Finger Print Recognition System

CONTENTS

1. ABSTRACT

This document is limited to the description of the personal identification project "FINGERPRINT RECOGNITION SYSTEM", a security facility provided to the users which supports decision to make on the access rights to the authorized users by authentication. This project extrapolates the necessary fingerprint data verification and enrollment and requires the users to make decisions taking high quality image, more responsibility, and accountability and making comparisons on the ridge patterns of the fingerprints of the users. This project is based on the fact that each person has a unique pattern of the fingerprint that differentiates him from others.

Fingerprint recognition is a biometric technique for personal identification. The personal identification techniques are popularly used in the scientific, industrial, medical and forensic applications. Biometrics based fingerprint recognition provides one of the promising solutions for the security of the software and the domain of applying this techniques for security is increasing day by day.

Biometric features also include speech, handwriting, face identification etc. Face identification is one of the popular techniques for personal identification, but may fail in certain situations where two people look very similar. For example, in case of identical twins it may be very difficult to differentiate them. Even the speech and handwriting recognition systems may fail in certain situations, because there are experts who can modulate their speech or copy the handwriting in such a way that it is difficult to differentiate it from the original. Fingerprints' being complex patterns has the advantage of being a passive, noninvasive system for personal identification and its success depends on solving the two problems:

- Representation of the complex patterns of the fingerprints and
- Matching these fingerprint patterns.

This project uses both, algebraic and geometric features to representation fingerprint images. Here we divide both the existing finger print in the database and the scanned finger print into frames and compare the pixel values of the same and the user is authenticated based on the percentage of values being compared. The constraints of the percentage of fingerprint being matched can me modified as needed and hence the authentication can be made as strict as possible based on the criticality of its application.

This project is best suited for Law Enforcement Agency, Forensic application, Security of the software and the management applications.

2. INTRODUCTION

BASIC CONCEPTS

BIOMETRIC SYSTEMS

A biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioral characteristic possessed by that person. An important issue in designing a practical biometric system is to determine how an individual is recognized. Depending on the application context, a biometric system may be called either a *verification* system or an *identification* system:

- A verification system authenticates a person's identity by comparing the captured biometric characteristic with her own biometric template(s) pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true. A verification system either rejects or accepts the submitted claim of identity (*Am I whom I claim I am?*);
- An identification system recognizes an individual by searching the entire template databasefor a match. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (*Who am I?*).

The term *authentication* is also frequently used in the biometric field, sometimes as a synonym for verification; actually, in the information technology language, authenticating a user means

to let the system know the user identity regardless of the mode (verification or identification). The enrollment module is responsible for registering individuals in the biometric system database (system DB). During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristic. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the raw digital representation is usually further processed by a feature extractor to generate a compact but expressive representation, called a *template*. Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a *magnetic card* or *smartcard* issued to the individual. The verification task is responsible for verifying individuals at the point of access. During the operation phase, the user's name or PIN (Personal Identification Number) is entered through a keyboard (or a keypad); the biometric reader captures the characteristic of the individual to be recognized and converts it to a digital format, which is further processed by the feature extractor to produce a compact digital representation. The resulting representation is fed to the feature matcher, which compares it against the template of a single user (retrieved from the system DB based on the user's PIN). In the identification task, no PIN is provided and the system compares the representation of the input biometric against the templates of all the users in the system database; the output is either the identity of an enrolled user or an alert message such as "user not identified." Because identification in large databases is computationally expensive, classification and indexing techniques are often deployed to limit the number of templates that have to be matched against the input. A

biometric system could operate either as an *online* system or an *off-line* system. An on-line system requires the recognition to be performed quickly and an immediate response is imposed (e.g., a computer network logon application). On the other hand, an off-line system usually does not require the recognition to be performed immediately and a relatively long response delay is allowed (e.g., an employee background check application. An application could operate either in a *positive* or a *negative* recognition mode:

- In a positive recognition application, the system establishes whether the person is who he (implicitly or explicitly) claims to be. The purpose of a positive recognition is to prevent multiple people from using the same identity. For example, if only Alice is authorized to enter a certain secure area, then the system will grant access only to Alice. If the system fails to match the enrolled template of Alice with the input, a rejection results; otherwise, an acceptance results;
- In a negative recognition application, the system establishes whether the person is who he (implicitly or explicitly) denies being. The purpose of negative recognition is to prevent a single person from using multiple identities. For example, if Alice has already received welfare benefits and now she claims that she is Becky and would like to receive the welfare benefits of Becky (this is called "double dipping"), the system will establish that Becky is not who she claims to be. If the system fails to match the input biometric of Becky with a database of people who have already received benefits, an acceptance results; otherwise, a rejection results.

A biometric system can be classified according to a number of other application-dependent characteristics. Wayman suggests

that all the biometric applications may be classified into categories based on their characteristics:

1. cooperative versus non-cooperative,
2. overt versus covert,
3. habituated versus non-habituated,
4. attended versus non-attended,
5. standard versus non-standard operating environment,
6. public versus private, and
7. open versus closed.

Cooperative versus non-cooperative dichotomy refers to the behavior of the impostor in interacting with the system. Electronic banking is an example of a cooperative application whereas an airport application to identify terrorists who will try to break the system is an example of a non-cooperative application.

If a user is aware that he is being subjected to a biometric recognition, the application is categorized as overt. If the user is unaware, the application is covert. Facial recognition can be used in a covert application while fingerprint recognition cannot be used in this mode (except for criminal identification based on latent fingerprints)

Habituated versus non-habituated use of a biometric system refers to how often the enrolled

users are subjected to biometric recognition. For example, a computer network logon application typically has habituated users (after an initial “habituation” period) due to their use of the system on a regular basis. However, a driver’s license application typically has nonhabituated users since a driver’s license is renewed only once in several years.

Attended versus non-attended classification refers to whether the process of biometric data acquisition in an application is observed,

guided, or supervised by a human (e.g., a security officer). Furthermore, an application may have an attended enrollment but non-attended recognition. For example, a banking application may have a supervised enrollment when an ATM card is issued to a user but the subsequent uses of the biometric system for ATM transactions will be non-attended.

Non-cooperative applications generally require attended operation. Standard versus non-standard environments refer to whether the system is being operated in a controlled environment (such as temperature, pressure, moisture, lighting conditions, etc.).

Public or private dichotomy refers to whether the users of the system are customers or employees of the organization deploying the biometric system. For example, a network logon application is used by the employees and managed by the information technology manager of the same company. Thus it is a private application. The use of biometric data in conjunction with electronic identity cards is an example of a public application.

Closed versus open systems refers to whether a person's biometric template is used for a

single or multiple applications

Note that the most popular commercial applications have the following attributes: cooperative,

Overt, habituated, attended enrollment and non-attended recognition, standard environment, closed, and private.

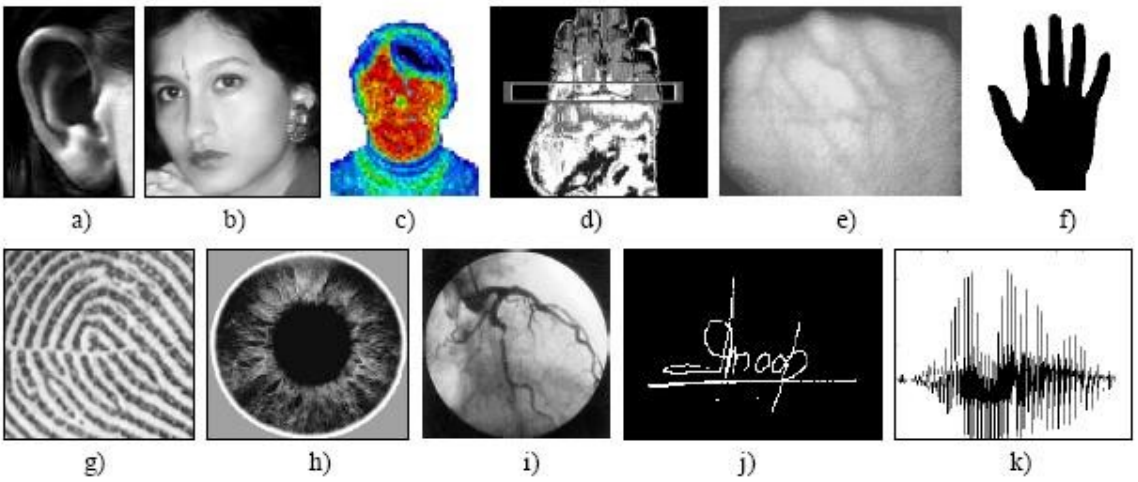
COMPARISON OF VARIOUS BIOMETRICS

Any human physiological and/or behavioral characteristic can be used as a biometric identifier to recognize a person as long as it satisfies these requirements:

- ***universality*****,** which means that each person should have the biometric;
- ***distinctiveness*****,** which indicates that any two persons should be sufficiently different in terms of their biometric identifiers;
- ***permanence*****,** which means that the biometric should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- ***collect ability*****,** which indicates that the biometric can be measured quantitatively. However, in a practical biometric system, there are a number of other issues that should be considered, including:
- ***performance*****,** which refers to the achievable recognition accuracy, speed, robustness, the resource requirements to achieve the desired recognition accuracy and speed, as well as operational or environmental factors that affect the recognition accuracy and speed;
- ***acceptability*****,** which indicates the extent to which people are willing to accept a particular biometric identifier in their daily lives;

- ***circumvention,*** which reflects how easy it is to fool the system by fraudulent methods. A practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, harmless to the users, accepted by the intended population, and sufficiently robust to various fraudulent methods.

