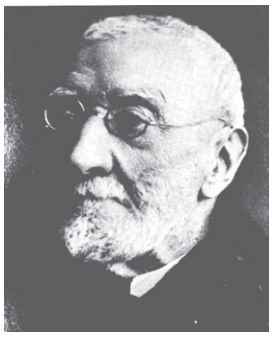
Appendix II

Fingerprint

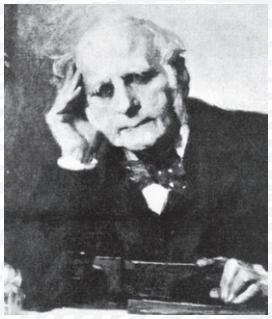
JUNE 2005 • VERSION 1

History of Fingerprints

Humans have used fingerprints for personal identification for a very long time. Modern fingerprint matching techniques were initiated in the late 16th century. Henry Fauld, in 1880, first scientifically suggested the individuality and uniqueness of fingerprints. At the same time, Herschel asserted that he had practiced fingerprint identification for about 20 years. This discovery established the foundation of modern fingerprint identification. In the late 17th century, Sir Francis Galton conducted an extensive study of fingerprints. He introduced the minutiae features for single fingerprint classification in 1888. The discovery of uniqueness of fingerprints caused an immediate decline in the prevalent use of anthropometric methods of identification and led to the adoption of fingerprints as a more efficient method of identification.



Dr. Henry Faulds studied fingerprints during the 1880's

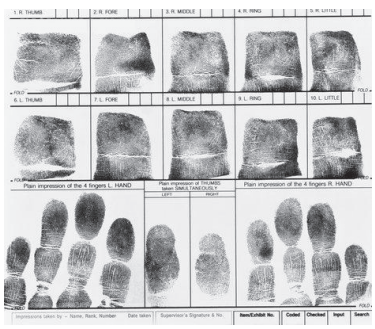


Sir Francis Galton conducted an extensive study of fingerprints

An important advance in fingerprint identification was made in 1899 by Edward Henry, who (actually his two assistants from India) established the famous "Henry system" of fingerprint classification: an elaborate method of indexing fingerprints very much tuned to facilitating the human experts performing (manual) fingerprint identification. In the early 19th century, fingerprint identification was formally accepted as a valid personal identification method by law enforcement agencies and became a standard procedure in forensics. Fingerprint identification agencies were setup worldwide and criminal fingerprint databases were established. With the advent of livescan fingerprinting and availability of cheap fingerprint sensors, fingerprints are increasingly used in government and commercial applications for positive person identification.

Sir Edward Richard Henry established the famous "Henry system" of fingerprint classification

Friction ridges contain rows of sweat pores, and sweat mixed with other body oils and dirt produces fingerprints on smooth surfaces. Fingerprint experts use powders and chemicals to make such prints visible. The visibility of a set of prints depends on the surface from which they are lifted; however, with the help of computer enhancement techniques that can extrapolate a complete pattern from mere fragments, and laser technology that can read otherwise invisible markings, fingerprint experts increasingly can retrieve identifiable prints from most surfaces.



Fingerprints are used in government and commercial applications for positive person identification

Fingerprint Automatic Identity Authentication System

Automatic identity authentication is becoming more and more important in our modern society. A number of automatic identity authentication techniques have been investigated, including blood vessel patterns in the retina or hand, fingerprint, hand geometry, iris, signature, and voiceprints. Among them, fingerprint is one of the most reliable techniques. An automatic identity authentication system which is capable of authenticating the identity of an individual automatically using his/her fingerprints. Such a system has great utility in a variety of identity authentication applications such as time & attendance, access control and credit card verification.

