An Identity-Authentication System Using Fingerprints

Mr. Ratnakar Anandrao Kharade, Mr. M.S. Kumbhar H.O.D.

1 Asst. Professor, Department of Electronics and Telecommunication Engg., Dr Daulatrao Aher College Of Engineering, Karad,
2 Professor, Department of Electronics and Telecommunication Engg., R.I.T. college of engineering, Sakharale.

Abstract

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 (verifica-tion) 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 increas-ingly 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 be-tween 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%. 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.

In practice, there are some other important requirements.
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 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 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 that are either widely used or under investigation, including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms.

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 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 automated teller machines; 2) government benefits distribution, such as welfare disbursement programs; 3) information system security, such as access to data bases via login privileges; 4) national ID systems, which provide a unique ID to the citizens and integrate different government services; 5) customs and immigration, such as the Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry; 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 that are either widely used or under investigation, including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms.

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 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 automated teller machines; 2) government benefits distribution, such as welfare disbursement programs; 3) information system security, such as access to data bases via login privileges; 4) national ID systems, which provide a unique ID to the citizens and integrate different government services; 5) customs and immigration, such as the Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry; 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 that are either widely used or under investigation, including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms.

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 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 automated teller machines; 2) government benefits distribution, such as welfare disbursement programs; 3) information system security, such as access to data bases via login privileges; 4) national ID systems, which provide a unique ID to the citizens and integrate different government services; 5) customs and immigration, such as the Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry; 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 that are either widely used or under investigation, including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms.

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 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 automated teller machines; 2) government benefits distribution, such as welfare disbursement programs; 3) information system security, such as access to data bases via login privileges; 4) national ID systems, which provide a unique ID to the citizens and integrate different government services; 5) customs and immigration, such as the Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry; 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 that are either widely used or under investigation, including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms.

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 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.
the Sandia National Laboratory found that the same system had an FRR of 25% with an unknown FAR [10].

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 century [25], [53]. In 1684, English plant morphologist N.

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 to 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 latenineteenth century, Sir F. Galton conducted an extensive study of fingerprints [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 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: inked 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 is 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 theridges and valleys) [41], sensing of differential capacitance [47], and noncontact three-dimensional scanning [44].

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 grayscale 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 (fingertips) and therefore has the potential to be robust to wider variations of fingerprint images. For instance, it is extremely difficult to extract a landmark-based representation from a (degenerate) finger devoid of any ridge structure. Typically, automatic fingerprint identification and authentication systems rely on representing the two most prominent structures: ridge endings and ridge bifurcations. Fig. 3 shows examples of ridge endings and ridge bifurcations. These two structures are background-foreground duals of each other; and pressure variations could convert one type of structure into the other. Therefore, many common representation schemes do not distinguish between ridge endings and bifurcations. Both the structures are treated equivalently and are collectively called minutiae. The simplest of the minutia-based representations constitute a list of points defined by their spatial coordinates with respect to a fixed image-centric coordinate system. Typically, though, these minimal minutiae-based representations are further enhanced by tagging each minutia (or each combination of minutiae subset, e.g., pairs, triplets) with additional features. For instance, each minutia could be associated with the orientation of the ridge at that minutia; or each pair of the minutiae could be associated with the ridge count: the number of ridges visited during the linear traversal between the two minutiae. The American National Standards Institute–National Institute of Standards and Technology (NIST) standard representation of a fingerprint is based on minutiae and includes minutiae location and orientation [2]. The minutiae-based representation might also include one or more global attributes like orientation of the finger, locations of core or delta, and fingerprint class. Our representation is minutiae based, and each minutia is described by its location (coordinates) and orientation. We also store a short segment of the ridge associated with each minutia.

3) Feature Extraction: A feature extractor finds the ridge endings and ridge bifurcations from the input fingerprint images. If ridges can be perfectly located in an input fingerprint image, then minutiae extraction is just a trivial task of extracting singular points in a thinned ridgemap. In practice, however, it is not always possible to obtain a perfect ridge map. The performance of currently available minutiae-extraction algorithms depends heavily on the quality of input fingerprint images.