A number of biometric identifiers as shown in the figure below are in use in various applications. Each biometric has its strengths and weaknesses and the choice typically depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. The match between a biometric and an application is determined depending upon the characteristics of the application and the properties of the biometric.



Some of the biometrics are shown: a) ear, b) face, c) facial thermo gram, d) hand thermo gram, e) hand vein, f) hand geometry, g) fingerprint, h) iris, i) retina, j) signature, and k) voice.

When choosing a biometric for an application the following issues have to be addressed:

- Does the application need verification or identification? If an application requires an identification of a subject from a large database, it needs a scalable and relatively more distinctive biometric (e.g., fingerprint, iris, or DNA).
- What are the operational modes of the application? For example, whether the application is attended (semi-automatic) or unattended (fully automatic), whether the users are habituated (or willing to be habituated) to the given biometrics, whether the application is covert or overt, whether subjects are cooperative or non-cooperative, and so on.
- What is the storage requirement of the application? For example, an application that performs the recognition at a remote server may require a small template size.
- How stringent are the performance requirements? For example, an application that demands very high accuracy needs a more distinctive biometric.
- What types of biometrics are acceptable to the users? Different biometrics are acceptable in applications deployed in different demographics depending on the cultural, ethical, social, religious, and hygienic standards of that society. The acceptability of a biometric in an application is often a compromise between the sensitivity of a community to various perceptions/taboos and the value/convenience offered by biometrics- based recognition.

A brief introduction to the most common biometrics is provided below.

- ***Ear*:** It is known that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The features of an ear are not expected to be unique to an individual. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear.
- ***Face*:** The face is one of the most acceptable biometrics because it is one of the most common methods of recognition that humans use in their visual interactions. In addition, the method of acquiring face images is nonintrusive. Facial disguise is of concern in unattended recognition applications. It is very challenging to develop face recognition techniques that can tolerate the effects of aging, facial expressions, slight variations in the imaging environment, and variations in the pose of the face with respect to the camera (2D and 3D rotations).
- ***Facial, hand, and hand vein infrared thermograms*:** The pattern of heat radiated by the human body is a characteristic of each individual body and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition and could distinguish between identical twins. A thermogram-based system is non-contact and non-invasive but sensing challenges in uncontrolled environments, where heat-emanating surfaces in the vicinity of the body, such as, room heaters and vehicle exhaust pipes, may drastically affect the image acquisition phase. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infrared sensors are prohibitively expensive which a factor inhibiting widespread use of the thermograms.

- ***Hand and finger geometry*:** Some features related to a human hand (e.g., length of fingers) are relatively invariant and peculiar (although not very distinctive) to an individual. The image acquisition system requires cooperation of the subject and captures frontal and side view images of the palm flatly placed on a panel with outstretched fingers. The representational requirements of the hand are very small (nine bytes in one of the commercially available products), which is an attractive feature for bandwidth- and memory-limited systems. Due to its limited distinctiveness, hand geometry-based systems are typically used for verification and do not scale well for identification applications. Finger geometry systems (which measure the geometry of only one or two fingers) may be preferred because of their compact size.
- ***Iris*:** Visual texture of the human iris is determined by the chaotic morphogenetic processes during embryonic development and is posited to be distinctive for each person and each eye. An iris image is typically captured using a non-contact imaging process. Capturing an iris image involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera. The iris recognition technology is believed to be extremely accurate and fast.
- ***Retinal scan*:** The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image capture requires a person to peep into an eyepiece and focus on a specific spot in the visual field so that a predetermined part of

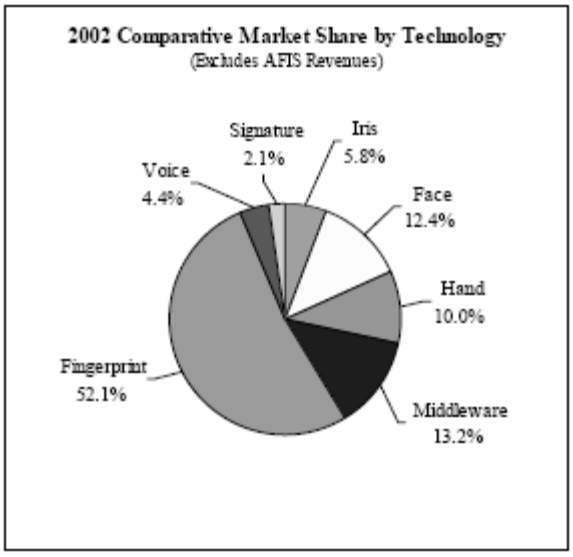
the retinal vasculature may be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect public acceptability of retinal biometrics. Retinal vasculature can reveal some medical conditions (e.g., hypertension), which is another factor standing in the way of public acceptance of retinal scan-based biometrics.

- ***Signature*:** The way a person signs his name is known to be a characteristic of that individual. Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary a lot: even successive impressions of their signature are significantly different. Furthermore, professional forgers can reproduce signatures to fool the unskilled eye.
- ***Voice*:** Voice capture is unobtrusive and voice print is an acceptable biometric in almost all societies. Voice may be the only feasible biometric in applications requiring person recognition over a telephone. Voice is not expected to be sufficiently distinctive to permit identification of an individual from a large database of identities. Moreover, a voice signal available for recognition is typically degraded in quality by the microphone, communication channel, and digitizer characteristics. Voice is also affected by a person's health (e.g., cold), stress, emotions, and so on. Besides, some people seem to be extraordinarily skilled in mimicking others.

These various biometric identifiers described above are compared in Table below. **Note that fingerprint recognition has a very good balance of all the desirable properties.** Every human being possesses fingerprints with the exception of any hand-related disabilities. Fingerprints are very distinctive fingerprint details are permanent, even if they may temporarily change slightly due to cuts and bruises on the skin or weather conditions. Live-scan fingerprint sensors can easily capture high-quality images and they do not suffer from the problem of segmentation of the fingerprint from the background (e.g., unlike face recognition). However, they are not suitable for covert applications (e.g., surveillance) as live-scan fingerprint scanners cannot capture a fingerprint image from a distance without the knowledge of the person. The deployed fingerprint-based biometric systems offer good performance and fingerprint sensors have become quite small and affordable because fingerprints have a long history of use in forensic divisions worldwide for criminal investigations, they have a stigma of criminality associated with them. However, this is changing with the high demand of automatic recognition to fight identity fraud in our electronically interconnected society. With a marriage of fingerprint recognition, cryptographic techniques, and vitality detection, fingerprint systems are becoming quite difficult to circumvent. Fingerprint recognition is one of the most mature biometric technologies and is suitable for a large number of recognition applications. This is also reflected in revenues generated by various biometric technologies in the year 2002.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table comparing various biometric technologies
High, Medium, and Low are denoted by H, M, and L, respectively



Biometric Market Report (International Biometric Group) estimated the revenue of various biometrics in the year 2002 and showed that fingerprint-based biometric systems continue to be the

leading biometric technology in terms of market share, commanding more than 50% of non-AFIS biometric revenue. Face recognition was second with 12.4%. Note that AFIS are used in forensic applications.

PROJECT DESCRIPTION

In each and every organization security plays an important role. All employees working in the organization are allowed entrance only when they satisfy the security requirements. The security guards at the main entrance check the identity of the person with the help of his ID card. A record is maintained where the person has to enter the details of the time he is walking in, his name, ID, designation, department etc. and when he walks out he has to enter his out time.

This process is time consuming and not foolproof. The employees as well as the visitors have to spend so much time and effort at the entrance to enter in the records and satisfy the security requirements. We can as well utilize this time and effort in something productive.

To provide a solution to this problem we took up the job of automating the security check and providing the security guard with a personal computer to crosscheck with the employee details. Now an employee or visitor can gain entrance when their ID is scanned and the fingerprint of the employee is matched with the database maintained with the security. First the employee ID is retrieved from the ID card and then the employee record is opened and the fingerprint is matched electronically, if there is a match the other

details are matched and if we are successful in identifying the person the person gains entrance.
The whole process is fast and accurate.