System Architecture of Automatic Identity Authentication System

It is widely known that a professional fingerprint examiner relies on minutiae details of ridge structures to match fingerprints. The topological structure of the minutiae details of ridge structures of a fingerprint is unique and invariant with aging and impression deformations. Eighteen different types of local ridge descriptions have been identified. Among them, the two most prominent minutia details that are suitable for automatic detection from input fingerprint images are ridge endings and ridge bifurcations which are usually called minutiae. Therefore, in an automatic identity authentication system using fingerprint, the two most important components are:

a. Minutia extraction which detects minutiae from input fingerprint images, and
b. Minutia pattern matching which matches two minutia patterns to establish the identity of an individual.

The system architecture of our automatic identity authentication system is shown in Figure 1. It consists of four components:

i. User interface;
ii. System database;
iii. Enrollment module, and;
iv. Authentication module.

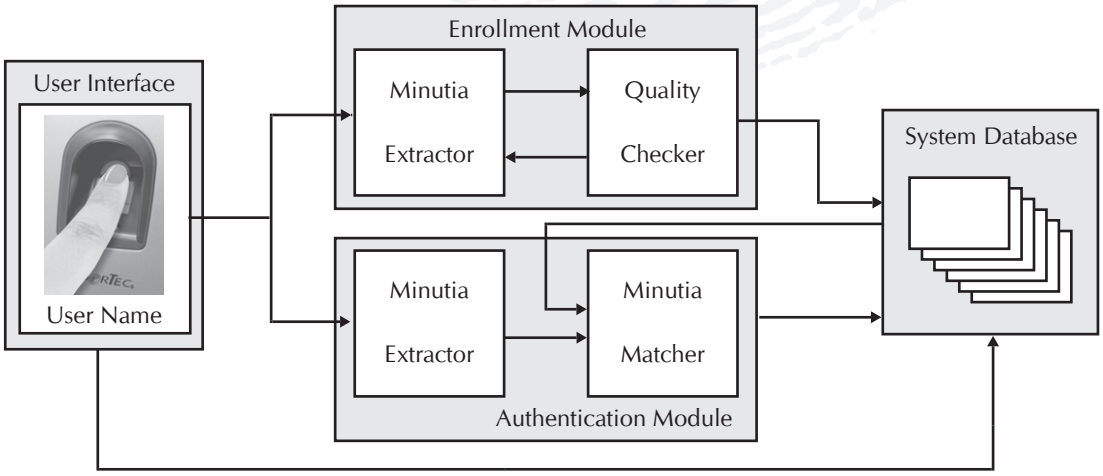
The user interface provides a mechanism for a user to indicate his/her identity and input his/her fingerprint into the system.

The system database consists of a collection of records each of which corresponds to an authorized individual that has access to the system. Each record contains the following fields:

i. User name of the individual, and;
ii. Several minutia patterns of the individual's finger;

The task of enrollment module is to enroll individuals and their fingerprints into the system database. When the fingerprint images and the user name of an individual to be enrolled are fed to the enrollment module, a minutia extraction algorithm is first applied to the fingerprint images and the minutia patterns are extracted. A quality checking algorithm is used to ensure that the records in the system database only consist of minutia patterns of good quality. This is important for the performance of system. A fingerprint image of poor quality is enhanced to improve the clarity of ridge/valley structures and mask out all the regions that cannot be reliably recovered. The enhanced fingerprint image is fed to the minutia extractor. If at least minimum minutia points are recovered, then the fingerprint is accepted. Otherwise, it is rejected.

The task of authentication module is to authenticate the identity of the individual who intends to access the system. The individual indicates his/her identity and places his/her finger on the fingerprint scanner; a digital image of his/her fingerprint is captured; minutia pattern is extracted from the captured fingerprint image and fed to a matching algorithm; the matching algorithm then matches it against the individual's minutia patterns stored in the system database to establish the identity.



