2 FINGERPRINT VERIFICATION

Lawrence O'Gorman
Veridicom Inc.
Chatham, NJ
log@veridicom.com

Abstract *The use of fingerprints for identification has been employed in law enforcement for about a century. A much broader application of fingerprints is for personal authentication, for instance to access a computer, a network, a bank-machine, a car, or a home. The topic of this chapter is fingerprint verification, where "verification" implies a user matching a fingerprint against a single fingerprint associated with the identity that the user claims. The following topics are covered: history, image processing methods, enrollment and verification procedures, system security considerations, recognition rate statistics, fingerprint capture devices, combination with other biometrics, and the future of fingerprint verification.*

Keywords: *fingerprint verification, fingerprint matching, biometric, image enhancement, image filtering, feature detection, minutiae, security, fingerprint sensor.*

1. Introduction[1]

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. However, this widespread use of fingerprints has been and still is largely for law enforcement applications. There is expectation that a recent combination of factors will favor the use of fingerprints for the much larger market of personal authentication. These factors include: small and inexpensive fingerprint capture devices, fast computing hardware, recognition rate and speed to meet the needs of many applications, the explosive growth of network and Internet transactions, and the heightened awareness of the need for ease-of-use as an essential component of reliable security.

This chapter contains an overview of fingerprint verification methods and related issues. We first describe fingerprint history and terminology. Digital image processing

[1] Portions of this chapter have previously appeared in, L. O'Gorman, "Overview of fingerprint verification technologies," *Elsevier Information Security Technical Report,* Vol. 3, No. 1, 1998.

methods are described that take the captured fingerprint from a raw image to match result. Systems issues are discussed including procedures for enrollment, verification, spoof detection, and system security. Recognition statistics are discussed for the purpose of comparing and evaluating different systems. We describe different fingerprint capture device technologies. We consider fingerprints in combination with other biometrics in a multi-modal system and finally look to the future of fingerprint verification.

It is necessary to state at the onset that there are many different approaches used for fingerprint verification. Some of these are published in the scientific literature, some published only as patents, and many are kept as trade secrets. We attempt to cover what is publicly known and used in the field, and cite both the scientific and patent literature. Furthermore, while we attempt to be objective, some material is arguable and can be regarded that way.

2. History

There is archaeological evidence that fingerprints as a form of identification have been used at least since 7000 to 6000 BC by the ancient Assyrians and Chinese. Clay pottery from these times sometimes contain fingerprint impressions placed to mark the potter. Chinese documents bore a clay seal marked by the thumbprint of the originator. Bricks used in houses in the ancient city of Jericho were sometimes imprinted by pairs of thumbprints of the bricklayer. However, though fingerprint individuality was recognized, there is no evidence this was used on a universal basis in any of these societies.

In the mid-1800's scientific studies were begun that would established two critical characteristics of fingerprints that are true still to this day: no two fingerprints from different fingers have been found to have the same ridge pattern, and fingerprint ridge patterns are unchanging throughout life. These studies led to the use of fingerprints for criminal identification, first in Argentina in 1896, then at Scotland Yard in 1901, and to other countries in the early 1900's.

Computer processing of fingerprints began in the early 1960s with the introduction of computer hardware that could reasonably process these images. Since then, automated fingerprint identification systems (AFIS) have been deployed widely among law enforcement agencies throughout the world.

In the 1980s, innovations in two technology areas, personal computers and optical scanners, enabled the tools to make fingerprint capture practical in non-criminal applications such as for ID-card programs. Now, in the late 1990s, the introduction of inexpensive fingerprint capture devices and the development of fast, reliable matching algorithms has set the stage for the expansion of fingerprint matching to personal use.

Why include a history of fingerprints in this chapter? This history of use is one that other types of biometric do not come close to. Thus there is the experience of a century of forensic use and hundreds of millions of fingerprint matches by which we can say with some authority that fingerprints are unique and their use in matching is extremely reliable. For further historical information, see [2].

3. Matching: Verification and Identification

Matching can be separated into two categories: verification and identification. *Verification* is the topic of this chapter. It is the comparison of a *claimant* fingerprint against an *enrollee* fingerprint, where the intention is that the claimant fingerprint matches the enrollee fingerprint. To prepare for verification, a person initially enrolls his or her fingerprint into the verification system. A representation of that fingerprint is stored in some compressed format along with the person's name or other identity. Subsequently, each access is authenticated by the person identifying him or herself, then applying the fingerprint to the system such that the identity can be verified. Verification is also termed, *one-to-one matching*.

Identification is the traditional domain of criminal fingerprint matching. A fingerprint of unknown ownership is matched against a database of known fingerprints to associate a crime with an identity. Identification is also termed, *one-to-many matching*.

There is an informal third type of matching that is termed *one-to-few matching*. This is for the practical application where a fingerprint system is used by "a few" users, such as by family members to enter their house. A number that constitutes "few" is usually accepted to be somewhere between 5 and 20.

4. Feature Types

The lines that flow in various patterns across fingerprints are called *ridges* and the spaces between ridges are *valleys*. It is these ridges that are compared between one fingerprint and another when matching. Fingerprints are commonly matched by one (or both) of two approaches. We describe the fingerprint features as associated with these approaches.

The more microscopic of the approaches is called *minutia matching*. The two minutia types that are shown in Figure 2.1 are a ridge *ending* and *bifurcation*. An ending is a feature where a ridge terminates. A bifurcation is a feature where a ridge splits from a single path to two paths at a Y-junction. For matching purposes, a minutia is attributed with features. These are type, location *(x, y)*, and direction (and some approaches use additional features).

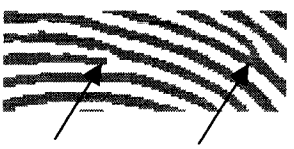

Figure 2.1 Fingerprint minutiae: ending and bifurcation.

The more macroscopic approach to matching is called *global pattern matching* or simply *pattern matching*. In this approach, the flow of ridges is compared at all locations between a pair of fingerprint images. The ridge flow constitutes a global pattern of the fingerprint. Three fingerprint patterns are shown in Figure 2.2. (Different classification schemes can use up to ten or so pattern classes, but these three are the basic patterns.)

Two other features are sometimes used for matching: *core* and *delta*. (Figure 2.2.) The core can be thought of as the center of the fingerprint pattern. The delta is a singular point from which three patterns deviate. The core and delta locations can be used as landmark locations by which to orient two fingerprints for subsequent matching – though these features are not present on all fingerprints.

There may be other features of the fingerprint that are used in matching. For instance, pores can be resolved by some fingerprint sensors and there is a body of work (mainly research at this time) to use the position of the pores for matching in the same manner that the minutiae are used. Size of the fingerprint, and average ridge and valley widths can be used for matching, however these are changeable over time. The

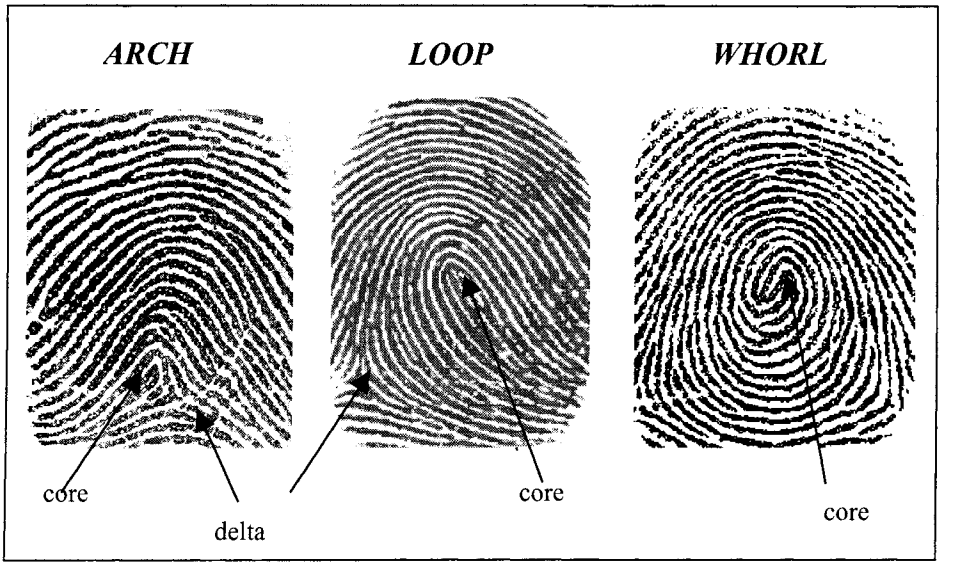

Figure 2.2 Fingerprint patterns: arch, loop, and whorl. Fingerprint landmarks are also shown: core and delta. (No delta locations fall within the captured area of the whorl here.)

positions of scars and creases can also be used, but are usually not used because they can be temporary or artificially introduced.

5. Image Processing and Verification

Following image capture to obtain the fingerprint image, image processing is performed. The ultimate objective of image processing is to achieve the best image by which to produce the correct match result. The image processing steps are the following: image noise reduction and enhancement, feature detection, and matching.

This section is organized to describe first the sequence of processing and verification via a "common" minutia-based approach. This is described without variants and optional methods (of which there are many) for the sake of reading flow and simplicity. It is important to note that, though many researchers and product developers follow this approach, all do not, and even the choice of what constitutes "common" may be contentious. In the final subsections of this section, variations of this approach, both minutia-based and non-minutia-based, are described.

Image Specifications

Depending upon the fingerprint capture device, the image can have a range of specifications. Commonly, the pixels are 8-bit values, and this yields an intensity range from 0 to 255. The image resolution is the number of pixels per unit length, and this ranges from 250 dots per inch (100 dots per centimeter) to 625 dots per inch (250 dots per centimeter), with 500 dots per inch (200 dots per centimeter) being a common standard. The image area is from 0.5 inches square (1.27 centimeter) to 1.25 inches (3.175 centimeter), with 1 inch (2.54 centimeter) being the standard. We discuss more on image capture devices in Section 8.

Image Enhancement

A fingerprint image is one of the noisiest of image types. This is due predominantly to the fact that fingers are our direct form of contact for most of the manual tasks we perform: finger tips become dirty, cut, scarred, creased, dry, wet, worn, etc. The image enhancement step is designed to reduce this noise and to enhance the definition of ridges against valleys. Two image processing operations designed for these purposes are the adaptive, matched filter and adaptive thresholding. The stages of image enhancement, feature detection, and matching are illustrated in Figure 2.3.

There is a useful side to fingerprint characteristics as well. That is the "redundancy" of parallel ridges. Even though there may be discontinuities in particular ridges, one can always look at a small, local area of ridges and determine their flow. We can use this "redundancy of information" to design an adaptive, matched filter. This filter is applied to every pixel in the image (spatial convolution is the technical term for this operation). Based on the local orientation of the ridges around each pixel, the matched filter is applied to enhance ridges oriented in the same direction as those in the same locality, and decrease anything oriented differently. The latter includes noise that may be joining adjacent ridges, thus flowing perpendicular to the local flow. These incorrect "bridges" can be eliminated by use of the matched filter. Figure 2.3(b) shows an orientation map where line sectors represent the orientation of ridges in each locality. Thus, the filter is adaptive because it orients

itself to local ridge flow. It is matched because it should enhance – or match – the ridges and not the noise.

After the image is enhanced and noise reduced, we are ready to extract the ridges. Though the ridges have gradations of intensity in the original grayscale image, their true information is simply binary: ridges against background. Simplifying the image to this binary representation facilitates subsequent processing. The binarization operation takes as input a grayscale image and returns a binary image as output. The image is reduced in intensity levels from the original 256 (8-bit pixels) to 2 (1-bit pixels).

The difficulty in performing binarization is that all the fingerprint images do not have the same contrast characteristics, so a single intensity threshold cannot be chosen. Furthermore, contrast may vary within a single image, for instance if the finger is pressed more firmly at the center. Therefore, a common image processing tool is used, called locally adaptive thresholding. This operation determines thresholds adaptively to the local image intensities. The binarization result is shown in Figure 2.3(c).

The final image processing operation usually performed prior to minutia detection is thinning. Thinning reduces the widths of the ridges down to a single pixel. See Figure 2.3(d). It will be seen in the next section how these single-pixel width ridges facilitate the job of detecting endings and bifurcations. A good thinning method will reduce the ridges to single-pixel width while retaining connectivity and minimizing the number of artifacts introduced due to this processing. These artifacts are comprised primarily of spurs, which are erroneous bifurcations with one very short branch. These artifacts are removed by recognizing the differences between legitimate and erroneous minutiae in the feature extraction stage described below.

Image enhancement is a relatively time-consuming process. A 500x500-pixel fingerprint image has 250,000 pixels; several multiplications and other operations are applied at each pixel. Both matched filtering and thinning contribute largely to this time expenditure. Consequently, many fingerprint systems are designed to conserve operations at this stage to reach a match result more quickly. This is not a good tradeoff. The results of all subsequent operations depend on the quality of the image as captured by the sensor and as processed at this stage. Economizing for the sake of speedup will result in degraded match results, which in turn will result in repeated attempts to verify or false rejections. Therefore, it is our contention that a system offering reasonable speed with a correct answer is much better than a faster system that yields poorer match results.

Feature Extraction

The fingerprint minutiae are found at the feature extraction stage. Operating upon the thinned image, the minutiae are straightforward to detect. Endings are found at termination points of thin lines. Bifurcations are found at the junctions of three lines. See Figure 2.3(e).

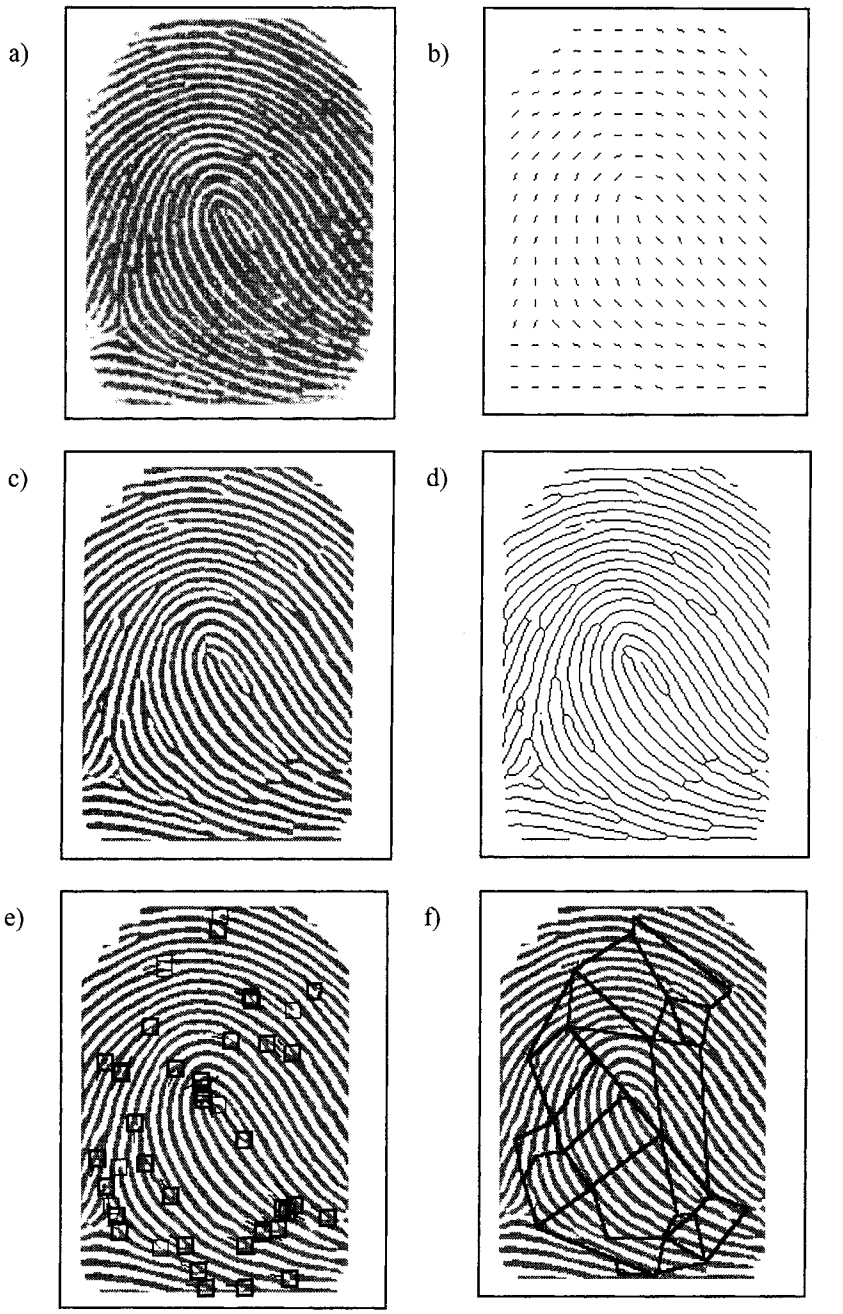

Figure 2.3 Sequence of fingerprint processing steps: a) original, b) orientation, c) binarized, d) thinned, e) minutiae, f) minutia graph.

There will always be extraneous minutiae found due to a noisy original image or due to artifacts introduced during matched filtering and thinning. These extraneous features are reduced by using empirically determined thresholds. For instance, a bifurcation having a branch that is much shorter than an empirically determined threshold length is eliminated because it is likely to be a spur. Two endings on a very short isolated line are eliminated because this line is likely due to noise. Two endings that are closely opposing are eliminated because these are likely to be on the same ridge that has been broken due to a scar or noise or a dry finger condition that results in discontinuous ridges. Endings at the boundary of the fingerprint are eliminated because they are not true endings but rather the extent of the fingerprint in contact with the capture device.

Feature attributes are determined for each valid minutia found. These consist of: ridge ending or bifurcation type, the *(x,y)* location, and the direction of the ending or bifurcation. Although minutia type is usually determined and stored, many fingerprint matching systems do not use this information because discrimination of one from the other is often difficult.

The result of the feature extraction stage is what is called a *minutia template*. This is a list of minutiae with accompanying attribute values. An approximate range on the number of minutiae found at this stage is from 10 to 100. If each minutia is stored with type (1 bit), location (9 bits each for x and y), and direction (8 bits), then each will require 27 bits – say 4 bytes – and the template will require up to 400 bytes. It is not uncommon to see template lengths of 1024 bytes.

Verification

At the verification stage, the template from the claimant fingerprint is compared against that of the enrollee fingerprint. This is done usually by comparing neighborhoods of nearby minutiae for similarity. A single neighborhood may consist of three or more nearby minutiae. Each of these is located at a certain distance and relative orientation from each other. Furthermore, each minutia has its own attributes of type (if it is used) and minutia direction, which are also compared. If comparison indicates only small differences between the neighborhood in the enrollee fingerprint and that in the claimant fingerprint, then these neighborhoods are said to match. This is done exhaustively for all combinations of neighborhoods and if enough similarities are found, then the fingerprints are said to match. Template matching can be visualized as graph matching, that is comparing the shapes of graphs joining fingerprint minutiae. This is illustrated in Figure 2.3(f).

Note that the word, "similar" is used in the paragraph above instead of "same". Neighborhoods will rarely match exactly because of two factors. One is the noisy nature of a fingerprint image. The other is that the skin is an elastic surface, so distances and minutia directions will vary.

One result of the verification stage is a match score, usually a number between 0 and 1 (or 10 or 100). Higher values in the range indicate higher confidence in a match. This match score is then subject to a user-chosen threshold value. If the score is greater than the threshold, the match result is said to be true (or 1) indicating a correct

verification, otherwise the match is rejected and the match result is false (or 0). This threshold can be chosen to be higher to achieve greater confidence in a match result, but the price to pay for this is a greater number of false rejections. Conversely, the threshold can be chosen lower to reduce the number of false rejections, but the price to pay in this case is a greater number of false acceptances. The trade-off between false acceptance and false rejection rates is further discussed in Section 7.

The user has control of only one parameter, the threshold, for most commercial verification products. This customization procedure is called *back-end adjustment*, because a match score is calculated first and a threshold can be chosen after to determine the match result. There are systems that, in addition to offering back-end adjustment, offer *front-end adjustment* as well. This enables the user to adjust some of the parameter values before the match score is calculated, then to adjust the threshold after. Systems with front-end adjustment offer more versatility in obtaining the best results for different conditions, but are more complex for the user to adjust. This is why, for most systems, the vendor sets the optimum front-end parameter values and the user has control only of the matching threshold value via back-end adjustment.

Identification and One-to-Few Matching

Although the emphasis in this chapter is verification, we briefly mention identification and one-to-few matching methods. For identification, the objective is to determine a match between a test fingerprint and one of a database of fingerprints whose size may be as high as 10,000 to tens of millions. One cannot simply apply the verification techniques just described to all potential matches because of the prohibitive computation time required. Therefore, identification is usually accomplished as a two-step process. Fingerprints in the database are first categorized by pattern type, or *binned*. The same is done for the test fingerprint. Pattern comparison is done between test fingerprint and database fingerprints. This is a fast process that can be used to eliminate the bulk of non-matches. For those fingerprints that closely match in pattern, the more time-consuming process of minutia-based verification is performed.

One-to-few matching is usually accomplished simply by performing multiple verifications of a single claimant fingerprint against the 5 to 20 potential matches. Thus the execution time is linear in the number of potential matches. This time requirement becomes prohibitive if "few" becomes too large, then an approach akin to identification must be used.

Variations on the Common Approach: Other Methods

Since one of the most vexing challenges of fingerprint processing is obtaining a clean image upon which to perform matching, there are various methods proposed to perform image enhancement. Most of these involve filtering that is adaptively matched to the local ridge orientations [23, 19, 25, 22, 24, 37, 26, 27, 14]. The orientation map is first determined by dividing the image into windows (smaller regions) and calculating the local ridge orientations within these. The orientation can

be determined in each window by spatial domain processing or by frequency domain processing after transformation by a 2-dimensional fast Fourier transform.

After image enhancement and binarization of the fingerprint image, thinning is usually performed on the ridges. However, a different approach eliminates the binarization and thinning stages (both computationally expensive and noise producing) [20]. This approach involves tracing ridges not from the binary or thinned image, but from the original grayscale image. The result of grayscale ridge-following is the endpoint and bifurcation minutiae similar to the common approach.

Instead of using only a single size window to determine the orientation map, multiple window sizes can be used via a multi-resolution approach [24, 15]. Local orientation values are determined first throughout the image at a chosen, initial resolution level – that is a chosen window size of pixels within which the orientation is calculated. A measure of consistency of the orientation in each window is calculated. If the consistency is less than a threshold, the window is divided into four smaller sub-windows and the same process is repeated until consistency is above threshold for each window or sub-window. This multi-resolution process is performed to avoid smoothing over small areas of local orientation, as will be the case especially at the fingerprint core.

Because of the difficulty of aligning minutiae of two fingerprints, neighborhood matching was one of the earliest methods of facilitating a match [28, 1, 42]. Groups of neighboring minutiae are identified in one fingerprint, usually two to four minutiae to a neighborhood, and each of these is compared against prospective neighborhoods of another fingerprint. There are two levels to matching. One is matching the configurations of minutiae within a neighborhood against another neighborhood. The other is matching the global configurations formed by the separate neighborhoods between enroll and verify fingerprints.

Because it is time-consuming to compare all neighborhood combinations between enroll and verify fingerprints, methods have been proposed to align the fingerprints to reduce the number of comparisons. A common method, and also a traditional method used for visual matching, is to locate a core and delta and align the fingerprints based on these landmarks [29]. The core and delta are usually found on the basis of their position with respect to the ridge flow, therefore the orientation map is determined and used for this [41]. An elegant method to locate singular points in a flow field is the Poincaré index [17, 36, 16]. For each point in the orientation map, the orientation angles are summed for a closed curve in a counter-clockwise direction around that point. For non-singular points, the sum is equal to 0 degrees; for the core, the sum is equal to 180 degrees; for a delta, the sum is equal to –180 degrees.

Other methods have been proposed to reduce the computational load of minutia matching. One approach is to sort the list of minutiae in some order conducive to efficient comparisons prior to matching. (This is especially appropriate for one-to-many matching, since sorting is done once per fingerprint, but matching many times.) A linearly sorted list of minutiae can be compiled by scanning the fingerprint from a selected center point outward by a predetermined scanning trajectory such as a spiral [39]. In this way, one-dimensional vectors of minutiae, including their characteristics, can be compared between enroll and verify fingerprints. Another method to linearize the minutia comparison is the "hyperladder" matcher [11]. This hyperladder is constructed sequentially by comparing minutia pairs in enroll and verify fingerprints

and adding more rungs as consecutive neighboring minutiae match. In another approach, an attributed graph can be constructed where branches constitute nearest-neighbor minutiae and these emanate like "stars" on the graph [10]. These stars are compared between fingerprint pairs, the number of matching branches constituting the degree of confidence in the match.

Because there is so little discriminating information at a single minutia (even the type is unreliable), a different approach is to describe minutiae by more features [47, 40]. For instance, a minutia can be described by the length and curvature of the ridge it is on and of similar features on neighboring ridges.

Variations on the Common Approach: Correlation Matching

This discussion of matching has been minutia-focused to this point, to the exclusion of the global pattern matching approach mentioned in Section 4. Instead of using minutiae, some systems perform matches on the basis of the overall ridge pattern of the fingerprint. This is called *global matching*, *correlation*, or simply *image multiplication* or *image subtraction.*

It is visibly apparent that a pair of fingerprints of different pattern types, for instance whorl and arch, does not match. Global matching schemes go beyond the simple (and few) pattern categories to differentiate one whorl from a different whorl, for instance. Simplistically, this can be thought of as a process of aligning two fingerprints and subtracting them to see if the ridges correspond. There are four potential problems (corresponding to three degrees of freedom and another factor).

1. The fingerprints will likely have different locations in their respective images (translational freedom). We can establish a landmark such as a core or delta by which to register the pair, however if these are missing or not found reliably, subsequent matching steps will fail.

2. The fingerprints may have different orientations (rotational freedom). If a proper landmark has been found in (1), the fingerprint can be rotated around this, but this is error-prone, computationally expensive, or both. It is error-prone because the proper center of rotation depends on a single, reliably determined landmark. It is computationally expensive because performing correlation for many orientations involves repeatedly processing the full image.

3. Because of skin elasticity (non-linear warping), even if matching fingerprints are registered in location and orientation, all sub-regions may not align.

4. Finally, there is the inevitable problem of noise. Two images of matching fingerprints will have different image quality, ridges will be thicker or thinner, discontinuities in ridges will be different depending on finger dryness, the portion of the fingerprint captured in each image will be different, etc.

The descriptions below are more sophisticated modifications and extensions to the basic correlation approach to deal with the problems listed.

Strictly speaking, correlation between two images involves translating one image over another and performing multiplication of each corresponding pixel value at each translation increment [38]. When the images correspond at each pixel, the sum of these multiplications is higher than if they do not correspond. Therefore, a matching

pair will have a higher correlation result than a non-matching pair. A threshold is chosen to determine whether a match is accepted, and this can be varied to adjust the false acceptance rate versus false rejection rate tradeoff similarly to the case for minutia matching.

Correlation matching can be performed in the spatial frequency domain instead of in the spatial domain as just described [12]. The first step is to perform a 2-dimensional fast Fourier transform (FFT) on both the enrollee and claimant images. This operation transforms the images to the spatial frequency domain. The two transformed images are multiplied pixel-by-pixel, and the sum of these multiplications is equivalent to the spatial domain correlation result. An advantage of performing frequency domain transformation is that the fingerprints become translation-independent; that is, they do not have to be aligned translationally because the origin of both transformed images is the zero-frequency location, (0,0). There is a trade-off to this advantage however, that is the cost of performing the 2-dimensional FFT.

Frequency domain correlation matching can be performed optically instead of digitally [43, 44, 21]. This is done using lenses and a laser light source. Consider that a glass prism separates projected light into a color spectrum, that is it performs frequency transformation. In a similar manner, the enrollee and claimant images are projected via laser light through a lens to produce their Fourier transform. Their superposition leads to a correlation peak whose magnitude is high for a matching pair and lower otherwise. An advantage of optical signal processing is that operations occur at the speed of light, much more quickly than for a digital processor. However, the optical processor is not as versatile – as programmable – as a digital computer, and because of this few or no optical computers are used in commercial personal verification systems today.

One modification of spatial correlation is to perform the operation not upon image pixels but on grids of pixels or on local features determined within these grids [8, 6]. The enrollee and claimant fingerprint images are first aligned, then (conceptually) segmented by a grid. Ridge attributes are determined in each grid square: average pixel intensity, ridge orientation, periodicity, or number of ridges per grid. Corresponding grid squares are compared for similar attributes. If enough of these are similar, then this yields a high match score and the fingerprints are said to match.

The relative advantages and disadvantages between minutia matching and correlation matching differ between systems and algorithmic approaches. In general, minutia matching is considered by most to have a higher recognition accuracy. Correlation can be performed on some systems more quickly than minutia matching, especially on systems with vector-processing or FFT hardware. Correlation matching is less tolerant to elastic, rotational, and translational variances of the fingerprint and of extra noise in the image.

6. Systems Issues

The effectiveness of a complete fingerprint verification system depends on more than the verification algorithms just described. There are other, higher level considerations, which we will call systems issues. These include enrollment and verification

procedures, speed and ergonomics, user-feedback, anti-spoofing, and security considerations.

It is essential to the goal of high recognition rate that the enrollment procedure results in the capture of the highest quality fingerprint image(s) obtainable because enrollment occurs once while verification occurs many times. Therefore, a well-designed verification system will require the user to go through more time and effort for enrollment than for verification. A fingerprint may be captured multiple times and the best taken or some combination of each taken as the enrolled fingerprint.

There are options in the design of the verification procedure as well. The fingerprint can be captured once or a few times until a positive match is made. A procedure such as this will decrease false rejections, but increase false acceptances. Verification can be performed on not just one, but two or more fingers. This will enhance the recognition rate, however it will also cause the user to expend more time.

System ergonomics are important. For instance, there are limits to the amount of time that a person is willing to wait in personal authentication applications. That amount of time varies with the particular application and depends on what the person is also doing during processing, for instance swiping a bankcard or entering an identification number. Between 0.5 and 1 second are usually regarded as an acceptable range for processing time. Other user ergonomics considerations include: the number of repeated attempts in case of false rejections, the procedures for enrollment and verification, the design of the capture device, and the recognition setting that determines the trade-off between false acceptance and false rejection.

Quality feedback is useful when an image is captured to indicate to the user how to place the finger for the best possible image quality. The type of feedback includes: "finger is placed too high", "finger is not pressed hard enough", etc.

Anti-spoofing deterrents must be built into a fingerprint system to prevent use of an artificial fingerprint, a dead finger, or latent fingerprint. A latent fingerprint sometimes remains on a sensor surface due to skin oil residue from the previously applied fingerprint. Countermeasures are built into some sensors, such as the ability to distinguish true skin temperature, resistance, or capacitance.

Since the fingerprint system is only as secure as its weakest link, a complete, secure system must be designed. For instance, minutia templates must be secured by some means such as encryption to prevent impostors from inserting their templates into the database in place of properly enrolled users. The end result of fingerprint verification is a "yes" or "no" that is used to gain access. If it is simple just to circumvent the fingerprint system to send a "yes", then the system provides little security. A solution to this problem is to ensure that the host receiving the recognition decision knows that this is from the trusted client, such as by digitally signing the information passed to the host. (For further information on encryption, see reference [33].)

7. Recognition Rate

Terminology and Measurement

The ultimate measure of utility of a fingerprint system for a particular application is recognition rate. This can be described by two values. The *false acceptance rate (FAR)* is the ratio of the number of instances of pairs of different fingerprints found to (erroneously) match to the total number of match attempts. The *false rejection rate (FRR)* is the ratio of the number of instances of pairs of the same fingerprint are found not to match to the total number of match attempts. FAR and FRR trade off against one another. That is, a system can usually be adjusted to vary these two results for the particular application, however decreasing one increases the other and vice versa. FAR is also called, *false match rate* or *Type II error*, and FRR is also called *false non-match rate* or *Type I error*. These are expressed as values in [0, 1] interval or as percentage values.

The ROC-curve plots FAR versus FRR for a system. (ROC stands for Receiver Operating Curve for historical reasons. Yes, "ROC-curve" is redundant, but this is the common usage.) ROC-curves are shown in Figure 2.4. The FAR is usually plotted on the horizontal axis as the independent variable. The FRR is plotted on the vertical axis as the dependent variable. Because of the range of FAR values, this axis is often on a logarithmic scale. Figure 2.4 contains two solid curves and three dotted curves. The solid curves do not represent any particular data; they are included for illustrative purposes to show better and worse curve placements. The typical ROC-curve has a shape whose "elbow" points toward (0,0) and whose asymptotes are the positive x- and y-axes. The sharper the elbow and (equivalently) the closer is the ROC-curve to the x- and y-axes, the lower is the recognition error and the more desirable is the result.

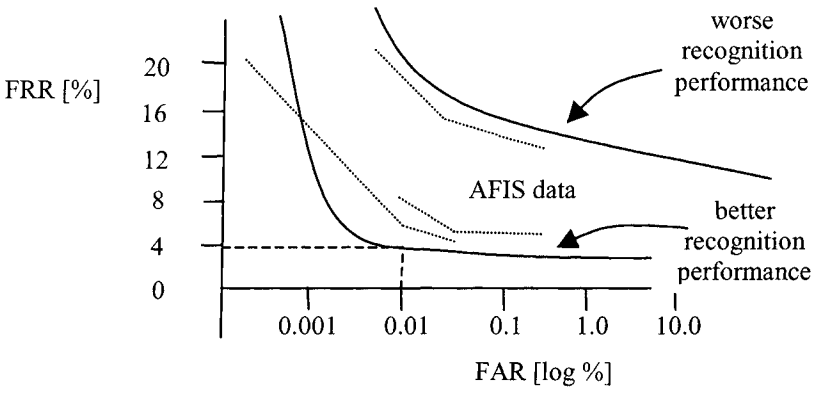

Figure 2.4 ROC-curves. The 2 solid curves are of hypothetical data illustrating desirable and less desirable recognition performance. The 3 dotted curves are of real data measuring the performance of 3 commercial AFIS [46].

The procedure for using the ROC-curve is as follows. Choose an acceptable level of FAR. On Figure 2.4, a dashed line is shown at 0.01% FAR. The FRR corresponding to this choice is the attainable FRR, in this example about 4%. Alternatively, the FRR can be specified and the FAR found on the curve.

There is no single set of FAR and FRR specifications useful for all different applications. If the fingerprint system is specified for very high security situations such as for military installations, then the FAR will be chosen to be very low (e.g., <0.001%). However, this results in higher FRR, sometimes in the range from 5% to 20%. Typical customer applications such as for automatic teller machines cannot afford to alienate users with such a high FRR. Therefore, the choice in these applications is low FRR (e.g., <0.5%), at the sacrifice of higher FAR. (An FRR specification that is sometimes quoted for automatic teller machines is less than 1 per 100,000 false rejection.)

Third-Party Benchmarking

In Figure 2.4, we include three ROC-curves of AFIS data from third-party benchmarking [46]. The database was compiled from employees of the Philippine Social Security System, mostly white-collar workers. The database consists of 600 people, 8 fingers per person, and two sets per person, where enrollment and verification sets were captured with an intervening interval of 2 to 8 weeks. From this database, 3278 matching fingerprint pairs and 4129 non-matching pairs were tested. These images were captured with an Identicator DF-90 optical scanner at 500dpi, 512x512 pixels, 1x1" image size.

We include these AFIS data from a respected third-party tester for the reader to compare against other data whose validity may be suspect. There is much misleading information in the commercial biometric industry regarding recognition rates. In general, these AFIS can be expected to yield better recognition results than most verification systems (though AFIS generally have higher cost, they are slower for 1-to-1 matching, and require more memory). Note that this AFIS test is only for single image comparisons. A verification system can take advantage of the real-time nature of its application to perform multiple verification attempts so as to improve the recognition rate.

Specifying and Evaluating Recognition Rate Statistics

For statistical results to be properly evaluated, they must be accompanied by the following information: sample size, description of population, and testing description. The *sample size* should contain the following information: the number of subjects (people), the number of fingers, the number of images per finger, and the total number of fingerprint images. In addition, the image number should be broken out into number of match and non-match images. For example, a test might consist of 100 subjects, 2 fingers per subject and 4 images per finger. The total number of images is 100x2x4=800. If each finger (200) is compared against each of the other images from the same finger (4 choose 2 = 6 pairs per unique finger), there are 200x6=1200 matching pairs. If one image from each finger (200) is compared against all images from different subjects (99x4x2=792), there are 200x792=158,400 non-match pairs.

The *description of population* states the type of subjects included in the sample. Of particular importance in judging fingerprint statistics is the type of work engaged in by the subjects. A study involving masons will have different statistical results than that involving white-collar workers whose hands are subject to less abuse. The age statistics should be described, at least stating a relative breakdown on the number of children, adults, and elderly people included in the sample. The proportion of males and females should also be stated.

Finally, the *test design* should be described. Of particular interest is who performed the tests. The strong preference is that a reputable third-party conducts and reports the test. Was the capture procedure supervised or not? Were the subjects given training or visual feedback to place the finger correctly on the fingerprint capture device? Was the sample manually filtered in any way to remove "goats" (people whose fingerprints are very difficult to capture and match with reliable quality)? Was the procedure adjusted using a practice sample of fingerprints, then tested separately on different images to yield the published results? What was the range of rotational and translational variance allowed, or were the fingerprints manually centered in the image? What were the make and specifications of the capture device? Where and when were the tests conducted (e.g., Florida humid summer or Minnesota dry winter)? What components of the system were involved in the test: just matching algorithms, just sensor, full system? Most test results do not list all these conditions, but the most possible information enables more valid evaluation.

It is important to emphasize that results cannot be compared if determined under different test conditions. It is a misrepresentation of test data to state that a matcher achieved certain results for test design A, so it can be compared against the results from test design B. Valid comparisons between results can be done only for the same database under the same conditions.

8. Image Capture Devices

We organize image capture devices into three categories: optical, solid-state, and other. There is yet another category, fingerprint acquisition via inking, which is the traditional mode of criminal fingerprint capture. It is evident that this is inappropriate for fingerprint verification due to the inconvenience involved with ink, the need for subsequent digitization, and perhaps the stigma of this type of capture. The type of image acquisition for fingerprint verification is also called "live-scan fingerprint capture".

Optical fingerprint capture devices have the longest history and use of these categories, dating back to the 1970s. These operate on the principal of frustrated total internal reflection (FTIR). A laser light illuminates a fingerprint placed on a glass surface (platen). The reflectance of this light is captured by a CCD array (solid-state camera). The amount of reflected light is dependent upon the depth of ridges and valleys on the glass and the finger oils between the skin and glass. The light that passes through the glass into valleys is not reflected to the CCD array, whereas light that is incident upon ridges on the surface of the glass (more precisely, the finger oils on the ridges that constitute the ridge-to-glass seal) is reflected.

Innovations in optical devices have been made recently, primarily in an effort to reduce the size of these devices. Whereas an optical sensor was housed in a box about 6x3x6 inches as recently as the mid-1990s, smaller devices have recently appeared that are in the order of 3x1x1 inches. Different optical technologies than FTIR have also been developed. For instance, fiber optics has been proposed to capture the fingerprint [7]. A bundle of optical fibers is aimed perpendicularly to the fingerprint surface. These illuminate the fingerprint and detect reflection from it to construct the image. Another proposal is a surface containing an array of microprisms mounted upon an elastic surface [4]. When a fingerprint is applied to the surface, the different ridge and valley pressures alter the planar surfaces of the microprisms. This image is captured optically via the reflected light (or absence of it) from the microprisms.

Solid-state sensors have appeared on the marketplace recently, though they have been proposed in the patent literature for almost two decades. These are microchips containing a surface that images the fingerprint via one of several technologies. Capacitive sensors have been designed to capture the fingerprint via electrical measurements [45, 18, 48, 13]. Capacitive devices incorporate a sensing surface composed of an array of about 100,000 conductive plates over which is a dielectric surface. When the user places a finger on this surface, the skin constitutes the other side of an array of capacitors. The measure of voltage at a capacitor drops off with the distance between plates, in this case the distance to a ridge (closer) or a valley (further). Pressure-sensitive surfaces have been proposed where the top layer is of an elastic, piezoelectric material to conform to the topographic relief of the fingerprint and convert this to an electronic signal [30, 31, 9, 34]. Temperature sensitive sensors have been designed to respond to the temperature differential between the ridges touching the surface of the device and the valleys more distant from them [9].

Ultrasonic scanning falls into the final category of fingerprint capture technologies [32]. An ultrasonic beam is scanned across the fingerprint surface much like laser light for optical scanners. In this case, it is the echo signal that is captured at the receiver, which measures range, thus ridge depth. Ultrasonic imaging is less affected by dirt and skin oil accumulation than is the case for optical scanning, thus the image can be a truer representation of the actual ridge topography.

Two of the three most important factors that will decide when fingerprint verification will be commercially successful in the large-volume personal verification market are low cost and compact size. (The other factor is recognition rate, discussed in Section 7.) Capture device prices have fallen over an order of magnitude between the early to late 1990s (from approximately $1500 (US) to $100), and manufacturers promise close to another order of magnitude decrease in the next few years. As far as size, we have mentioned the reduction of optical sensor size from 6x3x6 inches to 3x1x1. Solid-state sensor systems are this size or smaller, and as further integration places more circuitry on the chip (such as digitizer circuitry to convert the fingerprint measurements to digital intensities), these systems are becoming even smaller. Solid-state sensors are approaching the lower limit of size needed to capture the surface area of the finger, about 1x1 inch with a fraction of an inch depth.

A functionality that has not been available before solid-state sensors is locally adjustable, software-controlled, automatic gain control (AGC). For most optical devices, gain can be adjusted only manually to change the image quality. Some solid-state sensors, however, offer the capability to automatically adjust the sensitivity of a

pixel or row or local area to provide added control of image quality. AGC can be combined with feedback to produce high quality images over different conditions. For instance, a low-contrast image (e.g., dry finger) can be sensed and the sensitivity increased to produce an image of higher contrast on a second capture. With the capability to perform local adjustment, a low-contrast region in the fingerprint image can be detected (e.g., where the finger is pressed with little pressure) and sensitivity increased for those pixel sensors on a second capture.

Optical scanners also have advantages. One advantage of larger models is in image capture size. It is costly to manufacture a large, solid-state sensor, so most current solid-state products have sub-1 inch square image area, whereas optical scanners can be 1 inch or above. However, this advantage is not true for some of the smaller optical scanners. The small optical scanners also have smaller image capture areas because a larger area would require a longer focal length, thus larger package size. Optical scanners are subject to linear distortion at the image edges when larger image capture area is combined with smaller package size.

9. Multi-Modal Biometrics

Multi-modal biometrics refers to the combination of two or more biometric modalities into a single system. The most compelling reason to combine different modalities is to improve recognition rate. This can be done when features of different biometrics are statistically independent. For the different modalities listed in Table 2.1, it is likely that each is largely independent from the other (though we know of no research study to date that confirms this).

There are other reasons to combine biometrics. One is that different modalities are more appropriate in different situations. For a home banking application for instance, a customer might enroll both with fingerprint and voice. Then, the fingerprint can be used from a home or laptop sensor; while voice and a PIN (personal identification number) can be used over the phone. Another reason is simply customer preference. For instance, an automatic teller machine could offer eye and fingerprint and face biometrics, or a combination of two of these for the customer to choose.

Although fingerprints can be combined with other modalities, there are reasons to suggest that this would not be the first biometric to require complementing. One reason is that, along with eye systems, fingerprint systems already have very high recognition rates. This contrasts with less reliable modalities where combining one with another or with a PIN is more advantageous. Another reason is that a single person has up to ten statistically independent samples in ten fingers, compared to two for eye and hand, and one for face, voice, and signature.

Table 2.1 shows selected features of each modality and can be used to determine complementary modalities for multi-modal systems. A few notes on this table:

- Biometric technologies are changing rapidly; for the most up-to-date information, check company literature and industry reports such as at reference [3] and review issues such as [35, 5].

- The row for the eye biometric describes features applying to either iris or retinal scanning technologies.
- In the matching column, whereas all technologies are appropriate for 1-to-1 matching, only fingerprint and eye technologies are proven to have acceptable recognition rates to be practical for 1-to-many matching. This is an indication that these two modalities provide the highest recognition rates for verification as well.
- Variation of the salient features used for recognition is very different for different modalities. Fingerprint and eye features remain consistent for a lifetime, whereas the others change with growth. On a day-to-day basis, there is far less variation for all modalities, though voice can change with illness and signature with demeanor.
- As far as sensor cost, eye systems are currently more costly than the others; voice systems can be zero cost to the user if a telephone is used.
- Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest.

Biometric	Matching 1-to-1, 1-to-many	Variation: Lifetime, Day-to-Day	Maximum Independent Samples per Person	Sensor Cost [$US]	Sensor Size
fingerprint	yes, yes	none, little	10	$10\text{-}10^2$	very small
eye	yes, yes	none, very little	2	$10^2\text{-}10^3$	medium
hand	yes, no	much, very little	2	10^2	medium
face	yes, no	much, medium	1	10^2	small
voice	yes, no	much, medium	1	$0\text{-}10^2$	very small
signature	yes, no	much, medium	1	10^2	medium

Table 2.1 Features of different biometric modalities.

10. Future

Where is biometric technology going? System price will continue to decrease along with size, while recognition rates will improve (at a slower rate than price and size

changes). Recognition rate will be a deciding factor in acceptance for demanding applications such as automatic teller machines (requiring a very low rate of false rejections), and military (requiring a very low rate of false acceptances). For especially demanding applications, multi-modal systems will evolve to combine biometrics to provide an optimum level of security and convenience to users. Alternatively, multiple verifications, such as by using multiple fingers, will be used to enhance recognition reliability. If costs plummet as the industry projects, personal use of biometric systems will grow to replace the current reliance on passwords, PINs, and door keys that are used for computers, home security systems, restricted entry, ATMs, credit cards, Internet access, corporate networks, confidential databases, etc. The biometrics promise is to make access much simpler while at the same time providing a higher level of security.

References

[1] K. Asai, H. Izumisawa, H. Owada, S. Kinoshita, and S. Matsuno, "Method and Device for Matching Fingerprints with Precise Minutia Pairs Selected from Coarse Pairs," *US Patent 4646352*, 1987.

[2] J. Berry, "The history and development of fingerprinting," *in Advances in Fingerprint Technology*, (H. C. Lee and R. E. Gaensslen, ed.s), CRC Press, Florida, 1994, pp. 1-38, 1994.

[3] Biometric Consortium Web page: www.biometrics.org.

[4] W. S. Chen and C. L. Kuo, "Apparatus for Imaging Fingerprint or Topgraphic Relief Pattern on the Surface of an Object," *US Patent 5448649*, 1995.

[5] C. Ciechanowicz, *Special issue on biometric technologies*, Elsevier Information Security Technical Report, Vol. 3, No. 1, 1998.

[6] L. Coetzee and E. C. Botha, "Fingerprint Recognition in Low Quality Images," *Pattern Recognition*, Vol. 26, No. 10, pp. 1441-1460, 1993.

[7] R. F. Dowling Jr. and K. L. Knowlton, "Fingerprint Acquisition System With a Fiber Optic Block," *US Patent 4785171*, 1988.

[8] E. C. Driscoll Jr., C. O. Martin, K. Ruby, J. J. Russell, and J. G. Watson, "Method and Apparatus for Verifying Identity Using Image Correlation," *US Patent 5067162*, 1991.

[9] D. G. Edwards, "Fingerprint Sensor," *US Patent 4429413*, 1984.

[10] M. A. Eshera and R. E. Sanders, "Fingerprint Matching System," *US Patent 5613014*, 1997.

[11] S. Ferris, R. L. Powers, and T. Lindh, "Hyperladder Fingerprint Matcher," *US Patent 5631972*, 1997.

[12] R. C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Addison-Wesley, Massachusetts, 1992.

[13] D. Inglis, L. Manchanda, R. Comizzoli, A. Dickinson, E. Martin, S. Mendis, P. Silverman, G. Weber, B. Ackland, and L. O'Gorman, ``A robust, 1.8V, 250 microWatt, direct contact 500dpi fingerprint sensor,'' *IEEE Solid State Circuits Conference*, San Francisco, 1998.

[14] A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 19, No. 4, pp. 302-313, 1997.

[15] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An Identity-Authentication System Using Fingerprints," *Proceedings of the IEEE*, Vol. 85, No. 9, pp. 1365-1388, 1997.

[16] K. Karu and A. K. Jain, "Fingerprint Classification," *Pattern Recognition*, Vol. 29, No. 3, pp. 389-404, 1996.

[17] M. Kawagoe and A. Tojo, "Fingerprint Pattern Classification," *Pattern Recognition*, Vol. 17, pp. 295-303, 1984.

[18] A. G. Knapp, "Fingerprint Sensing Device and Recognition System Having Predetermined Electrode Activation," *US Patent 5325442*, 1994.

[19] H. E. Knutsson, R. Wilson, and G. H. Granlund, "Anisotropic Nonstationary Image Estimation and its Applications: Part I – Restoration of Noisy Images," *IEEE Trans. Communications*, Vol. 31, pp. 388-397, 1983.

[20] D. Maio and D. Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 19, No. 1, pp. 27-40, 1997.

[21] R. A. Marsh and George S. Petty, "Optical Fingerprint Correlator," *US Patent 5050220*, 1991.

[22] B. M. Mehtre, N. N. Murthy, and S. Kapoor, "Segmentation of Fingerprint Images Using the Directional Image," *Pattern Recognition*, Vol. 20, No. 4, pp. 429-435, 1987.

[23] O. Nakamura, K. Goto, and T. Minami, "Fingerprint Classification by Directional Distribution Patterns," *Systems, Computers, and Controls*, Vol. 13, pp. 81-89, 1982.

[24] L. O'Gorman and J. V. Nickerson, "An approach to fingerprint filter design", *Pattern Recognition*, Vol. 22, No. 1, pp. 29-38, 1989.

[25] E. Peli, "Adaptive Enhancement Based on a Visual Model," *Optical Engineering*, Vol. 26, No. 7, pp. 655-660, 1987.

[26] N. K. Ratha, S. Chen, and A. K. Jain, "Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images," *Pattern Recognition*, Vol. 28, No. 11, pp. 1657-1672, 1995.

[27] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A Real-Time Matching System for Large Fingerprint Databases", *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 18, No. 8, pp. 799-813, 1996.

[28] J. P. Riganati and V. A. Vitols, "Minutiae Pattern Matcher," *US Patent 4135147*, 1979.

[29] J. P. Riganati and V. A. Vitols, "Automatic Pattern Processing System," *US Patent 4151512*, 1979.

[30] H. Ruell, "Input Sensor Unit for a Fingerprint Identification System," *US Patent 4340300*, 1982.

[31] H. Ruell, "Fingerprint Sensor," *US Patent 4394773*, 1983.

[32] J. K. Schneider and W. E. Glenn, "Surface Feature Mapping Using High Resolution C-span Ultrasonography," *US Patent 5587533*, 1996.

[33] B. Schneier, *Applied Cryptography*, John Wiley and Sons, Inc., New York, 1996.

[34] T. Scheiter, M. Biebl, and H. Klose, "Sensor for Sensing Fingerprints and Method for Producing the Sensor," *US Patent 5373181*, 1994.

[35] W. Shen and R. Khanna (eds.), "Special issue on automated biometrics," *Proceedings of the IEEE*, Vol. 85, No. 9, Sept., pp. 1343-1492, 1997.

[36] B. G. Sherlock and D. M. Munro, "A Model for Interpreting Fingerprint Topology," *Pattern Recognition*, Vol. 26, No. 7, pp. 1047-1055, 1993.

[37] B. G. Sherlock, D. M. Munro, and K. Millard, "Algorithm for Enhancing Fingerprint Images," *Electronics Letters*, Vol. 28, No. 18, pp. 1720-1721, 1992.

[38] A. Sibbald, "Method and Apparatus for Fingerprint Characterization and Recognition Using Auto-correlation Pattern," *US Patent 5633947*, 1997.

[39] M. K. Sparrow, "Fingerprint Recognition and Retrieval System," *US Patent 4747147*, 1988.

[40] M. K. Sparrow, "Vector Based Topological Fingerprint Matching," *US Patent 5631971*, 1997.

[41] V. S. Srinivasan and N. N. Murthy, "Detection of Singular Points in Fingerprint Images," *Pattern Recognition*, Vol. 25, No. 2, pp. 139-153, 1992.

[42] K. E. Taylor and J. B. Glickman, "Apparatus and Method for Matching Image Characteristics Such as Fingerprint Minutiae," *US Patent 4896363*, 1990.

[43] C. E. Thomas, "Method and Apparatus for personal Identification," *US Patent 3704949*, 1972.

[44] G. J. Tomko, "Method and Apparatus for Fingerprint Verification," *US Patent 4876725*, 1989.

[45] C. Tsikos, "Capacitive Fingerprint Sensor," *US Patent 4353056*, 1982.

[46] J. L. Wayman, "Biometric Identification Standards Research," *Report to U.S. Federal Highway Administration (FHWA)*, San Jose State University, December 1997.

[47] M. Yamada, A. Kodata, and H. Tominaga, "A Method of Describing Fingerprint Structure and Identification Algorithm Using Geometric Characteristics," *Systems and Computers in Japan*, Vol. 25, No. 5, pp. 100-112, 1994.

[48] N. D. Young, G. Harkin, R. M. Bunn, D. J. McCulloch, R. W. Wilks, and A. K. Knapp, "Novel fingerprint scanning arrays using polysilicon TFT's on glass and polymer substrates," *IEEE Electronic Device Letters*, Vol. 18, No. 1, pp. 19-20, 1997.