4) Matching: Given two (test and reference) representations, the matching module determines whether the prints are impressions of the same finger. The matching phase typically defines a metric of the similarity between two fingerprint representations. The matching stage also defines a threshold to decide whether a given pair of representations are of the same finger (mated pair) or not. In the case of the minutiae-based representations, the fingerprint-verification problem may be reduced to a point pattern matching (minutiae pattern matching) problem. In the ideal case, if 1) the correspondence between the template minutiae pattern and input minutiae pattern is known, 2) there are no deformations such as translation, rotation, and deformations between them, and 3) each minutia present in a fingerprint image is exactly localized, then fingerprint verification is only a trivial task of counting the number of spatially matching pairs between the two images. Determining whether two representations of a finger extracted from its two impressions, possibly separated by a long duration of time, are indeed representing the same finger is an extremely difficult problem. Fig. 4 illustrates the difficulty with an example of two images of the same finger. The difficulty can be attributed to two primary reasons. First, if the test and reference representations are indeed mated pairs, the correspondence between the test and reference minutiae in the two representations is not known. Second, the imaging system presents a number of peculiar and challenging situations, some of which are unique to fingerprint image capture scenario. 1) Inconsistent contact: the act of sensing distorts the finger. Determined by the pressure and contact of the finger on the glass platen, the three-dimensional shape of the finger gets mapped onto the two-dimensional surface of the glass platen. Typically, this mapping function is uncontrolled.
and results in different inconsistently mapped fingerprint images across the impressions.  

2) **Nonuniform contact:** The ridge structure of a finger would be completely captured if ridges of the part of the finger being imaged are in complete optical contact with the glass platen. However, the dryness of the glass platen is nonuniform, and this causes the fingerprint images to be inconsistently mapped.  

Fig. 4. Two different fingerprint impressions of the same finger. To know the correspondence between the minutiae of these two fingerprint images, all of the minutiae must be precisely localized and the deformations must be recovered.  

3) **Irreproducible contact:** manual work, accidents, etc. inflict injuries to the finger, thereby changing the ridge structure of the finger either permanently or semipermanently. This may introduce additional spurious minutiae.  

4) **Feature extraction artifacts:** The feature extraction algorithm is imperfect and introduces measurement errors. Various image-processing operations might introduce inconsistent biases to perturb the location and orientation estimates of the reported minutiae from their gray-scale counterparts.  

5) **Sensing act:** the act of sensing itself adds noise to the image. For example, residues are leftover from the previous fingerprint capture. A typical finger-imaging system distorts the image of the object being sensed due to imperfect imaging conditions. In the FTIR sensing scheme, for example, there is a geometric distortion because the image plane is not parallel to the glass platen. In light of the operational environments mentioned above, the design of the matching algorithms needs to establish and characterize a realistic model of the variations among the representations of mated pairs. This model should include the properties of interest listed below.  

a) The finger may be placed at different locations on the glass platen, resulting in a (global) translation of the minutiae from the test representation from those in the reference representation.  

b) The finger may be placed in different orientations on the glass platen, resulting in a (global) rotation of the minutiae from the test representation from that of the reference representation.  

c) The finger may exert a different (average) downward normal pressure on the glass platen, resulting in a (global) spatial scaling of the minutiae from the test representation from those in the reference representation.  

d) The finger may exert a different (average) shear force on the glass platen, resulting in a (global) shear transformation (characterized by a shear direction and magnitude) of the minutiae from the test representation from those in the reference representation.  

e) Spurious minutiae may be present in both the reference and the test representations.  

f) Genuine minutiae may be absent in the reference or the test representations.  

g) Minutiae may be locally perturbed from their “true” location, and the perturbation may be different for each individual minutia. (Further, the magnitude of such perturbation is assumed to be small and within a fixed number of pixels.)  

h) The individual perturbations among the corresponding minutiae could be relatively large (with respect to ridge spacings), but the perturbations among pairs of the minutiae are spatially linear.  

