Contract No: FCS 53-3198-6-025
Use of Biometric Technology to Reduce
Fraud in the Food Stamp Program

INTRODUCTION TO BIOMETRIC IDENTIFICATION TECHNOLOGY: CAPABILITIES AND APPLICATIONS TO THE FOOD STAMP PROGRAM

December 1999

Authors:

Paul J. Sticha
J. Patrick Ford
R. Lewis & Company, Inc.

Submitted to:

U.S. Department of Agriculture
Food and Nutrition Service
3101 Park Center Drive
Alexandria, VA 22302

Project Officer:
Sharron Cristofar

Submitted by:

R. Lewis & Company, Inc.
1235 Jefferson Davis Highway
Suite 606
Arlington, VA 22202

Project Director:
Paul J. Sticha

NON-DISCRIMINATION POLICY

The U.S. Department of Agriculture (USDA) prohibits discrimination in all its programs and activities on the basis of race, color, national origin, gender, religion, age, disability, political beliefs, sexual orientation, or marital or family status. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2660 (voice and TDD).

To file a complaint of discrimination, write USDA, Director, Office of Civil Rights, Room 326-W, Whitten Building, 14th and Independence Avenue, S.W., Washington D.C. 20250-9419 or call (202) 720-5964 (voice and TDD). USDA is an equal opportunity provider and employer.

ACKNOWLEDGMENTS

The authors are grateful to the vendor representatives who took the time to share with us information about the capabilities of their biometric systems, components, and algorithms. We especially thank Ellsworth Clark from National Registry, Inc., Tim Nitzsche-Ruggles and Roger Todd from SAGEM Morpho, Erin Phelps and Edward de Vries from Printrak, Dawn Wilder from EDS, Wally Briefs from Cogent Systems, Inc., Paul Collier from Identicator, and Shanna Haag from Identix. These individuals graciously agreed to participate in our interviews and reviewed our summaries for accuracy. Though their review improved the quality this report, the authors remain responsible for any errors that remain.

Several other vendors responded to a request for information that we sent to the internet mailing list organized by the Biometric Consortium. Although we were not able to interview them, some sent technical and promotional materials that we reviewed in the preparation of this report. Additional information was provided by vendors through their web sites.

Finally, we thank Sharron Cristofar, the project officer from Food and Nutrition Service, who provided guidance throughout the project. This report has also benefited from the thoughtful comments of Cecilia Fitzgerald.

TABLE OF CONTENTS

Table

List of Figures

EXECUTIVE SUMMARY

In its continuing efforts to safeguard the integrity of the Food Stamp Program (FSP), the U.S. Department of Agriculture's Food and Nutrition Service (FNS) initiated this study of the use of biometric identification technologies in the FSP. As a method of reliably verifying the identity of applicants, biometric identification has the potential to reduce the vulnerability of the Food Stamp Program to duplicate participation, which has also been referred to as "double dipping."

Biometric identification technology provides automated methods to identify a person based on physical characteristics – such as fingerprints, hand shape, and characteristics of the eyes and face – as well as behavioral characteristics – including signatures and voice patterns. Although used in law enforcement and defense for several years, it has recently been used in civilian applications, such as the FSP and other assistance programs. This technology has the potential to identify individuals who attempt to apply for benefits on more than one case, or who attempt to obtain benefits belonging to someone else.

This report presents an overview of biometric identification technology with particular attention to its potential use to improve the integrity of the FSP. It briefly describes some of the major technologies, summarizes their capabilities, gives examples of applications, and discusses issues that should be considered in evaluating biometric identification technology. It pays particular attention to applications of the technology to the FSP, or to other welfare programs. Although it describes several specific biometric identification technologies, it focuses on finger imaging, which has been the primary technology used in social service programs. A companion report (Sticha, Thomas, Zamberlan, & Gribben, 1999) describes the efforts of nine States that have incorporated or plan to incorporate biometric technology in their social service programs, and discusses the cost and effectiveness of these programs, as well as the reactions to them by the client population.

Description of Biometric Technology

Biometric identification technology uses automated methods to recognize the identity or verify the claimed identity of an individual based on physical or behavioral characteristics (Mansfield & Roethenbaugh, 1998). A biometric identification device is capable of measuring individual biometric information, comparing the resulting measurement with one or more stored biometric reference templates, deciding whether they match sufficiently to indicate that they represent the same person, and indicating whether or not a recognition or verification of identity has been achieved.

One of the most common methods of biometric identification is based on the analysis of finger images. Most automated finger image identification technology uses a process analogous to that used by a human fingerprint analyst. Finger images are processed by the software to identify the location and orientation of minutiae, which include points where fingerprint ridges diverge and points where ridges stop. The minutiae of a live image are then compared to one or more stored images. If they are sufficiently similar, then a match is declared. The steps in

processing a finger image include capture of the image, image processing, feature detection, and matching.

