iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** I **Month of publication:** January 2020

DOI: http://doi.org/10.22214/ijraset.2020.1083

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

Enhancing Privacy in Photo Based Location Information Services using Encryption Free Framework

M. Chandraleka[1], Mrs. D. Anitha [2]

[1]*Final Year PG Student,.*[2]*M.E., Ph. D , Assistant Professor, Department of computer science and engineering, Government college of Engineering, Tirunelveli.*

Abstract: ***Mobile devices such as smartphones have been widely used all over the world. In mobile, many applications provide services to the users based on the photos provided by the user. Certain applications, client users take a photo of a certain spot and send it to a server, the server identifies the spot with an image recognizer and returns its related information to the users. It can cause a privacy issue because image recognition results are sometimes privacy sensitive. To overcome the problems of existing approaches, proposed an Encryption-Free framework for Privacy preserving Image Recognition, called Enfpire. Enfpire does not impose any restrictions on the server's recognition algorithm because it does not rely on a cryptographic techniques. In proposed approach user transform the extracted image feature x into y on the user server and sends it to the public server. With the transformation, the effectiveness of the original feature x is degraded so that the public server cannot uniquely recognize the spot-ID of user from y. It only retrives the relevant spot ID's. After that, results are processed by user's server. The unique spot ID will identify and information regarding the spot and relevant images will be given to the user.***
Keywords: SIFT, Privacy protection, Feature extraction, Feature Transformation, Information retrieval.

I. INTRODUCTION

Nowadays mobile devices are very common and widely used all over the world. There are lot of free or expensive services and applications working on smartphones. Mobile security is the protection of portable devices such as laptops, smartphones, tablets from threats and vulnerabilities.

Mobile devices are having applications for every activity of human life and are used to perform bank transactions and sensitive data transfer in the form of E-mails, messages, etc. Most of the communications happened in mobile devices in a client-server model. Applications in mobile devices act as a client and they communicate with their servers to store different types of data belong to the user. Many photo based applications, working on mobile devices are getting popular to provide services to the user.

In that client users take a photo of the spot, extract a visual feature from the photo working on mobile devices are getting popular[1][3]. Information security refers to protect information system resources from unauthorized access. It is important in the organization because it can protect the confidential information, enables to the organization function. In information services, the service provider creates a server system consisting of a database and an image recognizer. In the database, the related information for each spot such as a product list, bargain products, customer evaluations (e.g tweets for the spot) and congestion level is stored and updated in real time.

To get the and send it to the server using their own smartphones. When receiving the visual feature from the users, the server recognizes the spot in the photo using the image recognizer and returns the corresponding information in the databse to the users[12].

Visual data is responsible for one of the largest shares of global Internet traffic in both corporate and personal use scenarios. The amount of pictures, graphics associated photos being generated and shared everyday is growing at an ever increasing rate. The storage needs for such large amounts of data has been a driving factor for data outsourcing services such as the ones leveraging Cloud Storage and Computing solutions[4]. Such services have been reported to be among the largest growing internet services. The availability of large amounts of images in public and private repositories naturally leads to the need for Content-Based Image retrieval solutions (CBIR)[2]. The data outsourcing to support large scale image storage and retrieval systems, it actually raises new challenges in terms of data control and privacy.

Visual contents such as images and video generally have two types of privacy-sensitive information: visual data itself and processing results of the visual data. Examples of the former include human faces, entire bodies, car license plates, and so on. In CBIR, not only a query image but also the gallery images retrieved with the query are sometimes privacy-sensitive because they reflect users interest or preference[9].

Hence, systems that can perform CBIR without disclosing such information to a retrieval server are called privacy-preserving CBIR (PCBIR) systems. Since CBIR and image recognition have a lot of common processes, research on privacy-preserving image recognition[16].

In cryptographic technique the users send the server an encrypted of a feature vector and the server runs its recognition process in the encrypted domain. It can only work with a specific recognition algorithm. An encryption cost is computationally high for mobile devices. In this paper to propose an Encryption-Free framework for Privacy-preserving Image Recogniton called EnfPire, to a privacy preserving framework for image retrieval. EnfPire does not impose any restrictions on the servers recognition algorithm because it does not rely on cryptographic techniques.

