Encryption-Free Framework of Privacy-Preserving Image Recognition for Photo-Based Information Services

R.V. UdayKumar[1] N. PrasadReddy[2] G. Hanesh[3] N. Teja[4] Mr. A. M. Rangarajan[5]
[1,2,3,4]Student [5]Assistant Professor
[1,2,3,4,5]Department of Computer Applications
[1,2,3,4,5]Sri Venkateswara College of Engineering and Technology, Chittoor, India

Abstract— Mobile phones ,smart phones, computers, Laptops are widely used all over the world . To protect the data that is stored in these devices are protected by using different types of privacy option like patterns, passwords etc., along with this privacy options there is one more option nothing but the image recognition and the performance of image recognition has drastically increased along with the learning and advanced technologies. Usually photo based information are provided in the client server architecture are getting popular from the background. Customer or the client used to take a picture and send it to the server there it checks or spots it with an image recognizer and returns the related information to the user as result. This type of image recognition causes the privacy issues because image recognition results are sometimes privacy sensitive. In order to tackle with this problem, in this paper one if the framework of privacy image recognition called Enfpire, by this the user can uniquely determine the recognition result where the server cannot uniquely determine the recognition result. Here first a visual feature from their taken photo and transform it by the client so that the server cannot uniquely determine the recognition result. Later the user send the transformed feature to the server, and it returns a set of candidates to the users. Finally to obtain the final result, the user compare the candidates to the original visual feature.

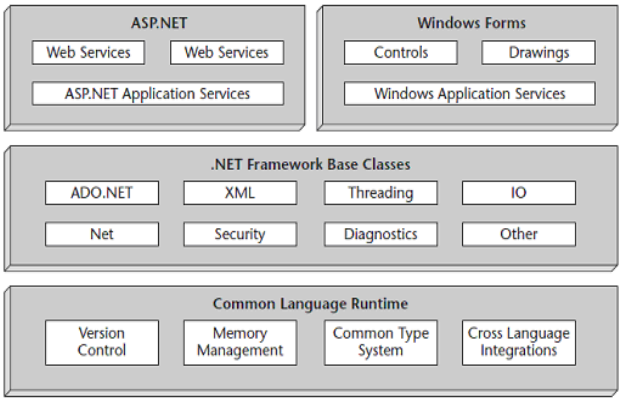
Keywords: Image Recognition, client server Architecture, Enfpire

I. Introduction

One of such research areas is image recognition including object recognition and scene recognition whose performance has drastically increased in the past decade. Moreover, nowadays mobile devices such as smartphones are very common and widely used all over the world. There are a lot of free or inexpensive services and applications working on smartphones. From these backgrounds, image recognition-based information services working on mobile devices are getting popular. In fact, at non-commercial level several prototypes of such services have been already developed. A typical example is non-marker-based mobile Augmented Reality in which the object captured by a built-in camera on a smartphone is recognized by image recognition techniques and some visual contents of the recognized object are overlaid on the camera image for providing information to users. Another example is a tourist assistance system proposed by Zeng et al. [12], in which users can get guide information by taking a photo of a landmark, street, building, and so on and sending it to a cloud server that hosts image recognition services. Client-server-based information services like the one developed in Zeng's work [12] are advantageous in that they can provide the latest information only by updating the server's information database and recognition criteria. However, they can also cause a privacy issue because image recognition results are sometimes privacy-sensitive, whose situation is described in detail in the following subsections.

.NET Framework, is the first Microsoft development environment designed from the ground up for Internet development by the Microsoft's new software development platform. Although .NET is not only to be used exclusively for Internet development but also in windows development, its innovations were driven by the limitations of current Internet development tools and technology.

There are three primary components or layers in the basis of this new development platform: the common language runtime, the .NET Framework base classes, and the user and program interfaces, as demonstrated in following figure



It is important to note that the IL code is not interpreted to the code. The common language runtime uses just in time compilers to compile the IL code to native binary code before execution. The following are the other significant features of the common language runtime includes

- Version control
- Memory management
- Cross language integration
- Common data type system

For example, ASP.NET hosts the runtime to provide a scalable, server side environment for managed code in the intermediate language. ASP.NET works directly with the runtime to enable .asp pages and Web services.

II. Literature Survey

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. The latter examples are results of content-based image retrieval (CBIR) and those of image recognition.

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.

Hence, systems that can perform CBIR without disclosing such information to a retrieval server have been studied, which are called privacy-preserving CBIR (PCBIR) systems.

