GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

FINGERPRINT RECOGNITION SYSTEM

A Report for the Capstone Project 2

Submitted by

MUDIT RAJPUT

(1613101420 / 16SCSE101463)

in partial fulfillment for the award of the degree

of

Bachelor of Technology

IN

Computer Science and Engineering

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of

Dr. B. BALAMURUGAN

Professor

MAY- 2020

GALGOTIAS UNIVERSITY

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "FINGERPRINT RECOGNITION SYSTEM" is the bonafide work of "MUDIT RAJPUT" who carried out the project work under my supervision.

SIGNATURE of HEAD
Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
Professor & Dean,
School of Computing Science & Engineering

SIGNATURE of SUPERVISOR
Dr. B.BALAMURUGAN,
B.E(CSE).,M.E(CSE).,Ph.D(CSE)
Professor
School of Computing Science & Engineering

TABLE OF CONTENTS

1. Abstract

Fingerprints are considered to be the best and fastest method for biometric identification. They are secure to use, unique for every person and do not change in one's lifetime. Human fingerprints are rich in details called minutiae, which can be used as identification marks for security purposes. This paper is a study and implementation of a fingerprint recognition using image processing. The approach mainly involves extraction of minutiae points from sample fingerprint images and then performing matching based on the number of minutiae pairing among two fingerprints in question. For each task, some classical and up-to date methods in literatures are analyzed. Based on the analysis, an integrated solution for fingerprint recognition is developed for demonstration. It finally generates a percentage score which tells whether two fingerprints match or not.

Keywords: Biometric identification, Minutiae Extraction, Normalization, Preprocessing.

2. Introduction

Basically Skin of human fingertips consists of ridges and valleys and they mixing together form the distinctive patterns. At the time of pregnancy these distinctive patterns are fully developed and are permanent throughout the whole lifespan. Those patterns are called fingerprints. From different researches it has been observed that no two persons have the same fingerprints, so they are unique for each individual .because of the above mentioned characteristic, fingerprints are very popular for biometrics applications. Finger print matching is a very complex pattern recognition problem so Manual finger print matching is not only time taking but experts also takes long time for education and training. Fingerprints have remarkable permanency and uniqueness through out the time. From observations we conclude that the fingerprints offer more secure and reliable personal identification than passwords, id-cards or key can provide. Examples such as computers and mobile phones equipped with fingerprint sensing devices for fingerprint based password protection are being implemented to replace ordinary password protection methods.

What is Fingerprint?

A finger prints are the most important part of human finger. It is experienced from the research that all have their different finger prints and these finger prints are permanent for whole life. So fingerprints have been used for the forensic application and identification for a long time. Finger print image acquired by a Sensor A fingerprint is the composition of many ridges and furrows. Finger prints can‟t distinguished by their ridges and furrows. It can be distinguished by Minutia, which are some abnormal points on the ridges. Minutia is divided in to two parts such as: termination and bifurcation. Termination is also called ending and bifurcation is also called branch. Again minutia consists of ridges and furrows. valley is also referred as furrow.

Figure 1.1.1 Finger print image acquired by a Sensor

2.1 Overall description

Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection and their established use and collection by law enforcement and immigration. Digital image processing is a process of manipulating images in a digital computer. This processing can be achieved by development of a computer based algorithm in order to process these images. It is a technology widely used for digital image operations like feature extraction, pattern recognition, segmentation and morphology.

2.2 Purpose

The project mainly aims to come up with a solution to the fingerprint recognition problem by Sub Problems dividing it into sub-problems of classifications of some specific Action Units. The projects scope includes not only the two class problems which tell about whether an Action Unit is on or off, but also the multi-class problems that will inform the user about multi occurrences of more than one Action Unit at the same time. For this, different methodologies and techniques for feature extraction, normalization, selection and classification. Solutions to these problems as well as taking the computational complexity and timing issues into consideration. The project objective is to implement fingerprint recognition in an optimum way in terms of run time onto the embedded system. Various algorithms and methodologies are studied and hardware resources planning will be done to achieve the goal. This kind of fingerprint recognition embedded system can be widely used in our daily life in

different sectors. We hope that human life can be greatly helped with this technology. Some typical applications are listed as follows:-

- UIDAI (aadhar card in India)
- Banking (as Authentication)
- Attendance Marking

2.3 Motivation and Scope

High correct recognition rate (CRR), significant performance improvements in our system. Promising results are obtained under fingerprint registration errors, fast processing time. System is fully automatic and has the capability to work with images. It is able to recognize people who have already registered in the system. In security systems which can identify a person with minimum possibilities of errors or failures and with maximum accuracy.

3. Existing System

There are two Fingerprint Recognition System which are getting majorly used now a days:

1. **Correlation Based Matching:**

Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments.

