DigitalPersona White Paper
Guide to Fingerprint Recognition

A DigitalPersona, Inc.

White Paper

July 2007

DigitalPersona, Inc.
1+ 650.474.4000
www.digitalpersona.com

Table of Contents

DigitalPersona White Paper Guide to Fingerprint Recognition 1

Introduction 1

Biometric Identification 1

Advantages of Fingerprint Authentication 1

The Basics of Fingerprint Identification 2

Fingerprint Identification Terminology 2

Global Versus Local Features 2

Global Features 2

Basic Ridge Patterns 3

Minutia Points 3

Are Fingerprints Really Distinctive and Persistent? 4

DigitalPersona Fingerprint Recognition Algorithm Advantages 4

False Acceptance Rate (FAR) 4

False Rejection Rate (FRR) 4

History of Fingerprint Recognition 5

About DigitalPersona 6

This white paper is for information purposes only. DIGITALPERSONA MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

DigitalPersona may have patents, patent applications, trademark, copyright or other intellectual property rights covering the subject matter of this document. Except as expressly provided in any written license agreement from DigitalPersona, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

DigitalPersona is a trademark of DigitalPersona, Inc., registered in the United States and other countries.

In this guide, we discuss the advantages of fingerprint authentication, the basics of fingerprint characteristics and recognition that form the foundation of the DigitalPersona technology.

Fingerprints are distinctive and persistent. Every one has different fingerprints which do not change over a lifetime. The objective of the DigitalPersona® Fingerprint Recognition Engine is to use these two properties of fingerprints for the purpose of reliable automatic personal recognition. DigitalPersona's engine reliably decides whether two fingerprint images are from different fingers (based on the distinctive property) or whether two fingerprints are from the same finger (based on the persistence property).

Introduction

Since the beginning of civilization, recognizing the identity of fellow human beings has been a central thread in the fabric of society. Until the 20th century, such personal recognition was manually carried out in person among small communities of friends and acquaintances based on visual appearances such as face, hairstyle, body type, gait, and voice.

With advances in communication technology and transportation, we have become interconnected to form a much larger global community. Often, business deals are no longer done in person with a handshake or signature on paper. Conducting business from remote locations has become the norm. As a result, it has become necessary to carry out reliable personal recognition often remotely and through automated means.

Surrogate representations of identity such as passwords (prevalent for electronic access control) and tokens (prevalent for physical access control) provide a lower level of authentication security that does not strongly link the authorized user with their digital identity.

Biometric Identification

Biometrics refers to automatic recognition of individuals based on their distinctive anatomical (fingerprint, face, iris, hand geometry) and behavioral (signature, voice) characteristics. Because biometric identifiers cannot be shared or misplaced, and they intrinsically represent the individual's bodily identity, biometrics is quickly becoming an essential component of effective identification solutions. Recognition of a person by their body, then linking that body to an externally established "identity", forms a powerful authentication tool. Biometrics usage is reducing fraud, and enhancing user convenience. Among the different biometrics, fingerprints have the right balance of qualities including distinctiveness, persistence, accuracy, throughput, size and cost of readers, maturity of technology and convenience of use, making it the dominant biometric technology in commercial applications.

Advantages of Fingerprint Authentication

Fingerprint solutions offer many advantages which address the human factors of authentication.

- One of a kind identifier - Fingerprints from each one of our ten fingers is distinctive, different from one another and from those of other persons. Even identical twins have distinctive fingerprints.

- Greater convenience - Users no longer have to remember multiple, long and complex, frequently changing passwords or carry multiple keys.

- Relatively equal security level for all users in a system - One account is not easier to break into than any other (such as an easily guessed password or through social engineering).

- Ensures the user is present at the point and time of recognition and later cannot deny having accessed the system.

- Cannot be shared, lost, stolen, copied, distributed or forgotten unlike passwords, PINs, and smart cards. Fingerprints strongly link an identity to a physical human being making it difficult for attackers to forge.

- Long history of successful use in identification tasks. Fingerprints have been used in forensics for well over a century and there is a substantial body of scientific studies and real world data supporting the distinctiveness and permanence of fingerprints.

The Basics of Fingerprint Identification

Fingerprint Identification Terminology

Fingerprints are extremely complex. Defining characteristics are used, many of which have been established by law enforcement agencies, to “read” and classify fingerprints. 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 same methodologies established over the years in law enforcement are used for our digital algorithms.

Biometric systems authenticate users by comparing the ridges and patterns on the finger. To break it down further, the software looks for distinctions within these areas:

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 provide friction making it easier for us 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, distinctive.

Global Versus Local Features

Two types of fingerprint characteristics are used in identification of individuals: Global features and local features.