Architecture of an automatic identity authrntication system (18). © IEEE

Market Needs

Fingerprint-based identification has come along way since inception more than 100 years back. The first primitive scanners designed by Cornell Aeronautical Lab/North American Aviation Inc. were unwieldy beasts with many problems as compared to sleek, inexpensive and relatively, miniscule semiconductor sensors. Over the past few decades, research and active use of fingerprint matching and indexing have also advanced our understanding of individuality information in fingerprints and efficient ways of processing this information. Increasingly inexpensive computing power, cheap fingerprint sensors, demand for security, efficiency, convenience have lead to viability of fingerprint matching information for every day positive person identification in the last few years.

Fingerprint Applications in Market

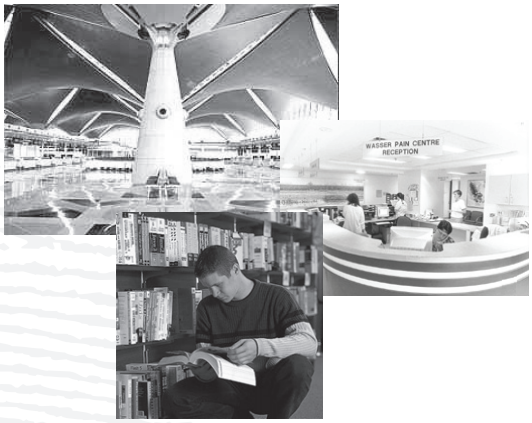
As biometric technology matures, there will be an increasing interaction among the (biometric) market, (biometric) technology, and the (identification) applications. The emerging interaction is expected to be influenced by the added value of the technology, the sensitivities of the population, and the credibility of the service provider. It is too early to predict where, how, and which biometric technology would evolve and be mated with which applications. But it is certain that biometrics based identification will have a profound influence on the way we conduct our daily business. It is also certain that, as the most mature and well understood biometric, fingerprints will remain an integral part of the preferred biometric-based identification solutions and time attendance solutions in the years to come.

Users of fingerprint devices are to be found in all sectors of the economy and all areas of government and commerce.

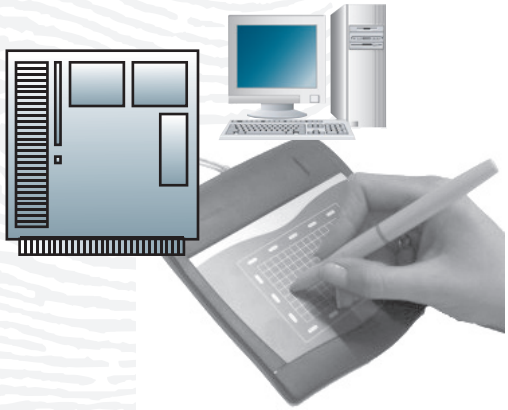
Specific areas to benefit from such technologies include:

- Government Agencies - Areas of applications include border control and immigration, driver license, national ID, social services, voter identification, etc;

- Public Infrastructure - airports, libraries, hospitals, educational institutions.



- Enterprise-wide network security infrastructures - PC Logon, e-commerce system, file protection, membership verification, electronic signature;



- Financial - Automated Teller Machines (ATMs), Point-of-Sales (POS), Teller Counter, Mobile Banking, Smart Cards, Safe Box.

