Mr. Ratnakar anandrao kharade, Mr. M.S. Kumbhar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 6, November- December 2012, pp.303-311

An Identity-Authentication System Using Fingerprints

Mr.Ratnakar anandrao kharade [1], Mr. M.S. Kumbhar H.O.D. [2*]

[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 al-gorithm 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, dynamicprogramming, fingerprint iden-tification, 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 ªsomething that you know,º such as a personal identifica-tion number (PIN), or ªsomething that you have,º 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 per-son based on his physiological or behavioral characteristics. It relies on ªsomething that you areº 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 ªyes/noº personal identification like some of the traditional technologies, it can be used to achieve a ªpositive identificationº 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 aresomeotherimportantrequirements

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 inpractical systems [13], [18], [20], [53] or has the potential to become a valid biometric technique [53], not many ofthem are acceptable (in a court of law) as indisputable evidence of identity. For example, despite the fact thatextensive studies have been conducted on automatic face recognition and that a number of face-recognition systemsare 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 fingerprintidentification 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

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.

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 systemsused for physical access control alone is expected to expand to $100 million [53].

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].

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. Grew published a paper reporting his systematic study onthe ridge, furrow, and pore structure in fingerprints, which isbelieved to be the first scientific paper on fingerprints [42].Since then, a number of researchers have invested a hugeamount of effort in studying fingerprints. In 1788, a detaileddescription of the anatomical formations of fingerprints wasmade by Mayer [16], in which a number of fingerprintridge characteristics were identified. Starting from 1809, T.Bewick began to use his fingerprint as his trademark, whichis believed to be one of the most important contributions inthe early scientific study of fingerprint identification [42].Purkinje proposed the first fingerprint classification schemein 1823, which classified fingerprints into nine categoriesaccording to the ridge configurations [42]. H. Fauld, in1880, first scientifically suggested the individuality anduniqueness of fingerprints. At the same time, Herschelasserted that he had practiced fingerprint identification forapproximately 20 years [42]. This discovery established thefoundation of modern fingerprint identification. In the latenineteenth century, Sir F. Galton conducted an extensive
study of fingerprints [42]

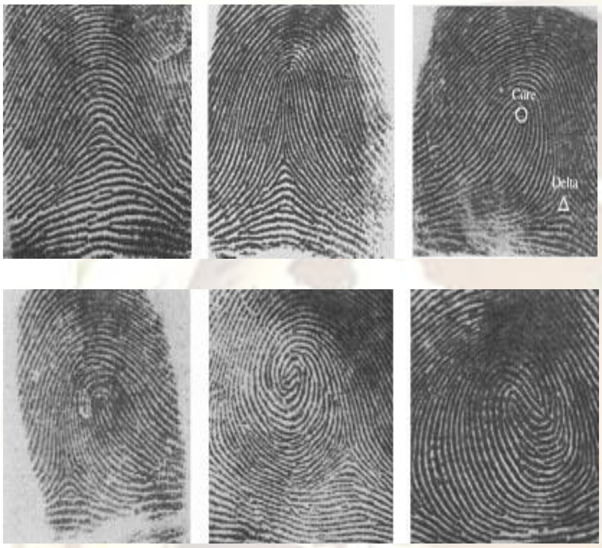


Fig. 2. Fingerprints and a fingerprint classification schema of six categories: (a) arch, (b) tented
arch, (c) right loop, (d) left loop, (e) whorl, and (f) twinloop. Critical points in a fingerprint, called
core and delta, are marked on (c).