The paper is organized as follows: Section II to discuss the related work of proposed system, Section III to discuss the implement of proposed system, and also discuss the feature extraction, feature transformation, Image recognizer, Information Retrieval. In addition ,to experimentally discuss the performance evaluation.

II. RELATED WORK

S. Wang et al.[1] proposed an shape based image feature extraction to deal with raw image data without any keyword annotations to computational task.For each image, Data owner specifies the shape to be based on encrypt each pixel in the image by the Homomorphic encryption scheme.

Then Data owner to split the image randomly into two shares and send one share to S1,the other to S2 these two server perform the accumulation process.

To be used no. of practical situation for extracting features securely. The server has encrypted image and client want a feature extracted representation of those that are feature rich. Their experimentally demonstrated their viability and quantified their securely and efficiency trade-offs.

B. Ferria et al.[2] propose an secure framework for outsourced privacy-preserving storage and retrieval in large image repositories supported IES-CBIR, Image Encryption scheme that displays content based Image Retrieval properties. To enable the both encrypted storage and searching using CBIR queries while preserving privacy.

To fully protect image content and therefore the encryption algorithm: pseudo random pixel position permutation, through pixel rows and columns shifting. Implement the IES-CBIR to protect the image texture with probabilistic encryption and color information with deterministic encryption.

IES-CBIR with two different types of cryptographic keys, repository keys(rk) and image keys(ik) which are generated by the GENPK and GENIK algorithm. Searching-Trapdoor Generation: The TRPGEN algorithm generates searching trapdoors that user can leverage to look over image repositories.

To provide more efficient operations both in term of time and space complexity.

C. Hsu et al.[3] implement the privacy-preserving realization of the SIFT method based on homomorphic encryption. In PPSIFT, privacy-preserving feature extraction and representation addresses the issue of extracting and representing meadia features in the encrypted domain to allowing exhibition of inherent properties within the plain text/un-encrypted domain. To the protection analysis supported distinct power downside and RSA that PPSIFT is secure against ciphertext ony attack and celebrated plaintext attack.

Ciphertext only attack, the adversary, can access to the ciphertext, which is the encrypted data available at the server or access, the threshold table used for encrypted data comparison. In KPA model is assumed to known a no.of pair of plaintext images and their corresponding encrypted version. The proposed pailler cryptosystem based PPSIFT scheme provide additive homomorphism and achieves provable security based on DLP and RSA.

R. Cheng et al.[4] propose an framework where uncertainty can be controlled to provide high quality and privacy-preserving services. Based on this framework, suggest a data model to augment uncertainty to location data and propose imprecise queries that hide the location of the query issuer and yield probanblistic result. using the location cloacking model for location privacy is user cloaking provides a simple way for a user to control the release of private information to untrusted parties. The degree of privacy can be measured in two ways:1.size of uncertainty region 2.coverage of sensitive area. imprecise queries, which hide the identity question institution and alter analysis of cloaked data.