Initial applications of biometric identification technology were for police or military organizations. More recently, biometric technology has been applied to a wider variety of civilian applications. The technology provides authentication for computer system access, eases entry into the country for frequent international travelers, replaces passwords in automated teller machines (ATMs), and verifies the time workers spend on the job. Applications differ in several ways; the specific characteristics of an application can affect the performance of the technology and its vulnerability to certain attempts at fraud.

Applications to the FSP

There are two ways to use biometric identification technology to reduce FSP fraud: when an individual enrolls for benefits and when the benefits are redeemed at a local grocery store. The goal of biometric identification technology at enrollment is to eliminate individuals who apply for duplicate benefits using more than one identity by detecting or deterring those who apply for duplicate benefits. The goal of biometric technology at disbursement is to reduce trafficking or other unlawful uses of benefits by those who are not entitled to receive them.

System Performance and Effectiveness Issues

A biometric method used at the time of application to reduce fraud in the FSP must be quick, accurate, resistant to fraud, and acceptable to clients. In addition, the technology will not be effective if it is vulnerable to attempts to change the appearance of a finger image in order to avoid detection of a duplicate applicant. Analysis of existing data suggests that finger-imaging systems are capable of detecting more than 95% of attempts to obtain duplicate benefits while incorrectly indicating fraud in fewer than 1% of legitimate applicants. System error rates can be improved by using human minutiae analysts to examine candidate matches or performing periodic unfiltered searches of the entire finger-image data base.

The performance of a biometric identification system is affected by policy decisions. For systems used at the time of enrollment, the policies regarding exemptions from biometric requirements might affect the likelihood of catching fraudulent attempts to obtain duplicate benefits. Though exemptions are required for those who are missing fingers or who cannot provide an image with sufficient quality for identification, exemptions for other reasons, such as individuals who are certified outside of the office or who have a religious objections to finger imaging, depend on agency policy.

1. INTRODUCTION

This report presents an overview of biometric identification technology with particular attention to its potential use to improve the integrity of the Food Stamp Program (FSP). It briefly describes some of the major technologies, summarizes their capabilities, gives examples of applications, and discusses issues that should be considered in evaluating biometric identification technology. It pays particular attention to applications of the technology to the FSP, or to other welfare programs. Although it describes several specific biometric identification technologies, it focuses on finger imaging, which has been the primary technology used in social service programs. A companion report (Sticha, Thomas, Zamberlan, & Gribben, 1999) describes the efforts of nine States that have incorporated or plan to incorporate biometric technology in their social service programs, and discusses the cost and effectiveness of these programs, as well as the reactions to them by the client population.

Improving the Integrity of the Food Stamp Program

The Food Stamp Program provided more than $19 billion in benefits to over 22 million individuals in 1997. As part of its ongoing effort to improve program integrity, the Food and Nutrition Service (FNS) of the Department of Agriculture (USDA) monitors the level of food stamp overpayments, and has developed and promoted procedures to reduce the ability of households to obtain benefits to which they are not entitled.

Summarizing annual FNS quality control reviews, the General Accounting Office (GAO, 1997, 1998a) reported that households receive more benefits than they are entitled to in approximately 15% of all food stamp *cases*; these overpayments represent 7% of the *benefits* that are issued. Approximately one-quarter of these overpayments were judged to be caused by intentional program violations by clients (GAO, 1994). The report enumerates four potential sources of fraud, waste, and abuse in the FSP: (1) The eligibility and benefit determination process, (2) the use of benefits for nonfood purposes, (3) the counterfeiting of food stamp coupons or their use by unauthorized individuals, and (4) the theft or loss of coupons in the mail.

Fraud Reduction Approaches

Since the integrity of the FSP is a major concern to FNS, they have pursued several approaches to maintain and enhance it by reducing the likelihood of program fraud. Until recently, investigation of questionable information given by an applicant for food stamps was a labor-intensive activity that often severely taxed the capabilities of local welfare offices (GAO, 1997). Furthermore, the resulting information – based on interviews with employers, landlords, friends and neighbors of the applicant – was often of limited reliability.

Recent technological advances have provided tools that can be used to make fraud more difficult to commit and easier to detect. For example, the Income Eligibility Verification System (IEVS), established in 1986, mandates that case records be matched with six external data bases. Relevant data bases may contain information about wages, income taxes, unemployment insurance benefits, or other information that can be used to verify the income or assets in a recipient or

applicant household. A study sponsored by FNS established the cost-effectiveness of IEVS when appropriate targeting methods were used (Maxfield & Allin, 1995). GAO (1997, 1998b) has suggested other data bases that can be used to verify the legitimacy of an application for food stamp aid. These data bases include death records maintained by the Social Security Administration (GAO, 1998b) and records of prison inmates (GAO, 1997). Comparison of case records to the information in these data bases can help ensure that ineligible individuals are not included as members of the recipient or applicant household.

A second approach to combat food stamp fraud has been the use of electronic benefit transfer (EBT) to replace paper coupons. EBT uses a card similar to a bank debit card to access benefits when food is purchased. One of the major advantages of such a system in combating fraud is that it creates an electronic record of each transaction, allowing FNS to determine where food stamp benefits were used. Most States are currently using EBT or are developing EBT programs for the FSP, as well as for other welfare programs. The welfare reform act of 1996 requires EBT programs to be in place in all States by 2002.

