VISVESVARAYA TECHNOLOGICAL UNIVERSITY,
BELGAUM.

B.L.D.E.Association's
VACHANA PITAMAHA Dr P.G.HALAKATTI
COLLEGE OF ENGINEERING & TECHNOLOGY,
BIJAPUR - 586103.

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING.

A PROJECT REPORT ON

"FINGER PRINT AUTHENTICATION FOR ATM MACHINES"

SPONSORED BY KSCST

BACHELOR OF ENGINEERING
IN
INFORMATION SCIENCE & ENGINEERING

VIII Semester (2008-2009)

Submitted by :

ROHIT H HALAGANI	2BL05IS038
SUDHA S KYADIGGERI	2BL05IS050
SHILPA S PATIL	2BL05IS046

Under the Guidance of
Prof. S.M.CHADCHAN

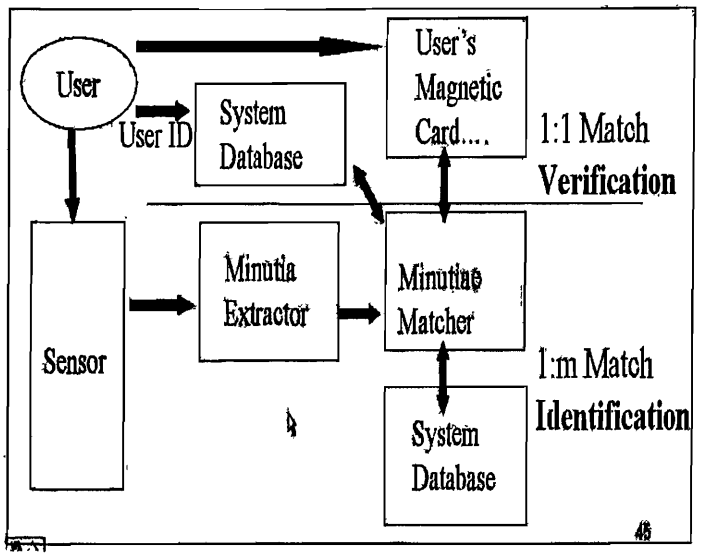

Figure 1.2. Verification vs. Identification

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System).

However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint. As long as the representation of fingerprints remains the uniqueness and keeps simple, the fingerprint matching, either for the 1-to-1 verification case or 1-to-m identification case, is straightforward and easy.

Two representation forms for fingerprints separate the two approaches for fingerprint recognition. The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has

been intensively studied, also is the backbone of the current available fingerprint recognition products. I also concentrate on this approach in my honors project.

The second approach, which uses image-based methods[6][7], tries to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition. And it is useful to solve some intractable problems of the first approach. But my project does not aim at this method, so further study in this direction is not expanded in my thesis.

1.2. 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 database for 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). Throughout this book we use the generic term *recognition* where we are not interested in distinguishing between verification and identification. The block diagrams of a verification system and an identification system are depicted in Figure 1.2; user enrollment, which is common to both tasks is also graphically illustrated. 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.

These applications may be divided into the following groups: i) applications such as banking, electronic commerce, and access control, in which biometrics will replace or enforce the current token- or knowledge-based techniques and ii) applications such as welfare and immigration in which neither the token-based nor the knowledge-based techniques are currently being used.