Fingerprint basically uses a uses a fingerprint's minutiae – the ridges, bifurcations, islands and other traits. The fingerprint is collected by the software, then processed and threshold the image and simplifying the features using standard image processing techniques.

Hence the main criterion for checking whether the employee belongs to the organization is done by crosschecking the ID and mainly the fingerprint of the employee with the database of employee records. In the process we are making the task of the security personnel easy and fast and guaranteeing that only authenticated employees and visitors gain entrance and the safety of the organization is maintained.

FINGERPRINT CLASSIFICATION AND INDEXING

Large volumes of fingerprints are collected and stored every day in a wide range of applications, including forensics, access control, and driver's license registration. Automatic identification based on fingerprints requires the input fingerprint to be matched with a large number of fingerprints stored in a database (e.g., the FBI database contains more than 200 million fingerprint cards). To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner such that the input fingerprint needs to be matched only with a subset of the fingerprints in the database. Fingerprint classification is a technique used to assign a fingerprint to one of the several pre-specified types

already established. Fingerprint classification can be viewed as a coarse-level matching of the fingerprints. An input fingerprint is first matched to one of the pre-specified types and then it is compared to a subset of the database corresponding to that fingerprint type. For example, if the fingerprint database is binned into five classes, and a fingerprint classifier outputs two classes (primary and secondary) with extremely high accuracy, then the identification system will only need to search two of the five bins, thus decreasing (in principle) the search space 2.5-fold. Unfortunately, only a limited number of major fingerprint categories have been identified (e.g., five), the distribution of fingerprints into these categories is not uniform, and there are many "ambiguous" fingerprints (see figure below), whose exclusive membership cannot be reliably stated even by human experts. In fact, the definition of each fingerprint category is both complex and vague. A human inspector needs a long period of experience to reach a satisfactory level of performance in fingerprint classification. About 17% of the 4000 images in the NIST Special Database 4 (Watson and Wilson, 1992) have two different ground truth labels. This means that even human experts could not agree on the true class of the fingerprint for about 17% of the fingerprint images in this database. Therefore, in practice, fingerprint classification is not immune to errors and does not offer much selectivity for fingerprint searching in large databases.

Examples of fingerprints that are difficult to classify; a) tented arch; b) a loop; c) a Whorl; it seems that all the fingerprints shown here should be in the loop category.

To overcome this problem, some authors have proposed methods based on "continuous classification" or on other indexing techniques. In continuous classification, fingerprints are not partitioned into non-overlapping classes, but each fingerprint is characterized with a numerical vector summarizing its main features. The continuous features obtained are used for indexing fingerprints through spatial data structures and for retrieving fingerprints by means of spatial queries, rule-based approaches, syntactic approaches, structural approaches, statistical approaches, neural networks, and multiple classifiers. A separate section introduces the "standard" notation used to compute classification performance and compares existing methods on NIST Special Database 4 (Watson and Wilson, 1992) and NIST Special Database 14 (Watson, 1993) which are the most commonly used benchmarks for fingerprint classification studies

EXISTING AND PROPOSED SYSTEM

In each and every organization security plays an important role. All employees working in the organization are allowed entrance only when they satisfy the security requirements. The security guards at the main entrance check the identity of the person with the help of his ID card. A record is maintained where the person has to enter the details of the time he is walking in, his name, ID, designation, department etc. and when he walks out he has to enter his out time.

This process is time consuming and not foolproof. The employees as well as the visitors have to spend so much time and effort at the entrance to enter in the records and satisfy the security requirements. We can as well utilize this time and effort in something productive.

To provide a solution to this problem we took up the job of automating the security check and providing the security guard with a personal computer to crosscheck with the employee details. Now an employee or visitor can gain entrance when their ID is scanned and the fingerprint of the employee is matched with the database maintained with the security. First the employee ID is retrieved from the ID card and then the employee record is opened and the fingerprint is matched electronically, if there is a match the other details are matched and if we are successful in identifying the person the person gains entrance.

The whole process is fast and accurate.

Fingerprint basically uses a uses a fingerprint's minutiae – the ridges, bifurcations, islands and other traits. The fingerprint is collected by the software, then processed and threshold the image and simplifying the features using standard image processing techniques. Hence the main criterion for checking whether the employee belongs to the organization is done by crosschecking the ID and mainly the fingerprint of the employee with the database of employee records. In the process we are making the task of the security personnel easy and fast and guaranteeing that only authenticated employees and visitors gain entrance and the safety of the organization is maintained.

3. DESIGN PRINCIPLES & EXPLANATION

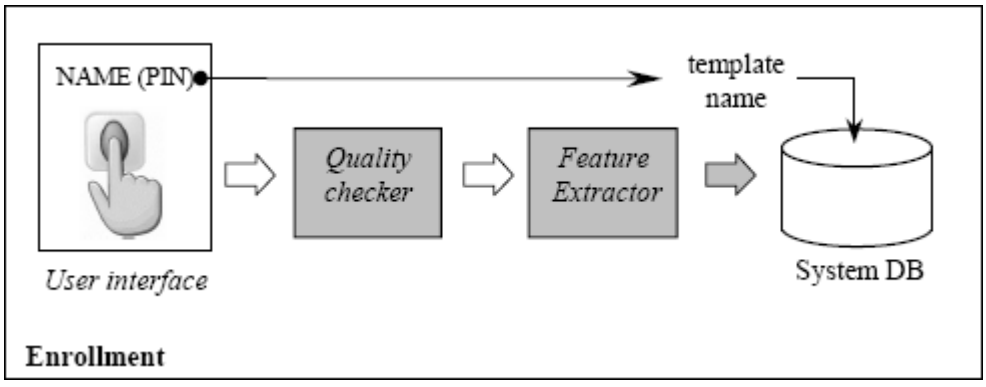
3.1. MODULES

- **FINGERPRINT SENSING AND STORAGE**
- **FINGERPRINT REPRESENTATION AND FEATURE EXTRACTION**
- **FINGERPRINT MATCHING AND AUTHENTICATION**

3.2. MODULE DESCRIPTIOIN

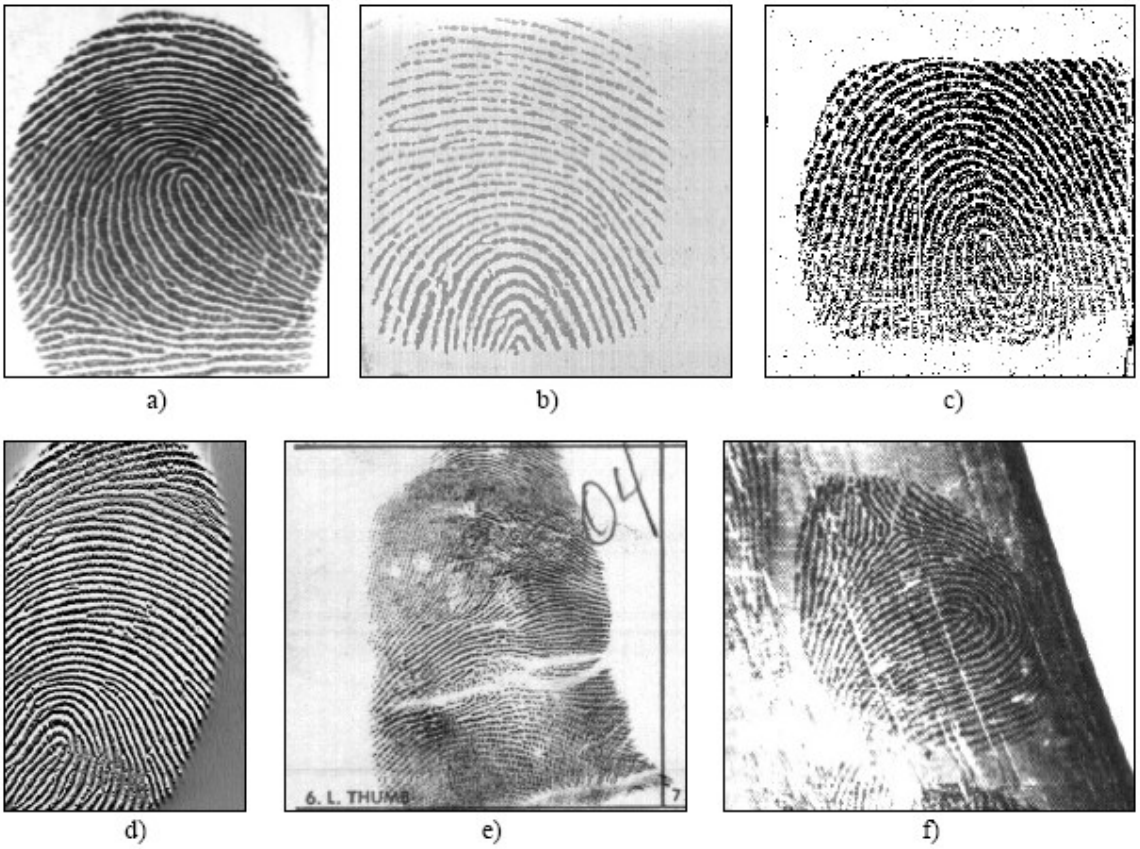
FINGERPRINT SENSING AND STORAGE

Based on the mode of acquisition, a fingerprint image may be classified as off-line or live scan. An off-line image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on paper. The inked impression is then digitized by scanning the paper using an optical scanner or a high-quality video camera. A live-scan image, on the other hand, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact. Special kind of off-line images, extremely important in forensic applications, are the so-called *latent* fingerprints found at crime scenes. The oily nature of the skin results in the impression of a fingerprint being deposited on a surface that is touched by a finger. These latent prints can be "lifted" from the surface by employing certain chemical techniques.