Recent developments in biometric identification technology have potential to provide positive identification of applicants and recipients of food stamp benefits, and consequently to reduce the level of fraud in the program. This technology provides automated methods to identify a person based on physical characteristics – such as fingerprints, hand shape, and characteristics of the eyes and face – as well as behavioral characteristics – including signatures and voice patterns. Although these technologies have been used in law enforcement and defense for several years, they have recently been used in civilian applications and show some promise to reduce fraud in the FSP and other assistance programs (GAO, 1995). This technology has the potential to identify individuals who attempt to apply for benefits on more than one case, or who attempt to use an EBT card that does not belong to them.

Sources of Information for this Report

Most of the information contained in this report was obtained from biometric technology vendors. Information from vendors was solicited through the Internet mailing list maintained by the Biometric Consortium. Several vendors sent promotional and technical information as a result of this request. The material obtained directly from vendors was supplemented with information obtained at conferences and on vendor websites, as well as reports from professional journals and articles from the popular press.

In the second phase of the data collection for this report, members of the project staff interviewed representatives of seven companies that had direct current experience applying finger-imaging technology to social services. These companies had one of three different roles in the development of biometric systems for social service applications. Four of the companies were prime contractors that integrated hardware and algorithms to produce a complete system. Two companies produced software algorithms that compared the features of finger images to determine whether or not they came from the same finger. Finally, one company manufactured one or more components of a biometric identification system. This characterization of vendors should not be considered absolute. Most of the vendors had performed some work in all three areas, although not in social service applications.

The interviews covered image capture, image processing, image matching, and overall system factors (e.g., time requirements, cost effectiveness, susceptibility to fraud). The specific questions included in the interview are listed in Appendix A. Integrators addressed all areas; manufacturers and algorithm developers discussed issues related to their products. Members of the project staff summarized each interview and asked the representative to review the summary for accuracy and appropriateness.

Organization of this Report

The remainder of this report is organized around the following ten questions addressing the capability of biometric technology to enhance the integrity of the FSP.

Description of Biometric Technology

- *What is biometric identification technology?*
- *What kinds of information can be used by biometric systems to identify individuals?*
- *How does a biometric identification system capture and analyze a finger image?*
- *How can a biometric identification system be used?*
- *How should biometric technology be evaluated?*

Applications to the FSP

- *How can biometric technology be applied to the Food Stamp Program?*
- *What impact will large-scale applications have on the cost and structure of finger imaging systems?*

System Performance and Effectiveness Issues

- *Does the technical performance of finger-imaging technology meet the needs of the Food Stamp Program?*
- *To what extent can biometric technology reduce fraud in the Food Stamp Program?*
- *How can policy determine the effectiveness of biometric technology?*

2. DESCRIPTION OF BIOMETRIC TECHNOLOGY

What Is Biometric Identification Technology?

An individual's identity can be established based on an object or token that the person possesses, something that the person knows, or a physical characteristic of the person. Keys, identification cards, and credit and debit cards are all examples of objects that can be used to establish our identity and authorize our access to our homes, cars, workplaces, funds, and credit. Although physical objects are often effective means of identification, they can be lost, stolen, copied, or counterfeited. Information an individual knows can be a combination, an account number, a password, or some other information (such as mother's maiden name). This information can increase security when it is used properly, but it is often forgotten, or it is written where it can be copied or stolen. An individual physical and behavioral characteristic, which we will term biometric information, has often been used to supplement other types of information to increase security. Pictures, physical descriptions, and signatures are examples of biometric information that has been used to establish identity. Use of biometric information can avoid some of the problems that are present with physical tokens or specific knowledge. However, because biometric information is complex and may change over time, the process used to judge whether two biometrics come from the same individual is difficult and may be prone to error.

Biometric identification technology uses automated methods to recognize the identity or verify the claimed identity of an individual based on physical or behavioral characteristics (Mansfield & Roethenbaugh, 1998). A biometric identification device is capable of measuring individual biometric information, comparing the resulting measurement with one or more stored biometric reference templates, deciding whether they match sufficiently to indicate that they represent the same person, and indicating whether or not a recognition or verification of identity has been achieved. Devices differ according to the type of biometric information they collect and the algorithms they use to process the information and detect matches.

What Kinds of Information Can Be Used by Biometric Systems to Identify Individuals?

Identification can be based on physiological characteristics – such as fingerprints, the shape of the hand, or the characteristics of the face or eye – or on behavioral characteristics – such as voice patterns, signature, or typing dynamics (Miller, 1994). Some of the more common biometric identification technologies are described in the following sections.

Finger image. Fingerprints have been used to identify individuals for hundreds of years. Law enforcement agencies have collected fingerprints of criminals since the late nineteenth century (Hopkins, 1997). These fingerprints form a data base that can be used to identify criminals from latent prints left at a crime scene. When it was done manually, the process of searching the fingerprint data base to find a match to a latent print was time consuming. Use of an Automated Finger Identification System (AFIS) has increased both the speed and accuracy of the identification process. The AFIS reviews the fingerprint data base to identify candidate matches for a latent print. The fingerprint officer then reviews the set of candidates to verify the

existence of a match. Because latent prints are often incomplete or of poor quality, the system usually produces several candidates for any set of latent prints.