C. Design of a Fingerprint-Verification System

An automatic fingerprint identity authentication systemhas 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 acquiredin the following way: a trained professional3 obtains animpression of an inked finger on a paper, and the impression is then scanned using a flat-bed document scanner. The livescanfingerprint is a collective term for a fingerprint imagedirectly obtained from the finger without the intermediatestep of getting an impression on a paper. Acquisition ofinked fingerprints is cumbersome; in the context of anidentity-authentication system, it is both infeasible and socially unacceptable for identity verification.4 The mostpopular 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 contactwith the platen while the valleys of the finger are not. The rest of the imaging system essentially consists of anassembly of a light emitting diode (LED) light source and a charge-couple device (CCD) placed on the other side ofthe glass platen. The laser light source illuminates the glass at a certain angle, and the camera is placed such that it cancapture the laser light reflected from the glass. The light that is incident on the plate at the glass surface touched bythe ridges is randomly scattered, while the light incident at the glass surface corresponding to valleys suffers totalinternal reflection, resulting in a corresponding fingerprint image on the imaging plane of the CCD.A number of other live-scan imaging methods are nowavailable, 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]. *) Representation (Template):* Which machine-readable representation completely captures the invariant anddiscriminatory information in a fingerprint image? This representation issue constitutes the essence of fingerprintverificationdesign and has far-reaching implications on the design of the rest of the system. The unprocessed grayscalevalues of the fingerprint images are not invariant over the time of capture.Representations based on the entire gray-scale profile ofa fingerprint image are prevalent among the verificationsystems using optical matching [4], [50]. The utility ofthe systems using such representation schemes, however,may be limited due to factors like brightness variations,image-quality variations, scars, and large global distortionspresent in the fingerprint image because these systems areessentially resorting to template-matching strategies for verification.Further, in many verification applications, terserrepresentations are desirable, which preclude representationsthat involve the entire gray-scale profile fingerprintimages. Some system designers attempt to circumvent thisproblem by restricting that the representation is derivedfrom a *small* (but consistent) part of the finger [50]. If thissame representation is also being used for identificationapplications, however, then the resulting systems mightstand a risk of restricting the number of unique identitiesthat could be handled simply because of the fact that thenumber of distinguishable templates is limited. On theother hand, an image-based representation makes fewerassumptions about the application domain (fingerprints) andtherefore has the potential to be robust to wider varieties offingerprint images. For instance, it is extremely difficult toextract a landmark-based representation from a (degenerate)finger devoid of any ridge structure. Typically, automatic fingerprint identification and authentication systems rely on representingthe two most prominent structures5: ridge endings and ridge bifurcations. Fig. 3 shows examples of ridgeendings and ridge bifurcations. These two structures are background-foreground duals of each other, and pressurevariations could convert one type of structure into the other. Therefore, many common representation schemesdo not distinguish between ridge endings and bifurcations. Both the structures are treated equivalently and arecollectively called minutiae. The simplest of the minutiaebased representations constitute a list of points defined bytheir spatial coordinates with respect to a fixed imagecentric coordinate system. Typically, though, these minimalminutiae-based representations are further enhanced by tagging each minutiae (or each combination of minutiae subset,e.g., pairs, triplets) with additional features. For instance, each minutiae could be associated with the orientation of theridge at that minutiae; or each pair of the minutiae could beassociated with the ridge count: the number of ridges visitedduring the linear traversal between the two minutiae. TheAmerican National Standards Institute–National Institute ofStandards and Technology (NIST) standard representationof a fingerprint is based on minutiae and includes minutiaelocation and orientation [2]. The minutiae-based representationmight also include one or more global attributes likeorientation of the finger, locations of core or delta,6 andfingerprint class. Our representation is minutiae based, and each minutiais described by its location (coordinates) and theorientation. We also store a short segment of the ridgeassociated with each minutia.