The main parameters characterizing a digital fingerprint image are: resolution, area, number of pixels, geometric accuracy, contrast, and geometric distortion. To maximize compatibility between digital fingerprint images and to ensure good quality of the acquired fingerprint impressions, the US Criminal Justice Information Services (the largest division within the FBI) released a set of specifications that regulate the quality and the format of both fingerprint images and FBI-compliant off-line/live-scan scanners. Most of the commercial live-scan devices, designed for the non-AFIS market, do not meet FBI specifications but, on the other hand, are usually more user friendly, compact, and significantly cheaper.

Storing raw fingerprint images may be problematic for large AFISs. In 1995, the size of the FBI fingerprint card archive contained over 200 million items, and archive size was increasing at the rate of 30,000 to 50,000 new cards per day. Although the digitization of fingerprint cards seemed to be the most obvious choice, the resulting digital archive could become extremely large. In fact, each fingerprint card, when digitized at 500 dpi requires about 10 Mbytes of storage. A simple multiplication by 200 million yields the massive storage requirement of 2000 terabytes for the entire archive. The need for an effective compression technique was then very urgent. Unfortunately, neither the well-known lossless methods nor the JPEG methods were found to be satisfactory. A new compression technique (with small acceptable loss), called Wavelet Scalar Quantization (WSQ), became the FBI standard for the compression of 500 dpi fingerprint images. Besides WSQ, a number of other compression techniques.



Fingerprint images from: a) a live-scan FTIR-based optical scanner; b) a live-scan capacitive scanner; c) a live-scan piezoelectric scanner; d) a live-scan thermal scanner; e) an off-line inked impression; f) a latent fingerprint.

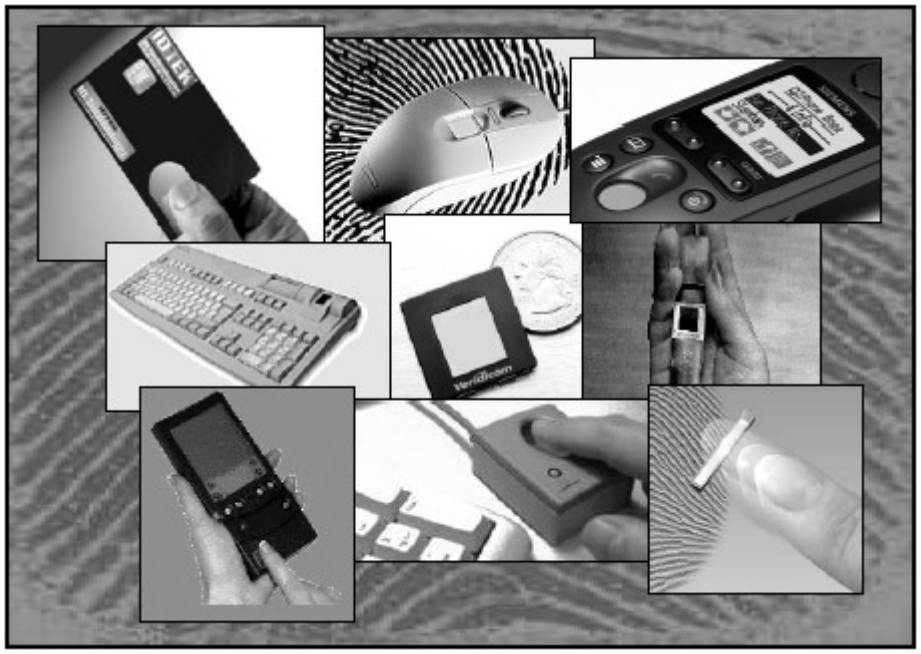
There are a number of live-scan sensing mechanisms (e.g., optical FTIR, capacitive, thermal,

pressure-based, ultrasound, etc.) That can be used to detect the ridges and valleys present in the fingertip. Figure below shows an off-line fingerprint image acquired with the ink technique, a latent fingerprint image, and some live-scan images acquired with different types of commercial live-scan devices.

Although optical scanners have the longest history, the new solid-state sensors are gaining great popularity because of their compact size and the ease of embedding them into laptop computers, cellular phones, smart pens, and the like. shows some examples of fingerprint sensors embedded in a variety of computer peripherals and other devices. Discussed below are some fingerprint sensing technologies, provides some indications about the characteristics of commercially available scanners and shows images acquired with a number of devices in different operating.

FINGERPRINT REPRESENTATION AND FEATURE EXTRACTION

The representation issue constitutes the essence of fingerprint recognition system design and has far-reaching implications for the design of the rest of the system. The pixel intensity values in the fingerprint image are typically not invariant over the time of capture and there is aneed to determine salient features of the input fingerprint image that can discriminate between identities as well as remain invariant for a given individual. Thus the problem of representation is to determine a measurement (feature) space in which the fingerprint images belonging to the same finger form a compact cluster and those belonging to different fingers occupy different portions of the space (low *intra-class* variation and high *inter-class* variations).



Fingerprint sensors can be embedded in a variety of devices for user recognition purposes.

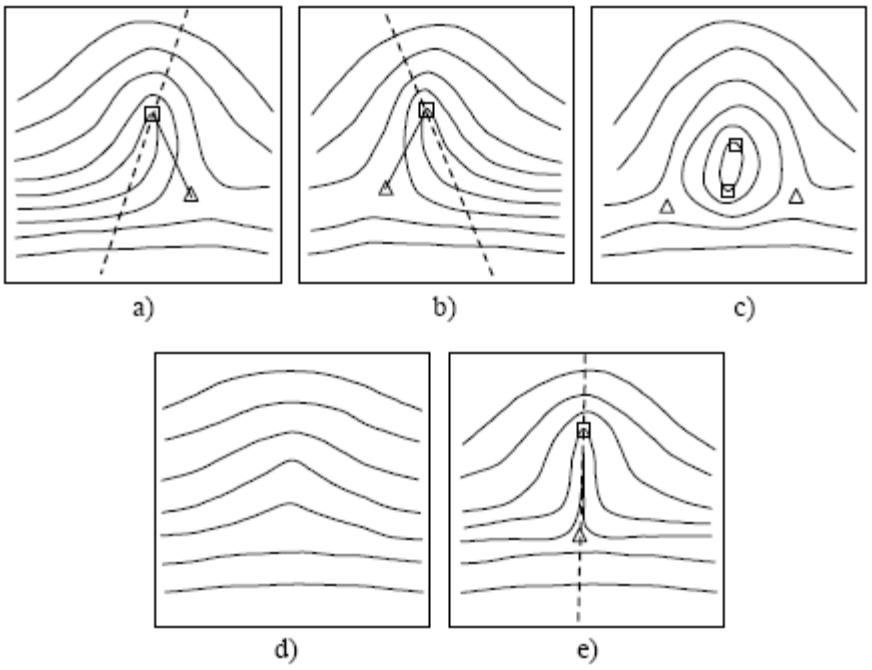
A good fingerprint representation should have the following two properties: *saliency* and *suitability*. Saliency means that a representation should contain distinctive information about the fingerprint. Suitability means that the representation can be easily extracted, stored in a compact fashion, and be useful for matching. Saliency and suitability properties are not generally correlated. A salient representation is not necessarily a suitable representation. In addition, in some biometrics applications, storage space is at a premium. For example, in a smartcard application, typically about 2 Kbytes of storage are available. In such situations, the representation also needs to be parsimonious.

Image-based representations, constituted by raw pixel intensity information, are prevalent among the recognition systems using optical matching and correlation-based matching. However, the utility of the systems using such representation schemes may be limited due

to factors such as brightness variations, image quality variations, scars, and large global distortions present in the fingerprint image. Furthermore, an image-based representation requires a considerable amount of storage. On the other hand, an image-based representation preserves the maximum amount of information, makes fewer assumptions about the application domain, and therefore has the potential to be robust to wider varieties of fingerprint images. For instance, it is extremely difficult to extract robust features from a (degenerate) finger devoid of any ridge structure.

