An Identity-Authentication System Using Fingerprints

ANIL K. JAIN, FELLOW, IEEE, LIN HONG, SHARATH PANKANTI, ASSOCIATE MEMBER, IEEE, AND RUUD BOLLE, FELLOW, IEEE

Fingerprint verification is an important biometric technique for personal identification. In this paper, we describe the design and implementation of a prototype automatic identity-authentication system that uses fingerprints to authenticate the identity of an individual. We have developed an improved minutiae-extraction algorithm that is faster and more accurate than our earlier algorithm [58]. An alignment-based minutiae-matching algorithm has been proposed. This algorithm is capable of finding the correspondences between input minutiae and the stored template without resorting to exhaustive search and has the ability to compensate adaptively for the nonlinear deformations and inexact transformations between an input and a template. To establish an objective assessment of our system, both the Michigan State University and the National Institute of Standards and Technology NIST 9 fingerprint data bases have been used to estimate the performance numbers. The experimental results reveal that our system can achieve a good performance on these data bases. We also have demonstrated that our system satisfies the response-time requirement. A complete authentication procedure, on average, takes about 1.4 seconds on a Sun ULTRA 1 workstation (it is expected to run as fast or faster on a 200 HMz Pentium [7]).

Keywords*—*Biometrics, dynamic programming, fingerprint identification, matching, minutiae, orientation field, ridge extraction, string matching, verification.

I. INTRODUCTION

There are two types of systems that help automatically establish the identity of a person: 1) authentication (verification) systems and 2) identification systems. In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc., and the system either rejects or accepts the submitted claim of identity (Am I who I claim I am?). In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system data base) without the subject's having to claim an identity (Who am I?). The topic of this paper is a verification system based on fingerprints, and the terms verification, authentication, and identification are used in a loose sense and synonymously.

Accurate automatic personal identification is becoming more and more important to the operation of our increasingly electronically interconnected information society [13], [20], [53]. Traditional automatic personal identification technologies to verify the identity of a person, which use "something that you know," such as a personal identification number (PIN), or "something that you have," such as an identification (ID) card, key, etc., are no longer considered reliable enough to satisfy the security requirements of electronic transactions. All of these techniques suffer from a common problem of inability to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of the authorized person [53]. Biometrics is a technology that (uniquely) identifies a person based on his physiological or behavioral characteristics. It relies on "something that you are" to make personal identification and therefore can inherently differentiate between an authorized person and a fraudulent impostor [13], [20], [53]. Although biometrics cannot be used to establish an absolute "yes/no" personal identification like some of the traditional technologies, it can be used to achieve a "positive identification" with a very high level of confidence, such as an error rate of 0.001% [53].

A. Overview of Biometrics

Theoretically, any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies the following requirements [13]:

1) universality, which means that every person should have the characteristic;
2) uniqueness, which indicates that no two persons should be the same in terms of the characteristic;
3) permanence, which means that the characteristic should be invariant with time;
4) collectability, which indicates that the characteristic can be measured quantitatively.

Manuscript received October 31, 1996; revised April 26, 1997.

A. K. Jain and L. Hong are with the Department of Computer Science, Michigan State University, East Lansing, MI 48824 USA (e-mail: jain@cps.msu.edu; honglin@cps.msu.edu).

S. Pankanti and R. Bolle are with the Exploratory Computer Vision Group, IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA (e-mail: sharat@watson.ibm.com; bolle@watson.ibm.com).

Publisher Item Identifier S 0018-9219(97)06635-8.

Table 1 Comparison of Biometric Technologies

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Hand Vein	medium	medium	medium	medium	medium	medium	high
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F.Thermograms	high	high	low	high	medium	high	high

In practice, there are some other important requirements [13], [53]:

1) performance, which refers to the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy;
2) acceptability, which indicates to what extent people are willing to accept the biometric system;
3) circumvention, which refers to how easy it is to fool the system by fraudulent techniques.

Biometrics is a rapidly evolving technology that has been widely used in forensics, such as criminal identification and prison security, and has the potential to be widely adopted in a very broad range of civilian applications:

1) banking security, such as electronic fund transfers, ATM security, check cashing, and credit card transactions;
2) physical access control, such as airport access control;
3) information system security, such as access to data bases via login privileges;
4) government benefits distribution, such as welfare disbursement programs [49];
5) customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry [35];
6) national ID systems, which provide a unique ID to the citizens and integrate different government services [31];
7) voter and driver registration, providing registration facilities for voters and drivers.