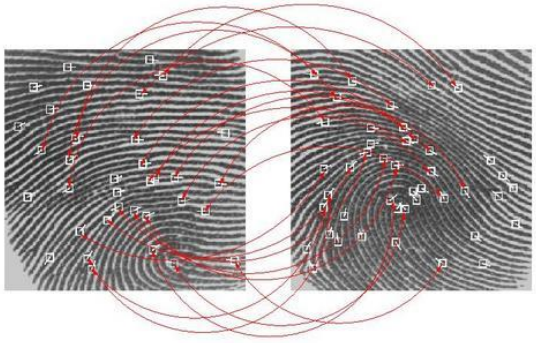


Fig. Correlation based matching

2. Minutiae Based Matching:

Minutiae points are the major features of a fingerprint image and are used in the matching of fingerprints. These minutiae points are used to determine the uniqueness of a fingerprint image. A good quality fingerprint image can have 25 to 80 minutiae depending on the fingerprint scanner resolution and the placement of finger on the sensor.

What is the definition of minutiae? Minutiae can be defined as the points where the ridge lines end or fork. So the minutiae points are the local ridge discontinuities and can be of many types. These types are –

- **Ridge ending** is the point where the ridge ends suddenly.
- **Ridge bifurcation** is the point where a single ridge branches out into two or more ridges.
- **Ridge dots** are very small ridges.
- **Ridge islands** are slightly longer than dots and occupy a middle space between two diverging ridges.
- **Ponds or Lakes** are the empty space between two diverging ridges.
- **Spurs** is a notch protruding from a ridge.
- **Bridges** are the small ridges that join two longer adjacent ridges.
- **Crossovers** are formed when two ridges cross each other.

Ridge endings and ridge bifurcations are the most commonly used minutia types since all other types of minutiae are based on a combination of these two types. Figure below shows some of the common minutiae patterns.

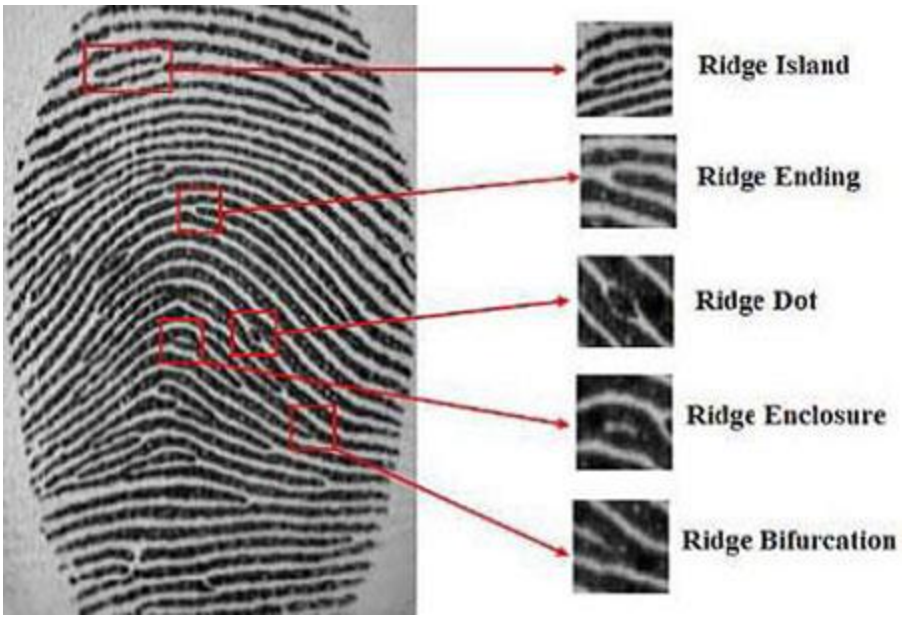


Photo: Some common minutiae patterns

Minutiae based fingerprint recognition:

It is the most widely used technique of fingerprint representation and its configuration is highly distinctive. It is more accurate compared to other correlation based systems and the template size is smaller in minutiae-based fingerprint representation. In this system, two fingerprints match if their minutiae points match. Minutiae based fingerprint technique is the backbone of most currently available fingerprint recognition products.

Compared to other fingerprint features, the minutia point features having corresponding orientation maps are distinct enough to distinguish between fingerprints robustly. Fingerprint representation using minutiae feature reduces the complex issue of fingerprint recognition to an issue of point pattern matching.

Since the original image cannot be reconstructed using only the minutiae information, the minutiae-based fingerprint identification systems can also assist privacy issues and the minutiae are actually sufficient enough to prove finger individuality. In terms of contrast, image resolution and global distortion the minutiae are more stable and robust in relation to other fingerprint matching schemes.

However, the primary challenge lies in extracting the minutiae from a poor quality image.
A good quality image is absolutely essential for minutiae extraction. However, sometimes the image quality might be poor due to various reasons and hence it becomes necessary to enhance the fingerprint images before minutiae matching of fingerprints.