The fingerprint pattern, when analyzed at different scales, exhibits different types of features.

- . At the global level, the ridge line flow delineates a pattern similar to one of those shown in Figure. *Singular points*, called loop and delta (denoted as squares and triangles, respectively in Figure below), are a sort of control points around which the ridge lines are “wrapped”. Singular points and coarse ridge line shape are very important for fingerprint classification and indexing, but their distinctiveness is not sufficient for accurate matching. External fingerprint shape, orientation image, and frequency image also belong to the set of features that can be detected at the global level.

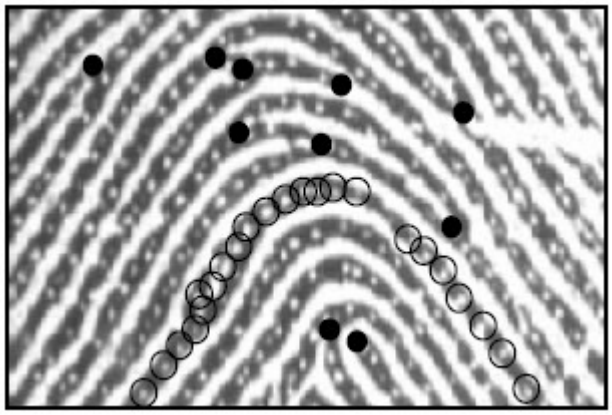


Fingerprint patterns as they appear at a coarse level: a) left loop; b) right loop; c) whorl; d) arch; and e) tented arch; squares denote loop-type singular points, and triangles delta type singular points.

- . At the local level, a total of 150 different local ridge characteristics, called *minute details*, have been identified. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics, called *minutiae* (see Figure below), are: *ridge termination* and *ridge bifurcation*. A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges. Minutiae in fingerprints are generally stable and robust to fingerprint impression conditions. Although a minutiae-based representation is characterized by a high saliency, a reliable automatic minutiae extraction can be

problematic in low-quality fingerprints (hence the suitability of this kind of representation is not optimal).

- At the very-fine level, intra-ridge details can be detected. These are essentially the finger *sweat pores* (see Figure below) whose position and shape are considered highly distinctive. However, extracting pores is feasible only in high-resolution fingerprint images (e.g., 1000 dpi) of good quality and therefore this kind of representation is not practical for most applications.

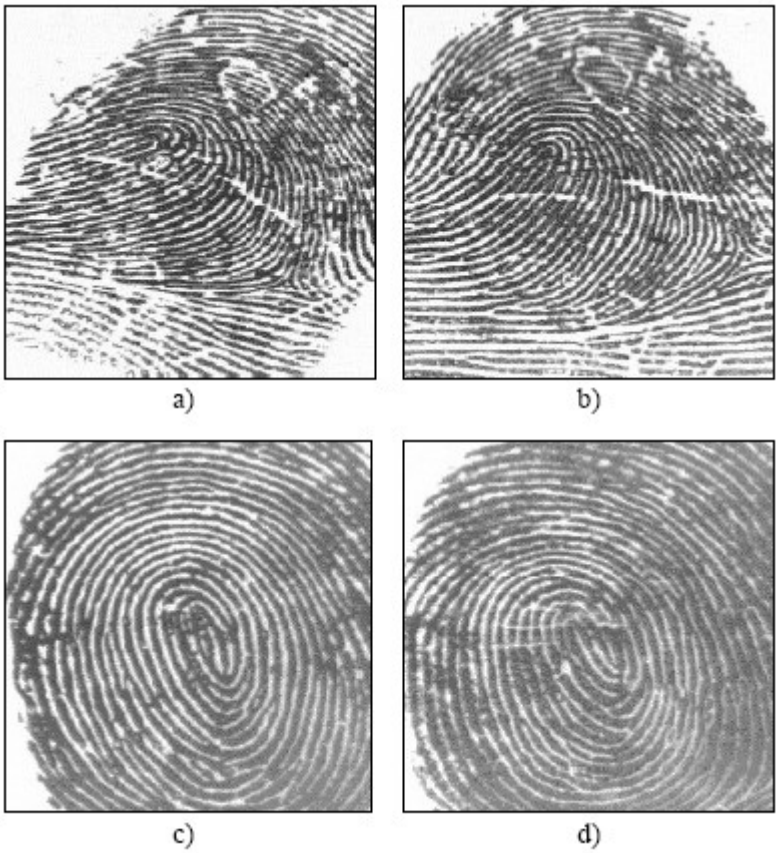


Minutiae (black-filled circles) in a portion of fingerprint image; sweat pores (empty circles) on a single ridge line.

The article below describes fingerprint anatomy and introduces the techniques available for processing fingerprint images and extracting salient features. Specific sections are dedicated to the definition and description of approaches for computing local ridge orientation, local ridge frequency, singular points, and minutiae. Particular emphasis is placed on fingerprint segmentation (i.e., isolation of fingerprint area from the background), fingerprint image enhancement, and binarization, which are very important intermediate steps in the extraction of salient features.

FINGERPRINT MATCHING AND AUTHENTICATION

Reliably matching fingerprint images is an extremely difficult problem, mainly due to the large variability in different impressions of the same finger (i.e., large intra-class variations). The main factors responsible for the intra-class variations are: displacement, rotation, partial overlap, non-linear distortion, variable pressure, changing skin condition, noise, and feature extraction errors. Therefore, fingerprints from the same finger may sometimes look quite different whereas fingerprints from different fingers may appear quite similar (see Figure 1.14).



Difficulty in fingerprint matching: Fingerprint images in a) and b) look different to an untrained eye but they are impressions of the same finger. Fingerprint images in c) and d) look similar to an untrained eye but they are from different fingers. Human fingerprint examiners, in order to claim that two fingerprints are from the same finger, evaluate several factors: I) global pattern configuration agreement, which means that two fingerprints must be of the same type, ii) qualitative concordance, which requires that the corresponding minute details must be identical, iii) quantitative factor, which specifies that at least a certain number (a minimum of 12 according to the forensic guidelines in the United States) of corresponding minute details must be found, and iv) corresponding minute details, which must be identically inter-related. In practice, complex protocols have been defined for fingerprint matching and a

detailed flowchart is available to guide fingerprint examiners in manually performing fingerprint matching. Given below is a figure showing the general method by which fingerprints are matched.

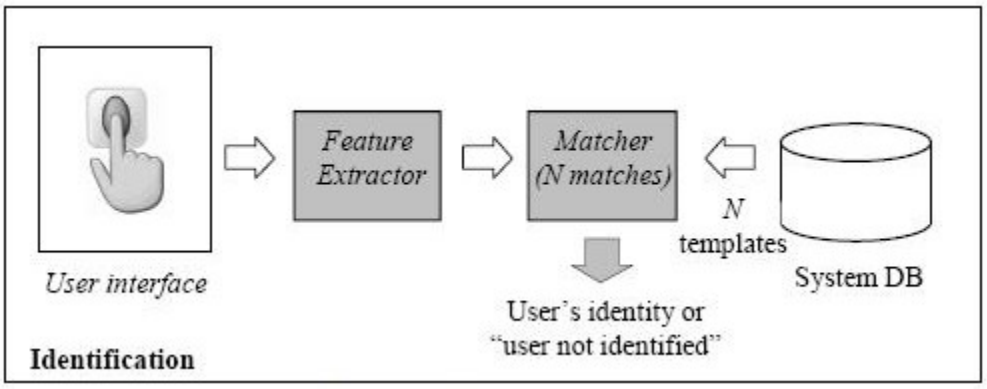
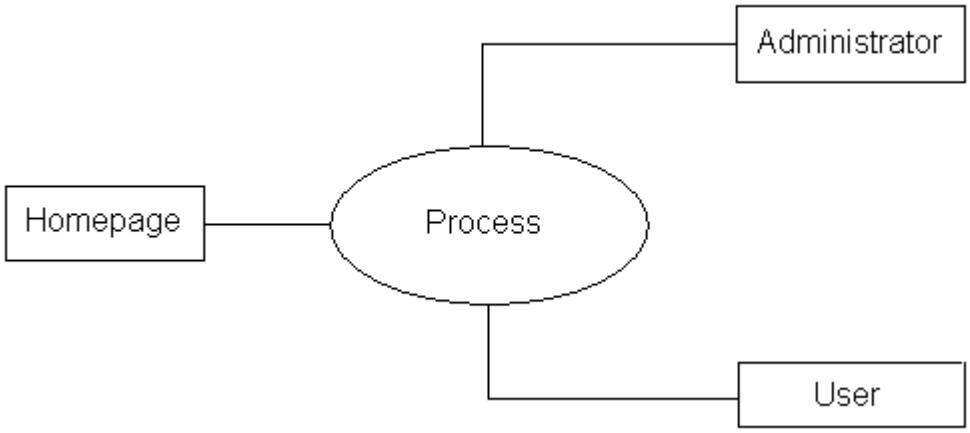