More recently, finger-imaging technology has been configured to meet the requirements of civilian applications, which differ in several respects from those of its traditional criminal uses. For example, criminal fingerprinting usually involves all ten fingers, and fingerprints are obtained by rolling the finger so that a complete picture of each finger is obtained. Civilian applications, on the other hand, usually consider one or two fingers, and are based on a "flat scan" of the finger that only records the central portion of the fingerprint. Moreover, there is a difference in the relative importance of different types of identification errors in the two applications, with a false match carrying a much higher penalty in civilian applications (Wayman, 1997).

At the heart of AFIS technology is an algorithm that compares two finger images, which may vary in both quality and orientation, to determine whether they come from the same finger. Most matching algorithms work in a way that is modeled after the human fingerprint expert. They compare the details or minutiae that describe the ridges making up the fingerprint. Two finger images match if a sufficient number of corresponding minutiae can be identified on the two images. These algorithms have evolved to the point that they can correctly identify a match between two finger images as much as 98% of the time, according to a recent benchmark evaluation conducted for the Government of the Philippines (Wayman, 1997). A more detailed discussion on the interpretation of error rates is given in a later section.

Hand geometry. The three-dimensional shape of the hand has been used as the basis of accurate biometric identification device (Sidlauskas, 1994). Currently, there is only one commercially available biometric identification device based on hand geometry. The user of this device punches in a numeric code or swipes a magnetic card, then places a hand on a plate. Several guidance pins are used to ensure that the hand is properly positioned. A charge-coupled device (CCD) digital camera and mirror are then used to capture both top and side views of the hand. The device software then encodes the shape of the hand in a 9-byte code. This code is small enough to be stored on the magnetic strip on a credit card. Tests of this device conducted by Sandia National Laboratories (Holmes, Wright, & Maxwell, 1991) have shown it to have high accuracy (approximately 99.8%) and low recognition time (approximately 5 seconds). In addition, it has a relatively low cost. Hand geometry is not as nearly unique as some other biometrics and may change over time (McManus, 1996). Furthermore, the susceptibility of the system to faking by an artificial arm, and the relatively large space required by the sensor make it inappropriate for some applications (Sidlauskas, 1994).

Facial imaging and thermograms. Although the face includes many recognizable features, it can vary greatly due to aging, illness, changes in hairstyles, injuries, surgery, and other factors. Consequently, the attempt to develop automated methods for face recognition has been difficult and has met with mixed success. There is considerable variation among approaches to automated face recognition. These approaches may be classified according to whether they use visible or infrared light, and according to the specific recognition algorithm.

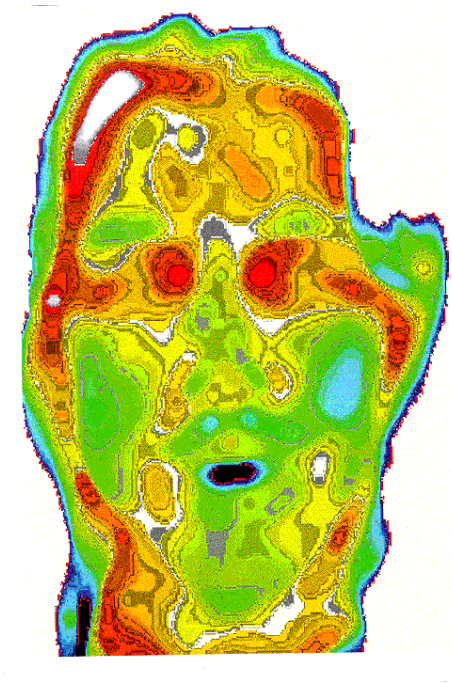

Figure 1. Illustration of a facial thermogram.

One approach to face recognition using visible light uses a neural network as the basis of its face recognition algorithm (Phillips, 1997). Another method, based on a statistical analysis of facial images, is being used to recognize the faces of drivers who are crossing the U.S./Mexico border as a part of a project sponsored by the Immigration and Naturalization Service (INS) to speed up the entry process (Visionics Corporation, 1997).

An alternative approach to facial imaging uses an infrared image measuring temperature differences in the face, rather than a visual image, as the basis for recognition. The temperature is determined by the underlying vascular structure of the face (Beale, 1997). Such an infrared image, termed a thermogram, does not look at all like a traditional photographic image (See Figure 1). However, this information seems to uniquely identify individuals; even identical twins have different thermograms.

Iris recognition. The iris of the eye has features that can be used to identify an individual with a level of accuracy that is better than most other biometrics. Like fingerprints and thermograms, the patterns in the iris are unique; even between identical twins. An image of the iris can be taken using a video camera at a distance of up to one meter. Figure 2 shows how the iris is partitioned to identify its features. The code that is used to represent the iris is represented in the upper left-hand corner of the figure. The advantages of this method include high accuracy, fast identification, and lack of physical contact with the sensor. However, the system cost is currently relatively high, compared to alternative technologies.