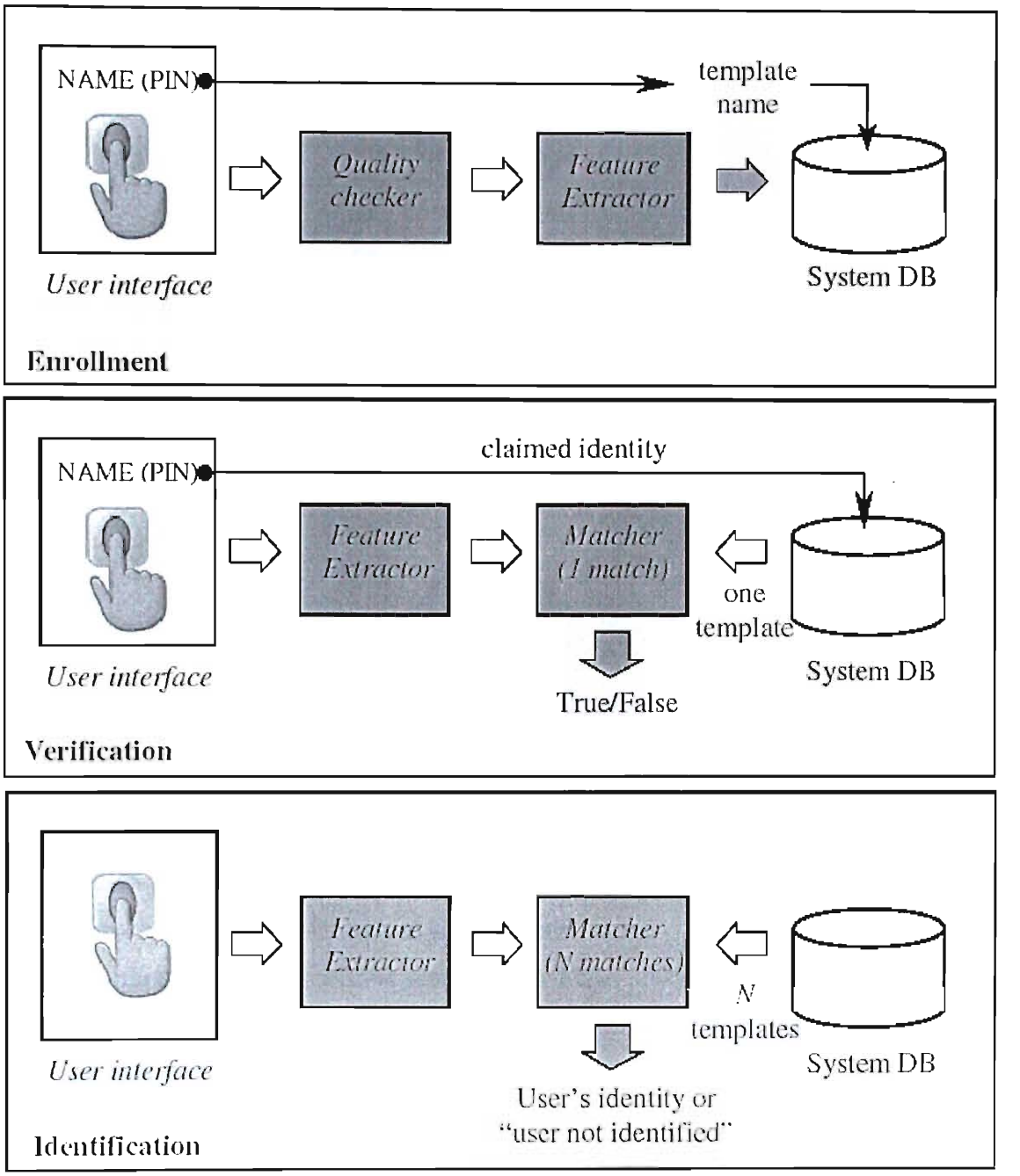

Figure 1.3. Block diagrams of enrollment, verification, and identification tasks.