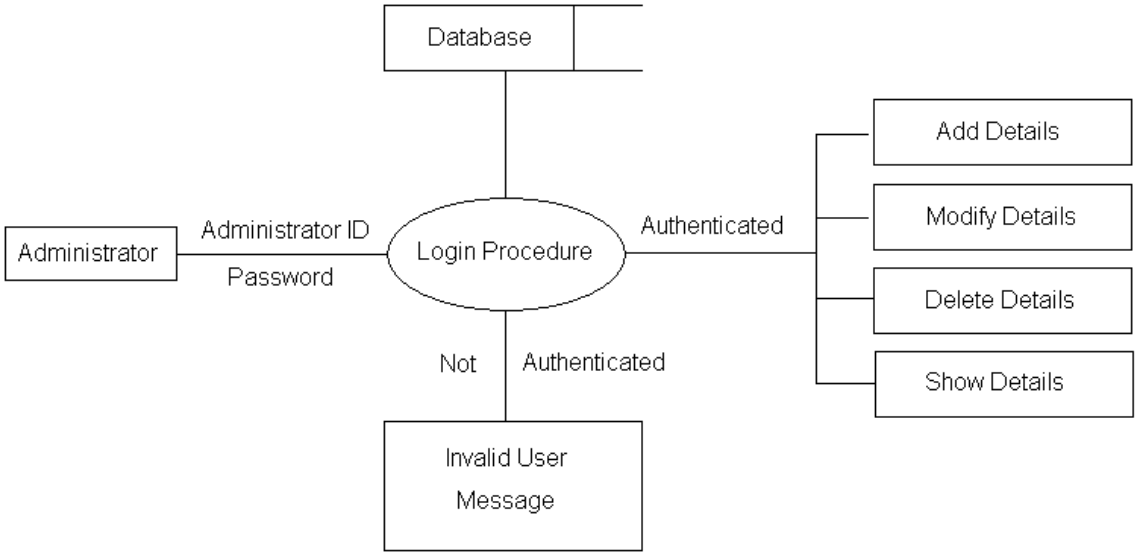
Figure showing a general method as to how the finger print is matched and compared with an existing fingerprint from the database.

4. PROJECT DICTIONARY

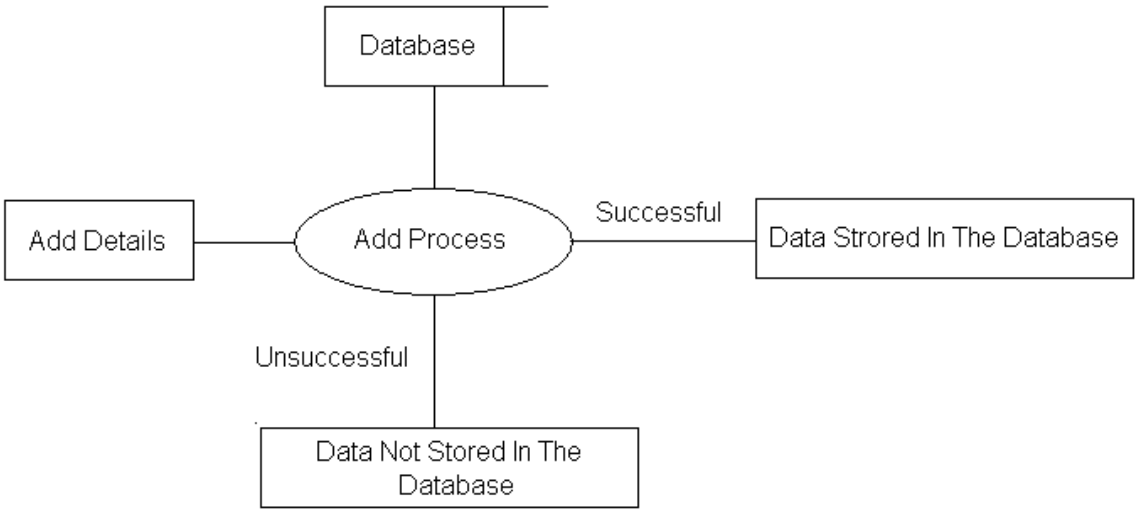
4.1. DATAFLOW DIAGRAMS



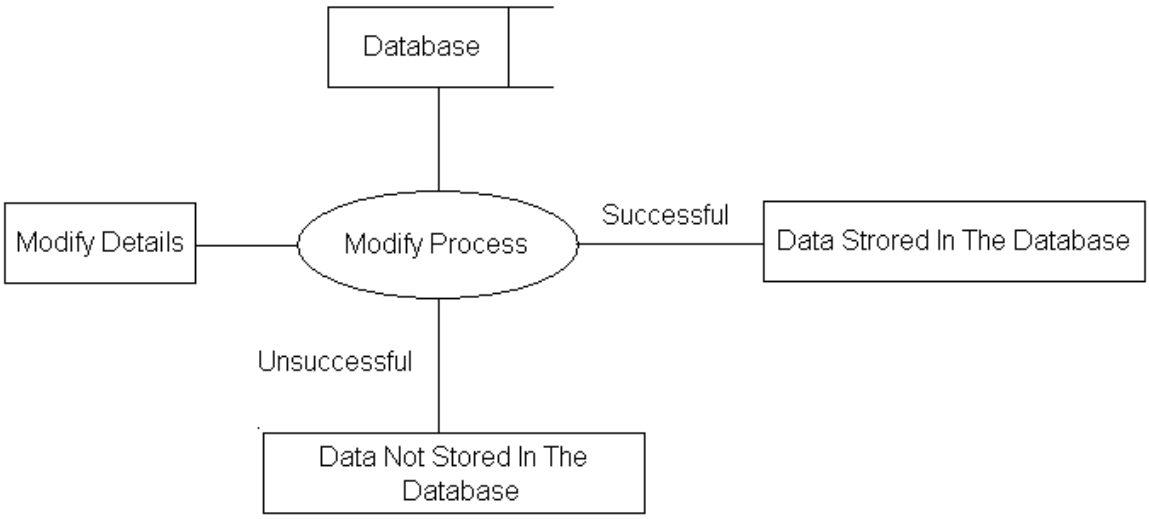
DFD SHOWING THE FLOW OF DATA IN THE HOMEPAGE



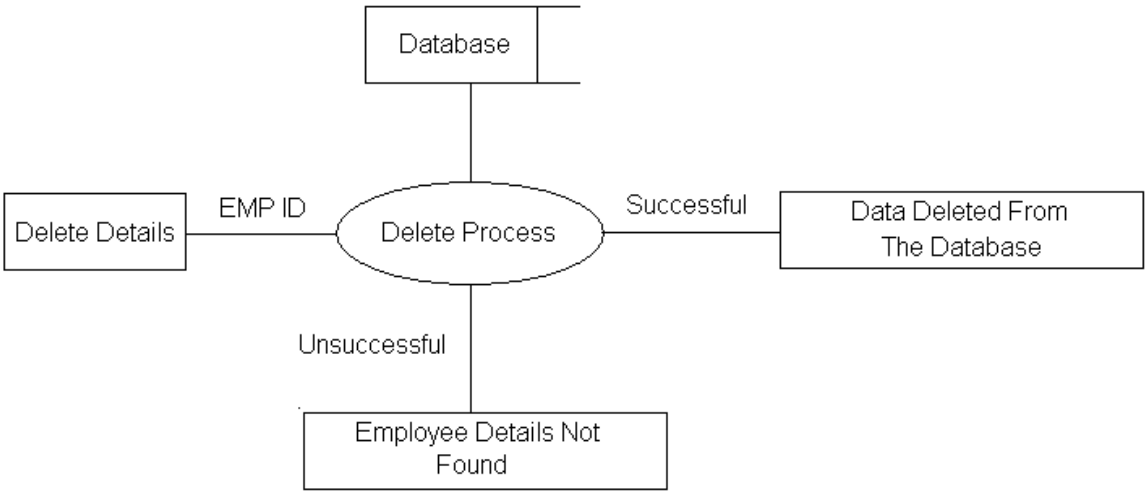
DFD TO SHOW THE FLOW OF DATE IN THE ADMINISTRATIVE SCREEN



