process until there is one string in {0,1}s{0,1}s left. When SS is a synthesizer, FNRFNR is a PRF. It turns out trapdoor permutations imply synthesizers. An open problem is to construct a parallel PRF from one-way permutations.

- Let G returns two times more bits than it has bits in its internal state: G: K -> K^2
- It is possible to define a 1-bit pseudorandom function:F: K x {0, 1} -> K as:F(k, b)=G(k)[b]where:**b** can be equal to either 0 or 1.
- The function F returns the first or the second half of generator's output data, based on the received input bit.
- If the generator G is secure, then the function F is also secure.

The presented procedure can be repeated any number of times and one can receive a pseudorandom function which could be of any size. This method of creating pseudorandom functions is known as Goldreich-Goldwasser-Micali Construction, based on the names of people who invented it.It can be proved that if the generator G is secure, then a pseudorandom function working on input data of length of n bits and defined in a way described above is also secure.

V. RESULT AND EVALUATION

Experiments are conducted to verify the proposed differential privacy preserving method which can enhance expected utility error. The experimental data came from the Indoor Loc Data Set in UCI Machine Learning Repository. We will make a numerical experiment by using the filtered noise combined with user’s expected utility error. For each of the classifications, the feature extraction method which provided the best resulting average accuracy is used. The results of the entire system are then evaluated. That is done by describing which images are retrieved as worthy of further analysis and how well it conforms to which images that should be. Images that are worthy of further analysis are images that are good, salient and unique with respect to the other retrieved images. The final output for an image is whether its retrieval is true or false, the same way as for the retrieval part. That way, true/false negatives/positives are achieved.

All results will be evaluated using the measures precision, recall and accuracy which are defined as:

Accuracy = true positives + true negatives all samples

The user can set the n-1 dummy location information which randomly generated by location service client, the user's real location information Li(latitude,longitude) and n-1 dummy location information constitute data set D. Then, the user can set his own expected utility error and request service. After the location service provider received the data set which be sent by the user's client, provider recommends the specific needs of each data and returns results to the user. According to his own real location Li corresponding to the tag Ti in the data set, when the user received the recommended content by location service provider, user can view his real location information corresponding to the recommended content. By adding n-1 dummy locations, enhancing the user's location privacy preserving, that is to say, the user sends n location information to the location service provider; the attackers attack the user's real location information with the probability of 1/ n.

We also analyze security properties of the proposed scheme. In particular, we focus on how the scheme can resist various attacks and achieve privacy preservation.

Resistance to Impersonation Attack: For LBS users, each user has a unique identity UID which is distributed by TA and only known by himself and TA, which can assist receiver to check whether the message is from an valid user. For fog servers and LBS provider, identity-based signature is employed to verify whether the message is legal or not.

Resistance to Internal Attack: Although both fog server and LBS provider can obtain the privacy location information, they cannot obtain the users' identity UID because that it is difficult to know where this message came from.

Resistance to Colluding Attack: The colluding users cannot infer another user's private information because they don't have the original location. Even if the fog server and LBS provider have the collusion activity, it is also impossible, because it is difficult to infer where this message came from. **VI. CONCLUSION AND FUTURE WORK**

In this paper, we propose an efficient and reliable location privacy-preserving scheme, which preserve users' privacy data by making their identity be anonymity for LBS provider and fog server. In the proposed scheme. Many users worry about whether their privacy be leaked when they request location service, and some users use dummy location information, so privacy control is transferred to the client, users can set the expected utility error. By using this model which allows users to clearly understand their privacy information is protected, thereby inciting users to send real information, so that users have a better service experience. Empirical results showed that filtering noise approach can enhance utility. This method has a certain theoretical and practical significance for design of privacy preserving systems. Besides, we also provide security analysis to demonstrate that our scheme can resist internal attack, external attack and colluding attack.

For the future work, we plan to further improve the schemes and deploy them in real-world vehicular network system with different information system. The privacy based system can be enhanced with a high security. The system can add privacy for other features in every attributes.

REFERENCES

[1] B N Jagdalea and J W Bakal. 2015. Controlled Broadcast Protocol for Location Privacy in Mobile Applications. International Conference on Information Security and Privacy (ICISP 2015), 11-12.

[2] Chunyong Yin ; Jinwen Xi ; Ruxia Sun and Jin Wang. 2018. Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things. IEEE Transactions on Industrial Informatics (Volume: 14 , Issue: 8)

[3] Hui Xie, Ying Ji and Yueming Lu. 2013. An Analogy-Relevance Feedback CBIR Method Using Multiple Features. Key Laboratory of Trustworthy Distributed Computing and Service (BUPT).

[4] Kazuaki Nakamura, Naoko Nitta and Noboru Babaguchi,.2018. Encryption-Free Framework of Privacy-Preserving Image Recognition for Photo-Based Information Services. VOL. 13, NO. 12, OCT 2018

[5] LinaNiab, YanfengYuana, XiaoWanga, Mengmeng and ZhangaJinquanZhang. 2018. A Location Privacy Preserving Scheme Based on Repartitioning Anonymous Region in Mobile Social Network. Volume 129, 368-371.

[6] Qingqing Xie and Liangmin Wang. 2016. Privacy-Preserving Location-Based Service Scheme for Mobile Sensing Data, Sensors.

[7] Reza Shokri ; George Theodorakopoulos ; Jean-Yves Le Boudec and Jean-Pierre Hubaux,.2012. Quantifying Location Privacy, IEEE Symposium on Security and Privacy.

[8] Rong Tan, Junzhong Gu, Peng Chen and Zhou Zhong. 2013. Link Prediction Using Protected Location History. International Conference on Computational and Information Sciences.

[9] SunGangab, SongLiangjuna, LiaoDana, YuHongfangab and ChangVictor. 2019. Towards privacy preservation for "check-in" services in location-based social network. Volume 481, 616-634.

[10] Yuan Tian ; Hai Liu ; Zhenqiang Wu and Jing Hu. 2017. Enhancing utility approach for user-centered location privacy service. IEEE International Conference on Software Engineering and Service Science (ICSESS).