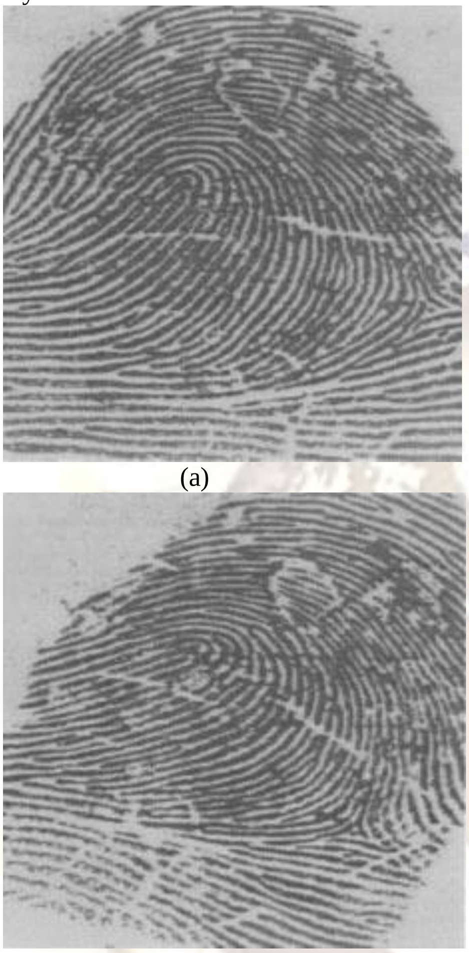
3) Feature Extraction*:* A feature extractor finds the ridgeendings and ridge bifurcations from the input fingerprint images. If ridges can be perfectly located in an input fingerprint image, then minutiae extraction is just a trivial task of extracting singular points in a thinned ridgemap. In practice, however, it is not always possible to obtain a perfect ridge map. The performance of currentlyavailable 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 phasetypically defines a metric of the similarity between two fingerprint representations. The matching stage also definesa threshold to decide whether a given pair of representationsare 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 pointpattern matching (minutiae pattern matching) problem. In

the ideal case, if 1) the correspondence between the templateminutiae 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, thenfingerprint 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 bya long duration of time, are indeed representing the same finger is an extremely difficult problem. Fig. 4 illustratesthe difficulty with an example of two images of the same finger. The difficulty can be attributed to two primaryreasons. First, if the test and reference representations are indeed mated pairs, the correspondence between the test andreference minutiae inthetwo representations isnot known.Second, the imaging system presents a number of peculiarand challenging situations, some of which are unique to afingerprint image capture scenario.1) *Inconsistent contact:* the act of sensing distorts thefinger. Determined by the pressure and contact of the finger on the glass platen, the three-dimensional shapeof the finger gets mapped onto the two-dimensional surface of the glass platen. Typically, this mappingfunction is uncontrolled

and results in different inconsistently mapped fingerprint images across theimpressions.2) *Nonuniform contact:* The ridge structure of a fingerwould be completely captured if ridges of the part of the finger being imaged are in complete opticalcontact with the glass platen. However, the dryness of



(a)

(b)

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 localizedand 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 orsemipermanently. This may introduce additional spurious minutiae.4) *Feature extraction artifacts:* The feature extractionalgorithm is imperfect and introduces measurement errors. Various image-processing operations mightintroduce inconsistent biases to perturb the location and orientation estimates of the reported minutiaefrom their gray-scale counterparts. 5) *Sensing act:* the act of sensing itself adds noise to theimage. For example, residues are leftover from theprevious fingerprint capture. A typical finger-imagingsystem distorts the image of the object being sensed due to imperfect imaging conditions. In the FTIRsensing scheme, for example, there is a geometric distortion because the image plane is not parallel tothe glass platen.In light of the operational environments mentioned above,the design of the matching algorithms needs to establish andcharacterize a realistic model of the variations among therepresentations of mated pairs. This model should includethe properties of interest listed below. a) The finger may be placed at different locations on theglass platen, resulting in a (global) translation of the minutiae from the test representation from those inthe reference representation.b) The finger may be placed in different orientations onthe glass platen, resulting in a (global) rotation of theminutiae from the test representation from that of thereference representation.c) The finger may exert a different (average) downwardnormal pressure on the glass platen, resulting in a(global) spatial scaling of the minutiae from the testrepresentation from those in the reference representation.d) The finger may exert a different (average) shear forceon the glass platen, resulting in a (global) sheartransformation (characterized by a shear direction andmagnitude) of the minutiae from the test representationfrom 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 test representations.g) Minutiae may be locally perturbed from their “true”location, and the perturbation may be different foreach individual minutiae. (Further, the magnitude ofsuch perturbation is assumed to be small and within a fixed number of pixels.)h) The individual perturbations among the correspondingminutiae could be relatively large (with respectto ridge spacings), but the perturbations among pairsof the minutiae are spatially linear.i) Theindividual perturbations among the correspondingminutiae could be relatively large (with respect to ridge spacings), but the perturbations among pairs ofthe minutiae are

