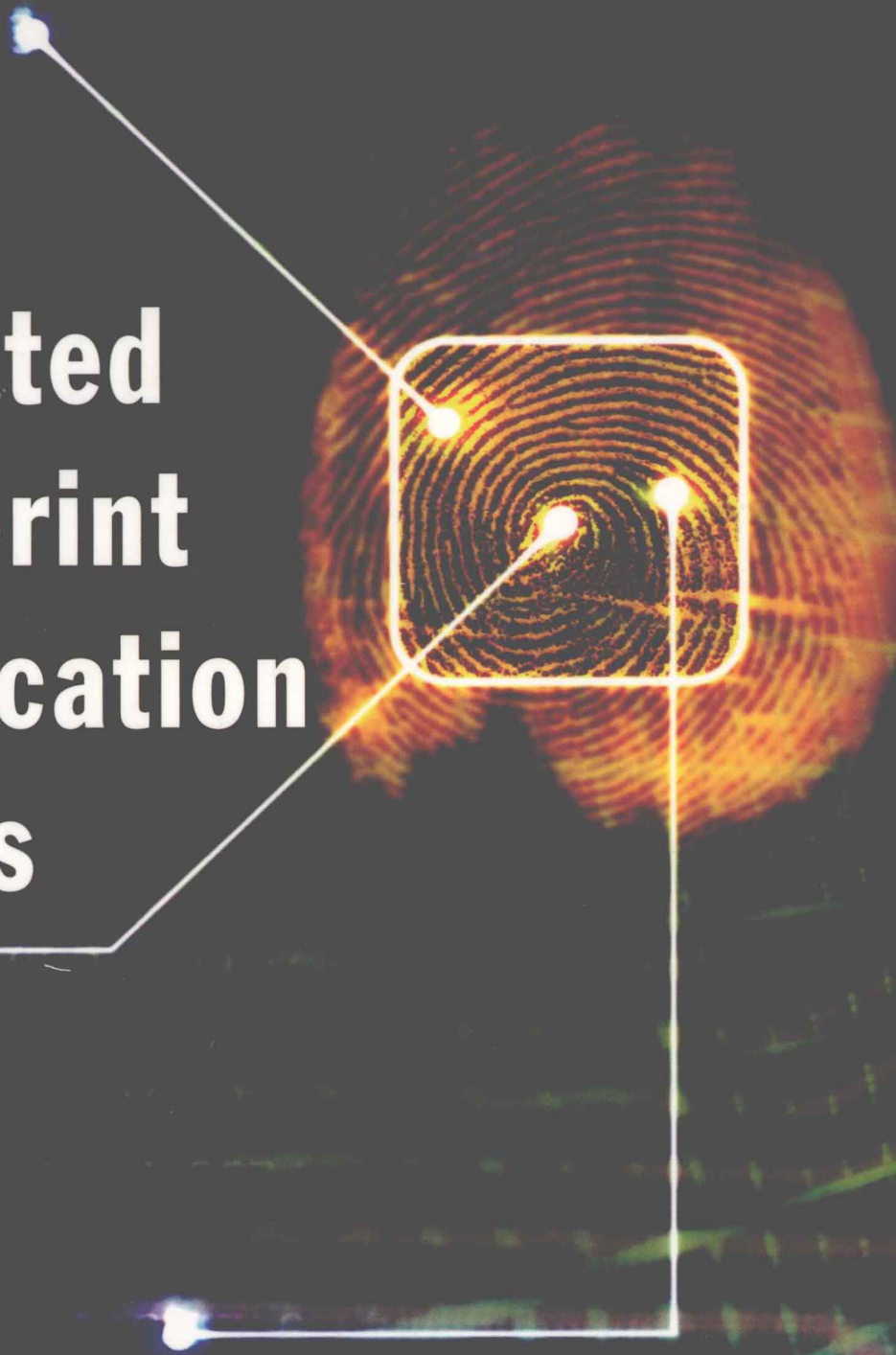
ELSEVIER
ACADEMIC
PRESS

Automated Fingerprint Identification Systems (AFIS)



PETER KOMARINSKI

Contributing Authors

Peter T. Higgins • Kathleen M. Higgins

Lisa K. Fox

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS (AFIS)

Peter Komarinski

With contributions by:
Peter T. Higgins and Kathleen M. Higgins
Lisa K. Fox

ELSEVIER
ACADEMIC
PRESS

Amsterdam • Boston • Heidelberg • London • New York • Oxford • Paris
San Diego • San Francisco • Singapore • Sydney • Tokyo

Acquisitions Editor	Mark Listewnik
Project Manager	Sarah M. Hajduk
Associate Acquisitions Editor	Jennifer Soucy
Developmental Editor	Pamela Chester
Marketing Manager	Christian Nolin
Cover Design	Eric DeCicco
Interior Design	Kenneth Burnley
Composition	SNP Best-set Typesetter Ltd., Hong Kong
Cover Printer	Phoenix Color
Printer	The Maple-Vail Book Manufacturing Group