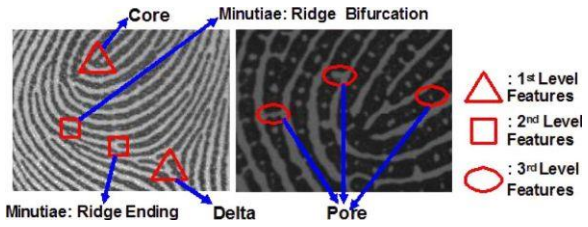


Fig. minutiae based matching

4. Proposed system

The system we are using is a *Pattern-based (or image-based) matching with minutiae extraction:*

Pattern based matching compares two fingerprints. This requires that the images be aligned in the same orientation. In order to do this, the Pattern-based finds a middle point in the fingerprint image. In the image-based matching, the template contains the size, type and pattern orientation within the fingerprint image. The person fingerprint image is compared with the template to recognize the degree. Which focuses on implementation of minutiae based matching technique.
These 7 steps we are using to get the system working properly:

Normalization & Segmentation

First the image is normalized to have 0 mean and 1 standard deviation. With a threshold of 0.1 and block size of 16x16, standard deviation is calculated of each non-overlapping block of the image, if the deviation is more than the threshold, the block is a part of the segmented mask. This is because, foreground tends to have larger variance than the background.

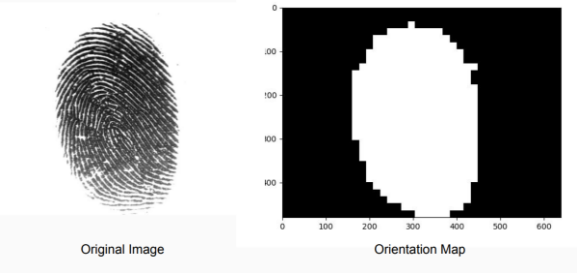


Fig. preprocessing at normalization level

Orientation Map

Fingerprint enhancement is done using a gabor filter followed by thresholding. The gabor filter requires local ridge orientation and local ridge frequency as arguments, hence before applying the filter, these two parameters have to be calculated.

Local ridge orientation formula:

$$O(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right).$$

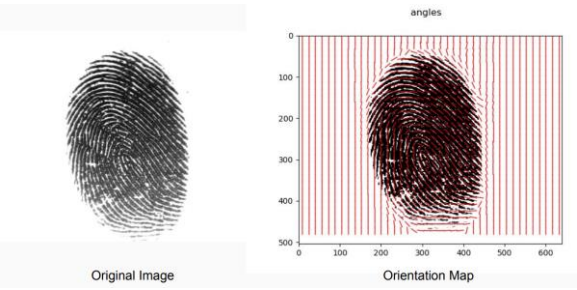


Fig. local ridge orientation

Frequency Map

The gray levels along ridges and valleys can be modeled as a sinusoidal-shaped wave along a direction normal to the local ridge orientation. For each block, a window of size 32x16 normal to the block was created. Elements along the orientation direction were summed and peaks were found. The frequency

of the block were 1/(average number of pixels between two peaks). This was followed by median filtering for better results.

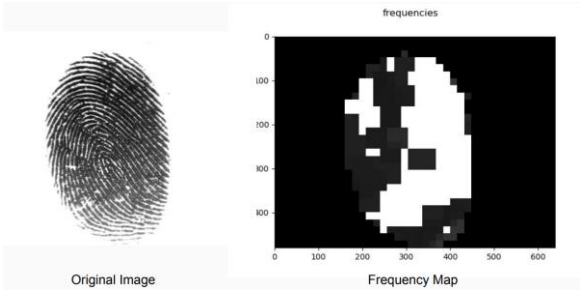


Fig. local ridge frequency

Gabor Filter & Binarization

Gabor filters have both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains. Currently we are using this code, to apply the gabor filters, which takes our calculated parameters and apply it to the image. Gabor Filter has the following formula:

$$h(x, y : \phi, f) = \exp\left\{-\frac{1}{2}\left[\frac{x_\phi^2}{\delta_x^2} + \frac{y_\phi^2}{\delta_y^2}\right]\right\} \cos\left(2\pi f x_\phi\right),$$

$$x_\phi = x \cos\phi + y \sin\phi,$$

$$y_\phi = -x \sin\phi + y \cos\phi,$$

Fig. Gabor filtering

Thinning

There are two steps in thinning:

Following conditions are checked in step 1 :

1. The pixel is black and has eight neighbours
2. 2 <= B(i,j) <= 6
3. A(i,j) = 1
4. At least one of the north, east, and south neighbors is white.
5. At least one of east, south, and west neighbors is white Thinning

The result of the above algorithm is the thinned image.

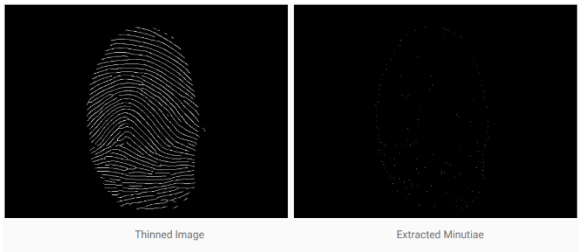
Fig. Thinned images

Minutiae Extraction

Minutiae extraction is done using the following technique: he CN (Crossing Number) is calculated for each pixel. Following is the definition of CN: CN =

$$CN = 0.5\sum_{i=1}^{8} |P_i - P_{i+1}|$$

CN = 1 means a ridge ending and CN = 3 means a ridge bifurcation. Both of which are minutiae points.