A. *Requirements*

1) *Privacy Protection for Visual Data*

Methods for protecting privacy-sensitive regions in images and video have been widely studied in the past decade. Some of them visually abstract the privacy-sensitive regions by blocking out, silhouetting, pixelization, complete removal, and so on. Chinomi et al. proposed a system called PriSurv, which adaptively applies such operations to surveillance video based on the relationship between people in the video and its viewer.

2) *Privacy Protection in CBIR*

The purpose of PCBIR is to hide users' query image from a retrieval server as well as make the server unable to identify which gallery images are matched to the query image. This can be achieved by cryptographic techniques; that is, the users encrypt a visual feature extracted from their query image before sending it to the server and the server calculates the similarity between the visual feature of the query image and that of each gallery image in the encrypted domain.

3) *Privacy Protection in Image Recognition*

Compared to PCBIR, there are relatively fewer studies addressing privacy issues in image recognition, one of whose examples is privacy-preserving face recognition (PFR) firstly studied by Erkin et al. They assume a client-server architecture in which client users send a face image as a request to a recognition server, which only has a single face image per person as gallery images and compares the request face image with each gallery image to recognize the ID of the person in the request. Finally, the recognized ID is returned to the users. The purpose of PFR is to successfully perform the above protocol without disclosing the request face image and its recognition result to the server.

4) *Protection of Location Privacy*

The client users' locations are represented as a *spot*-ID. Unlike this, 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. These methods can be classified into three types: cloaking area-based, transformation-based, and dummy-based.

III. PROPOSED SYSTEM

A. *System Framework*

We designed a standard keyword search protocol in this framework. During setup, the data owner generates the required encryption keys for hashing and encryption operations. Then, all documents in the database are parsed for keywords. The documents are then symmetrically encrypted and uploaded to the cloud server. To add files to the database, the data owner parses the files as in setup and uploads to the cloud server. To perform a search, the data user enters keyword then it computes and sends a trapdoor encryption of the queried keywords to the cloud to initiate a protocol and returns accurate file. Here we implement some modules they are Data Owner, Data User and Cloud Server.

B. *Algorithm*

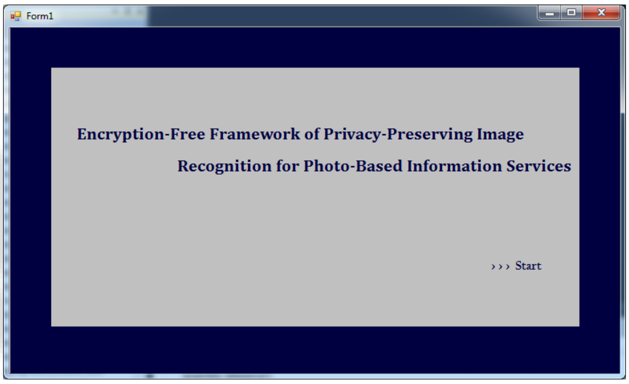
The AES algorithm is an extension of the Advanced Encryption Standard algorithm .The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for classified and secure data decryption and encryption. The AES cipher is one of the part of a family known as block ciphers, which are algorithms that encrypt data on a per-block basis .These "blocks" which are measured in bits determine the input of plaintext and output of ciphertext.

The key size used for this cipher specifies the number of repetitions or "rounds" required to put the plaintext through the cipher and convert it into ciphertext.

Protecting privacy associated with the phrase search operation, which consists of three types of privacy, namely the document set privacy, the index privacy, and the trapdoor privacy. The document set privacy can be easily achieved by encrypting the documents using a block cipher, such as AES, before outsourcing them to the cloud server.

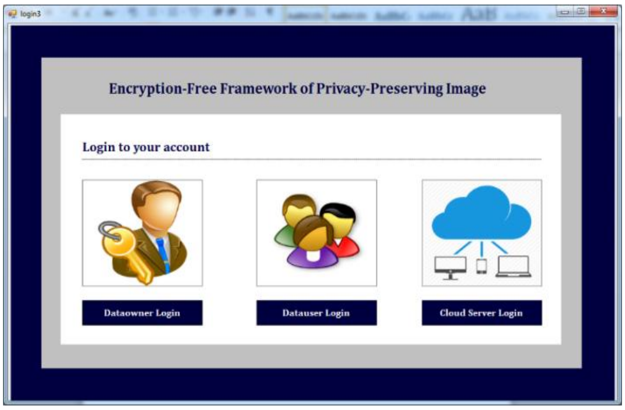
IV. RESULT AND ANALYSIS

A. *Home Page*



Encryption-Free Framework of Privacy-Preserving Image
Recognition for Photo-Based Information Services