Elsevier Academic Press
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
525B Street, Suite 1900, San Diego, California 92101-4495, USA
84 Theobald's Road, London WC1X 8RR, UK

This book is printed on acid-free paper. ∞

Library of Congress Cataloging-in-Publication Data
APPLICATION SUBMITTED

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 0-12-418351-4

For all information on all Elsevier Academic Press Publications
visit our Web site at www.books.elsevier.com

Printed in the United States of America
04 05 06 07 08 09 9 8 7 6 5 4 3 2 1

To my family, especially my wife Mary Kay, who supported my endeavors, and my friends in the AFIS community who work tirelessly to make the world better. It is an honor to work with so many dedicated and talented individuals.

FOREWORD

AFIS systems are amazing. With AFIS, people can be fingerprinted and have their criminal history records checked in a matter of minutes; a mug shot and palm print might be included on the rap sheet returned to the inquiring agency. The technology has moved from exclusively forensic or criminal applications into other areas, such as social services benefits and other emerging applications.

The greatest use of AFIS technology is for tenprint identifications, in which rolled fingerprint images are compared against enrolled records. The greatest potential value of AFIS systems lies in the area of latent print identifications. The ability of AFIS systems to search millions of records in minutes and present candidates to the latent print examiner borders on the incredible. As amazing as the AFIS systems are, however, they still rely on the latent print examiner to make the identification.

The New York City Police Department Latent Print Unit has made thousands of latent print identifications using the Statewide Automated Fingerprint Identification System (SAFIS), maintained by the New York State Division of Criminal Justice Services. Some of these identifications resulted in the arrest of burglars, some identified victims, and others resulted in the arrest of killers. Our latent print examiners have the background, training, and expertise to utilize AFIS.

Following the attacks of September 11, 2001, on the World Trade Center, the NYPD Latent Print Unit worked endlessly to identify the remains of the victims. Ultimately, the latent print examiners were able to identify over 300 victims, bringing closure and comfort to their families. This would not have been possible without AFIS technology.

AFIS systems have changed the way we do business. AFIS is a valuable tool, but nonetheless only a tool. It relies on the people who use it and those who

maintain it. AFIS can help to protect our communities by identifying those who might do us harm, and is an invaluable resource in solving crimes and making our communities safer.

Kenneth Calvey
Commanding Officer (Ret.)
NYPD Latent Print Unit

CONTENTS

CHAPTER 1

INTRODUCTION

1.1 WELCOME

There is a world in which every crime is solved in 60 minutes, DNA matches are made "While U Wait," and staff work on only one case at a time. But it is a fantasy land, an imaginary land; it is not the real world. This book is about the real world of biometric identification technology. It is a fascinating topic. This technology can confirm the identity of an individual in a split second; it can also reach back in time to place a suspect at the scene of a crime that occurred years ago.

With no more information than a picture or a fingerprint, it is possible to match a subject in question with a known individual. With or without the subject's cooperation, his or her DNA, fingerprint, portrait, or some other physical characteristic can be matched to a known person.

An identification can lead to a record, a description of a person's past. If the person has been previously arrested, the arrest information can be retrieved. If the person has previously applied for a job that required a fingerprint check, that information can be requested. Biometric identification does not need to rely on spoken information from the subject in question; even amnesia victims and the dead can be identified. Once the necessary information has been entered into a biometric database, future inquiries require only the successful comparison and matching of the biometric for confirmation of identity.

Biometrics has many implementations. Some are extremely complex, requiring massive arrays of computers and a dedicated staff. Others are relatively less complex, requiring only ink, paper, training, and experience. For example, access to secure areas can be allowed by the matching of a finger image or an iris scan. Telephone conversations using voice recognition technology can confirm the identity of the caller and allow transactions in the caller's financial account. The Federal Bureau of Investigation (FBI) master criminal file requires hundreds of people to support the database, communication lines, and inquiry processing. A latent print examiner can compare a print from a home

burglary, eliminating known prints such as those belonging to the home occupants. Each of these examples uses biometrics.

Biometric technology is often in the news. Since the events of September 11, 2001, biometrics has become increasingly of interest as public and private officials look at various methods of making positive identifications. The need for increased and improved security has become both a national priority and an area of opportunity. Many readers have experienced this increased demand for accurate personal identification firsthand when traveling on commercial flights. All air travelers must show both a boarding pass and a photograph on a form of government-issued identification, e.g., a driver's license, to pass through the airport security checkpoint. The airport Transportation Security Administration (TSA) personnel compare the photograph on the license with the face of the license holder in this simple form of biometric identification.