Removal of false minutiae points from other areas :

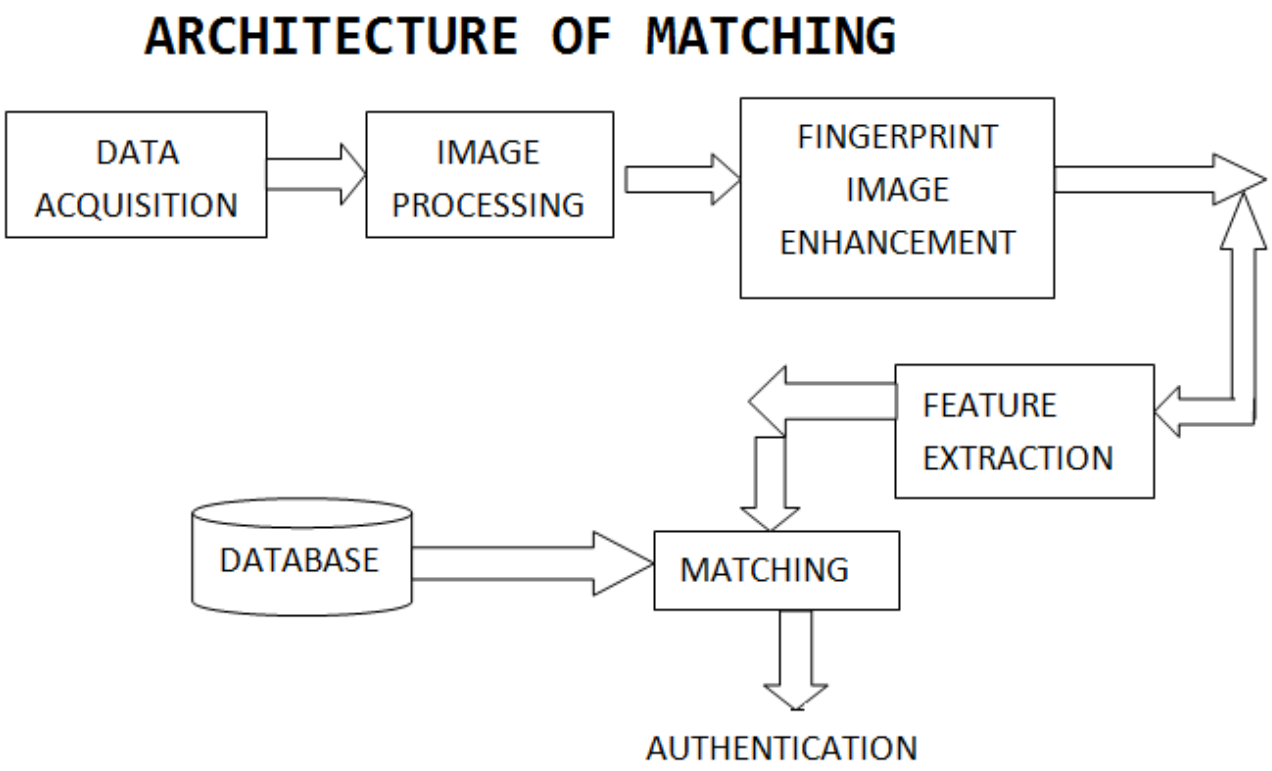
We loop through each pixel in the fingerprint image. If it is a minutiae point, we consider a grid of 17x17 around this point, if there is any other minutiae point in this grid we remove all minutiae points, otherwise we move to the next pixel. This removal is in order to avoid false minutiae due to ridge breaks.

Fig. image after minutiae extraction

Authentication

the algorithm computes pairwise similarity between minutiae of two fingerprints by comparing minutiae descriptors that are invariant to rotation and translation. Next, it aligns two fingerprints according to the most similar minutiae pair. The algorithm then establishes minutiae correspondence minutiae that are close enough both in location and direction are deemed to be corresponding (mated) minutiae. Finally, the algorithm computes a similarity score to reflect the degree of match between two fingerprints based on factors such as the number of matching minutiae, the percentage of matching minutiae in the overlapping area of two fingerprints, and the consistency of ridge count between matching minutiae. Which can be adjusted accordingly how much percentage of minutiae we require to authorize.

5. Implementation or architecture diagrams



Data Base models in the system:

There are only there models in the database of the project:

1. First Name: Text
2. Last Name: Text
3. Fingerprint Expression: Image

To implement the project we require these technologies:

1. Python: Python is the programming language or high level language which helps us in performing very big tasks by very short coding. And also is more secure which makes the language better to be used in the system. In this project python will perform all the backend tasks such as storing and retrieving data from the database and performing algebraic solutions.

2. SKimage: Skimage is a collection of algorithms for image processing and computer vision. The main package of this only provides a few utilities for converting between image data types.for most features, you need to import the subpackages.