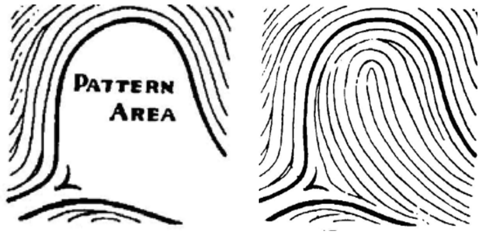
Global features are those characteristics that one can see with the naked eye and include:

- Pattern Area
- Core Area
- Type Lines
- Delta
- Ridge Count Basic
- Ridge Patterns

The local features are known as minutia points. They are the tiny characteristics of fingerprint ridges. Their two-dimensional arrangement is distinctive and is used for recognition. It is possible for two or more individuals to have similar global features but still have different and distinctive fingerprints because the local features, that is, the two dimensional arrangement of minutia points, is different.

Global Features

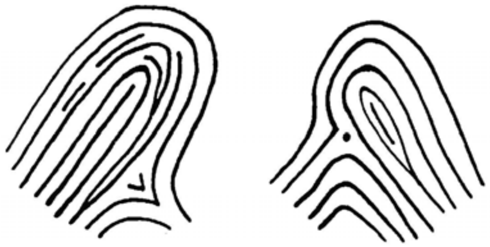
Pattern Area – The pattern area is the part of the fingerprint that contains the global features. Fingerprints are read and classified based on the information in the pattern area. Certain minutia points that are used for final recognition might be outside the pattern area.



Core Point -- The core point, located at the approximate center of the finger impression, is used as a starting 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 (where the ridge forks into two different directions), 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. The delta is located directly in front of the line’s point of divergence. It is a definite fixed point used to facilitate ridge counting and tracing.



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; each ridge that touches this line is counted.

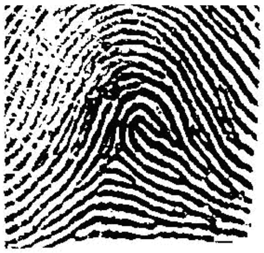
Basic Ridge Patterns

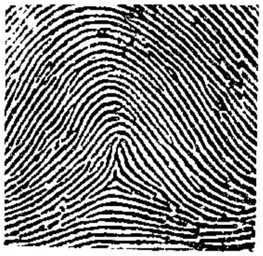
To make fingerprints easier to search against large fingerprint databases, experts categorize fingerprints into groups based on patterns in the ridges. These groupings or basic ridge patterns are not sufficient for identification in themselves, but they help narrow down the search and speed up the processing time. Once a fingerprint is identified as a particular group like a whorl, the search only continues to compare the print to all other whorl types in the database and ignores the other groupings.

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

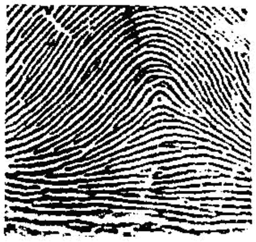
The loop is the most common type of fingerprint pattern and accounts for about 65% of all fingerprints.

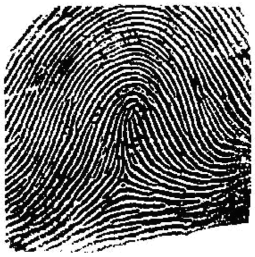




2. ARCH

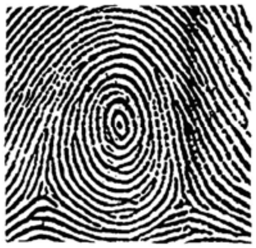
The arch pattern is a more open curve than the loop. There are two types of arch patterns – the plain arch and the tented arch.

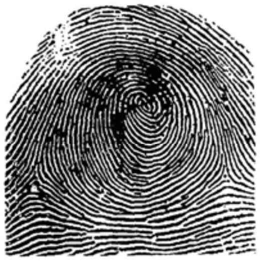




3. WHORL

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





Certain biometric products base identification on correlation of global ridge patterns, or matching one fingerprint pattern image to another. DigitalPersona believes that high quality fingerprint recognition algorithms must go one step further making the algorithm based on minutia points in addition to global features.

Minutia Points

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

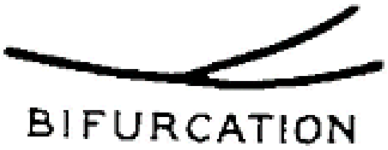
There are five characteristics of minutia points in fingerprints:

1. Type

There are several 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 branches.



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

Enclosure – a ridge that divides into two and then reunites 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 an Island.

2. Orientation

The point on the ridge on which a minutia resides is called the orientation of the minutia point.

3. Spatial Frequency

Spatial frequency refers to how far apart the ridges are in relation to 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 location, either in an absolute sense or relative to fixed points like the delta and core points.

Are Fingerprints Really Distinctive and Persistent?

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

- **Theoretical**:

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 several 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.

- **Empirical**:

F.B.I. files alone contain over 200 million fingerprints. In all the data that has been collected over the past hundred years, using the classification methodologies described above, there have never been two fingerprints that were found to be identical.