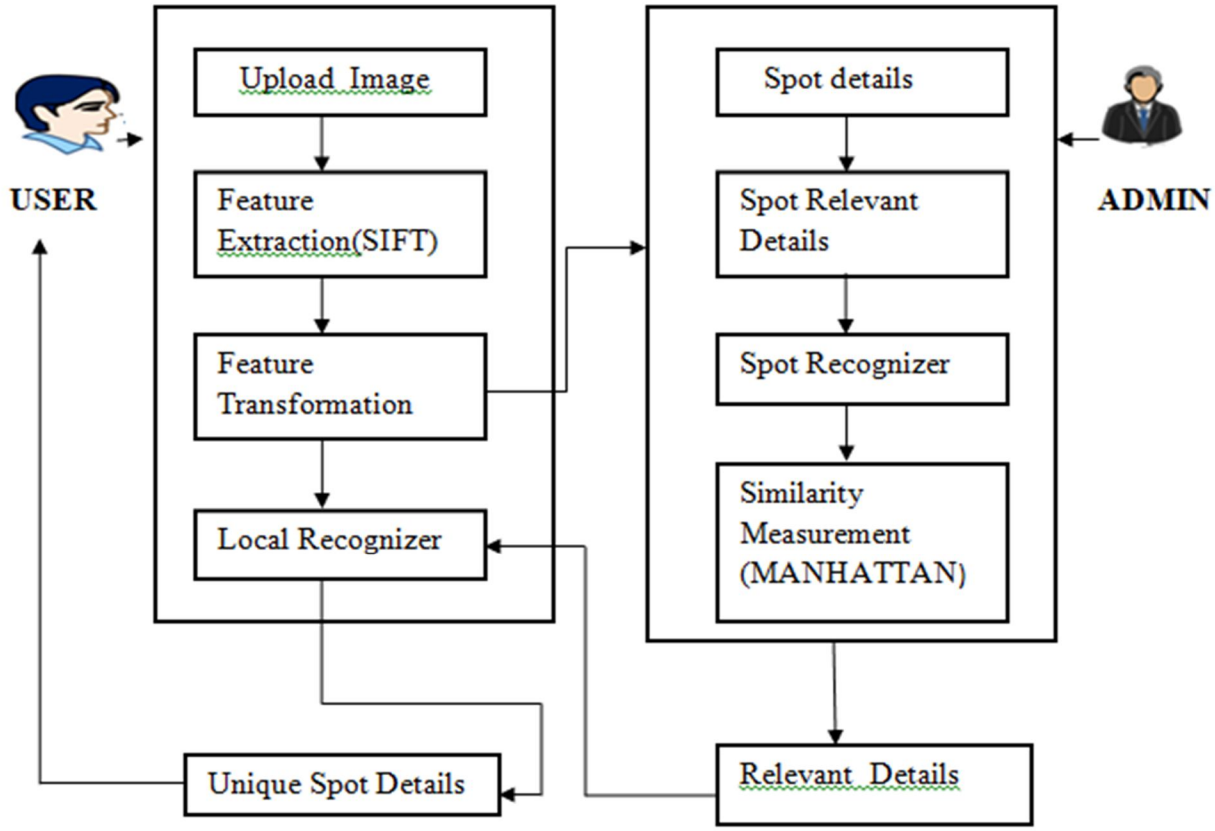


Figure.1 Photo based Information services

III. PROPOSED FRAMEWORK

An encryption-free framework for privacy-preserving image recognition called by EnfPire. In this approach the client users locations are represented as a spot-ID.In the mobile services based on GPS, the users locations are represented as a numerical coordinate. There have been proposed a lot of methods for protecting the numerical location data. In the transformation-based methods, the users transform their exact location coordinate into another coordinate before sending it to the server. To replace the exact location coordinate of a certain near-by landmark such as an temple or a building. The service provider creates a server system consisting of a database and an image recognizer.In the database, related information for each spot such as a product list, bargain products, customer evaluations and congestion level is stored and updated in realtime.

To get the information, client users take a photo of the spot, extract a visual feature from the photo, and send it to the server using their own smartphone. When receiving the visual feature from the users, the server recognizes the spot in the photo using the image recognizer and returns the corresponding information in the database to the users.It means the users current location is disclosed to the server in terms of spot ID at the spot-recognition stage on the server side. Moreover, when the users send a visual feature of the photo to the server, some identifiers of the users smartphone are also sent automatically It can be used by the server for making a correspondence between current and past results of spot-recognition. Not only the users current location but also their location history is disclosed to the server. Because the location history can be viewed as the users privacy information that reflects their interests and preference, it should be protected. Proposed system also supports privacy-preserving image storage and sharing among users[4].

A. Feature Extraction

Feature extraction is a type of dimensionality reduction that efficiently represent interesting parts of an image. The process of feature extraction is useful to reduce the number of resources needed for processing without losing important or relevant information. Feature extraction can also reduce the amount of redundant data for a given analysis.The Features extraction can be classified into two categories: Color extraction and Shape extraction[3][11][22].

B. Color Feature Extraction Using Histogram

1) *Step 1:* For extracting color histogram, the RGB color space is converted to HSV color space.
2) *Step 2:* The color histogram is calculated based on MPEG-7 Scalable color.
3) *Step 3:* The color space is uniformly quantized into 16 levels of hue, 4 levels of saturation and value giving a total of 256 bits.
4) *Step 4:* To lower this number and make the application scalable, the histogram is encoded using Haar transform.
5) *Step 5:* Usage of subset coefficient in Haar representation is 64 bins. Global color histogram is constructed for all images.