In an increasing number of situations, identity is confirmed by checking a verbal statement of identity or information on a written submission against a database or credential. Names on boarding passes are compared against the name on the document; faces are compared against photographs. Baggage is checked; packages and persons are subject to search.

More secure applications seek to connect a verbal statement or written document with a biometric that will not only absolutely link the person with the application, but also retrieve any personal history information stored on a database. A person's identity may be linked to a history of activities, as the identification connects to a history associated with that person. A police officer checking a driver's license, for example, can obtain the driving record of the holder. Any outstanding driving infractions, penalties, and convictions are visible for the inquiring officer to review so he or she can then determine how to proceed. To be secure, a paper form of personal identification such as a driver's license must include a biometric that is tamperproof and that will link the information on the license, not just the photograph, to the person in possession of that license. Government and industry are examining biometric options that will make driver's licenses more secure, for example, incorporating a biometric such as the characteristics from a finger image.

The U.S. government is also focusing on biometric methods used to identify terrorists, produce new passports, and allow passage into the United States by casual and business visitors. To this end, the federal government is pouring millions of dollars into biometric applications, research, and products to create new identification methods, revamp existing procedures, and make their processes more interactive from a security standpoint. New methods may include deployment of innovative software such as that used in facial recognition and improving upon technologies such as those based on fingerprints. An example of a revamped procedure is a state identification agency moving to a

24 hours a day, 7 days a week schedule rather than a 9 a.m. to 5 p.m. schedule in order to complete criminal background checks on all arrestees before arraignment. A more interactive process might include the need for agencies to collaborate on sharing database information. Decisions are being made today as to which of these changes will produce the greatest effect.

Most people have probably heard the word biometric and have a vague notion of what it means. It can conjure up images of laboratories and white coats, scientists peering over pipettes and reading printouts. A biometric is the measurement of a physical characteristic or personal trait. Certainly some of its applications do require laboratories, but many others do not.

There are also stereotypes about identification processes. Many forms of identification technology are emerging, with varying degrees of success and application. Iris scans, voice recognition, and DNA are just a few of the biometrics that have recently caught the interest of the general public, who is becoming more and more interested in security. More than ever, citizens and their governments want to have the ability to find the identity of a person and, from that identity, the history of the person. They want to know if a person has a criminal record in their own or another locale, if a person is a wanted fugitive or is dangerous, or if a person entrusted with the care of children or the elderly has any history that would make them unfit for a job with those age groups.

There is no "magic bullet" biometric. Each biometric application has strengths and weaknesses, supporters and detractors. Limitations for extensive use of a particular biometric might include the expense of the components, the speed of the processing, or the limitations on daily volumes. If a biometric device costs $100,000 per unit, plus $20,000 in maintenance per year, it may have less appeal than a device with the same accuracy but slightly slower throughput that costs $10,000 with $2,000 in annual maintenance.

The degree of public acceptance of one biometric over another is also a factor in the type of biometric used. The process of speaking to a machine that recognizes a voice pattern does not seem invasive to most people. Staring into an eyepiece for a retinal scan, however, produces a very different, very negative, reaction. Each has advantages and disadvantages, supporters and detractors.

1.2 FINGERPRINTS

There is one biometric that has been systematically used to make identifications for over 100 years. This is a biometric that has been measured, copied, and examined extensively, a biometric that does not change and is relatively easy to capture. It is a biometric that is not invasive and does not require sophisticated

hardware for analysis, making it relatively inexpensive on a per search level. This biometric, of course, is the fingerprint.

Compared to other biometrics, fingerprints are relatively inexpensive to capture. Making an identification of a print from a crime scene may not even require the use of a computerized identification system; the examiner may rely instead on the images from a tenprint card, the latent print, and the expertise of the examiner. Fingerprinting does not require a laboratory for analysis, and fingerprints remain relatively constant over time, with the exception of injury.

Each person has ten fingers, ten unique tokens tied to his or her identity. No two fingerprints have ever been found to be identical. The finger images may be scarred or cut, but can still contain enough information to link the image with the owner. The friction ridges on each person's palms also provide unique images.

Every day millions of identifications are made using fingerprint images. Each person arrested and charged with a felony, as well as many misdemeanants, are fingerprinted and have their criminal history checked. Officials want to know if people in custody have been truthful when asked for their name and background. They want to know similar information for job applicants. The huge numbers of these searches, the speed with which the identifications are completed and returned to the inquiring agency, and their accuracy verges on the unbelievable. This accomplishment would not be possible without fast computers, sophisticated software, and dedicated and talented people, and these searches would not be possible without Automated Fingerprint Identification Systems, or AFIS.