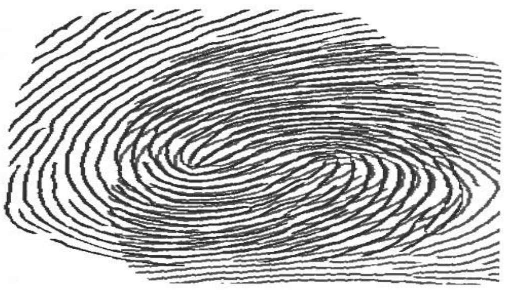


Fig. 5. Aligned ridge structures of mated pairs. Note that the best alignment in one part (top left)of the image results in a large displacements between the corresponding minutiae in the otherregions (bottom right).

spatially nonlinear.j) Only a (ridge) connectivity preserving transformationcould characterize the relationship between the testand reference representations [73].A matcher may rely on one or more of these assumptions,resulting in a wide spectrum of behavior. At the oneend of the spectrum, we have the "Euclidean" matchers,which allow only rigid transformations among the testand reference representations. At the other extreme, wehave a "topological" matcher, which may allow the mostgeneral transformations, including, say, order reversals.7The choice of assumptions often represents verificationperformance tradeoffs. Only a highly constrained systemwith not too demanding accuracies could get away with restrictive assumptions. A number of the matchers in theliterature assume similarity transformation [assumptions a),b), and c)]; they tolerate both spurious minutiae as wellas missing genuine minutiae. "Elastic" matchers in theliterature accommodate a small bounded local perturbationof minutiae from their true location but cannot handle largedisplacements of the minutiae from their true locations [59].Fig. 5 illustrates a typical situation of aligned ridgestructures of mated pairs. Note that the best alignment inone part (top left) of the image may result in a large amountof displacements between the corresponding minutiae in theother regions (bottom right). In addition, observe that thedistortion is nonlinear: given distortions at two arbitrarylocations on the finger, it is not possible to predict thedistortion at all of the intervening points on the linejoining the two points. In the authors' opinion, a good matcher needs to accommodate not only global similaritytransformations [assumptions a), b), and c)] but also shear transformation [assumption d)] and linear [assumption h)]

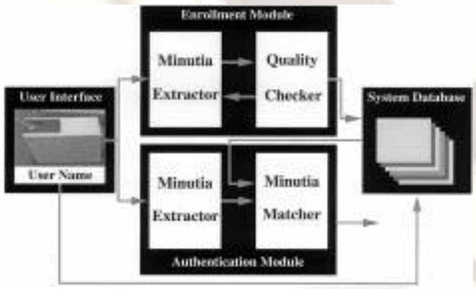


Fig. 6. Architecture of the automatic identity-authentication system.

And nonlinear [assumption i)] differential distortions. Inour experience, assumption j) is too general a model to characterize the impressions of a finger, and its inclusioninto the matcher design may compromise efficiency and discriminatory power of the matcher. In addition, the matchersbased on such assumptions need to use connectivityinformation, which is notoriously difficult to extract fromfingerprint images of poor quality.

D. An Automatic Identity-Authentication SystemWe will introduce a prototype automatic identity authentication system, which is capable of automatically authenticatingthe identity of an individual using fingerprints. Currently, it is mainly intended for user authentication.For example, our system can be used to replace password authentication during the log-in session in a multiusercomputing environment.

II. MINUTIAE EXTRACTION

Fingerprint authentication is based on the matching ofminutiae patterns. A reliable minutiae-extraction algorithm is critical to the performance of an automatic identityauthenticationsystem using fingerprints. In our system, we have developed a minutiae-extraction algorithm thatis an improved version of the technique described in [58]. Experimental results show that this algorithm performsvery well in operation. The overall flowchart of this algorithm is depicted in Fig. 7. It mainly consists ofthree 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 theresolution of input fingerprint images is 500 dots per inch.