Currently, there are mainly nine different biometric techniques including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms [13], [18], [20], [53], [68]. A brief comparison of these nine biometric techniques is provided in Table 1. Although each of these techniques, to a certain extent, satisfies the above requirements and has been used in practical systems [13], [18], [20], [53] or has the potential to become a valid biometric technique [53], not many of them are acceptable (in a court of law) as indisputable evidence of identity. For example, despite the fact that extensive studies have been conducted on automatic face recognition and that a number of face-recognition systems are available [3], [62], [70], it has not yet been proven that 1) face can be used reliably to establish/verify identity and 2) a biometric system that uses only face can achieve an acceptable identification accuracy in a practical environment. Without any other information about the people in Fig. 1, it will be extremely difficult for both a human and a face-recognition system to conclude that the different faces shown in Fig. 1 are disguised versions of the same person. So far, the only legally acceptable, readily automated, and mature biometric technique is the automatic fingerprint-identification technique, which has been used and accepted in forensics since the early 1970's [42]. Although signatures also are legally acceptable biometrics, they rank a distant second to fingerprints due to issues involved with accuracy, forgery, and behavioral variability. Currently, the world market for biometric systems is estimated at approximately $112 million. Automatic fingerprint-identification systems intended mainly for forensic applications account for approximately $100 million. The biometric systems intended for civilian applications are growing rapidly. For example, by the year 1999, the world market for biometric systems used for physical access control alone is expected to expand to $100 million [53].

The biometrics community is slow in establishing benchmarks for biometric systems [20]. Although benchmark results on standard data bases in themselves are useful only

Fig. 1. Multiple personalities: all of the people in this image are the same person. (From *The New York Times Magazine*, Sept. 1, 1996, sect. 6, pp. 48–49. Reproduced with permission of Robert Trachtenberg.)

system parameters to "improve" the system performance,[1] they constitute a good starting point for comparison of the gross performance characteristics of the systems.

No metric is sufficiently adequate to give a reliable and convincing indication of the identification accuracy of a biometric system. A decision made by a biometric system is either a "genuine individual" type of decision or an "impostor" type of decision, which can be represented by two statistical distributions, called genuine distribution and impostor distribution, respectively. For each type of decision, there are two possible decision outcomes, true or false. Therefore, there are a total of four possible outcomes: 1) a genuine individual is accepted, 2) a genuine individual is rejected, 3) an impostor is rejected, and 4) an impostor is accepted. Outcomes 1) and 3) are correct, whereas 2) and 4) are incorrect. In principle, we can use the false (impostor) acceptance rate (FAR), the false (genuine individual) reject rate (FRR), and the equal error rate (EER)[2] to indicate the identification accuracy of a biometric system [18], [19], [53]. In practice, these performance metrics can only be estimated from empirical data, and the estimates of the performance are very data dependent. Therefore, they are meaningful only for a specific data base in a specific test environment. For example, the performance of a biometric system claimed by its manufacturer had an FRR of 0.3% and an FAR of 0.1%. An independent test by the Sandia National Laboratory found that the same system had an FRR of 25% with an unknown FAR [10]. To provide a more reliable assessment of a biometric system, some more descriptive performance measures are necessary. Receiver operating curve (ROC) and d' are the two other commonly used measures. An ROC provides an empirical assessment of the system performance at different operating points, which is more informative than FAR and FRR. The statistical metric d' gives an indication of the separation between the genuine distribution and impostor distribution [19]. It is defined as the difference between the means of the genuine distribution and impostor distribution divided by a conjoint measure of their standard deviations [19]

$$d' = \frac{||M_{\text{impostor}} - M_{\text{genuine}}||}{\sqrt{(\text{SD}^2_{\text{impostor}} + \text{SD}^2_{\text{genuine}})/2}} \tag{1}$$

where M_{genuine}, $\text{SD}_{\text{genuine}}$, M_{impostor}, and $\text{SD}_{\text{impostor}}$ are the means and standard deviations of the genuine distribution and impostor distribution, respectively. Like FAR, FRR, and EER, both ROC and d' also depend heavily on test data and test environments. For such performance metrics to be able to generalize precisely to the entire population of interest, the test data should 1) be large enough to represent the population and 2) contain enough samples from each category of the population [19]. To obtain fair and honest test results, enough samples should be available, and the samples should be representative of the population and adequately represent all the categories (impostor and genuine). Further, irrespective of the performance measure, error bounds that indicate the confidence of the estimates are valuable for understanding the significance of the test results.

B. History of Fingerprints

Fingerprints are graphical flow-like ridges present on human fingers (see Fig. 2). Their formations depend on the initial conditions of the embryonic mesoderm from which they develop. Humans have used fingerprints as a means of identification for a very long time [42]. Modern fingerprint techniques were initiated in the late sixteenth

[1] Several additional techniques, like data sequestering [51] and third-party benchmarking [9], may also help in obtaining fairer performance results.