3. OpenCV2: OpenCV (*Open Source Computer Vision Library*) is a library of programming functions mainly aimed at real-time computer vision. The library is cross-platform and free for use under the open-source BSD license. This will help us in faster preprocessing of the fingerprint scan.

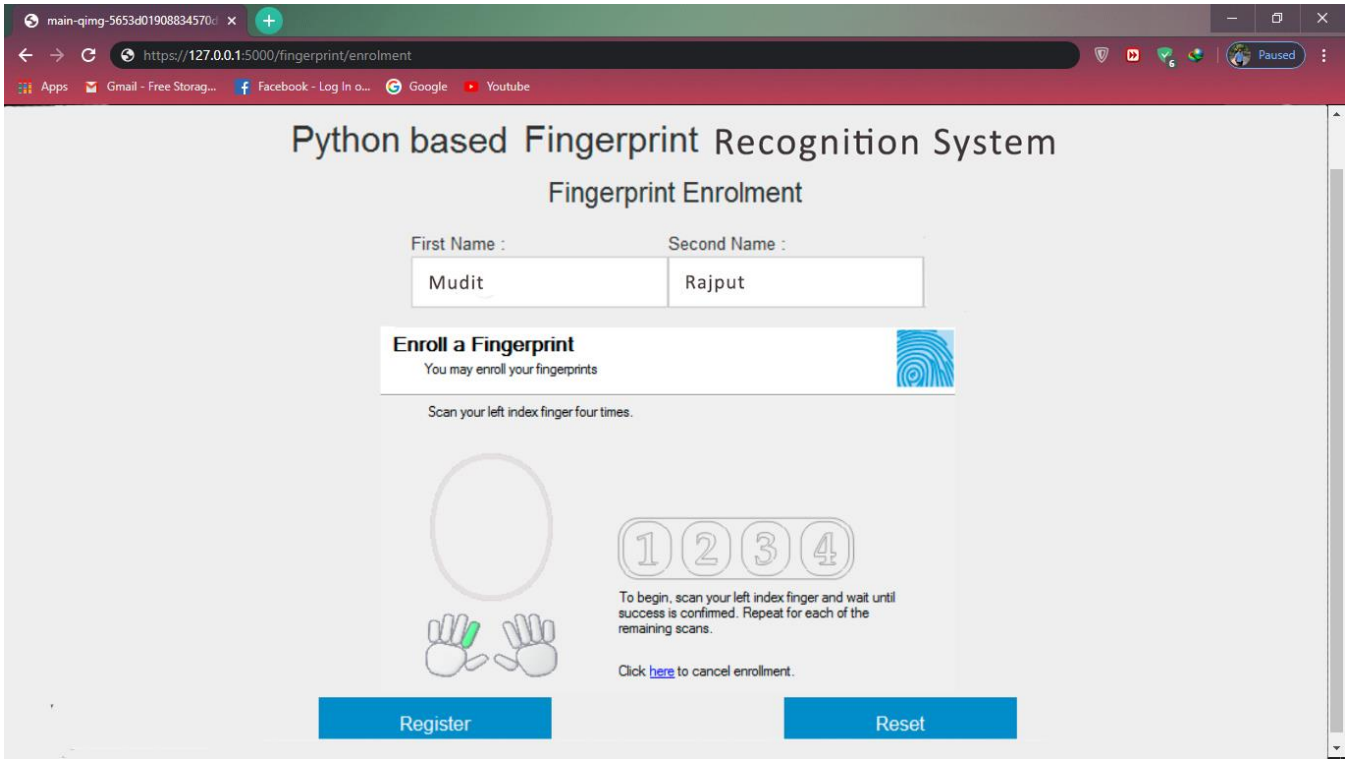
4. SQL Lite: SQL Lite is a platform which helps us in performing DBMS operations with less system consumption. It will store name and scan.

5. Google Chrome: It is a web browser which has not a major work in functioning. As it will represent the input or output in a structure which will make the output or input much interactive as compared to the terminal.