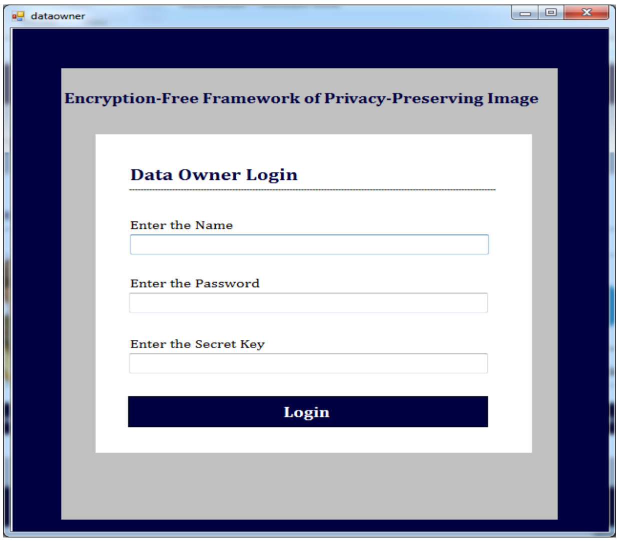
B. *Authentication Page*



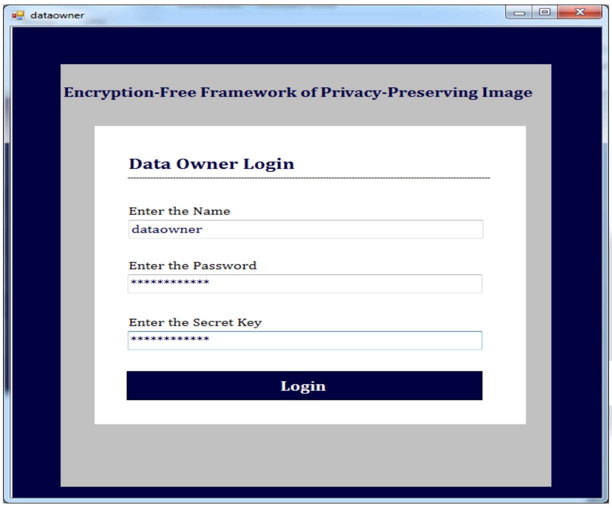
Encryption-Free Framework of Privacy-Preserving Image

Login to your account

C. *Data owner Login*



D. *Login→Dataowner*

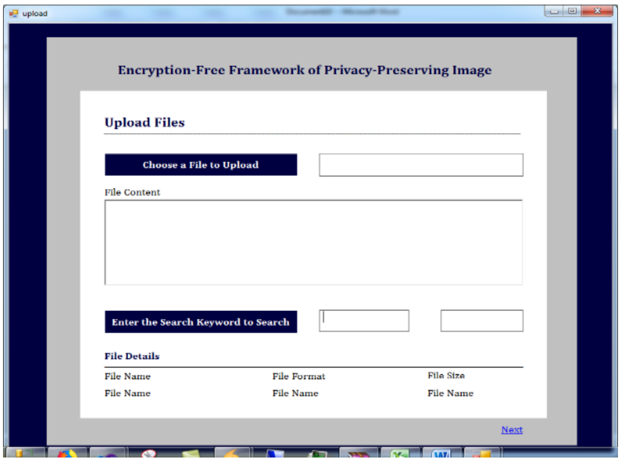


Enter the Name: dataowner

Enter the Password: ************

Enter the Secret Key: ************

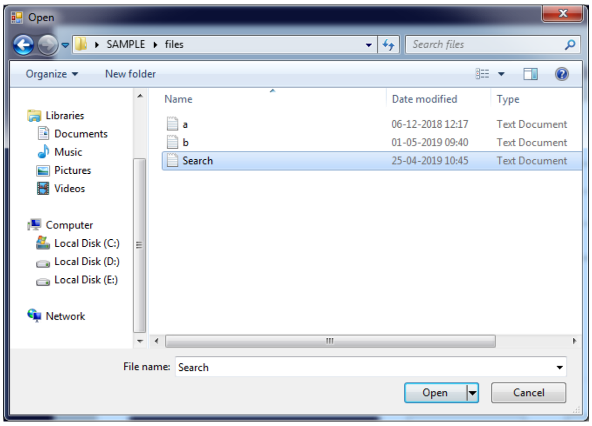
E. *Upload file Page*


upload
Encryption-Free Framework of Privacy-Preserving Image
Upload Files
Choose a File to Upload
File Content
Enter the Search Keyword to Search
Next