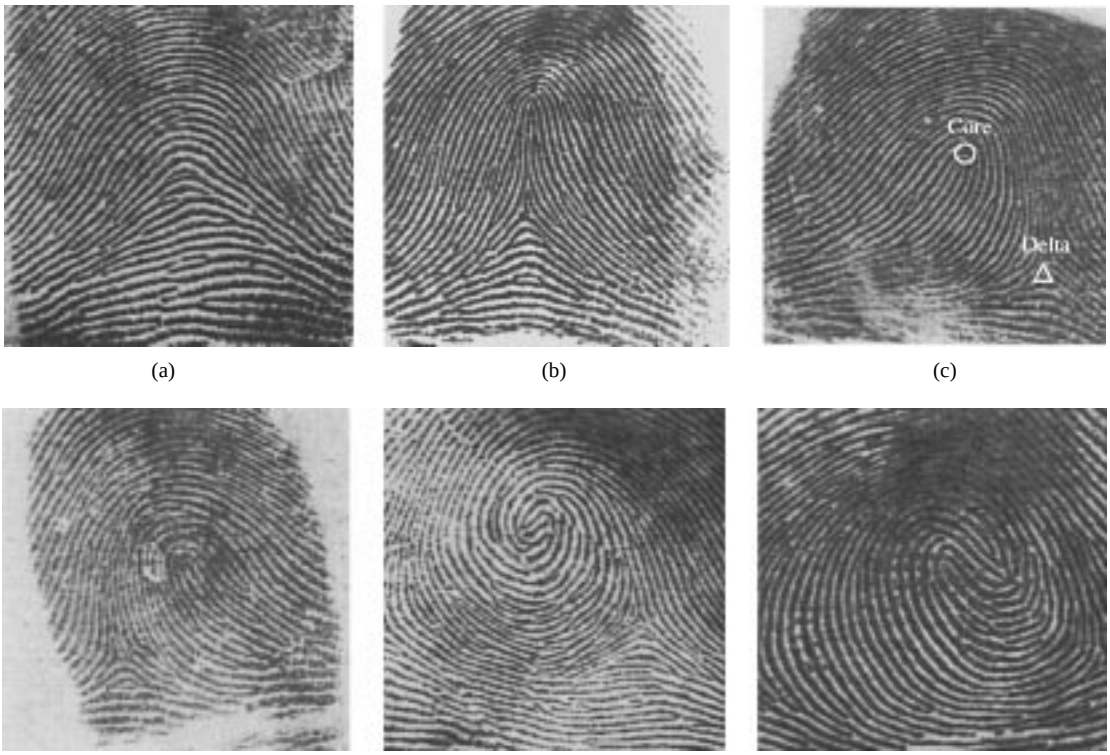

Fig. 2. Fingerprints and a fingerprint classification schema of six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twinloop. Critical points in a fingerprint, called core and delta, are marked on (c).

Grew published a paper reporting his systematic study on the ridge, furrow, and pore structure in fingerprints, which is believed to be the first scientific paper on fingerprints [42]. Since then, a number of researchers have invested a huge amount of effort in studying fingerprints. In 1788, a detailed description of the anatomical formations of fingerprints was made by Mayer [16], in which a number of fingerprint ridge characteristics were identified. Starting from 1809, T. Bewick began to use his fingerprint as his trademark, which is believed to be one of the most important contributions in the early scientific study of fingerprint identification [42]. Purkinje proposed the first fingerprint classification scheme in 1823, which classified fingerprints into nine categories according to the ridge configurations [42]. H. 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 approximately 20 years [42]. This discovery established the foundation of modern fingerprint identification. In the late nineteenth century, Sir F. Galton conducted an extensive study of fingerprints [42]. He introduced the minutiae features for single fingerprint classification in 1888. An important advance in fingerprint identification was made in 1899 by E. Henry, who (actually his two assistants from India) established the famous "Henry system" of fingerprint classification [25], [42], an elaborate method of indexing fingerprints very much tuned to facilitating the human experts in performing (manual) fingerprint identification

prints were well understood. The biological principles of fingerprints are summarized below.

- Individual epidermal ridges and furrows (valleys) have different characteristics for different fingers.
- The configuration types are individually variable but they vary within limits that allow for systematic classification.
- The configurations and minute details of individual ridges and furrows are permanent and unchanging for a given finger.

In the early twentieth century, fingerprint identification was formally accepted as a valid personal-identification method by law-enforcement agencies and became a standard routine in forensics [42]. Fingerprint-identification agencies were set up worldwide, and criminal fingerprint data bases were established [42].

