DigitalPersona™ White Paper

Guide to Fingerprint Recognition

For More Information:

DigitalPersona, Inc.

650.261.6070
www.digitalpersona.com

DigitalPersona
Guide to Fingerprint Recognition

All fingerprints are unique. The critical issue is whether we can get to the information that is unique and express it in a way that meets the objective of positive identification. Getting to and expressing the unique information in the fingerprint biometric is the mission of DigitalPersona and its Fingerprint Recognition Engine.

Introduction

When we interact with others we are used to identifying them by their physical appearance, their voice, or other sensory data. When we need proof of identity beyond physical appearance we obtain a signature or we look at a photo identification card. In Cyberspace, where people need to interact with digital systems or with one another remotely, we do not have these tried and true means of identification available. In almost all cases we cannot see, hear, or obtain a signature from the person with whom we are interacting.

Biometrics, the measurement of a unique physical characteristic, is an ideal solution to the problem of digital identification. Biometrics makes it possible to identify ourselves to digital systems, and through these systems identify ourselves to others in Cyberspace. With biometrics we create a digital persona that makes our transactions and interactions in Cyberspace convenient and secure. Of all the biometrics available, including face, iris and retina scanning, voice identification, and others, the fingerprint is one of the most convenient and foolproof.

The advantages of fingerprint biometrics for the purpose of personal digital identification include:

- Each and every one of our ten fingerprints is unique, different from one another and from those of every other person. Even identical twins have unique fingerprints!

- Unlike passwords, PIN codes, and smartcards that we depend upon today for identification, our fingerprints are impossible to lose or forget, and they can never be stolen.

- We have ten fingerprints as opposed to one voice, one face or two eyes.

- Fingerprints have been used for centuries for identification, and we have a substantial body of real world data upon which to base our claim of the uniqueness of each fingerprint. Iris scanning, for instance, is an entirely new science for which there is little or no real world data.

In the DigitalPersona Guide to Fingerprint Identification we explain how we know that the likelihood of two fingerprints being alike is so infinitesimal as to be impossible, how much unique information is available in each print, how fingerprints have been used over the centuries as proof of identity, and how DigitalPersona is adapting this standard of identification for the digital age.

The Basics of Fingerprint identification

Ridges

The skin on the inside surfaces of our hands, fingers, feet, and toes is "ridged" or covered with concentric raised patterns. These ridges are called friction ridges and they serve the useful function of making it easier to grasp and hold onto objects and surfaces without slippage. It is the many differences in the way friction ridges are patterned, broken, and forked which make ridged skin areas, including fingerprints, unique.

Fingerprint Identification Terminology

Fingerprints are extremely complex. In order to "read" and classify them, certain defining characteristics are used, many of which have been established by law enforcement agencies as they have created and maintained larger and larger databases of prints. Even though biometrics companies like DigitalPersona do not save images of fingerprints and do not use the same manual process to analyze them, many of the methodologies that have been established over the years in law enforcement are useful for digital algorithms as well.

Global Versus Local Features

We make use of two types of fingerprint characteristics for use in identification of individuals: Global Features and Local Features. Global Features are those characteristics that you can see with the naked eye. Global Features include:

- Basic Ridge Patterns

- Pattern Area

- Core Area

- Delta

- Type Lines

- Ridge Count

The Local Features are also known as Minutia Points. They are the tiny, unique characteristics of fingerprint ridges that are used for positive identification. It is possible for two or more individuals to have identical global features but still have different and unique fingerprints because they have local features - minutia points - that are different from those of others.

Global Features

- **Pattern Area** – The Pattern Area is the part of the fingerprint that contains all