File Details

File Name	File Format	File Size
File Name	File Name	File Name

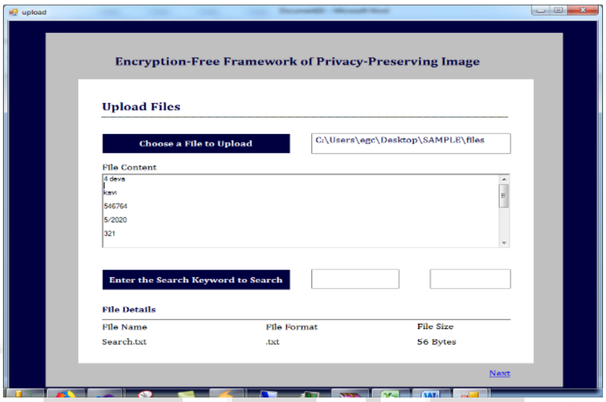
F. *Select File in Folder*



Name	Date modified	Type
a	06-12-2018 12:17	Text Document
b	01-05-2019 09:40	Text Document
Search	25-04-2019 10:45	Text Document

File name: Search

G. *View Content of File*


upload
Encryption-Free Framework of Privacy-Preserving Image
Upload Files
Choose a File to Upload
Enter the Search Keyword to Search
Next