i) The individual perturbations among the corresponding minutiae could be relatively large (with respect to ridge spacings), but the perturbations among pairs of the minutiae are spatially linear.
Only a (ridge) connectivity preserving transformation could characterize the relationship between the test and reference representations [73]. A matcher may rely on one or more of these assumptions, resulting in a wide spectrum of behavior. At the one end of the spectrum, we have the “Euclidean” matchers, which allow only rigid transformations among the test and reference representations. At the other extreme, we have a “topological” matcher, which may allow the most general transformations, including, say, order reversals. The choice of assumptions often represents verification performance tradeoffs. Only a highly constrained system with not too demanding accuracies could get away with restrictive assumptions. A number of the matchers in the literature assume similarity transformation [assumptions a), b), and c)]; they tolerate both spurious minutiae as well as missing genuine minutiae. “Elastic” matchers in the literature accommodate a small bounded local perturbation of minutiae from their true location but cannot handle large displacements of the minutiae from their true locations [59]. Fig. 5 illustrates a typical situation of aligned ridge structures of mated pairs. Note that the best alignment in one part (top left) of the image may result in a large amount of displacements between the corresponding minutiae in the other regions (bottom right). In addition, observe that the distortion is nonlinear: given distortions at two arbitrary locations on the finger, it is not possible to predict the distortion at all of the intervening points on the line joining the two points. In the authors’ opinion, a good matcher needs to accommodate not only global similarity transformations [assumptions a), b), and c)] but also shear transformation [assumption d)] and linear [assumption h)].

II. MINUTIAE EXTRACTION

Fingerprint authentication is based on the matching of minutiae patterns. A reliable minutiae extraction algorithm is critical to the performance of an automatic identity authentication system using fingerprints. In our system, we have developed a minutiae-extraction algorithm that is an improved version of the technique described in [58]. Experimental results show that this algorithm performs very well in operation. The overall flowchart of this algorithm is depicted in Fig. 7. It mainly consists of three components: 1) orientation field estimation, 2) ridge extraction, and 3) minutiae extraction and postprocessing. In the following subsections, we will describe in detail our minutiae-extraction algorithm. We assume that the resolution of input fingerprint images is 500 dots per inch.

A. Orientation Field Estimation

The orientation field of a fingerprint image represents the intrinsic nature of the fingerprint image. It plays a very important role in fingerprint-image analysis. A number of methods have been proposed to estimate the orientation field of fingerprint images [38], [40], [56]. In our system, a new hierarchical implementation of the algorithm proposed in [56] is used (Fig. 8). With this algorithm, a fairly smooth orientation-field estimate can be obtained. Fig. 9 shows the orientation field of a fingerprint image estimated.
with our hierarchical algorithm. After the orientation field of an input fingerprint image is estimated, a segmentation algorithm, which is based on the local certainty level of the orientation field, is used to locate the region of interest within the input fingerprint image. The certainty level of the orientation field at pixel is defined as follows: A. Orientation Field Estimation The orientation field of a fingerprint image represents the intrinsic nature of the fingerprint image. It plays a very important role in fingerprint-image analysis. A number of methods have been proposed to estimate the orientation field of fingerprint images [38], [40], [56]. In our system, a new hierarchical implementation of the algorithm proposed in [56] is used (Fig. 8). With this algorithm, a fairly smooth orientation field estimate can be obtained. Fig. 9 shows the orientation field of a fingerprint image estimated with our hierarchical algorithm.

III. MINUTIAE MATCHING

Fingerprint matching has been approached from several different strategies, like image-based [4], [50] and ridge pattern matching of fingerprint representations. There also exist graph-based schemes [22], [23], [26], [27], [34], [36] for fingerprint matching. Our automatic fingerprint verification algorithm instead is based on point pattern matching (minutiae matching). The reason for this choice is our need to design a robust, simple, and fast verification algorithm and to keep a small template size. A number of point pattern matching algorithms have been proposed in the literature [1], [55], [63], [66], [69], [71]. A general point matching problem is essentially intractable. Features associated with points and their spatial properties, such as the relative distances between points, are widely used in these algorithms to reduce the exponential number of search paths.