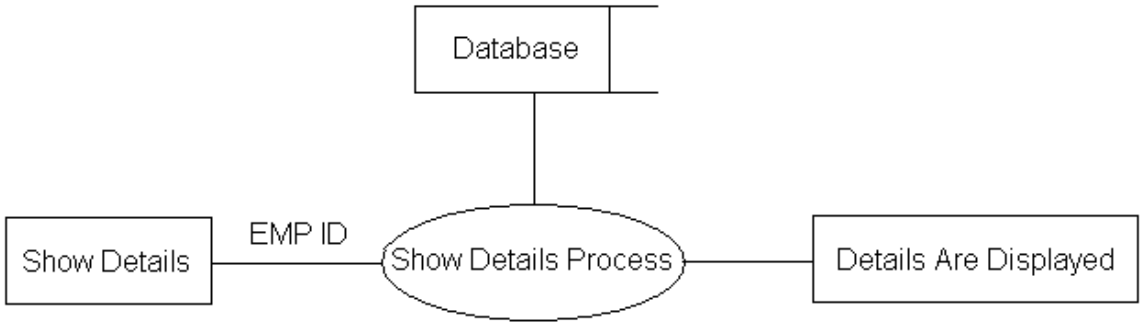
DFD SHOWING THE FLOW OF DATA TO ADD DETAILS OF A USER



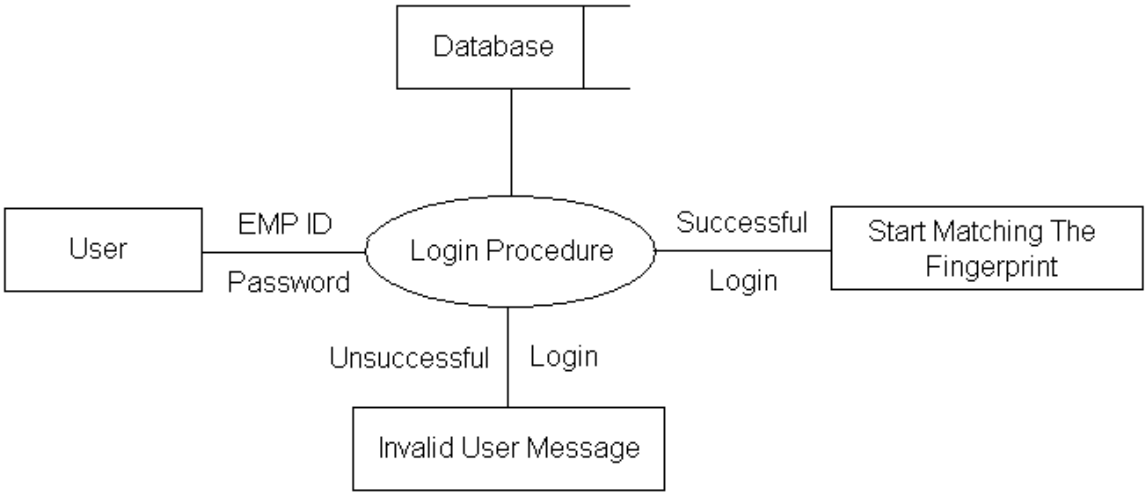
DFD SHOWING THE FLOW IN MODIFYING THE DETAILS OF A USER



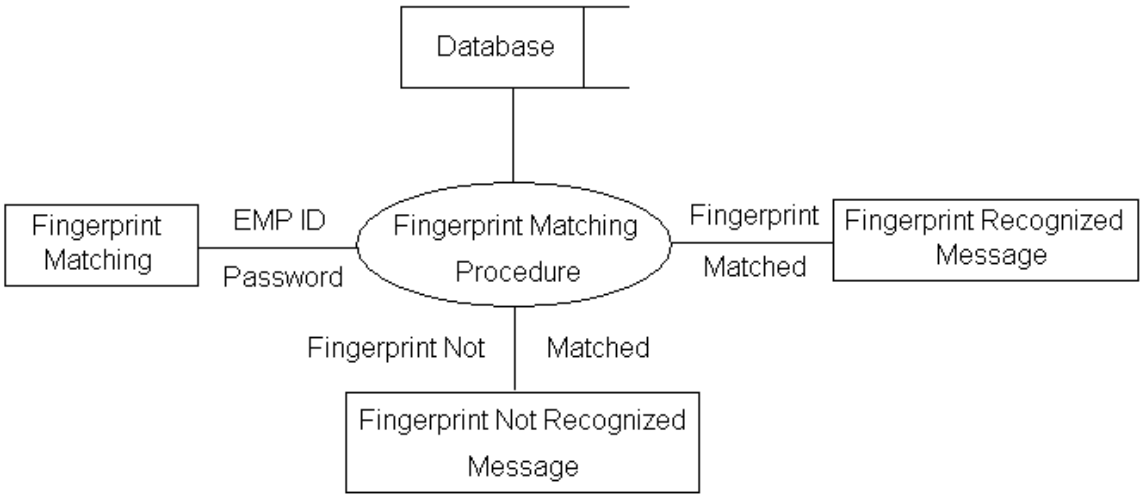
DFD SHOWING THE FLOW IN DELETING THE DETAILS OF A USER