C. Shape Feature Extraction Using SIFT

1) *Constructing A Scale Space:* It is the initial preparation to create internal representations of the original image to ensure scale invariance.
2) *LoG Approximation:* The Laplacian of Gaussian is great for finding key points in an image.
3) *Finding Keypoints:* To find key points that are maxima and minima in the Difference of Gaussian image calculate in step 2.
4) *Get Rid Of Bad Key Points:* Edges and low contrast regions are bad keypoints. Eliminating these makes the algorithm efficient and robust.
5) *Assigning An Orientation To The Keypoints:* An orientation is calculated for each key point.
6) *Generate SIFT Features:* Finally, with scale and rotation invariance in place, one more representation is generated. This helps uniquely identify features.

D. Feature Transformation

In feature transformation the visual feature extracted from images such as IP Address,Date,Time are considered as **X** and the properties features such as Shape,Color are considered as **Y**. **X** into **Y** on the user's server and sends it to the public server. With the transformation, the effectiveness of the original feature **X** is degraded so that the server cannot uniquely recognize the spot-ID. The original feature **X** is not disclosed to the server because the transformation is done on the user side. Because **Y** is less effective, the server does not uniquely recognize the spot-ID. Features are transformed into two categories called visual features and image properties features. Visual features are image color, shape, texture and edge features etc. Properties features consist of image capturing date, time, size and location etc.

E. Image Recognizer

The recognizer increases the server spot-recognition performance, it is not desirable from the aspect of privacy protection. This approach should provide a transformation method that makes the server unable to judge whether visual features sent from the users are original version or transformed version. The users have to use a relatively simple recognizer that involves no training phase because of their limited computational resources[5][18].

F. Similarity Measurement Algorithm

1) *Input:* X = {x1, x2, x3,…..,xn} be the set of data points , Y= {y1,y2,y3…yn} be the set of data points and V = {v1,v2,v3,….,vn} be the set of centers.

a) Step 1: Select 'c' cluster centers arbitrarily

b) Step 2: Calculate the distance between each pixels and cluster centers using the manhattan Distance metric.

$$Dist(X,Y) = \sqrt{\sum_{j=1}^{n}(X_{ij} - Y_{ij})^2}$$

X, Y are the set of data points

c) Step 3: Pixel is assigned to the cluster center whose distance from the cluster center is minimum of all cluster centers.

d) Step 4: New cluster center is calculated using

$$V_i = \frac{1}{C_i}\sum_{1}^{ci} x_i$$

Where Vi denotes the cluster center, ci denotes the number of pixels in the cluster.

e) Step 5: The space amoung each pixel element and new obtained cluster facilities is recalculated.

f) Step 6: If no pixels were reassigned then stop otherwise repeat steps from 3 to 5.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

G. Information Retrieval

When receiving the visual feature from the users, the server recognizes the spot in the photo using the image recognizer and returns the corresponding information in the database to the users. similarity based recognition method on the server side, whereas employed closest detection algorithm for a recognition method on the user side[10][16]. If I is the database image and query image, then the similarity measure is computed as follows,

1) *Step 1:* Calculate histogram vector vI = [vI1, vI2, ….vIn] and ccv vector cI = [cI1, cI2, ….cIn] of the database images.
2) *Step 2:* Calculate the vectors vI and cI for the query image also.
3) *Step 3:* The Manhattan distance between two feature vectors can then be used as the similarity measurement.
4) *Step 4:* If $d \leq \tau$ (threshold) then the images match.

IV. EXPERIMENTAL RESULTS

The database was created and each image has unique information. Image relevant information are generated and stored on database during the process. The proposed framework to protect the user current location information and improve the privacy preserving for image retrieval.