24a   24b
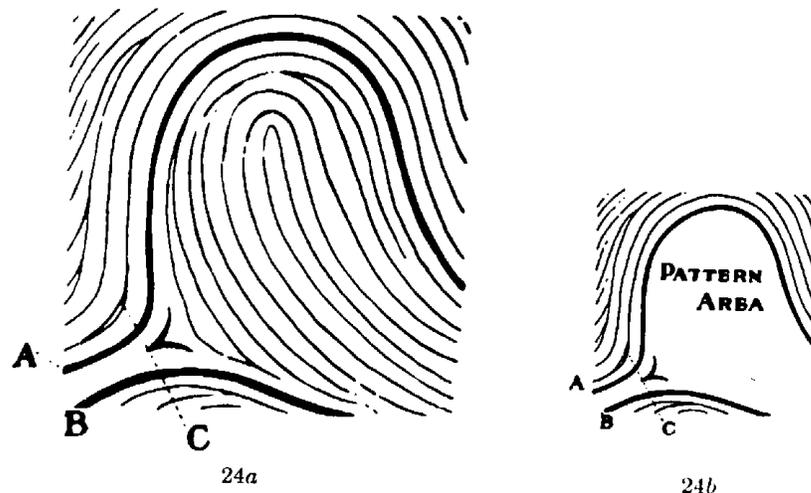
the global features. Fingerprints can be read and classified based on the information in the Pattern Area. Certain minutia points that are used for final identification might be outside the Pattern Area. One significant difference between DigitalPersona's fingerprint recognition algorithm and those of competing companies is that DigitalPersona uses the entire fingerprint for

analysis and identification, not just the Pattern Area. While other companies'
devices require users to line up their fingerprints on the sensor,
DigitalPersona acquires a greater amount of information over the entire
fingerprint, and can obtain enough information to "read" a print even if only
part of the print is placed on the sensor.[1]

- **Core Point** -- The Core Point, located at the approximate center of the finger
  impression, is used as a reference point for reading and classifying the print.

- **Type Lines** – Type Lines are the two innermost ridges that start parallel,
  diverge, and surround or tend to surround the pattern area. When there is a
  definite break in a type line, the ridge immediately outside that line is
  considered to be its continuation.

- **Delta** – The Delta is the point on the first bifurcation, abrupt ending ridge,
  meeting of two ridges, dot, fragmentary ridge, or any point upon a ridge at or
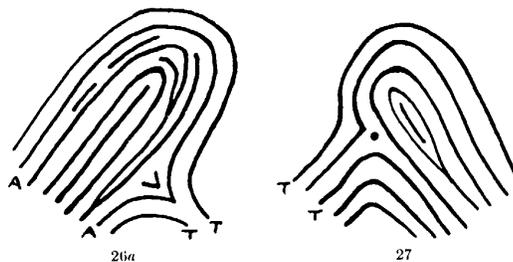
nearest the center of divergence of two type lines, located at or directly in
front of their point of divergence. It is a definite fixed point used to facilitate
ridge counting and tracing.[1]

- **Ridge Count** – The Ridge Count is most commonly the number of ridges
  between the Delta and the Core. To establish the ridge count, an imaginary

line is drawn from the Delta to the Core and each ridge that touches this line is counted.

Basic Ridge Patterns

Over the years those who work with fingerprints have defined groupings of prints based on patterns in the fingerprint ridges. This categorization makes it easier to search large databases of fingerprints and identify individuals. The basic ridge patterns are not sufficient for identification but they help narrow down the search.

Certain products base identification on "optical correlation" of global ridge patterns, or matching one fingerprint pattern image to another. DigitalPersona believes that positive identification must be based on verification of minutia points in addition to global features.

The new digital paradigm for fingerprint identification uses many elements of the categorization process that has been in place for years, as well as some newer concepts for understanding and categorizing global features. In addition to defining ridge patterns, DigitalPersona has determined that there are certain ways that ridges can flow around on a fingerprint, and that the constraints on flow behavior can be exploited for identification. The DigitalPersona Recognition Engine makes use of the characteristics of global ridge patterns and flow characteristics to identify individuals.

There are a number of basic ridge pattern groupings which have been defined. Three of the most common are loop, arch, and whorl.

1. LOOP

The loop is the most common type of fingerprint pattern and accounts for about 65% of all prints.[1]

89s. Loop.   89t. Loop.   89u. Loop.

2. ARCH

The Arch pattern is a more open curve than the Loop. There are two types of arch patterns – the Plain Arch and the Tented Arch.[1]

106   89q. Tented arch.

3. WHORL

Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.[1]

92b   92c   92d
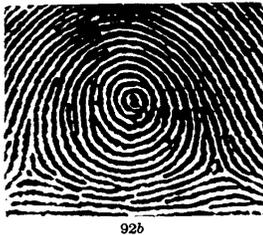
Minutia Points

Fingerprint ridges are not continuous, straight ridges. Instead they are broken, forked, changed directionally, or interrupted. The points at which ridges end, fork, and change are called minutia points, and these minutia points provide unique, identifying information.