C:\Users\egc\Desktop\SAMPLE\files

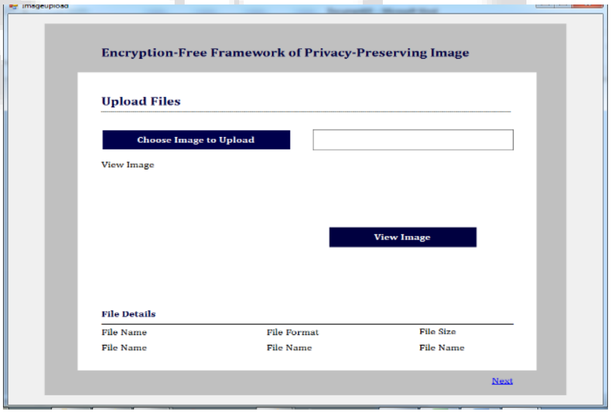
File Content

4 deva
kavi
546764
5/2020
321

File Details

File Name	File Format	File Size
Search.txt	.txt	56 Bytes

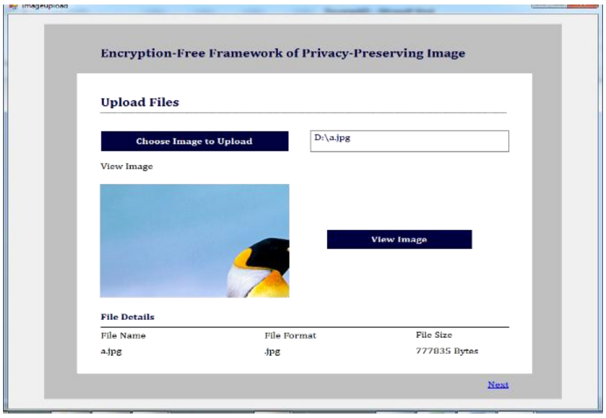
H. *Upload Image Page*



File Details

File Name	File Format	File Size
File Name	File Name	File Name

I. *View Image*

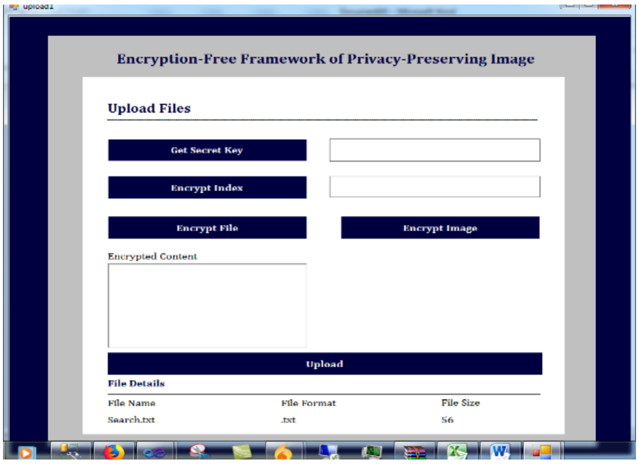


D:\a.jpg

File Details

File Name	File Format	File Size
a.jpg	.jpg	777835 Bytes

J. Encrypt Page



Encryption-Free Framework of Privacy-Preserving Image

Upload Files

Get Secret Key

Encrypt Index

Encrypt File | Encrypt Image

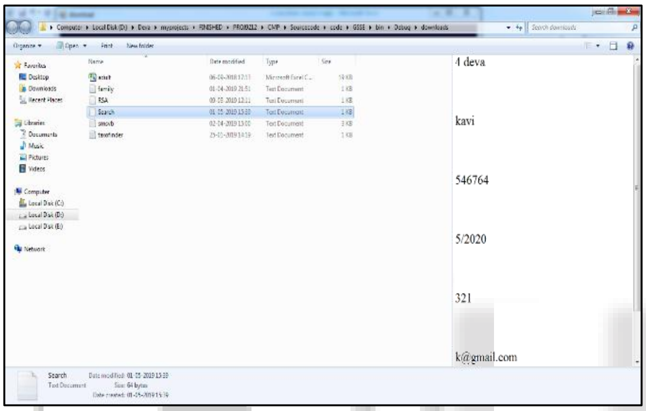
Encrypted Content

Upload

File Details

File Name	File Format	File Size
Search.txt	.txt	56

K. Show Download file



Computer ▸ Local Disk (D:) ▸ Deva ▸ myprojects ▸ FINISHED ▸ PROJ9212 ▸ CMP ▸ Sourcecode ▸ code ▸ GSSE ▸ bin ▸ Debug ▸ downloads

Name	Date modified	Type	Size
adult	06-03-2018 17:11	Microsoft Excel C...	59 KB
family	01-04-2019 21:51	Text Document	1 KB
RSA	09-03-2019 12:11	Text Document	1 KB
Search	01-05-2019 13:39	Text Document	1 KB
smsvb	02-04-2019 13:00	Text Document	3 KB
textfinder	25-01-2019 14:19	Text Document	1 KB

4 deva

kavi

546764

5/2020

321

k@gmail.com

Search Date modified: 01-05-2019 13:39
Text Document Size: 64 bytes
Date created: 01-05-2019 13:39

V. Conclusion

In this paper, we proposed a framework for privacy-preserving image recognition named EnfPire, focusing on photo-based information services. In such services, a server can easily recognize client users' current location as we experimentally showed. To protect the location information, EnfPire abstracts it using a linear subspace-based feature transformation. Because EnfPire does not rely on crypto-graphic techniques, it allows the use of various recognition algorithms on the server side.

References

[1] G. E. Hinton, S. Osindero, and Y. Teh: "A Fast Learning Algorithm forDeep Belief Nets," Neural Computation, Vol.18, No.7, pp.1527–1554,2006

[2] L. Deng and D. Yu: "Deep Learning: Methods and Applications,"Foundations and Trends in Signal Processing, Vol.7, No.3–4, pp.197–387, 2014

[3] Krizhevsky, I. Sutskever, and G. E. Hinton: "ImageNet Classification with Deep Convolutional Neural Networks," in Proceedings of the 25thInternational Conference on Neural Information Processing Systems,pp.1097–1105, 2012.

[4] P. Agrawal, R. Girshick, J. Malik: "Analyzing the Performance of Multilayer Neural Networks for Object Recognition," in Proceedings of the 13th European Conference on Computer Vision, pp.329–344, 2014.

[5] M. Liang and X. Hu: "Recurrent Convolutional Neural Network for Object Recognition," in Proceedings of the 28th IEEE Conference on Computer Vision and Pattern Recognition, pp.3367–3375, 2015.

[6] 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.

[7] Zhou, A. Lapedriza, J. Xiao, A. Torralba, and A. Oliva: "Learning Deep Features for Scene Recognition using Places Database," in Pro-ceedings of the 27th International Conference on Neural Information Processing Systems, pp.487–495, 2014.

[8] L. Herranz, S. Jiang, and X. Li: "Scene Recognition with CNNs: Objects, Scales and Dataset Bias," in Proceedings of the 29th IEEE Conference on Computer Vision and Pattern Recognition, pp.571–579, 2016.

[9] G. Xie, X. Zhang, S. Yan, and C. Liu: "Hybrid CNN and Dictionary-Based Models for Scene Recognition and Domain Adaptation," IEEE Transactions on Circuits and Systems for Video Technology, Vol.27,No.6, pp.1263–1274, 2017.

[10] 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.