Face Recognition and Geolocation based Authorization and Authentication: A Survey

Vivek Kumar
Student
School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab

Harpreet Kaur
Assistant Professor
School of Computer Science and Engineering
Lovely Professional University Phagwara, Punjab

Shashank Shekhar
Student
School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab

Bheshraj Patel
Student
School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab

Abstract— **For the past decades, information growth has taken over the internet and has made the task complex for handling or making secure and safe transaction of data. For security, Face recognition is one unique technique. This paper covers the detailed comparison of various research work. In addition, this paper also covers the detailed survey of Geo-location authentication, an another unique and frequently used technique. It is useful in authentication as well as authorization. In this paper, we discuss about the difference between available research on above topic, also provides an efficient approach of security with two step authentication using Face recognition and geo-locking.**

Keywords— **Face recognition, Geo-location, authentication, authorization.**

I. INTRODUCTION

Today, the digital world is much complex and so the security of it. It became difficult for an institution to match the user's choice and quality security at once. User friendly security were rarely available, like remembering of passwords. But, now a days, use of Face for securing our devices and data are playing a major role in cyber field. Face recognition is one user-friendly and highly accurate technique in providing security to data. Face Recognition is a technique which uses the computerized image or video to match the face of the human to perform identification and authentication. This technique takes use of various patterns of faces to first store in a database. Then, in another attempt, it verifies it with the databased faces. This is performed by various techniques like Eigenfaces, Fisher faces, and Local Binary Pattern Histogram(LPBH).

The system of Face Recognition has 2 methods, a face detector which scans or detects the face and face recognition which recognizes the face by matching the face to the database. This system is both a challenging and necessary detection technique.

Face Recognition techniques :

Eigenfaces : This technique is based on Principle of Component Analysis (PCA). In this, the face is predicted using the pre-defined sample images called the eigenfaces. This is the eigenvector of sets of faces. It performs are series of steps as follows:

- Acquiring Sample(Training)
- Estimating the eigenfaces
- Projecting the face image onto the face space.
- Projecting test face image onto the face space.
- Get eigen face component
- Estimate Euclidian distance between the input face image and training sample .

Based, on the above steps, the sample or face of a human is identified for further processing.

Fisher faces : This technique is based on Linear Discriminant Analysis (LDA). This technique is considered as more efficient and fast technique than eigen faces, also it works well in different surrounding and expressions.
This technique also follows a series of steps for completion of its task, is as follow:

- Fetch image from database
- Compute the average of all faces.
- Compute the average of each faces.
- Subtract average faces of each person from training face.
- Construction of matrix.

Based, on the above steps, the sample or face of a human is identified for further processing following this technique.

Local Binary Pattern Histogram (LBPH) : Considered as most efficient among all in labelling texture and image, follows a combined approach of histogram and local binary pattern.
Followings are the steps followed by LBPH for face recognition:

- Parameter Selection (Radius, neighbour)
- Training the algorithm (ID assignment)
- LBP algorithm (int. images to highlights feature)
- Extract histogram
- Perform the face recognition.

OpenCV, is used for analysing the performance of face detection algorithm. Its comparison results in LBPH as best. Table no. 1.1 is the output of comparison of various technique, as mentioned by Sharmila and her team.

Algorithm	Accuracy of Detection
Eigen Faces	70
Fisher Faces	78
LBPH	80

Table 1.1 Comparison between different Techniques

Basically, there are two types of features of face recognition.

- Global Feature : It describes the whole image. This feature is not robust, as any slight change in part of image may cause failure. In it, single feature vector uses as input to a classifier. It works well only for frontal views of face. To avoid problem face during pose, change an alignment stage can be added before classifying.
- Local Feature : It describes the patches within the image, multiple local descriptions are used to coordinate for the correlation to made. It is performed by independently matching template of three different facial region. The recognition process is based on wavelet coefficient that are computed on nodes of elastic graph.

Procedure and Structure

We generally separate the face recognition procedure into three steps: Face Detection, Feature Extraction, and Face Recognition below:
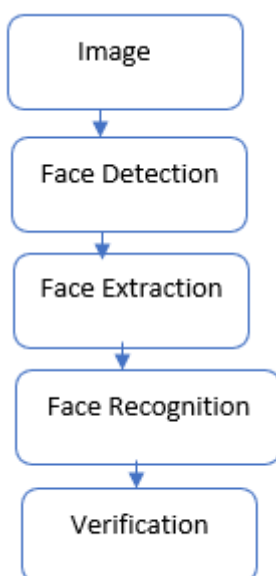

Fig 1.1 Structure of Face Recognition

There are certain elements of security that should be maintained before the communication takes place between hosts.

    a) Authentication
    b) Authorization

Authentication :
Authentication is a mechanism for identifying a user request with the available set of identified credentials. The credentials are available at local store or authorized server. It is performed to verify that whether the user is allowed or authorized user to this system or not.