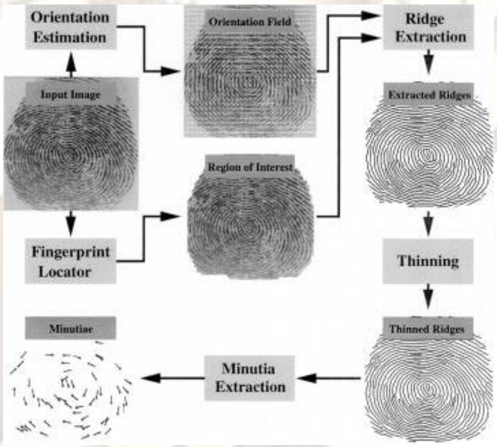


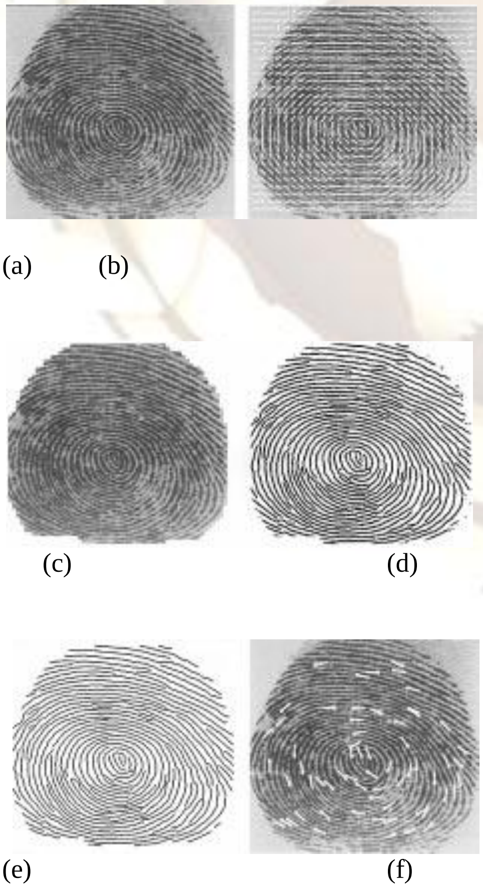
Fig. 7. Flowchart of the minutiae-extraction algorithm.

A. Orientation Field Estimation

The orientation field of a fingerprint image representsthe intrinsic nature of the fingerprint image. It plays a veryimportant role in fingerprint-image analysis. A number ofmethods have been proposed to estimate the orientationfield of fingerprint images [38], [40], [56]. In our system, anew hierarchical implementation of the algorithm proposedin [56] is used (Fig. 8). With this algorithm, a fairly smoothorientation-field estimate can be obtained. Fig. 9 shows theorientation field of a fingerprint image estimated with ourhierarchical algorithm.After the orientation field of an input fingerprint image is estimated, a segmentation algorithm, which is based onthe local certainty level of the orientation field, is used to locate the region of interest within the input fingerprintimage. 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 veryimportant role in fingerprint-image analysis. A number of methods have been proposed to estimate the orientationfield of fingerprint images [38], [40], [56]. In our system, a new hierarchical implementation of the algorithm proposedin [56] is used (Fig. 8). With this algorithm, a fairly smoothorientation-field estimate can be obtained. Fig. 9 shows theorientation field of a fingerprint image estimated with ourhierarchical algorithm.

III. MINUTIAE MATCHING

Fingerprint matching has been approached from several different strategies, like image-based [4], [50] and ridgepattern matching of fingerprint representations. There also exist graph-based schemes [22], [23], [26], [27], [34], [36] for fingerprint matching. Our automatic fingerprintverification 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) (b)

(c) (d)

(e) (f)

ithm on a fingerprint image (512 _ 512) captured with an inkless scanner. (a) Input image. (b) Orientation field superimposed on the input image. (c) Fingerprint region. (d) Extracted ridges. (e) Thinned ridge map. (f) Extracted minutiae and their orientations superimposed on the input image.

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.