The distinctiveness of fingerprints is clearly well established. The underlying biological persistent of fingerprints is also a well established fact reported in various fingerprint studies conducted in different scientific fields over the past century. However, there are a few factors that affect the persistence of fingerprints with respect to automatic fingerprint recognition systems:

- Automatic fingerprint recognition engines work on fingerprint images. The image is acquired by an interaction of a finger with a fingerprint reader. The quality of the fingerprint image is directly affected by the mechanism that is used to collect the print. Even fingerprints created with ink on paper; the degree of pressure, amount of ink and other factors which has nothing to do with the fingerprint itself, can still effect the information collected. The same holds true for electronic collection mechanisms. For example, a fingerprint reader may be dirty and consequently the acquired fingerprint image may have artifacts contributing to lowering the persistence.

- The underlying biological fingerprint characteristics do not change over a lifetime, barring scars from a major finger injury. However, skin conditions may change over time depending on weather, occupation, lifestyle, gender, race, and activities of the individual.

Still, even with these caveats, fingerprints are extremely reliable biometrics. While fingerprint matching is not perfect, the DigitalPersona Fingerprint Recognition Engine is best-of-the-breed, highly accurate, fast, and a reliable fingerprint matching engine.

DigitalPersona Fingerprint Recognition Algorithm Advantages

Developed by leading researchers in the field of fingerprint biometrics, DigitalPersona's Fingerprint Recognition Algorithm overcomes the issues and constraints the digital world imposes on standards of identification (passwords, smart cards, PINs, etc.). Our algorithm incorporates traditional fingerprint identification methodologies, creating each user's unique identifying information for recognition. With over ten years of study, extensive research, and testing, DigitalPersona's recognition engine is one of the most robust fingerprint recognition algorithms available today.
The performance of fingerprint algorithms is measured primarily 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 registered fingerprint user will be incorrectly 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 convenience, it may be preferable to decrease the FRR at the expense of an increased FAR.

DigitalPersona is continuously improving both the FAR and FRR of our Fingerprint Recognition Engine. Our 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. The 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 a majority of all users have such feature-rich fingerprints that they will virtually always be recognized accurately by the DigitalPersona engine and practically never obtain a false acceptance or a false rejection. The DigitalPersona 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 very difficult to match. A small fraction of users may sometimes have to try a second or even a third time to obtain an accurate reading.

Many automatic fingerprint 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 fingerprint reader that includes the basic ridge lines and minutia points on the fingerprint. 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, creating a problem for the engine. 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 fingerprint reader. It extracts the minutia points directly from this representation rather than attempting to impose an unrealistic and highly glossy skeleton model. This provides an inherently more reliable result.

In addition to making better use of the fingerprint image provided by the fingerprint reader, the DigitalPersona algorithm benefits from proprietary image processing, pattern recognition, and statistical techniques. This improves the results obtained from poor-quality dry, damaged, and minutia-impoverished prints, and blurred or skewed print images. This ability truly sets the DigitalPersona 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 their fingerprint onto the fingerprint reader at any angle. It also provides extremely low FAR and FRR. A report on the evaluation of the DigitalPersona Fingerprint Recognition Engine can be obtained from DigitalPersona upon request.

History of Fingerprint Recognition

One of the reasons fingerprint recognition is so promising is that the U.S. and other countries have extensive real-world experience with fingerprint recognition. The general public is aware of the use of fingerprint recognition in law enforcement. The history of fingerprint recognition for commerce and the long history of the study of fingerprint as a science are not so well known.

- 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 over 200 million.

About DigitalPersona

DigitalPersona is the leading provider of biometric authentication solutions for enterprise networks, developers and consumer OEMs. Founded in 1996, the company designs, manufactures and sells flexible solutions that improve security and regulatory compliance while resolving password management problems. DigitalPersona’s fingerprint readers utilize superior optical fingerprint scanning technology to more accurately authenticate users regardless of finger placement. The company’s interoperable biometric software solutions uniquely support the industry's widest array of notebooks with fingerprint readers in addition to its own line of optical placement readers. DigitalPersona’s award-winning technology is used worldwide by over 90 million people in the most diverse and challenging environments for fingerprint authentication.

DigitalPersona has strategic relationships with market-leading manufacturers and resellers including Microsoft and GTSI Corp. DigitalPersona Pro, the company's flagship turnkey security solution for enterprise authentication, is used by leading organizations such as NASDAQ, Sutter Health Network/CPMC, Royal Bank of Scotland, White Castle, Meijer’s, Lending Tools, United Banker’s Bank (UBB), Rite Aid Corp., Honda Federal Credit Union, La Caixa De Pensions De Barcelona, and Banco Azteca.

For more information contact DigitalPersona, Inc. at +1 650.474.4000 or at www.digitalpersona.com.

Fingerprint Illustrations:

J Edgar Hoover, Federal Bureau of Investigation, Department of Justice, Classification of Fingerprints, US Government