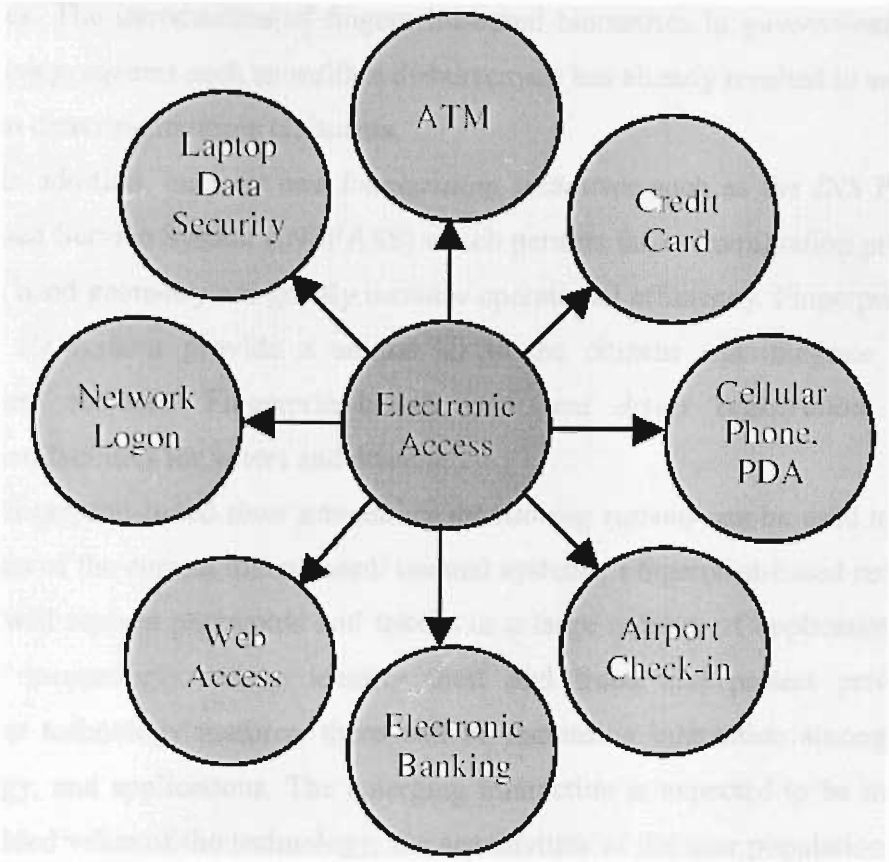

Figure 1.4. Applications of Automatic recognition

Information system/computer network security, such as user authentication and access to databases via remote login, is one of the most important application areas for fingerprint recognition. It is expected that more and more information systems/computer networks will be secured with fingerprints with the rapid expansion of the Internet. Applications such as medical information systems, distance learning, and e-publishing are already benefiting from deployment of such systems.

Electronic commerce and electronic banking are also important and emerging application areas of biometrics due to the rapid progress in electronic transactions. These applications include electronic fund transfers, ATM security, check cashing, credit card security, smartcard security, on-line transactions, and so on. Currently, there are several large fingerprint security projects under development in these areas, including credit card security (MasterCard) and smartcard security (IBM and American Express).

The *physical access control* market is currently dominated by token-based technology. However, it is increasingly shifting to fingerprint-based biometric

techniques. The introduction of fingerprint-based biometrics in *government benefits distribution programs* such as welfare disbursement has already resulted in substantial savings in deterring multiple claimants.

In addition, *customs and immigration initiatives* such as the *INS* Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry wil greatly increase operational efficiency. Fingerprint-based *national ID systems* provide a unique ID to the citizens and integrate different government services. Fingerprint-based *voter and driver registration* provides registration facilities for voters and drivers.

Fingerprint-based *time/ attendance monitoring systems* can be used to prevent any abuses of the current token based/ manual systems. Fingerprint-based recognition systems will replace passwords and tokens in a large number of applications. Their use will increasingly reduce identity theft and fraud and protect privacy. As fingerprint technology matures, there will be increasing interaction among market, technology, and applications. The emerging interaction is expected to be influenced by the added value of the technology, the sensitivities of the user population, and the credibility of the service provider.

It is too early to predict where and how fingerprint technology would evolve and be mated with which applications, but it is certain that fingerprint-based recognition will have a profound influence on the way we will conduct our daily business.

2. PROJECT DESIGN AND DEVELOPMENT

2.1. Problem definition

As the Technology is getting more and more advanced and networked, very high threats to security and personal identification are becoming serious concern.Today there is a strong need for a foolproof solution to secure personal data & information, as we all know ATM's have made our life very easy yet this technology comes with a downside where there are chances of stealing the ATM card and the number and misusing it.

Therefore a solution is required where this downside of ATM's can be reduced. The best solution would be to use age old techniques with new technology therefore we intend to build a solution where ATM machines will no more need ATM cards or PIN numbers but will scan the finger impression of the user and authenticate his identity as we all know that no two persons will have same finger impression nothing can be more better unique identity then the thumb impression

2.2. System Requirement Specification (SRS)

Software requirement specification is a fundamental document, which forms the foundation of software development process. Software requirement specification not only lists the requirements of a system but also has a description of its major features. This recommendation extends the standards and includes used cases and sequence diagram to incorporate UML standards. The recommendation would form the basis for providing clear visibility of the product to be developed serving as the baseline for execution of a contract between the client and the developer.

Software requirement specification constitutes of the agreement between client and developers regarding the contents of the software product that is going to be developed. Software requirement specification should accurately represent the system requirements as it makes a huge contribution to the overall large system or may be a component, Software requirement specification should state the interfaces between system and software portion.

2.3. System Analysis

Analysis is a detailed study of various operations performed by the system and their relationships within and outside the system.

I. **Identification of Needs:**

- The current security methods of using passwords, PIN codes, keys and cards are all unreliable.
- People have to remember so many passwords and PIN codes to gain access to different applications.

II. **Drawbacks of Existing System:**

- ATM cards may be lost, stolen or damaged.
- Passwords can be forgotten or misused if leaked.
- No complete security.

III. **Preliminary Investigation:**

Here preliminary investigation was carried out under following studies:-

- Understand present scenario.
- Understanding needs.
- Developing concept for the system.

2.4. Software Requirements and Hardware Requirements :-

Hardware Requirements :-

- Min Intel PIII Processor
- Min 128 MB RAM
- Flat bed Scanner
- 10 GB HDD

Software Requirements :-

- JDk 1.5.0
- J2EE Server