Starting in the early 1960's, the Federal Bureau of Investigation (FBI) home office in the United Kingdom and the Paris Police Department invested a large amount of effort in developing automatic fingerprint-identification systems (AFIS's) [25]. Their efforts were so successful that a large number of AFIS's are currently installed and in operation at law-enforcement agencies worldwide. These systems have greatly improved the operational productivity of these agencies and reduced the cost of hiring and training human fingerprint experts for manual fingerprint identification. Encouraged by the success achieved by AFIS's in law-

rapidly grew beyond law enforcement into civilian applications [25], [53]. In fact, fingerprint-based biometric systems are so popular that they have almost become the synonym of biometric systems [20]. Although significant progress has been made in designing automatic fingerprint-authentication systems over the past 30 years, a number of design factors (lack of reliable minutiae-extraction algorithms [48], [54], difficulty in quantitatively defining a reliable match between fingerprint images [43], [45], poor fingerprint classification algorithms [12], [14] [39], [46], [57], [74], etc.) create bottlenecks in achieving the desired performance [25], [42].

C. Design of a Fingerprint-Verification System

An automatic fingerprint identity authentication system has four main design components: acquisition, representation (template), feature extraction, and matching.

1) Acquisition: There are two primary methods of capturing a fingerprint image: inked (off-line) and live scan (ink-less). An inked fingerprint image is typically acquired in the following way: a trained professional[3] obtains an impression of an inked finger on a paper, and the impression is then scanned using a flat-bed document scanner. The live-scan fingerprint is a collective term for a fingerprint image directly obtained from the finger without the intermediate step of getting an impression on a paper. Acquisition of inked fingerprints is cumbersome; in the context of an identity-authentication system, it is both infeasible and socially unacceptable for identity verification.[4] The most popular technology to obtain a live-scan fingerprint image is based on the optical frustrated total internal reflection (FTIR) concept [28]. When a finger is placed on one side of a glass platen (prism), ridges of the finger are in contact with the platen while the valleys of the finger are not. The rest of the imaging system essentially consists of an assembly of a light emitting diode (LED) light source and a charge-couple device (CCD) placed on the other side of the glass platen. The laser light source illuminates the glass at a certain angle, and the camera is placed such that it can capture the laser light reflected from the glass. The light that is incident on the plate at the glass surface touched by the ridges is randomly scattered, while the light incident at the glass surface corresponding to valleys suffers total internal reflection, resulting in a corresponding fingerprint image on the imaging plane of the CCD.

A number of other live-scan imaging methods are now available, based on ultrasound total internal reflection [61], optical total internal reflection of edge-lit holograms [21], thermal sensing of the temperature differential (across the ridges and valleys) [41], sensing of differential capacitance [47], and noncontact three-dimensional scanning [44]. These alternate methods are primarily concerned with either reducing the size/price of the optical scanning system or improving the quality/resolution/consistency of the image capture. Typical specifications for the optical live-scan fingerprints are specified in [60].

2) Representation (Template): Which machine-readable representation completely captures the invariant and discriminatory information in a fingerprint image? This representation issue constitutes the essence of fingerprint-verification design and has far-reaching implications on the design of the rest of the system. The unprocessed gray-scale values of the fingerprint images are not invariant over the time of capture.

Representations based on the entire gray-scale profile of a fingerprint image are prevalent among the verification systems using optical matching [4], [50]. The utility of the systems using such representation schemes, however, may be limited due to factors like brightness variations, image-quality variations, scars, and large global distortions present in the fingerprint image because these systems are essentially resorting to template-matching strategies for verification. Further, in many verification applications, terser representations are desirable, which preclude representations that involve the entire gray-scale profile fingerprint images. Some system designers attempt to circumvent this problem by restricting that the representation is derived from a *small* (but consistent) part of the finger [50]. If this same representation is also being used for identification applications, however, then the resulting systems might stand a risk of restricting the number of unique identities that could be handled simply because of the fact that the number of distinguishable templates is limited. On the other hand, an image-based representation makes fewer assumptions about the application domain (fingerprints) and therefore has the potential to be robust to wider varieties of fingerprint images. For instance, it is extremely difficult to extract a landmark-based representation from a (degenerate) finger devoid of any ridge structure.

Representations that rely on the entire ridge structure (ridge-based representations) are largely invariant to the brightness variations but are significantly more sensitive to the quality of the fingerprint image than the landmark-based representations described below. This is because the presence of the landmarks is, in principle, easier to verify [75].

An alternative to gray-scale-based representation is to extract landmark features from a binarized fingerprint image. Landmark-based representations are also used for privacy reasons—one cannot reconstruct the entire fingerprint image from the fingerprint landmark information alone. The common hypothesis underlying such representations is the belief that the individuality of fingerprints is captured by the local ridge structures (minute details) and their spatial distributions [25], [42]. Therefore, automatic fingerprint verification is usually achieved with minute-detail matching instead of a pixel-wise matching or a ridge-pattern matching of fingerprint images. In total, there are approximately 150 different types of local ridge structures that have been identified [42]. It would be extremely difficult to automatically, quickly, and reliably extract these different representations from the fingerprint images because 1) some of them

[3] For reasons of expediency, MasterCard sends fingerprint kits to its credit card customers. The kits are used by the customers themselves to create an inked fingerprint impression to be used for enrollment.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.