Report

on

Recent Advancement in Fingerprint Verification

Submitted in partial fulfillment of the
requirement for the award of the degree of

B. Tech CSE

Submitted By
Nisha Varshney 21SCSE1010583
Abhinav Choudhary(21SCSE1011615)

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA
INDIA

Abstract

Fingerprints scanners are security systems of biometrics. Everyone has patterns of frictions ridges on their fingers, and it is this pattern that is called fingerprint. Fingerprintsare uniquely detailed, durable over an individual's lifetime, and difficult to alter. Because there are countless combinations, fingerprints have become an ideal means of identification. They are used in police stations, security industries, Smartphone, and other mobile devices.

So, in our project we have two directories inside of the main directory and those contain images of fingerprints now the real directory contains images of actual fingerprint so we can see here always a number then a character representing a gender so the number is the id of the main character is gender and then the name of the fingerprint. For example - leftindex finger and all the files are real fingerprints without any modifications and then we also have the altered directory and inside of the altered directory we have three sub- directories, easy, medium, hard, then we have data sets then by using an external library opencv in which we take the altered image and then we will find the real fingerprints.

Introduction

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. Fingerprints have been used by police agencies since the late 18OOs, and fingerprint processing by computer has been commonplace since the 196Os. However, this use of fingerprints remains predominantly for police purposes. There is an expectation that a recent combination of factors will favor the use of fingerprints for the much larger market of personal authentication. These factors include: small and inexpensive fingerprint capture devices, fast and less expensive computing hardware, the explosive growth of network and Internet transactions, authentication rate and speed to meet the needs of many applications, and the heightened awareness of the need for ease-of-use as an essential component of reliable security.

This report provides an overview of progress in fingerprint verification. It is important to note right away that there are numerous methodologies and technologies used for fingerprint verification, many of which are private. Within the bounds of public knowledge, we cover what is most frequently known and used. While we make every effort to be objective, some items.

Literature Survey

Matching can be separated into two categories: verification and identification. Verification is the topic of this paper. It is the comparison of a claimant fingerprint against an enrollee's fingerprint, where the intention is that the claimant fingerprint matches the enrollees fingerprint. To prepare for verification, a person initially enrolls his or her fingerprint into the verification system. A representation of that fingerprint is stored in some compressed format along with the person's name or other identity. Subsequently, each access is authenticated by the person identifying him or herself, then applying the fingerprint to the system such that the identity can be verified. Verification is also termed, one-to-one matching. Identification is the traditional domain of criminal fingerprint matching. A fingerprint of unknown ownership is matched against a database of known fingerprints to associate a crime with an identity. Identification is also termed, one-to-many matching. There is an informal third type of matching that is termed one-to- few matching. This is for the practical application where a fingerprint system is used by'a few' users, such as by family members to enter their house. A number that constitutes 'few' is usually accepted to be somewhere between five and 20.