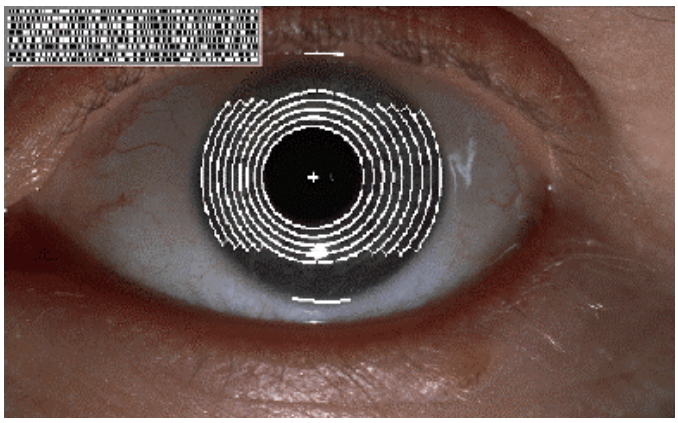

Figure 2. Illustration of iris coding scheme.[1]

Retinal scan. This technology bases identification on the pattern of blood vessels on the retina, in the back of the eye. The user of such a system looks into a viewer; the system illuminates the retina with a weak infrared light to obtain an image. These devices are very secure, with a near zero probability of a false match (de Vries, 1996). It has a fairly high likelihood of rejecting an actual match, which can be reduced to less than 1% by allowing up to three access attempts (Holmes, et al, 1991). One

[1] From *Innovation 97* [On-line]. Available: http://i97.labs.bt.com.

difficulty with this method comes from the necessity for close contact between the users' eyes and the system viewer. This level of contact makes many people uncomfortable. Currently, there is a single vendor providing systems based on retinal scanning. A pilot program using retinal scanning to prevent welfare fraud was conducted in Illinois. The retinal scanning system exhibited several difficulties with reliability and usability (Beckwith, 1997).

Voice recognition. Voice recognition is often used for controlling access to a building, because it can be conducted at a telephone at the building entrance. This technology requires an individual to enroll by speaking one or more phrases several times. The individual who seeks access will be asked to speak one of the phrases used at enrollment or a different one. For example, one system uses two random digit phrases for enrollment, and two other random digit phrases for verification (Higgins & Nichols, 1994). Using different phrases during the enrollment and verification phases makes the system less vulnerable to attack by a tape recording of the enrollment phrase. However, the identification problem is substantially more difficult when enrollment and verification phrases are different.

Signature recognition. Automated signature recognition has advantages over manual signature recognition because it takes into account the dynamics of the signature and the pressure used, as well as the shape of the characters. The user writes his or her signature with a stylus on an electronic tablet. The system tracks the location of the stylus and pressure as a function of time and uses this function as a template for verification (Falbo, 1995). A reasonable level of accuracy has been reported for such a system (GAO, 1995). However, signatures can change over time, which can reduce accuracy and require individuals to re-enroll.

How Does a Biometric Identification System Capture and Analyze a Finger image?

Manual fingerprint identification is done by comparing the characteristics of the ridges that make up each fingerprint. Of particular concern are the minutiae, which include points where ridges diverge (bifurcations) and points where ridges stop (ridge endings). Most automated finger image identification technology works in much the same way as the human fingerprint analyst. Finger images are processed by the software to identify the location and orientation of minutiae. The minutiae of a live image are then compared to one or more stored images. If they are sufficiently similar, then a match is declared.

The steps in processing a finger image include capture of the image, image processing, feature detection, and matching. The procedures used by different vendors vary in detail, but have a general similarity. This discussion is based primarily on a technical report by Hopkins (1997), but it includes information from several other vendors, as well.[2]

[2] Specifically, IBM, Advanced Precision Technology, East Shore Technologies, Identix, and Identicator.

Image capture. An example of a device for capturing a finger image is shown in Figure 3. This device consists of a light source, a prism on which the finger is placed, one or more lenses, and a digital video camera. The user of the sensor places his or her finger on the dark area of the sensor, where the prism is located. The output of the sensor is a digital image, as illustrated in the first pane of Figure 4. Although this technology is typical of the state of the art, other technologies can also be used, including holographic (Bahuguna & Corboline, 1996) and thermal imaging (Klett, 1997) technology.

Figure 3. Finger image capture device (Identix TouchView).[3]

Image processing. The image produced by the sensor must then be converted to an internal representation that can be analyzed to find identifying characteristics. Levels of gray in the original image are transformed to solid black lines representing fingerprint ridges on a white background. The algorithms that conduct this processing simplify the image, clarify smudged areas, and produce an unambiguous, skeletal image. This simplification process is called "thinning" and produces a result that is illustrated in the second pane in Figure 4.

Figure 4. Simulated image processing and minutiae extraction (from Hopkins, 1997).