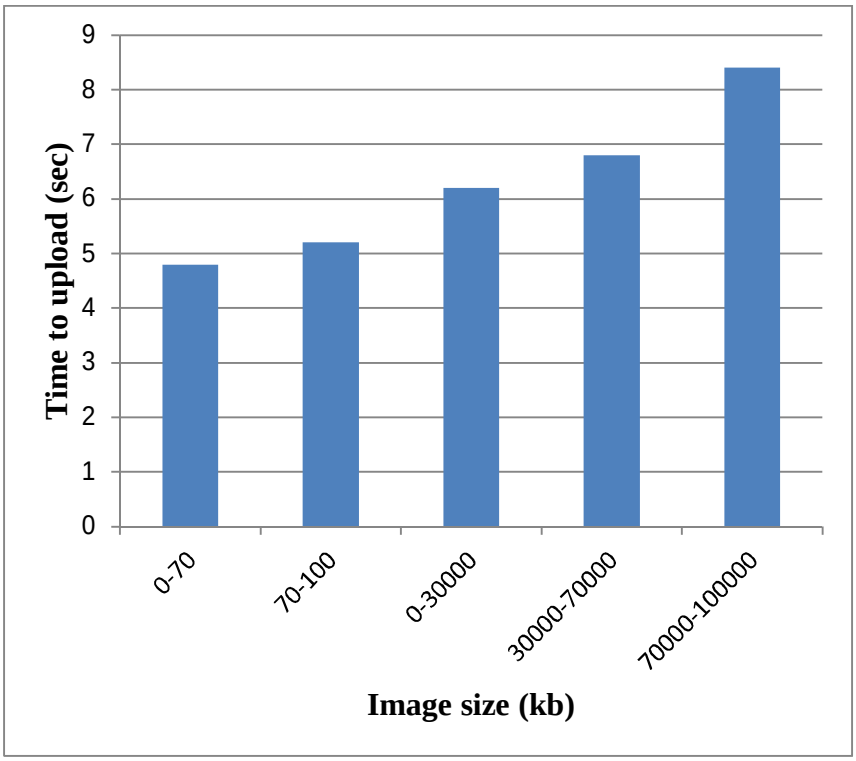


Figure 2: Graph for Image Uploading Time Evaluation

Figure 2 indicate the time taken to upload the images when compared with image size.The time taken to upload the image increases with the increasing image size.The uploading time is minimum,when the image size is less than 70 kb and it increases in the image and reaches maximum when the image size is 100000 kb.