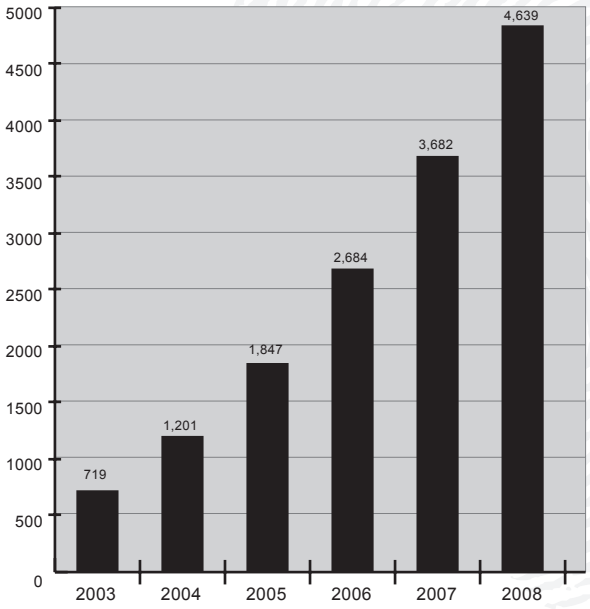
Fingerprint Applications in Market

The total biometric revenues including AFIS revenue for 5 years until 2008 is projected to increase at a steady rate. The 2004 International Biometric Group projected that the biometrics revenues will increase at 5.5 times from the USD719 million forecasted revenue for year 2003, which brings the total revenue of USD4.6 billion in 2008. (As shown in Total Biometric Revenues 2003-2008 chart below) Fingerprint technology, amongst all other biometric automatic identity authentication technologies, leads the market share in year 2004 with 48% compared to face (12%), middleware (12%), hand (11%), etc. (refer to 2004 Comparative Market Share by Technology)

Clearly, the market is vast and potential clients are waiting for your fingerprint-enabled products to reach them.

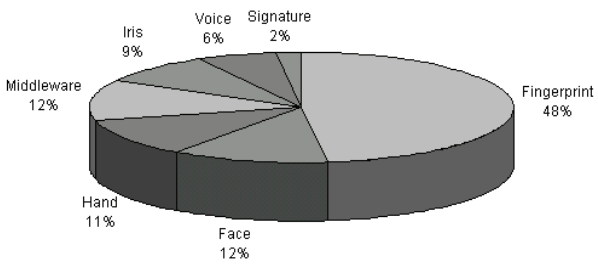
Total Biometric Revenues 2003- 2008 ($m)

(including AFIS revenue)



2004 Comparative Market Share by Technology

(not including AFIS revenue)



Performance of Fingerprint Applications in Market

There is a popular misconception that automatic fingerprint matching is a fully solved problem since it was one of the first applications of automatic pattern recognition. Despite notions to the contrary, there are a number of challenges that remain to be overcome in designing a completely automatic and reliable fingerprint matcher, especially when images are of poor quality and in the of latent prints. Although automatic systems are successfully, the level of sophistication of automatic systems in matching fingerprints today cannot rival that of a dedicated, well-trained, fingerprint expert. Still, automatic fingerprint matching systems offer a reliable, rapid, consistent and cost effective solution in a number of traditional and newly emerging applications.

Performance of various stages of an identification system, including feature extraction, classification, and minutiae matching, do not degrade gracefully with deterioration in the quality of the fingerprints. Most of these deficiencies in the existing automatic identification systems are overcome by having an expert interact with the system to compensate for the intermediate errors.

Future Prospects

Only few years back, it seemed as though, the interest in fingerprint matching research was waning. Due to increasing identity fraud in our society, there is a growing need for positive person identification, especially for time attendance solutions. Cheap fingerprint sensor prices, easy availability of inexpensive computing power, and our relatively better understanding of individuality information in fingerprints compared to other biometrics have attracted a lot of commercial interest in fingerprint-based time attendance and access control identification.

The critical factor for the widespread use of fingerprints is in meeting the performance (e.g.,matching speed and accuracy) standards demanded by time attendance and access control identification applications. There will be a growing demand for faster and more accurate fingerprint matching algorithms which can (particularly) handle poor quality images. Some of the emerging applications (e.g., fingerprint-based smartcards) will also benefit from a compact representation of a fingerprint. The design of highly reliable, accurate, and foolproof biometrics based identification systems may warrant effective integration of discriminatory information contained in several different biometrics and/or technologies. The issues involved in integrating fingerprint-based time attendance and access control identification with other biometric or non-biometric technologies may constitute an important research topic. Pervasive embedded applications of fingerprint-based identification (e.g. in a smart card or in a cell phone) may not be far behind.