Feature detection. In this step, the thinned image is analyzed to identify points where ridges end, and points where a single ridge diverges into two ridges. These points, termed ridge ends and bifurcations, are the minutiae that will be used to determine whether or not two images come from the same person. The third panel of Figure 4 shows a finger image with the minutiae highlighted. In addition, Figure 5 shows a representation of a finger image in which the ridge ends and bifurcations are clearer.

Figure 5. Processed finger image showing minutiae.[4]

[3] From Identix promotional material [On-line]. Available: http://www.identix.com/TView.htm.
[4] From East Shore Technologies [On-line]. Available: http://www.east-shore.com/tech.html.

The specific method that is used to encode minutiae is proprietary, and varies among vendors. Some vendors represent additional information, such as the direction of the ridge at each minutia, or the number of ridges between selected minutiae. Since only the minutiae are required to perform matching, the actual image may not be stored (as shown in the final panel in Figure 4). However, if a human analyst must verify matches, then the image must be retained.

Matching. Matching algorithms are proprietary products of their respective vendors, and consequently cannot be described in detail. However, all matching algorithms must be able to match images that may be different in quality, coverage, and orientation. Scanned images may be blurred, may contain smudges and discontinuities, and may vary in contrast. The matching algorithm must be able to ignore these quality differences between images taken at different times. In addition, individuals may present different parts of their finger to be imaged, and the orientation of their finger may vary between sessions. The matching algorithm must be able to identify the corresponding areas of the images under these conditions. The result of this step of the process is an index that indicates how similar the images are. If the index is over a threshold level, usually set by the user, then the two images being compared are judged to be made by the same person. In addition to matching software, some vendors manufacture special purpose hardware to speed up the matching processing.

When an image must be compared to a large data base of enrolled individuals, it may be necessary to reduce the number of comparisons that are made, so that a match may found in a reasonable time. Two procedures, termed binning and filtering, are used to reduce the number of comparisons required. Binning places images into categories based on their characteristics, such as classification type, ridge count, or some other aspect of the finger image. Filtering partitions images based on exogenous characteristics, such as sex or the identification of the finger that was imaged. The matching algorithm will then be applied only to images in the same bin or filter category. Binning and filtering can substantially decrease the time required to complete the matching algorithm. It also decreases the likelihood that the algorithm will incorrectly match two images from different fingers (termed a false match). However, because there may be errors in the assignment of images to bins or filter categories, use of binning or filtering increases the likelihood that the algorithm will miss a match between two images from the same finger (termed a false non-match).

It should be pointed out that some identification methods do not rely on minutiae to compare finger images.[5] These alternative methods often consider patterns of ridges in a more holistic fashion. Use of these methods may have the potential to increase the speed and accuracy of biometric identification technologies based on finger imaging.

How Can a Biometric Identification System Be Used?

Initial applications of biometric identification technology were in police and military applications. More recently, biometric identification technology has been applied to a wider variety of civilian applications. Some of these applications are briefly described below:

[5] See, for example, systems by Mytec Technologies, Inc., and Advanced Precision Technology, Inc.

- National Registry Inc. has developed an authentication system for computer networks based on finger images (Broderick, Morrey, & Fischer, 1997). Using this system, a computer network user would provide a finger image instead of a password in order to log on a computer network.

- The Immigration and Naturalization Service (INS) has developed a method that frequent international travelers can use to speed the entry process at selected airports (Wing, 1997). The traveler who has enrolled in the system goes to a kiosk, presents a card, and places the right hand in a hand geometry reader. After verifying the identity of the traveler, the system issues a receipt, and the traveler can bypass normal inspection lanes.

- INS has also used voice recognition as part of an automated point of entry at the U.S.-Canada border. It is also developing, along with other agencies, voice recognition capability for a similar system at the Mexican border (Wing, 1997).

- Several application of biometric technology are being tested or are in use in the banking and credit industries. For example, MasterCard is testing a finger-imaging system to verify the users of their credit cards. In addition, Chemical Bank is testing a voice verification system for check cashing (Dugas, 1996), and Citicorp is testing an automated teller machine (ATM) that incorporates iris scanning recognition technology (Sinton, 1997). Finally, a credit union at Purdue University has already incorporated finger imaging as a part of their ATMs (Chandrasekaran, 1997).

- Several companies, including Coca-Cola Co., have installed hand geometry devices to replace time cards (Chandrasekaran, 1997).

- Walt Disney World in Orlando, Florida is using hand-geometry readers to ensure that those who buy yearly passes do not lend their pass to others (Chandrasekaran, 1997).

Researchers at the National Biometric Test Center, located at San Jose State University, have developed the following taxonomy of applications of biometric technology (San Jose State University, 1996). This taxonomy can highlight the differences between applications, and identify the likely sources of error.

Verification vs. identification. There are two kinds of questions that a biometric system can answer. The first is whether a person is who he or she claims to be. This question is termed verification. Such a question must be answered when a person tries to get access to a secure facility, to a computer system, or to money at an ATM machine. In this class of application, the biometric information serves as a kind of a password used to permit access to the system. The biometric recognition software must determine if the live biometric information presented by the individual seeking access matches the information about the claimed identity. Since this method requires the system to compare one live image with one stored image, it is often termed one-to-one matching.