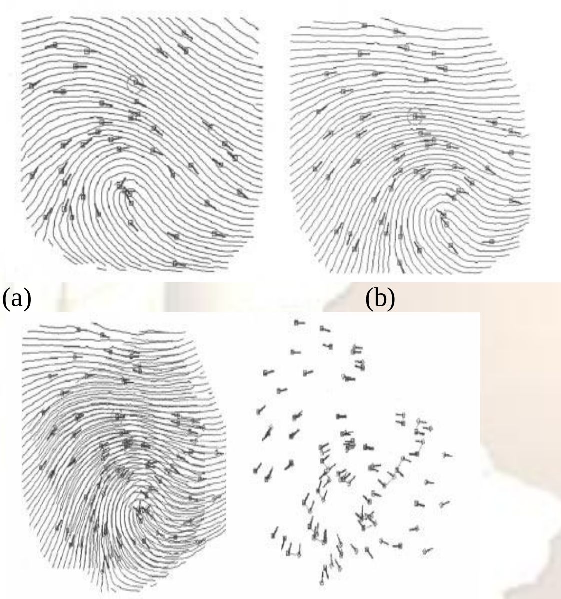
IV. EXPERIMENTAL RESULTS

A. Feature-Extraction Performance

It is very difficult to assess the performance of featureextraction algorithms independently. Accuracy of the extracted minutiae was subjectively confirmed in two ways. Visual inspection of a large number of typical minutiaeextraction 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 (640 480) 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.



(a) (b)

(c)

(d)

Fig. 15. Results of applying the matching algorithm to an input minutiae set and a template. (a) Input minutiae set. (b) Template minutiae set. (c) Alignment result based on the minutiae marked with green circles. (d) Matching result where template minutiae and their correspondences are connected by green lines.

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 (700x 699) 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 weuse 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 minutiaeextraction 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

[1] N. Ansari, M. H. Chen, and E. S. H. Hou, “A genetic algorithm for point pattern matching,” in *Dynamic, Genetic, and Chaotic Programming*, B. Souˆcek and the IRIS Group, Eds. New York: Wiley, 1992, ch. 13.

[2] “American national standard for information systems—Data format for the interchange of fingerprint information,” American National Standards Institute, New York, NY, Doc. No.ANSI/NIST-CSL 1-1993.

[3] J. Atick, P. Griffin, and A. Redlich, “Statistical approach to shape from shading: Reconstruction of 3D face surfaces from single 2D images,” *Neural Computation*, to be published.

[4] R. Bahuguna, “Fingerprint verification using hologram matched filterings,” in *Proc. Biometric Consortium Eighth Meeting*, San Jose, CA, June 1996.

[5] H. Baird, *Model Based Image Matching Using Location*. Cambridge, MA: MIT Press, 1984.

[6] D. H. Ballard, “Generalized Hough transform to detect arbitrary patterns,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. PAMI-3, no. 2, pp. 111–122, 1981.

[7] MFLOPS Benchmark Results. (Feb. 1997.) [Online]. Available: ftp://ftp.nosc.mil/pub/aburto/_flops_1.tbl.

[8] T. Biggs, personal communication, Department of Immigration and Naturalization Services, 1997.

[9] F. Bouchier, J. S. Ahrens, and G. Wells. (1996). Laboratory evaluation of the iriscan prototype biometric identifier. [Online].Available:http://infoserve.library.sandia.gov/sand_doc/1996/ 961033.pdf.

[10] J. P. Campbell, Jr., L. A. Alyea, and J. S. Dunn. (1996). Biometric security: Government applications and operations. [Online]. Available: http://www.vitro.bloomington.in.us:8080/ BC/.

[11] J. Canny, “A computational approach to edge detection,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. PAMI-8, no. 6, pp. 679–698, 1986.

[12] G. T. Candela, P. J. Grother, C. I. Watson, R. A. Wilkinson, and C. L. Wilson, “PCASYS: A pattern-level classification automation system for fingerprints,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Tech. Rep. NISTIR 5647, Aug. 1995.

[13] R. Clarke, “Human identification in information systems: Management challenges and public policy issues,” *Info. Technol.People*, vol. 7, no. 4, pp. 6–37, 1994.

[14] L. Coetzee and E. C. Botha, “Fingerprint recognition in low quality images,” *Pattern Recognit.*, vol. 26, no. 10, pp. 1441–1460, 1993.

[15] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*. New York: McGraw-Hill, 1990.