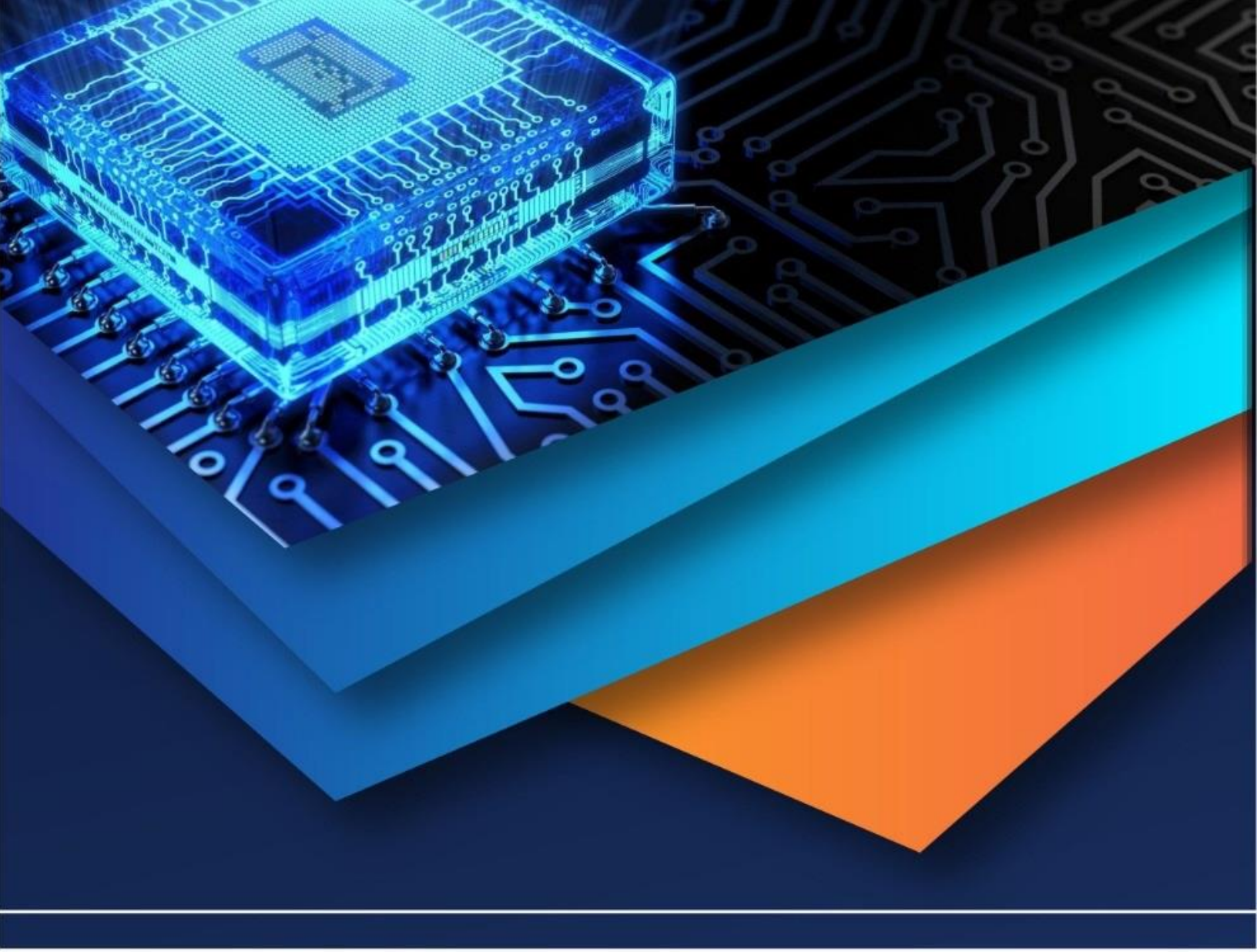
V. CONCLUSION

In this work an EnfPire framework is proposed for photo-based information services. In existing photo based information services, a server can easily recognize client users current location.The proposed system to protect the location information and extracting features from color and shape.Then features are transformed into two categories visual features(X) and properties features(Y).To recognizing the server spot details and retrieving the similar images from databases.The number of search results may vary counting on the amount of comparable images within the database.

Most of the storage systems does not take responsibility of secure storage.,So enhance the security of the image an encryption methodology can be added.Duplicate checking methodology can be also added to avoid repeated images in the storage.