There are five characteristics of minutia points in fingerprints:

1. **Type** – There are a number of types of minutia points. The most common are ridge endings and ridge bifurcations.

   - **Ridge Ending** -- occurs when a ridge ends abruptly.

   - **Ridge Bifurcation** -- the point at which a ridge divides into two or more branches.

     BIFURCATION

   - **Ridge Divergence** – the spreading apart of two lines which have been running parallel or nearly parallel.

     DIVERGENCE

- **Dot or Island –** a ridge that is so short it appears as a dot.

- **Enclosure** –a ridge that divides into two and then re-unites to create an enclosed area of ridge-less skin.

- **Short Ridge** – an extremely short ridge, but not so short that it appears as a Dot or Island

2. **Orientation** – Each minutia point faces a particular direction. This is the Orientation of the minutia point.

3. **Spatial Frequency** – Spatial frequency refers to how far apart the ridges are in the neighborhood of the minutia point.

4. **Curvature** –The curvature refers to the rate of change of ridge orientation.

5. **Position** – The position of the minutia point refers to its x, y location, either in an absolute sense or relative to fixed points like the Delta and Core points.

Advantages of the U.are.U® Fingerprint Recognition Algorithm

The U.are.U® Fingerprint Recognition Algorithm was developed by leading researchers in the field of fingerprint biometrics to overcome the new issues and constraints the digital world imposes on standards of identification.   It incorporates traditional fingerprint identification methodologies into creating each user's unique identifying information for Cyberspace. The result of years of study, extensive researching, and testing, DigitalPersona's recognition engine is the most robust recognition algorithm available today.

The performance of fingerprint algorithms is measured as a tradeoff between two attributes:

False Acceptance Rate (FAR) which is the probability that an intruder will be accepted by the system

False Rejection Rate (FRR) which is the probability that a legitimate person will be rejected by the system

By adjusting the threshold of acceptance, the FAR can be lowered at the expense of the FRR, and vice versa. In some installations, such as a highly confidential site, a higher FRR and a lower FAR are required. In other installations where security is not as significant an issue and the system is used primarily for the convenience it provides, it may be preferable to decrease the FRR and increase FAR.

DigitalPersona is continuously improving both the FAR and FRR of its algorithm. The goal is to increase the overall robustness of the algorithm as

measured by the reliability of the verification over time for different users, at different times, and under different conditions.

FAR and FRR offset one another and can be stated only in terms that are relative to one another. Currently the DigitalPersona algorithm provides an FAR of 0.01% at an FRR of 1.4%.

The above FAR and FRR rates and the accuracy of the system are a direct result of the quality of the fingerprint of the individual user. Testing with large groups of people over an extended period has shown that 80% of all users have such feature-rich fingerprints that they will virtually always be recognized accurately by U.are.U® and never obtain a false acceptance or a false rejection. Of the remaining 20%, about 15% of users have less information in their prints. They will have to put their finger onto the sensor twice to obtain secure system access. About 5% of all users have poor-quality prints and might have to try a second and third time to obtain an accurate reading.

The U.are.U® Recognition Engine is optimized to recognize prints of poor quality. However, a very small number of fingerprints are either worn from manual labor or have unreadable ridge lines and are impossible to image. Even U.are.U® will not register prints of exceptionally low quality.

Many digital recognition systems rely upon what is called a "Skeleton Model" as its basis. This is a line drawing derived from the image provided by the sensor that includes the basic ridge lines and minutia points on the fingerprint. The problem is that in addition to the basic information, the Skeleton Model also includes a great deal of spurious skeleton lines that do not correspond to real

minutia points at all. This is particularly the case with poor-quality prints. A major advantage of the DigitalPersona algorithm over those of its competitors is that it employs an enhanced version of the raw image that comes from the sensor. It extracts the minutia points directly from this representation rather than attempting to impose an unrealistic and highly lossy skeleton model. This provides an inherently more reliable result.

In addition to making better use of the image provided by the sensor, the U.are.U® algorithm benefits from proprietary machine-learning techniques. This improves the results obtained from poor-quality dry, damaged, and minutia-impoverished prints, and blurred or skewed print images. It also eliminates "latent" prints that are left on the platen from the previous time it was used. It is this ability that truly sets the U.are.U® Recognition Engine apart and makes it clearly superior to a traditional Skeleton Model algorithm.