The second question that can be addressed by a biometric system is determining who a person is, based on biometric information. This identification task is similar to the task that must

be performed in forensic investigations, when the perpetrator of a crime must be identified based on latent fingerprints at the crime scene. In an identification problem, the live image must be compared to many stored images in a data base. Hence, this question is termed a one-to-many match.

Because it requires multiple matches, all of which must be correct to obtain a correct answer, the identification problem is much more difficult than the verification problem. Both the time needed to perform the required comparisons and the likelihood of obtaining a false match increase as the number of individuals in the data base increases. On the other hand, the probability of missing a true match is independent of the size of the data base. Processing time and false match rates can be reduced by filtering based on demographic information and binning based on additional fingerprint characteristics. Those benefits, however, come at the expense of an increased false non-match rate.

Cooperative vs. non-cooperative. This variable describes the intentions of the individual who would attempt to commit fraud on the biometric identification system. For cooperative applications, the goal of the person committing fraud is to produce a match with a record stored in the system. For example, a person who stole an identification card would try to cooperate with the biometric system to produce a match with the corresponding biometric record, and consequently gain the access that the card provides. In a non-cooperative application, the goal of fraud is to produce a non-match with records in the system. For example, a person who enrolls for food stamp benefits under two different names would try to provide poor quality biometric information to reduce the likelihood of a match. In general, non-cooperative applications tend to involve identification.

Overt vs. covert. A covert application is one in which the biometric information is provided without the individual's knowledge. Some law enforcement applications, such as analysis of latent fingerprints, are covert, but the vast majority of other applications are overt.

Habituated vs. non-habituated. This factor reflects whether individuals use the biometric system regularly, or just occasionally. User experience can lead to a substantial improvement in false non-match performance within cooperative biometric systems. For example, a person who provides biometric information on a daily basis to log onto his computer network will become habituated to the system within the first few weeks of operation. On the other hand, individuals who provide biometric information to apply for a job or enroll for benefits will never have the opportunity to become habituated.

Supervised vs. not supervised. This factor assesses whether an operator supervises the operation of the biometric system. A system operator can help to ensure that the system is used properly, which, in turn, can improve the quality of the information contained in the system.

Standard environment vs. non-standard environment. This factor assesses whether the system is used in a standard environment, such as an office, or whether the environment varies. A non-standard environment could include outdoors use, or use in store checkout lanes.

How Should Biometric Technology Be Evaluated?

A variety of factors should be considered in an evaluation of a biometric identification system (de Vries, 1996). This section briefly describes several of these factors. A summary of the capabilities of finger-imaging technology related to these factors is included in a later section.

Accuracy. There are two types of error that a biometric identification system can make: (1) it can assess that two samples from different individuals are the same, and (2) it can assess that two samples from the same individuals are different. The first of these errors is termed a false match or a false accept error. The second of these errors is termed a false non-match or a false reject error. Because the terms false accept and false reject can cause some confusion in non-cooperative applications, we will use the terms, false match and false non-match.

It is often difficult to interpret false match and false non-match rates because there is an inverse relationship between them. Often a system threshold can be adjusted to decrease one of the errors at the expense of the other, as illustrated in Figure 6. One measure of accuracy that summarizes these two error rates is the crossover error rate, which represents the error rate obtained when the system is adjusted to make the false match and false non-match rates equal. A second factor that makes interpretation of error rates difficult is that they may be assessed in a variety of conditions. For example, individuals may be given one or more chances to verify their identity using the biometric information. The false non-match rate decreases as the number of chances increases.