DFD SHOWING THE FLOW TO DISPLAY THE DETAILS OF A USER

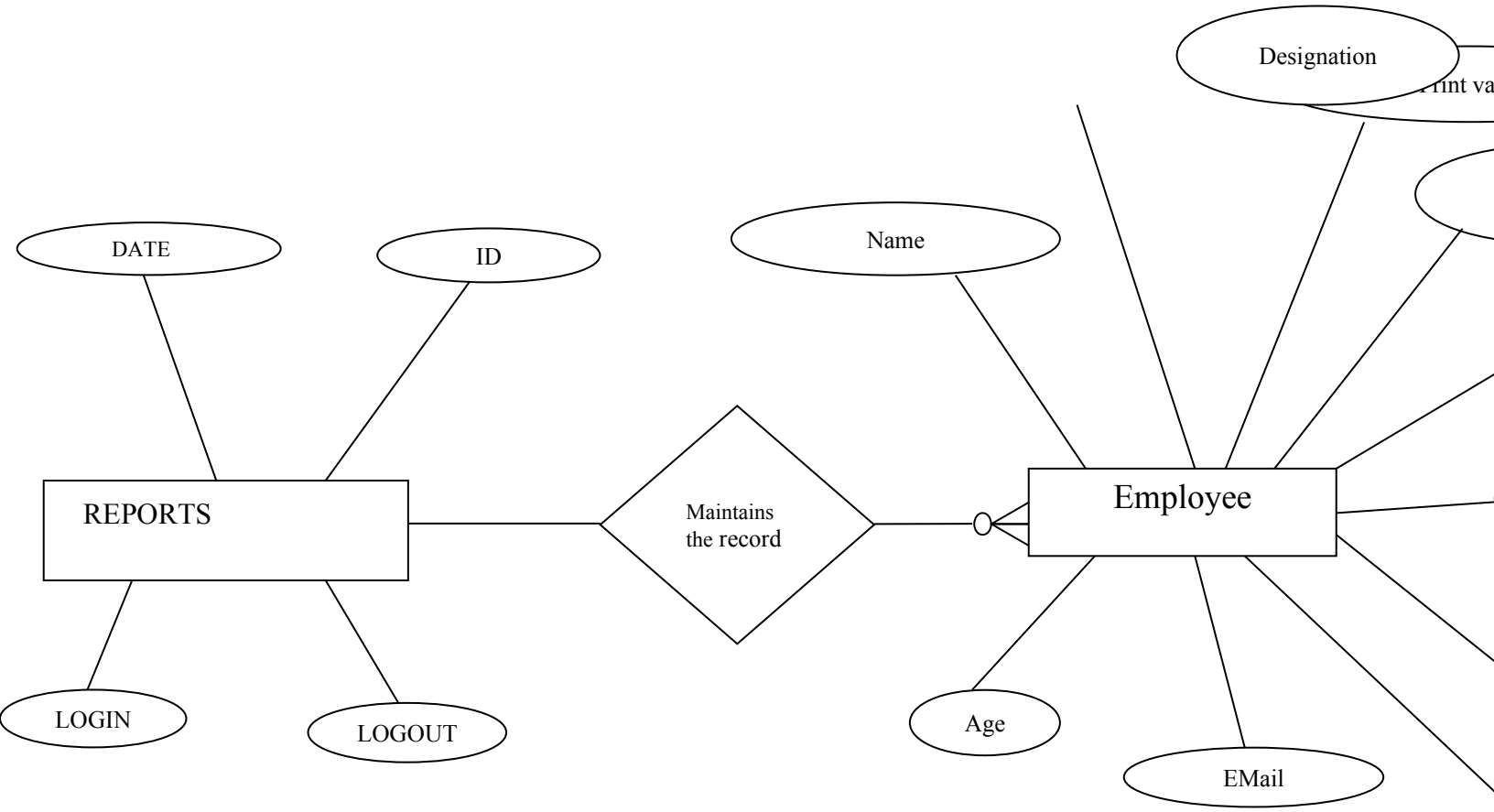


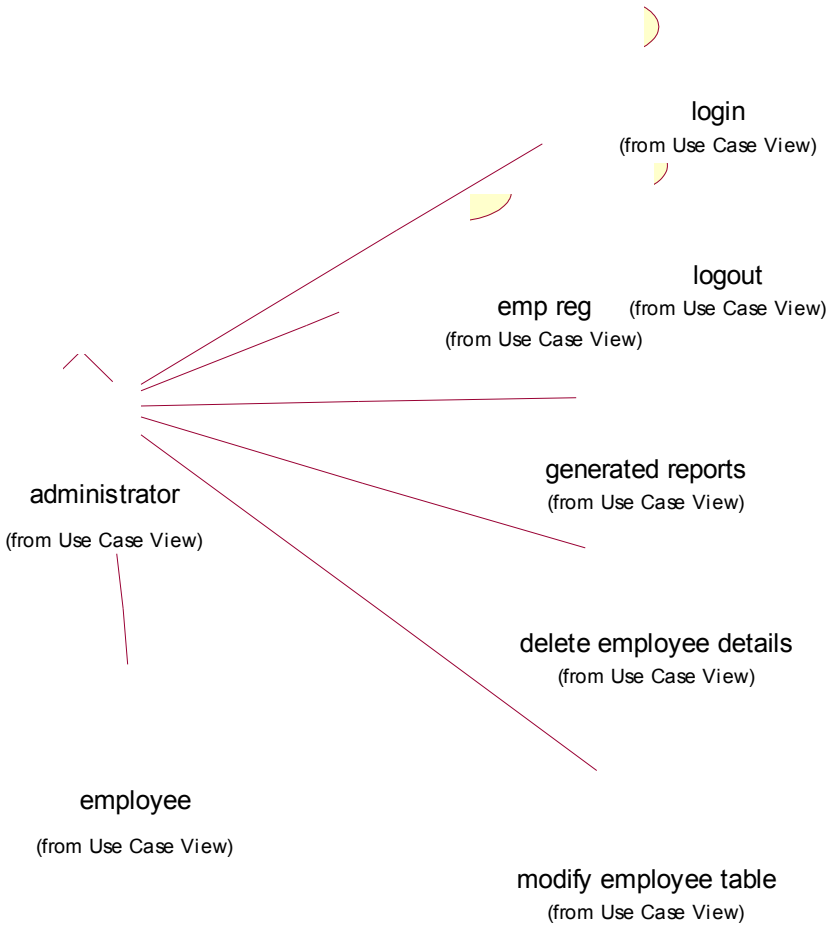
DFD SHOWING THE FLOW IN THE USER LOGIN PROCEDURE

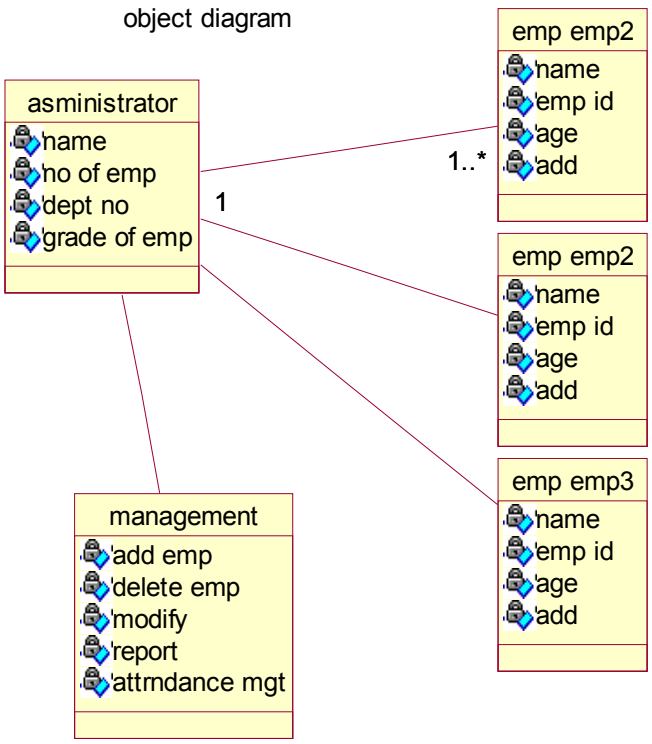


DFD SHOWING THE FLOW OF DATA WHEN THE FINGER PRINT OF A USER IS MATCHED

4.2. E-R DIAGRAMS



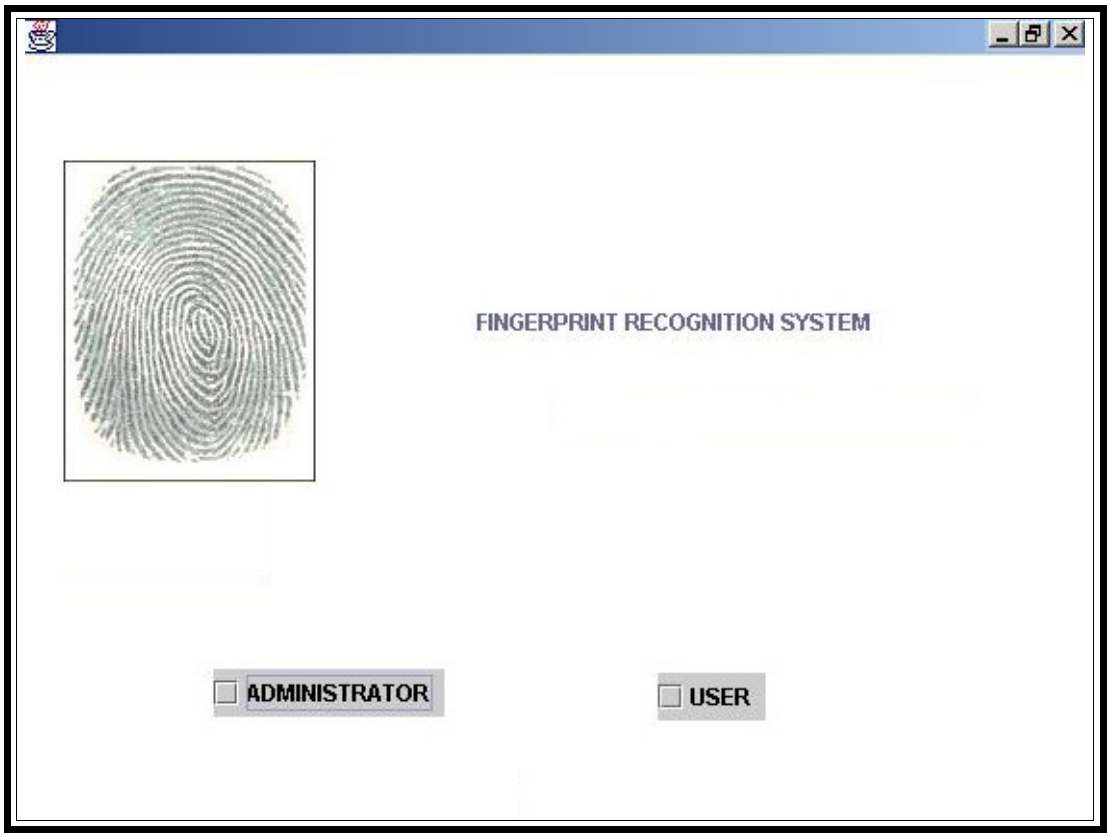

login
(from Use Case View)
logout
(from Use Case View)
emp reg
(from Use Case View)
generated reports
(from Use Case View)
administrator
(from Use Case View)
delete employee details
(from Use Case View)
employee
(from Use Case View)
modify employee table
(from Use Case View)


object diagram
asministrator
name
no of emp
dept no
grade of emp
1
1..*
emp emp2
name
emp id
age
add
emp emp2
name
emp id
age
add
emp emp3
name
emp id
age
add
management
add emp
delete emp
modify
report
attrndance mgt

5. FORMS & REPORTS

5.1. I/O SAMPLES

Here are some sample screens of our project.



THE ABOVE SCREEN SHOT IS THE HOMEPAGE

In the above screen we have two buttons, administrator and user. The administrator button takes us to an administrator screen to manage the database, add, delete or modify the details of the users. Given below is the screen shot of the administrator login page.

THE ABOVE SCREENSHOT SHOWS THE ADMINISTRATOR LOGIN SCREEN

Here the administrator has to enter his administrative User ID and password. If the administrator enters a correct User Id and password he gets a confirmation message saying the he is a valid user. Screenshot of the message is given below.

THE ABOVE SCREENSHOT SHOWS THE CONFIRMATION MESSAGE GOT BY THE ADMINISTRATOR AFTER ENTERING A VALID ID AND PASSWORD