6. Output / Result / Screenshot

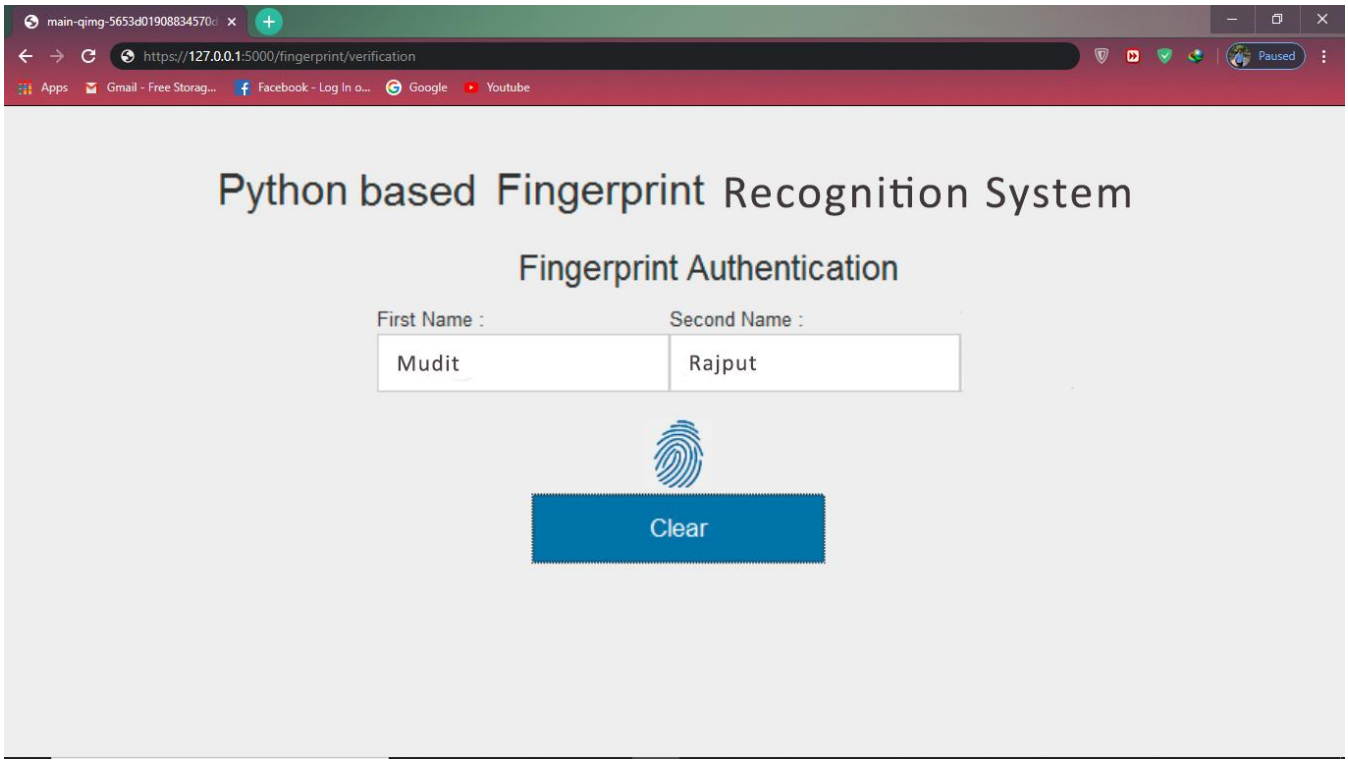
Here are some screenshots of the output screens:

1. New Fingerprint Enrollment:
   In the given snap the inputs are given to the system:
   First name: Mudit
   Last name: Rajput
   with Fingerprint scan of any finger