Authorization :
Authorization is a follow-up step of Authentication, i.e. it is performed after the latter. It is a mechanism to provide access to the user based on their position. The access based on position has already defined in the server, and it is performed after authentication (get position).

Another Unique and efficient technique for authorization and authentication is Geo-location. It is used to provide the geographical information to application. It maps IP address to geographical location of internet connected device. In this paper, the geo-locking technique is concerned. In geo-locking, the information send is accessible only to a specified location. A geo-location (Longitude and Latitude) is attached with data while sending, and when the receiver open the data, it automatically match the attached data with the location of device (from which data is accessed, can be mobile or Computer). If the geo-location matched, the data would be available, otherwise, it fails. the Geo-location technology in Google maps, the example of the most used satellites in Geo-location is all information source to destination pass through satellites whether it is GPS or anything else.
This technique can be useful for both authentication and authorization. Like, if a sender has sent an information based on geolocation to a military base. Then, only the military person inside to base are allowed to accessed (authentication at minimum level) and also, data can be different for different military bases, thus the geo-location will provide the authorization feature of which bases are authorized for accessing which data.

Automated Geocoding :
In automated geocoding, coordinates are extracted from a particular address or locality, such that the geographical address of a region is detected through the geocoding process, in this process of geocoding, taking reference to the given text instruction and converting it into a geographical coordinates

II   LITERARY WORK

In [1], the focus is at the variance in poses ,i.e., Global Approach and Component approach. The first approach has linear SVM for every machine in databases that help in distinguishing between all images of a single person. And in the latter approach, two level approach component-based detector is used. At first, facial components are classified independently, and then geometrical configuration performs face detection. Its results show that using facial components (eyes, nose and mouth) instead of whole face as input helps in face recognition process easily.
In [2], approach, it first extract vector of Gabor magnitude feature from given input image using a Gabor filters and then reduce it. This is used with PLDA and PGFC. After reduction, feature representation is derived from output of filter operation

into PCA probabilistic component analysis and LDA subspaces. PGFC provides better verification performance while PLDA is good in extraction process.

In [3], method reduces the storage requirement and provides important information. LBP, PCA and Gober Phase is used for feature extraction. DWT is used for preprocessing to extract important information from image. Daubechives wavelets are used to extract approximate coefficient that will reduce information to face recognition algorithm. This method results into reduction in amount of feature, storage capacity and computational problem. It is also fast and more accurate than other techniques.

In "Real Time vehicle tracking system using GSM and GPS technology- An Anti-theft Tracking System" method is based on GSM (Global system for mobile communication) and GPS (Global Positioning System). GSM is used to send longitudinal and latitudes position of vehicle from remote location. While GPS is a satellite-based radio-navigation system used to provide geolocation and time information to GPS server.

In [5], paper, the author has proposed a precise and more advanced technique for high precision selection of Landmark. Also, its results did not guarantee accuracy but able to enhance landmark location for probing. This method uses Landmark for examine target IP address, Round Trip Time (RTT) and traced hop count are measured for various landmark with distinct protocol and estimates the physical or geographical location of target. Latency distance is dependent on region and connectivity node in topology. To find location for landmark, DRAGON algorithm is used. Delay analysis is done to measure RTT, hop count and delay variance. Localization is done by literation and adapted data transformation.

Static image recognition system's different approaches are compared using Open CV and SVM. In [6], work, it is found that SVM have the best accuracy over LBPH, Eigenface, Fisher face. SVM is defined here as a method used to identify different patterns and resolve classification problem.

In [7], paper, GPS is defined as global navigation satellite system that helps in finding exact location, also GPRS(General Packet Radio Service) is uses as a medium between tracking device and server for data transferring on line connection between mobile device and central location. Contract between company and user for better security and monitoring fuel consumption, route guidance, speed limit, via connection GPS and GPRS with web-based application.

In [9], paper, the overall procedures of Face recognition from face detection to identification is defined. Along with its overall definition and working this also includes its application areas. This overall represents that how a face recognition system works.

This paper [10], has evaluated the privacy aspect of web browser using geolocation specification. Also, it recommends various ideas for the browser vendor and standard-setting bodies.