1.3 WHAT IS AFIS?

This book describes the AFIS process in summary and in detail. The following is a brief explanation of the four components of its name. The automation (A) process has eliminated the need for a print classifier to locate fingerprint cards from a file and compare two physical cards. The searchable database is composed of fingerprint (F) images collected from individuals either by using fingerprint cards or by electronic capture using a device similar to a scanner. The identification (I) aspect occurs when the person is fingerprinted, and the resulting images are searched against the database of fingerprint images on a local, state, or national database. It is considered a system (S) because it uses computers and software and can interact with subsystems and other identification systems, including other AFIS systems.

AFIS applications exist in almost every instance in which a finger image is rolled onto a fingerprint card. AFIS systems are the primary identification tool for virtually every law enforcement agency in the United States and the rest of

the world. An AFIS system can be immense, such as the 46 million records held by the FBI, or it can be small, such as when it contains information about only one city or county.

AFIS systems may be linked to other databases, even to other AFIS systems, but there are also some AFIS systems that stand alone and effectively do not communicate with any other agency. As more agencies begin working together, the number of AFIS systems connected together will grow. Stand-alone AFIS systems are more likely to join related systems, creating larger networks of fingerprints to search. The technology and applications of AFIS systems are just beginning to emerge from initial development. The scope of this technology has moved from a select few uses to everyday uses. The core of AFIS technology, the computer and related software, progresses on an almost daily basis. In particular, the software that runs AFIS systems improves constantly as companies develop faster, more accurate programs. New markets have emerged in AFIS-related applications as manufacturers carve out niche products. All of these advances, however, continue to rely on a biometric that has been systematically used for over 100 years: the fingerprint.

The use of fingerprints as a biometric used for identification of large population groups can be traced back to the 1890s, when Sir Edward Henry promoted a system of classifying the curving friction ridges and the direction and flow of ridges, patterns, and other image characteristics that allowed trained examiners to translate these images into a set of equations that could be understood by any other examiner trained in the rules of classification. The resulting classifications, in turn, dictated how the records were filed for future retrieval and comparison. A new industry emerged based on the ease with which fingerprints could be captured and a uniform method for measuring these images and storing them for future comparisons.

AFIS systems search databases for candidates based on these image characteristics. The characteristics include the points where ridges end, the points where they split, the directions that ridges appear to flow, and even dots. The AFIS system translates what a human sees as a picture, selects key features, searches these features against a database, and produces the best match from that database.

These systems are amazingly fast. It takes only a few minutes to capture the ten finger images at a booking station. Within another few minutes, the booking officer can send the images and arrest information to a state identification bureau. The state can determine the identity and return the identity information and criminal history file (known as a rap sheet) in as little as 30 minutes. If it is the first time the subject has been fingerprinted, the event becomes the first entry in the subject's computerized criminal history. If the search is for a subject charged with a criminal offense, it includes a check of all 46 million

records on the FBI database, yet it normally takes less than 2 hours, the same amount of time required to watch two episodes of JAG or the time it takes to read this book, to get the results. In that short time, the subject's images can be compared with millions of records at the state and federal level with surprising accuracy and speed.

It also takes about 2 hours for a latent print examiner to digitally capture the latent finger image found at a crime scene. By using photographic techniques and software, the latent print image can be made to appear more distinct as the image background is muted. AFIS coders extract the image characteristics from the print, such as location of ridge endings, bifurcations, and direction of ridge flow, and search all or any part of a criminal database. Databases containing millions of image records can be completely searched within minutes. This was not possible just a few years ago.

Not all AFIS systems are identical. Some large metropolitan areas have their own independent AFIS system that may or may not directly connect to the state identification bureau. The databases may be mutually exclusive or may overlap. The state AFIS system may come from a different vendor than a metropolitan area's AFIS, and one vendor's software may not seamlessly interact with another's. For example, some systems store images from the two index fingers, some use the two thumbs, and others use a combination.

In addition, some AFIS systems provide only identification information and are not connected to a computerized criminal history file. And not all AFIS systems operate on a round-the-clock schedule. Data entered into the database may not be immediately available if the database is updated only once a day. Yet in spite of these differences, the various AFIS systems have a great amount of commonality. They require the same maintenance that other computer systems require, and are subject to the same threats to security and database corruption that other information systems share.

Today, more image information, such as palm images and mug shots, are being captured and stored on AFIS systems. A single palm image may have as much ridge detail as that found in all ten fingers. Latent palm prints are estimated to be found at 30% of all crime scenes. Mug shots are used in photo arrays of suspects, and also help visually identify persons who are wanted. These are relatively new capacities made possible by better and less expensive data storage and transmission. In addition, more categories of people, such as health care workers, are being fingerprinted. These new information sources and fingerprintable categories lead to more extensive data-processing requirements, and to the increased responsibility of AFIS managers and technicians, who are handling increasingly larger and more complex systems. While not everyone in the United States is enrolled in a fingerprint-based identification system, images from an inquiry can be compared against perhaps over 50 million records. With