The key benefit of the DigitalPersona system is that it brings together ease of use and reliability. The system is entirely rotation-invariant, meaning that the user can put his\her fingerprint onto the sensor at any angle. It also provides extremely low FAR and FRR as described above – the ultimate test of the system.

Are All Fingerprints Really Unique?

Underlying all methods of fingerprint identification is the assertion that no two fingerprints are alike. DigitalPersona's belief in this assertion is based on two fundamental principles:

- We know how much information is included in one fingerprint and we can create statistical models around this. There are up to 70 minutia points on each print, and each of these points has 5 characteristics as described above. The chance of finding sets of minutia points that are alike with respect to these characteristics is so small as to be negligible.

- We have almost a century of real-world fingerprint data available to us. F.B.I. files alone contain over 200 million fingerprints, each of which is unique from all the rest. In all the data that has been collected over the past hundred years, using the classification methodologies described above, there have never been two prints that were classified exactly the same.

Even though we feel confident making the claim of the uniqueness of each fingerprint, there are certain conditions that make it impossible to state with absolute certainty that this is true:

- Every fingerprint is directly affected by the mechanism that is used to collect the print. Even with a manual system of inking the print and physically pressing it onto paper, the degree of pressure, amount of ink and other factors having nothing to do with the print itself affect the information that is gathered. The same holds true for electronic collection mechanisms.

- Because fingerprints are part of living organisms, the biological process is always at work. The physiological characteristics of skin differ depending on race, gender, and life-style. Skin changes over time depending on the life-style and activities of the individual.

Still, with all these caveats, fingerprints are extremely reliable biometrics which have stood up to the claim of uniqueness for over one hundred years and will continue to do so for as far into the future as we need to project.

History of Fingerprint Identification

One of the reasons fingerprint identification is so promising is that, unlike iris scanning or other relatively untested biometrics, the U.S. and other countries have extensive real-world experience with fingerprint identification. We are all aware of the use of fingerprint identification in law enforcement. Less well known is the ancient history of fingerprint identification for commerce, and the long history of the "science" of fingerprints in the U.S. and western Europe.

- Pre-historic picture writing found in Nova Scotia shows a hand with ridge patterns.
- In ancient China thumbprints were used on clay seals to prove identity in financial transactions.

1686 Marcello Malpighi, a professor of anatomy at the University of Bologna, wrote about ridges, loops, and spirals in fingerprints.

1823 Professor Purkinji from the University of Breslau described nine basic fingerprint patterns. These pattern descriptors are still used today.

1823 Dr. Henry Faulds wrote an article describing fingerprints as a means of personal identification. He is credited with the first fingerprint identification

in law enforcement by obtaining a conviction based on correctly identifying

a greasy print left on an alcohol bottle.

1882 Gilbert Thompson of the U.S. Geological Survey used his own fingerprint

on a document to prevent forgery.

1892 Sir Francis Galton, a British anthropologist, published the first fingerprint

classification system and established the individuality and permanence of

fingerprints. The "minutia points" Galton identified are still used today.

1901 Scotland Yard adopted the Galton-Henry fingerprint identification system,

an adaptation of Galton's observations by Sir Edward Henry, chief

commissioner of the London metropolitan police.

1903 The New York State prison system began the first systematic use of

fingerprints in the U.S. for identifying known criminals.

1904 The U.S. Army first began using fingerprints to identify enlisted personnel.

1904 Juan Vucetich of the Buenos Aires police published his system of

fingerprint identification, which helped him identify a murderer by studying

fingerprints left on a door-post. His method is still used today.

1905-1930

Law enforcement agencies across the U.S. turned to fingerprints for

personal identification. Many began to send copies of their fingerprint

cards to the National Bureau of Criminal Identification established by the

International Association of Police Chiefs.

1919 Congress established the Identification Division of the F.B.I. The National

Bureau and Leavenworth consolidated their files to form the nucleus of the

current F.B.I. fingerprint files. By 1946 the F.B.I had processed 100

million fingerprint cards, and by 1971 it had processed 200 million.

---

[1] Illustrations: J Edgar Hoover, Federal Bureau of Investigation, Department of Justice, *Classification of Fingerprints*, US Government Printing Office 1939