This paper [10], talks about various techniques and categories in geolocation. Localization techniques like Dedicated and Non-Dedicated techniques; Deterministic and probabilistic technique's algorithm. Triangulation, Trilateration for localization, offline and online phase for radio map. Various methods like NNSS, NNSS-AVG, APIT and Smallest Polygon for Radio map deterministic approach. Positioning method liked CID, RSS, Multipath, AOA, TOA, TDOA , OTDOA, U-TDOA, GPS, A-GPS, E-OTD, are explained. These all technique are in deep analysis for geolocation and hence provided a accurate and secure geolocation support.

This paper [11], discusses to use the geo-location technique as authentication purpose, also define location signature technique for providing security against spoofing. Geodetic method for continuous data transfers so that the connection cannot be hijacked. Various technology like, Cyberlocator, Remote

location-based authentication, local authentication , location-based authentication through multiple authentication technique are discussed. So, as it makes geo-location as accurate and secure way for remote authentication system.

This paper [12], focused on Location based authentication or geolocation-based authentication. It also proposes two new authentication techniques: STAT I (Space-Time Authentication Technique) and STAT II. These two techniques are considered good in comparison to triangulation in WLANs. STAT I uses GPS to inspect user's position and STAT II uses the existing infrastructure to provide space-time information.

This paper [13], discusses the various face recognition technique and determine the best of it. Various techniques compared in this paper are Eigenfaces, Fisher faces, Local Binary Patterns histogram. Of these techniques, LBPH is considered best of all, and thus an algorithm can use this method for better and accurate implementation of face recognition.

III   Conclusion

Face recognition with its best technique and Geo-location is a good approach for better and accurate Authentication and authorization of data. It became obvious to combine them both, i.e., Face recognition and geo-location (geo-locking) to prepare a strong algorithm to provide authentication and authorization at a single place. In this paper various aspects of face recognition technique and Geo-location are inspected. The papers also cover the summary of the procedure of face recognition. Geo-location is one of the major emerging technology and in future it would dominate the security field as of now also.

II.   REFERENCE

[1]   B. Heisele, P. Ho, and T. Poggio, "Face Recognition with Support Vector Machines: Global versus Component-Based Approach," 2001.

[2]   S. Dobrisek, V. Struc, J. Krizaj, and F. Mihelic, "Face recognition in the wild with the Probabilistic Gabor-Fisher Classifier," *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 2015.

[3]   S. Dalali and L. Suresh, "Daubechives Wavelet Based Face Recognition Using Modified LBP," *Procedia Computer Science*, vol. 93, pp. 344–350, 2016.

[4]   K. Maurya, M. Singh and N. Jain, " Real Time Vehicle Tracking System using GSM and GPS Technology – An Anti-theft Tracking System," *International Journal of Electronics and Computer Science Engineering, ,* 2012.

[5]   P. Hillmann, L. Stiemert, G. Dreo, and O. Rose, "On the Path to High Precise IP Geolocation: A Self-Optimizing Model," *International Journal of Intelligent Computing Research*, vol. 7, no. 1, 2016.

[6]   A. K. Singh, V. Bansal, "SVM Based Approach for Multiface Detection and Recognition in Static Images" *Journal of Image Processing and Artificial Intelligence,* vol. 5, Issue 2, pp . 1-11, 2018.

[7]   O. O. Alharaki, F. S. Alaieri, A.M. Zeki, " The integration of GPS Navigator Device with Vehicles Tracking System for Rental Car Firms", *International Journal of Computer Science and Information Security,* vol. 8, No. 6, September 2010.

[8]   W. L. Chao, " Face Recognition", *GICE, National Taiwan University.*

[9]   M. Caceres, "Privacy of Geolocation Implementations", *Opera Software ASA, Creative Commons Attributions-Share Alike 3.0 Unported License.*

[10]   A. Roxin, J. Gaber, M. Wack, and A. Nait-Sidi-Moh, "Survey of Wireless Geolocation Techniques," *2007 IEEE Globecom Workshops*, 2007.

[11]   B. Shivhare, G. Sharma, and S. P. S. Kushwah, "A Study on Geo-location Authentication Techniques," *2014 International Conference on Computational Intelligence and Communication Networks*, 2014.

[12]   D. Jaros and R. Kuchta, "New Location-Based Authentication Techniques in the Access Management," *2010 6th International Conference on Wireless and Mobile Communications*, 2010.

[13]   Sharmila, R. Sharma, D. Kumar, V. Puranik, and K. Gautham, "Performance Analysis of Human Face Recognition Techniques," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019.