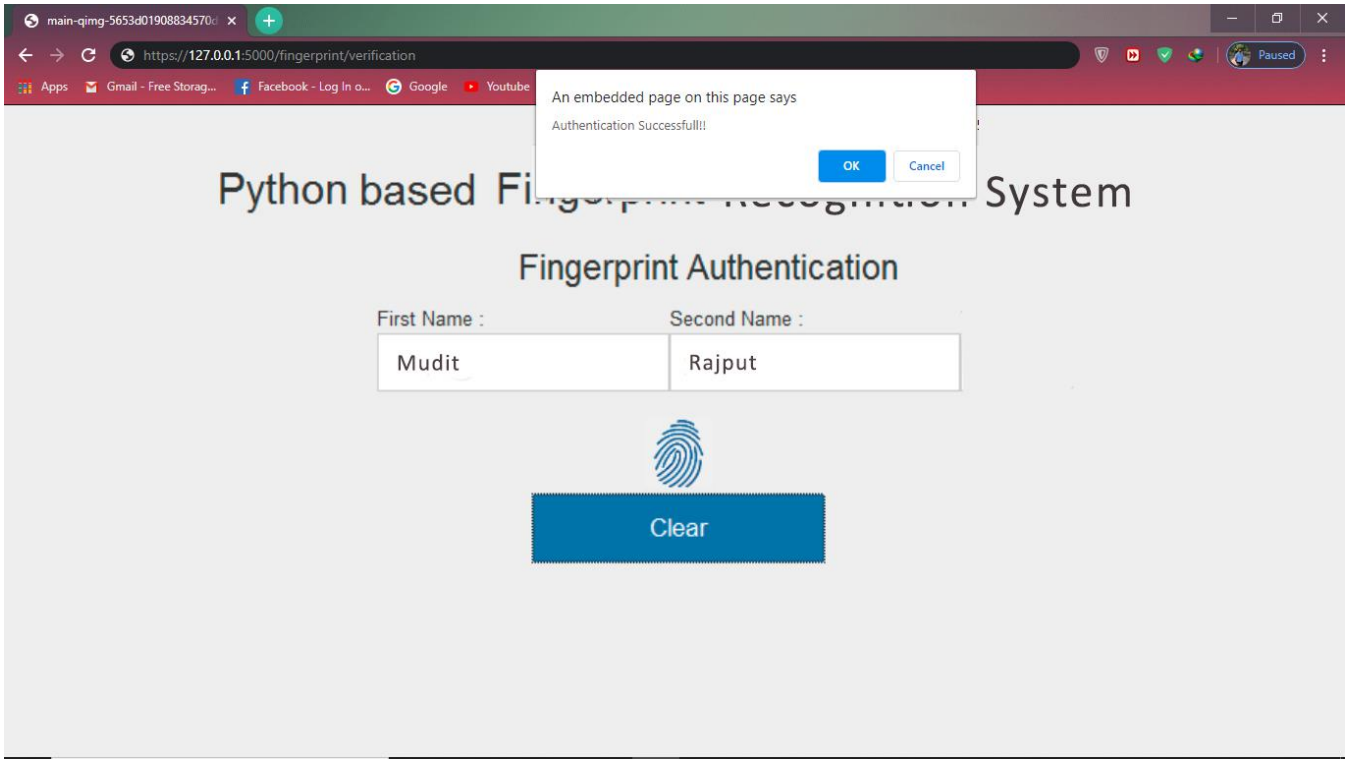


2. Verifcation of Registered Fingerprint:
    A. Successful Verification

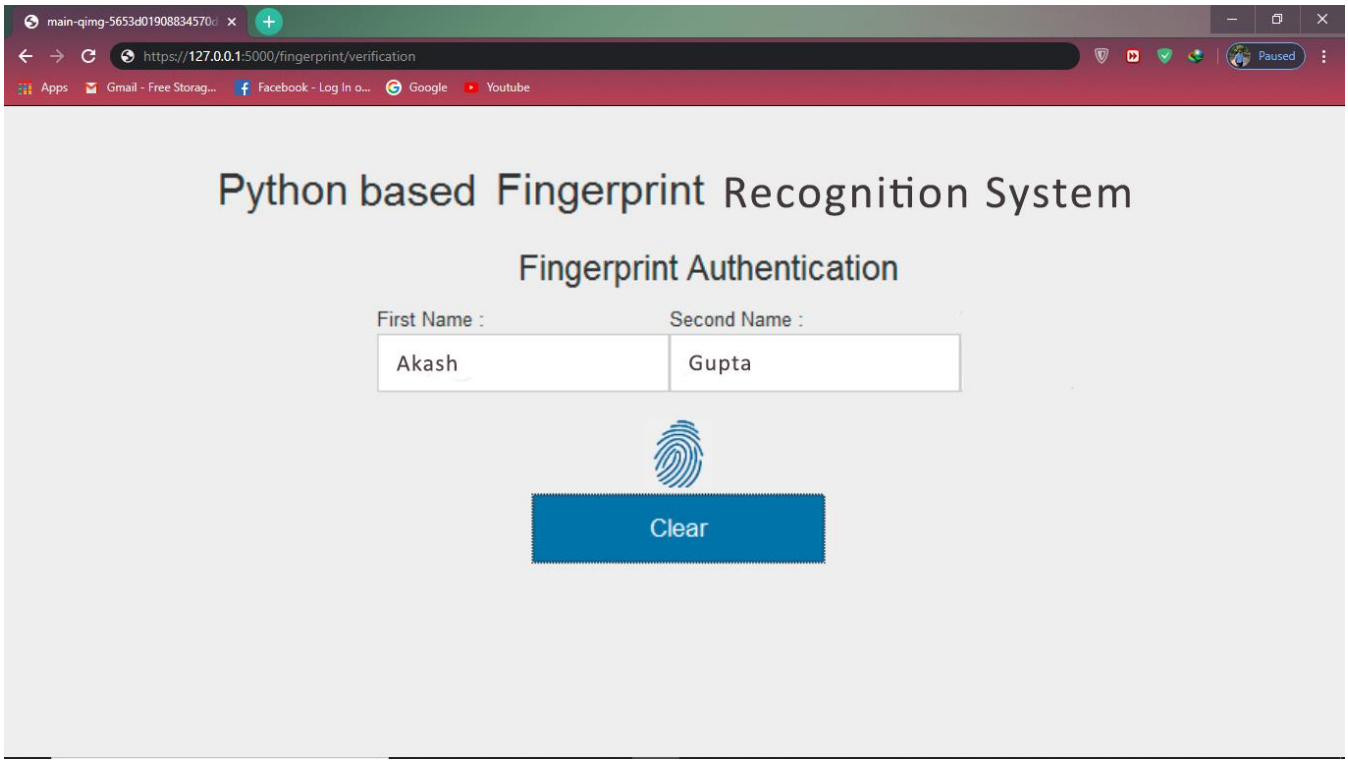
Here name and fingerprint is given as the input.



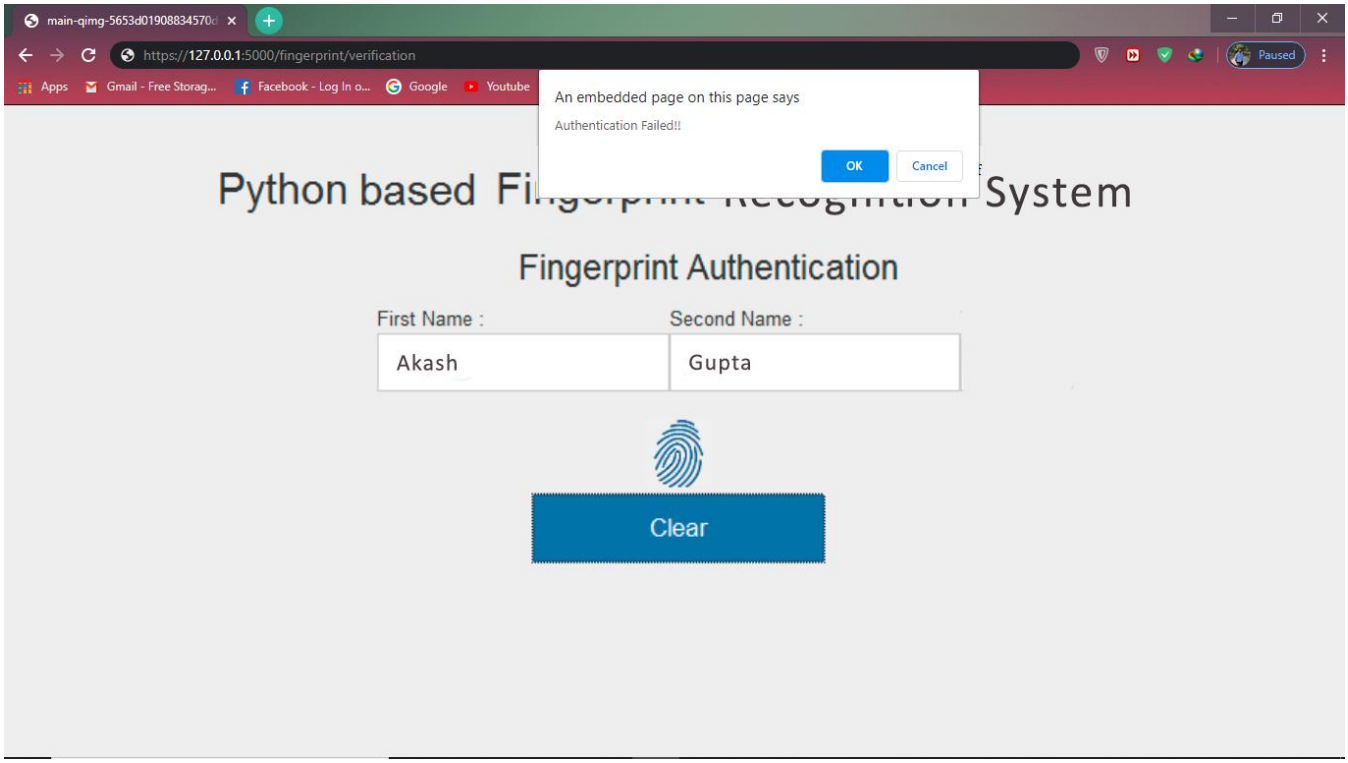
Result:



Failed Verification: Here name and fingerprint of unregistered member is given



Result:



7. Conclusion/Future Enhancement

Fingerprint Authentication has been studied for well over a century. However, Now a days due to cyber crimes and requirements to have more security due to the high confidentiality in data which can cause major effects on each and every individual. We need a better authentication service. and due to the uniqueness and individuality fingerprint recognition is one of the best way to get the work done. Now a days major countries like Ausralia, Canada, India and China etc. are using fingerprint recognition as the Unique identifaction of each and every person. So, a technology like Fingerprint Recognition should be used more. Due to lack of digital means such as cameras, high end processing units. Fingerprints are first capured then processed. But in future it is possible to make fingerprint recognition realtime by camera.

8. References

1. Amand, E., Anju, G., Simulink model Based Image Segmentation", Intellectual Journal of Advanced Research In Computer Science and Software Engineering, Vol. 2, issue 6. (2012).
2. Jain, A., Hong, L. and Boler, R., Online Fingerprint Verification, IEEE trans, PAMI-19, (4), pp. 302-314,
3. (1997).
4. Leung, W.F., Leung, S.H., Lau, W.H. and Luk, A, Fingerprint Recognition Using Neural Network, proc. of the IEEE workshop Neural Network for Signal Processing,(2000). pp. 226-235.
5. Lee, C.J., and Wang, S.D. Fingerprint feature extraction using Gabor filter, Electroni. Lett. 35, (4), (1999), pp.288-290.
6. Raymond, T. Fingerprint Image Enhancement and Minutiae Extraction,,Technical report, The University of Western Australi, (1991).
7. Tico, M., Kuosmanen, P. and Saarinen, J. Wavelet domain features for fingerprint recognition, Electroni.
8. Lett., 2001, 37, (1), (2001), pp.21-22.
9. Yang S. and Verbauwhede I. A Secure Fingerprint Matching Technique, Wanda Lee, Hong kong, (2003).
10. http://www.google.com