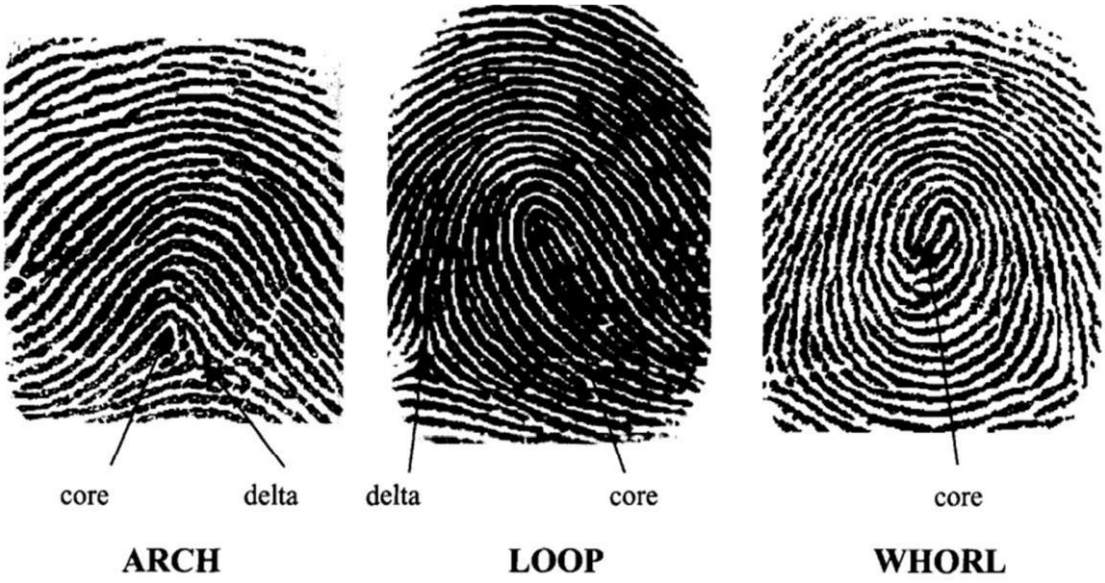
Feature Types

The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys. It is these ridges that are compared between one fingerprint and another when matching. Fingerprints are commonly matched by one (or both) of two approaches. We describe the fingerprint features as associated with these approaches. The more microscopic of the approaches is called minutia matching. The two minutia types that are shown in Figure are a ridge ending and bifurcation. An ending is a feature where a ridge terminates. A bifurcation is a feature where a ridge splits from a single path to two paths at a Y-junction. For matching purposes, a minutia is attributed with features. These are type, location (x, y), and direction (and many approaches use additional features). The more macroscopic approach to matching is called global pattern matching or simply pattern matching. In this approach, the flow of ridges is compared at all locations between a pair of fingerprint images. The ridge flow constitutes a global pattern of the fingerprint. Three fingerprint patterns are shown in (Different classification schemes can use up to 10 or so pattern classes, but these three are the basic patterns.)

ending bifurcation

Two other features are sometimes used in matching: core and delta. The core can be thought of as the center of the fingerprint pattern. The delta is a singular point from which three patterns deviate. The core and delta locations can be used as landmark locations by which to orientate two fingerprints for subsequent matching - though these

features are not present on all fingerprints. There may be other features of the fingerprint that are used in matching. For instance, pores can be resolved by some fingerprint sensors and there is a body of work (mainly research at this time) to use the position of the pores for matching in the same manner that the minutiae are used. Size of the fingerprint, and average ridge and valley widths can be used for matching, however, these are changeable over time. The positions of scars and creases can also be used, but are usually not because they can be temporary or artificially introduced.



Fingerprints Versus Other Biometrics

Table 1 shows a comparison among biometrics. Although the table does not capture all relative advantages and disadvantages, it does show that each modality has relative merits, especially for different applications. The specifications of the particular application will be the primary consideration in choosing a particular biometric modality. A few comments on entries in the table are sufficient. The row for the eye biometric describes attributes applying to either iris or retinal scanning technologies. Under the recognition column, all technologies will perform well under ideal conditions for that biometric. However, recognition rates suffer under less-than-ideal conditions. The fingerprint and eye have very good recognition rates; however, the fingerprint has more variability in image quality due to its tactile use versus the eye. Face recognition suffers when lighting cannot be controlled. Voice recognition works well with a properly designed microphone, but less well over the phone from an airport for instance. Inspecting the next two columns, whereas all technologies are appropriate for one-to-one matching, only fingerprint and eye technologies are proven to have low enough false

acceptance rates (at reasonable false rejection rates) to be practical for one-to-many matching. As far as sensor cost, eye systems are currently more costly than the others; voice systems can be zero cost to the user if the telephone is used. Fingerprint and voice systems have the smallest comparative sizes with eye systems currently largest.

Table - 1

	Recognition	Matching 1-to-1	Matching 1-to-many	Sensor Cost [SUS]	Size
fingerprint	very good	yes	yes	$10\text{-}10^2$	very small
eye	very good	yes	yes	$10^2\text{-}10^3$	large
hand	good	yes	no	10^2	medium
face	fair	yes	no	10^2	small
voice	variable	yes	no	$0\text{-}10^2$	very small
signature	variable	yes	no	10^2	small

- ## Existing Problem

Now a days a big number of security system uses fingerprint for authentication such as in fingerprint based atm withdrawals, Aadhar authorization, mobiles, laptops, etc. There are times when thefingerprints get fade or sometimes in an accident it gets damaged (suchas cut, wound, burn, etc.) and it becomes hard and sometimes impossible for the security system to recognize it.

- ## Proposed Solution

Our project will help matching the altered fingerprints which the normal fingerprint scanner is not able to do. So, in our project we have added two directories inside of the main directory that contain images of fingerprints. The real directory contains images of actual fingerprint. We also have the altered directory and inside the altered directory we have three sub-directories, easy, medium and hard, then by using an external library “opencv” in which we take the altered image and then we it will find the best fingerprint as output.

- ## Tools and Technology Used

In this project we are going to use python as main language. With the help of some prebuild libraries or python such as cv2 which is opencv inpython and os which help us to fetch directory (folder/file location) to get its contents in our code.

OpenCV: OpenCV is a Python open-source library, which is used for computer vision in Artificial intelligence, Machine Learning, face recognition, etc. In OpenCV, the CV is an abbreviation form of a computer vision, which is defined as a field of study that helps computers to understand the content of the digital images such as photographs and videos. So, import it using the import cv2 statement before using its functions.

- The OS module in Python provides functions for creating and removing a directory (folder), fetching its contents, changing and identifying the current directory, etc. first we need to import the os module to interact with the underlying operating system. So, import it using the import os statement before using its functions.

● Results and Output

After we have successfully built the project, we would be able to find the best match for a damaged fingerprint. After giving the input the system will run tests on the sample and will search for the best match form its database and give us the output.

● Conclusion and Future Scope

With the help of this project, we are going to solve fingerprint recognition problem. It will be helpful for Police investigation when the fingerprint found on the crime scene is not complete. It will run test on the incomplete portion of the fingerprint and find the criminal.