A. Alignment of Point Patterns

Ideally, two sets of planar point patterns can be aligned completely by only two corresponding point pairs. A true alignment between two point patterns can be obtained by testing all possible corresponding point pairs and selecting the optimal one. Due to the presence of noise and deformations, however, the input minutiae cannot always be aligned exactly with respect to those of the templates. To accurately recover pose transformations between two point patterns, a relatively large number of corresponding point pairs need to be used. This leads to a prohibitively large number of possible correspondences to be tested. Therefore, an alignment by corresponding point pairs is not practical even though it is feasible.

B. Aligned Point Pattern Matching

If two identical point patterns are exactly aligned with each other, then each pair of corresponding points are completely coincident. In such a case, point pattern matching can be simply achieved by counting the number of overlapping pairs. In practice, however, such a situation is not encountered. On the one hand, the error in determining and localizing minutiae hinders the alignment algorithm to recover the relative pose transformation exactly, while on the other hand, our alignment scheme described in Fig. 13 does not model the nonlinear deformation of fingerprints, which is an inherent property of fingerprint impressions.
IV. EXPERIMENTAL RESULTS

A. Feature-Extraction Performance

It is very difficult to assess the performance of feature-extraction algorithms independently. Accuracy of the extracted minutiae was subjectively confirmed in two ways. Visual inspection of a large number of typical minutiae-extraction results showed that our algorithm rarely missed minutiae in fingerprint images of reasonable quality.

B. System Performance

We have tested our system on the MSU fingerprint data base. It contains ten images (640x480) per finger from 70 individuals for a total of 700 fingerprint images, which were captured with a scanner manufactured by Digital Biometrics. When these fingerprint images were captured, no restrictions on the position and orientation of fingers were imposed.

C. Matching Scores

We first evaluated the matching scores of correct and incorrect matches. In test 1, each fingerprint in the MSU fingerprint data base was matched with all the other fingerprints in the data base. A matching was labeled correct if the matched fingerprint was from the same finger, and incorrect otherwise. A total of 489 300 (700x699) matchings were performed.

D. Authentication Test

In test 1, for each individual, we randomly selected three fingerprint images that passed the quality check as the template minutiae patterns for the individual and inserted them into the system data base. The major reason why we use three fingerprint templates is that a significant number of acquired fingerprint images from the same finger in the MSU data base do not have a sufficient amount of common region of interest due to the unrestricted acquisition process.

V. SUMMARY AND CONCLUSIONS

We have introduced an automatic identity-authentication system using fingerprints. The implemented minutiae-extraction algorithm is much more accurate and faster than our previous feature-extraction algorithm [58]. The proposed alignment-based elastic matching algorithm is capable of finding the correspondences between minutiae without resorting to an exhaustive search. The system types of inputs. It should not be confused with a practical system. In practice, a number of mechanisms need to be developed besides the minutiae extraction and minutiae matching. A biometric system based solely on a single biometric feature may not be able to meet the practical performance requirement in all aspects. By integrating two or more biometric features, overall verification performance may be improved. For example, it is well known that fingerprint verification tends to have a larger false reject rate due to the reasons discussed above, but it has a very low false accept rate. On the other hand, face recognition is not reliable in establishing the true identity but it is efficient in searching a large data base to find the top matches. By combining fingerprint matching and face recognition, the false reject rate may be reduced without sacrificing the false accept rate, and the system may then be able to operate in the identification mode. Currently, we are investigating a decision-fusion schema to integrate fingerprint and face.

The expected error rate of a deployed biometric system is usually a very small number (1%). To estimate such a small number reliably and accurately, large representative data sets that satisfy the two requirements mentioned in Section I are needed. Generally, under the assumption of statistical independence, the number of tests conducted should be larger than ten divided by the error rate [24]. Currently, we are evaluating the system on a large data set of live-scan fingerprint images.
REFERENCES