REFERENCES

[1] S. Wang, M. Nassar, M. Atallah, and Q. Malluhi: "Secure and Private Outsourcing of Shape-Based Feature Extraction," in Proceedings of the 15th International Conference on Information and Communications Security, 2013.
[2] B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos: "Privacy-Preserving Content Based Image Retrieval in the Cloud," in the Proceedings of the 34th IEEE Symposium on Reliable Distributed Systems, 2015.
[3] C. Hsu, C. Lu, and S. Pei: "Image Feature Extraction in Encrypted Transactions on Image Processing Domain with Privacy-Preserving SIFT," IEEE, Vol.21, No.11, pp.4593–4607, 2012.
[4] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar: "Preserving User Location Privacy in Mobile Data Management Infrastructures," in Proceedings of the 6th International Workshop on Privacy Enhancing Technologies, pp.393–412, 2006.
[5] Y.Zeng, Y.Chan, T.Lin, M.Shih, P.Hsieh,and G.Chao: "Scene Feature Recognition-Enabled Framework for Mobile Service Information Query System," in Proceedings of the 17th International Conference on Human Interface and the Management of Information, 2015.
[6] I. Mitsugami, M. Mukunoki, Y. Kawanishi, H. Hattori, and M. Minoh: "Privacy-Protected Camera for the Sensing Web," in Proceedings of the 13th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, pp.622–631, 2010.
[7] A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent: "Large-Scale Privacy Protection in GoogleStreetView,"inProceedingsofthe12thInternationalConference on Computer Vision, pp.2373–2380, 2009.
[8] K. Inai, M. Palsson, V. Frinken, Y. Feng, and S. Uchida: "Selective Concealment of Characters for Privacy Protection," in Proceedings of 22nd International Conference on Pattern Recognition, 2014.
[9] L. Zhang, T. Jung, P. Feng, K. Liu, X. Li, and Y. Liu: "PIC: Enable Large-Scale Privacy Preserving Content-Based Image Search on Cloud," in Proceedings of the 44th International Conference on Parallel Processing, 2015.
[10] W. Chu and F. Chang: "A Privacy-Preserving Bipartite Graph Matching Framework for Multimedia Analysis and Retrieval," in Proceeding of the 5th ACM International Conference on Multimedia Retrieval, pp.243– 250, 2015.
[11] C. Hsu, C. Lu, and S. Pei: "Secure and Robust SIFT," in Proceedings of the 17th ACM International Conference on Multimedia, pp.637–640, 2009.
[12] Z. Qin, J. Yan, K. Ren, C. Chen, and C. Wang: "Towards Efficient Privacy-Preserving Image Feature Extraction in Cloud Computing," in proceedings of the 22nd ACM International Conference on Multimedia,pp.497-506.2014.
[13] G.Fanti,M.Finiasz,andG.Friedland:"TowardEfficient,Privacy-Aware Media Classification on Public Databases," in Proceedings of the 4th International Conference on Multimedia Retrieval, 2014.
[14] B. Lee, J. Oh, H. Yu, and J. Kim: "Protecting Location Privacy using Location Semantics," in Proceedings of the 17th ACM International Conference on Knowledge Discovery and Data Mining, pp.1289–1297, 2011.
[15] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," Proc. SPIE, vol. 7254, pp. 1–11, Jan. 2009.
[16] J.Shashank,P.Kowshik, K. Srinathan, and C. Jawahar, "Private content based image retrieval," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2008, pp. 1–8.
[17] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni,"Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP J. Inf. Security, vol. 7, no. 2, pp. 1–20, 2007.
[18] B. Zhou, A. Lapedriza, J. Xiao, A. Torralba, and A. Oliva: "Learning Deep Features for Scene Recognition using Places Database," in Proceedings of the 27th International Conference on Neural Information Processing Systems, pp.487–495, 2014.
[19] -H. Bay, T. Tuytelaars, and L. V. Gool, "Surf: Speeded up robust features," in Proc. Eur. Conf. Comput. Vis., 2006, pp. 404–417.
[20] D. Lowe, "Distinctive image features from scale invariant keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, 2004.
[21] A. Sadeghi, T. Schneider, and I. Wehrenberg: "Efficient Privacy Preserving Face Recognition," in Proceedings of the 12th International Conference on Information Security and Cryptology, pp.229–244, 2009.
[22] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Homomorphic encryption-based secure sift for privacy-preserving feature extraction," Proc. IS&T/SPIE Media Watermark., Forensics, Security, vol. 7880, pp. 788005-1– 788005-17, Jan. 2011.
[23] M. Kantarcıo˘glu and C. Clifton: "Privately Computing a Distributed k-NN Classifier," in Proceedings of the 8th European Conference on Principles of Data Mining and Knowledge Discovery, 2004.
[24] K. Fujii, K. Nakamura, N. Nitta, and N. Babaguchi: "A Framework of Privacy-Preserving Image Recognition for Image-Based Information Services," in Proceedings of the 23rd International Conference on Multimedia Modeling, pp.40–52, 2017.
[25] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu: "Enabling Search over Encrypted Multimedia Databases," in Proceedings of the SPIE Conference on Media Forensics and Security, Vol.7254, pp.18–29, 2009.
[26] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie: "Dummy-Based User Location Anonymization Under Real-World Constraints," IEEE Access, Vol.4, pp.673-687, 2016.
[27] D. Kim and D. Hwang: "Non-Marker based Mobile Augmented Reality and its Applications using Object Recognition," Journal of Universal Computer Science, Vol.18, No.20, pp.2832–2850, 2012.
[28] G. Xie, X. Zhang, S. Yan, and C. Liu: "Hybrid CNN and DictionaryBased Models for Scene Recognition and Domain Adaptation," IEEE Transactions on Circuits and Systems for Video Technology, Vol.27, No.6, pp.1263–1274, 2017.
[29] M. Koskela and J. Laaksonen: "Convolutional Network Features for Scene Recognition," in Proceedings of the 22nd ACM International Conference on Multimedia, pp.1169–1172, 2014.
[30] C. Liu, Z. Shang, and Y. Y. Tangc: "An Image Classification Method That Considers Privacy-Preservation," Neurocomputing, Vol.208, No.5, pp.80–98, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY