identix
Empowering Identification™

Minutia vs. Pattern Based Fingerprint Templates

Introduction

The purpose of this white paper is to provide a detailed explanation of the two primary methods for storing and the subsequent matching of fingerprint templates: minutia-based and pattern-based. This paper further contrast the two methods in terms of such germane topics as template efficacy, security and playback, etc.

Definitions

Pattern-Based Templates

A capture device is used to take a graphical image of a fingerprint, typically captured as a TIFF (Tagged Image File Format) image. The graphical image obtained from the capture device is commonly referred to as a live scan to distinguish it from a template or print stored in a database. Processing software examines the fingerprint image and locates the image center, which may be off-center from the fingerprint core. The image is then cropped a fixed distance around this graphical center. The rectangle in Figure 1 details this cropped region. The cropped region is then compressed and stored for subsequent match.

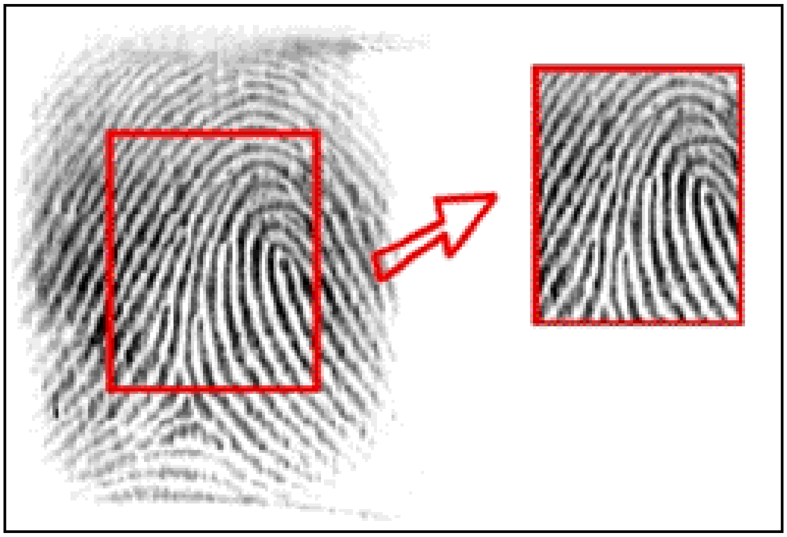

Figure 1. Pattern-based Template

Fingerprint matching with pattern-based templates involves making a graphical comparison of the two templates and determining a measure of the difference. The greater the difference the less likely the prints match.

Minutia-based Templates

As in a pattern-based system, a capture device is used to take a graphical image of a fingerprint (live scan). Special software then analyzes the fingerprint image and determines if the image actually contains a fingerprint, determines the location of the core, the pattern type (e.g. right loop, left arch, etc.), estimates the quality of the ridge lines, and finally extracts minutia. Minutia, from a simple perspective, indicate where a significant change in the fingerprint occurs. These changes are shown in Figure 2.

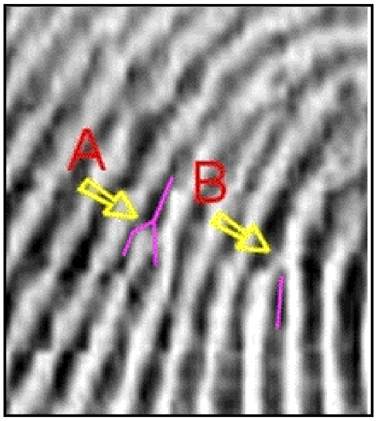

Figure 2. Fingerprint Changes

Understanding that dark lines in the image represent ridges and light lines represent valleys, Arrow A shows a region where one ridge splits into two ridges (called a bifurcation) and Arrow B shows where a ridge ends.

After locating these features in the fingerprint, the minutia extraction software determines a significant direction of the change (using Arrow B as an example, the significant direction starts at the end of the ridge and moves downward. The resultant minutia, in their simplest form are then the collection of all reasonable bifurcations and ridge endings, their location and their significant direction. Minutia are also assigned a measure of their strength. A set of minutia is shown in Figure 3.

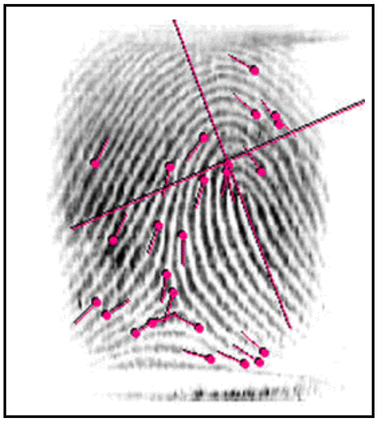

Figure 3. Extracted Minutia and Axis

Technical Comparison

Template Size vs. Search and Match Speed

On average, minutia-based templates are significantly smaller than pattern-based templates on a byte count basis. The size of a minutia template is directly related to the number of minutia extracted. Identix minutia templates typically average about 350 bytes, or approximately 35 minutia, but can be as small as 125 bytes. The minutia extraction software is easily able to affect the size of the template by controlling the number of final minutia based on their strength.

Pattern-based templates average about 300-400 bytes when compressed, and about 1024 bytes when uncompressed. Matching and other related functions can only operate on the uncompressed version. However, the size of the template is directly related to the image and cannot easily be controlled without sacrificing detail (and thus usefulness) in the image.

Template size and storage capacity are directly related, with minutia templates requiring about half the storage of pattern template. This impacts storage media costs, network bandwidths, etc., and has a direct effect on the time required to retrieve a template for searching and matching.

Template size also directly relates to the search and match speeds. Although search and match speeds are also dependant on the efficiencies of the algorithms involved, smaller templates will usually result in shorter match time.

Sensitivity to Physical Changes

Physical changes to the finger include such things as scars, cuts, folds, various blemishes, etc. Physical changes can occur through accident or as a normal course of work, such as cement workers, bricklayers, etc., whose fingerprint ridges are usually severely worn.

When a minutia based system processes a fingerprint, a scar, fold or other blemish may result in a few minutia, but these typically represents a small percentage of the total minutia extracted. For example, if 20% of the extracted minutia is disrupted due to physiological changes to the fingerprint since the template was first taken, then there are still 80% of the minutia available for matching. Since a good match can be made with as few as 30% of the minutia, 80% availability provides for a wide safety margin.

Minutia templates are therefore very forgiving of physical changes to the fingerprint without having to resort to re-extracting a new template from a new image of the finger.

On the other hand, pattern-based templates are more sensitive to physical changes in the fingerprint because the match is done using a cropped fingerprint image. Physical changes can obscure critical elements of the image and significantly increase differences between two images of the same finger, thus reducing the likelihood of obtaining an accurate match. In a pattern-based system, new scars or other blemishes typically require a new image of the fingerprint be obtained, converted to a template and stored in the system. This presupposes the person is readily available for this activity, which may not be the case if, for example, the original print was a latent print taken from a crime scene.

Template Efficacy

In practical applications, such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS), prints obtained by the FBI (from a ten print, for example) are matched against subsequent prints which may be taken from crime scenes, etc. Physical characteristics of a fingerprint, such as rotational orientation, completeness, ridge quality, etc., can vary greatly from crime scene to crime scene, and as contrasted to the AFIS database.

Consequently, for matching algorithms and their respective templates to work well in this real-world environment, they must be able tolerate oftentimes complex variations in the prints.

As previously discussed, pattern-based template matching is more sensitive to variations in the physiological characteristics of the fingerprint, which includes characteristics such as completeness, rotational orientation, etc. Understanding that scars and other blemishes can significantly hamper matching by obscuring relevant portions of the image, it is easy to see how a partial print, say from an edge of the print, can have the same adverse effect.

In the case of minutia templates, there can be great variations in the environmental and physiological affects on the print since only a relatively small percentage of the minutia have to match for two templates to be adjudged identical. If, for example, 12 minutia matching out of 40 constitute a successful match, then any 12 of the 40 will typically do. If the minutia extracted from a sample print are very poor on the left side of the print then matching minutia can come form the right side, etc. Consequently, minutia-based templates are more robust in practical applications than are pattern templates.

Security and Playback

Security is a major consideration when discussing template types. A possible technique to circumvent fingerprint biometric security would be to obtain an actual template and replay it to the authentication system. We note that even with a variety of security and encryption methods, templates must still be decrypted, etc., in order to be used by the match algorithms. Consequently, a determined individual can most likely obtain a template.

When a minutia-based template is extracted from a fingerprint, subtle variations in the orientation and centering of the finger on the capture device have subtle affects on the minutia generated. This means that the same finger placed on a capture device multiple times will produce slightly different minutia templates each time. This has no effect whatsoever on the accuracy of the matching algorithms (as previously discussed, minor variations in the minutia do not affect the match outcome). Consequently, the same finger presented multiple times will match, but not perfectly in the sense that the extracted templates will never be absolutely identical. This directly leads to a method for detecting the presentation of a stolen template: if the match is exact, the template must be an identical match, minutia for minutia, with the template in the database. The template must therefore be a duplicate of the one in the database and could not have come from a live scan.

With a pattern-based template, obtaining the template, since it is a cropped graphical image of the fingerprint, gives you the actual fingerprint. Adding logic in the authentication system to detect that the exact same fingerprint image is being presented increases the False Reject Rate, that is, the number of valid users being rejected. Further, the stolen print from the template can be subtly altered so as to prevent a duplication detection, but still result in a positive match.

With a minutia template, the fingerprint cannot be reconstructed, and thus the fingerprint itself cannot be subtly altered and then replayed to the authentication system.

Performance

Recent independent test results[1] have demonstrated exceptionally strong performance of the Identix minutia algorithm with respect to the False Rejection Rate (FRR) measurement over an extended period of time after initial enrollment. This important metric measures the likelihood of an authorized user being denied access as time passes beyond the initial enrollment and hence is very relevant to real-world performance.

These independent tests demonstrate other conditions under which the minutia template performs equal to or better than pattern-based templates. However, under the terms of the evaluation, Identix is permitted to provide only limited detail of the test results. Fpr more information on testing methodology and obtaining complete results, visit http://www.ibgweb.com/reports/public/comparative_biometric_testing.html

Major Systems Using Minutia-based Templates

U.S. Defense Enrollment and Eligibility Reporting System and Real Time Automated Personnel Identification System

Identix technology (fingerprint readers, feature extraction, and matching software) is installed throughout the Department of Defense DEERS and RAPIDS (Defense Enrollment and Eligibility Reporting System and Real Time Automated Personnel Identification System) programs. The DEERS system is the mechanism for all Deparement of Defense services to verify who is entitled to medical care at military treatment facilities. This system comprises an Oracle Relational database. The RAPIDS stations encompass the enrollment function of

[1] International Biometric Group's (IBG) Comparative Biometric Testing Round 4

DEERS. Candidate's demographic information as well as fingerprint images and Identix minutia templates are captured and then sent to DEERS for storage and later comparison.

FBI Integrated Automated Fingerprint Identification System

The Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) is being developed to sustain the FBI's mission to provide identification services to the nation's law enforcement community and to organizations where criminal background histories are a critical factor in consideration for employment. The IAFIS provides ten-print, latent print, subject search, and criminal history request services, document submission, and image request services to FBI Service Providers, and federal, state, and local law enforcement users.

Often times when investigating crimes, it is necessary for investigators to search what are known in the industry as latent fingerprint images against the FBI's database of fingerprints to see if a suspect is already in the database. Latent fingerprints images, which are frequently left behind at crime scenes are distorted and seldom complete fingerprint images. Investigators employ both latent fingerprint examiners and a latent workstation to create a useable fingerprint minutia-based reference template that will be used to search against the FBI's database. Consequently, the only method to search the FBI database is with a minutia-based record, and it is the Identix Minutia Template used in the IAFIS system.

Fingerprint Data Interoperability

Interoperability with fingerprint-based systems is a function of the record stored in that system. In the two examples provided – RAPIDS/DEERS and FBI, fingerprints are stored as minutia records. As a result, any fingerprint queries to these databases requires the use of a minutia-based template. Pattern-based system must request the fingerprint image and convert it to a template prior to use, a step not required by Identix minutia-based systems.

Standards

Standards are critical to insure the interoperability of various technologies and the agencies that employ them. Two key standards that relate to the format of fingerprint templates are discussed below. Note that no standard exists for pattern-based templates.

X.509

This standard requires that the minutia template be stored in an X.509 certificate as an information attribute within a fixed number of bytes. The Identix minutia template meets all applicable criteria. Pattern-based templates, by definition, cannot meet this standard.

AAMVA B10.8

The AAMVA B10.8 standard provides interoperability between different finger matchers for the purposes of one-to-one verification of an individual's identity against a previously collected and stored finger record. The interoperability is based on defining the finger minutia extraction rules and record format that are common to most all finger matchers for acceptable matching accuracy, while allowing for proprietary data to be attached so that the highest accuracy can be maintained for matching accomplished with the same matcher type. The Identix minutia template fully adheres to all specifications in this standard. Again, we note that this standard does not apply to pattern-based templates.

Minutia vs. Pattern Matching

	Minutia	Pattern
Definition	Analyzes the points at which the ridges on the fingerprints split, intersect or end.	Graphical comparison of fingerprint image.
How it works	Capture device analyzes the fingerprint image to determine the location of the fingerprint core, the pattern type (i.e., right loop, left arch, etc.), estimates the quality of the ridgelines and extracts the points in which the ridges split, intersect or end. These points are called minutia.	Graphical center of fingerprint image (not necessarily defined by the fingerprint core) is cropped a fixed distance and compressed for subsequent match. The greater the difference between the stored template and the live comparison, the less likely the match.
Template size	• Small template size (can be as small as 120 bytes; average size is 350 bytes) • Template size can be controlled by specifying the number of minutia to be analyzed	• Relatively large template size (500-700 bytes when compressed) • Cannot easily control template size without compromising accuracy
Search speed	Directly related to template size; the smaller the template, the faster the search speed.	
Sensitivity to Physical Changes	• Less sensitive due to the fact that only 30% of the available minutia are required for matching. Cuts and scars usually will not affect all the minutia on the fingerprint.	• If the scar or blemish affects the region of the fingerprint image that was scarred, a new template may be required.
Template Efficacy	• Can extract minutia from partial prints (as often found in crime scenes), making it more feasible to criminal related applications	• Requires the same central region to be patterned for the match to occur. • Not suitable for criminal applications where partial prints are often used as the basis for investigation.
Sensitivity to Time	• Less sensitive to changes over time	• More sensitive to physical changes and differences in the fingerprint placement on the sensor – both which become greater over time
Standards	X.509 AAMVA B10.8	None
Leading vendors	Identix	BioScrypt, Precise Biometrics, Digital Persona, Sony