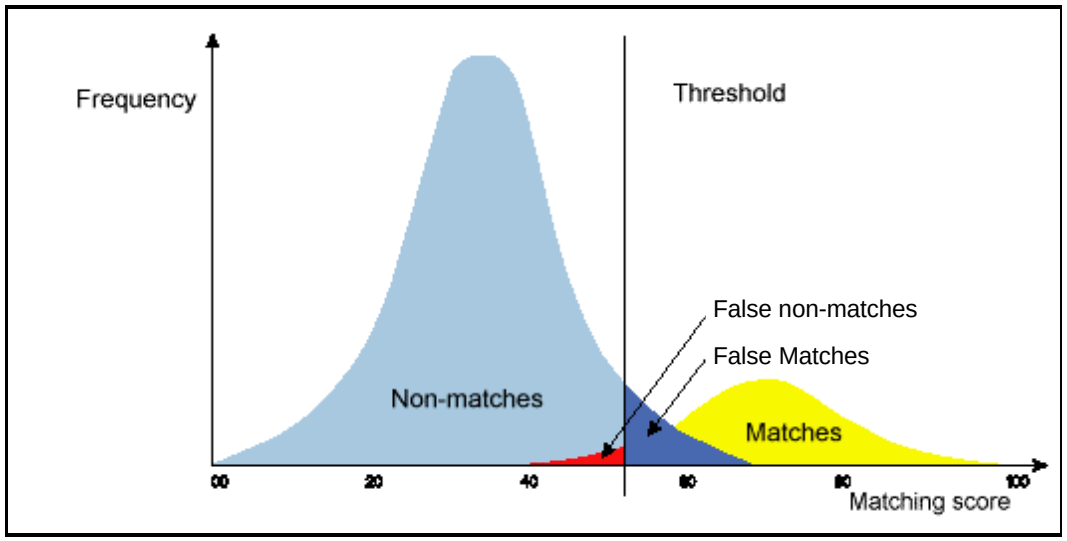

Figure 6. Illustration of identification error rates (adapted from Lee, Woodley, & Hopkins, 1997).

Whether a particular error rate is acceptable depends on the goals of the system. If the system is controlling entrance to a highly secure facility, then a low false match error rate is paramount. On the other hand, companies that are implementing biometric identification

technology for verification of credit cards are concerned with minimizing the false non-match error rate, so as not to inconvenience the customer.

Vulnerability to fraud. The types of fraud that may be committed depend on whether the application is cooperative or non-cooperative. In cooperative applications (i.e., the impostor tries to obtain a false match), technologies may be fooled by devices such as pictures, tape recordings, or artificial limbs. The effectiveness of such approaches depends in part on whether the application is supervised or not. For example, the most likely social service cooperative applications relate to disbursement of benefits and point of sale transactions. If a clerk is present to supervise the transaction, devices to obtain fraudulent false matches are not likely to be successful. Even in unsupervised applications, systems incorporate protocols to detect some types of fraud, such as the use of artificial or non-living body parts.

In non-cooperative applications, impostors try to fool the system into not recognizing that they have been previously enrolled. In social services, the most likely fraud is to enroll more than once. To be successful, each enrollment must be in a different jurisdiction, for example once in New Jersey and once in New York. Even that path to fraud is temporary because jurisdictions will increasingly conduct cross-checks. A demonstration of the practicality of cross-checking between those two jurisdictions found about 3000 matches, with about 400 potentially fraudulent.[6]

The highest vulnerability to fraud within a jurisdiction requires collusion of a clerk, for example allowing a client to register with a finger other than an index finger. There have been no recorded incidents of such collusion. There has been a case in which several people from out of the jurisdiction registered using the same address with the promise of the first month's check. In this and other scenarios within a jurisdiction, involving enough people for the gain to be meaningful increases the likelihood of getting caught. In the case of the multiple applicants, the scheme was reported through a fraud hotline.[7]

Ease of use. Ease of use is especially important in unattended environments and for non-habituated applications. In addition to the simplicity of the method, this factor assesses the social acceptability of the technology.

Applicability to entire population. For any technology, there are some people who cannot provide the biometric information required by the technology. For example, the vendor representatives we interviewed estimated that roughly .5 to 1% of the population cannot provide finger images, either because of accident or injury, or because their fingers are worn due to their occupation or age.

Speed of verification. The speed with which two samples can be compared is especially important for problems involving identification, because the candidate biometric information must be compared to each record in the data base. When the data base is large, it is possible to reduce the comparison time by restricting the search to a portion of the data base. For example, the

---

[6] Tim Nitzsche-Ruggles, SAGEM Morpho, personal communication, August 25, 1997.

[7] Dawn Wilder, EDS, personal communication, October 7, 1997.

search may be restricted to records from individuals with the same gender as the candidate. Such restriction strategies can reduce the search time, but will also increase the likelihood of a false non-match error.

Size of storage for identification tokens. The size of the biometric code is a concern when a large data base of individuals is required, or when biometric information must be stored on an access card. The size of the biometric code can impact the cost and performance of a system in several ways. First, a smaller code can be represented using a magnetic strip on an access card, while a larger code may require a smart card or other, more expensive storage method. In addition, a smaller code will require less system storage space, and can be transmitted between sites more quickly than a larger code. The 9-byte code used by hand geometry readers is the smallest code of any biometric; codes for other systems can be greater than 1,000 bytes.

Long term stability. This factor assesses the extent to which the biometric information changes over time. Behavioral attributes, such as a person's voice and signature, may change over time, as do some physical features, such as facial appearance. Stable characteristics include iris and retinal patterns, vascular structure, and fingerprints.

Proven technology. Systems that have been widely used have established the performance and reliability in the marketplace. Other technologies are in research and development stages.

Cost factors. Both the initial investment and the operating cost are important evaluation factors. The initial cost includes modifications to existing systems, initial training of operators, as well as actual procurement of the biometric identification equipment. The operating cost depends on other factors such as reliability and maintainability.

3. APPLICATIONS TO THE FSP

How Can Biometric Technology Be Applied to the Food Stamp Program?

Two types of applications. There are two ways to use biometric identification technology to reduce FSP fraud: when an individual enrolls for benefits and when the benefits are redeemed at a local grocery store. These two applications have different goals (GAO, 1995). The goal of biometric identification technology at enrollment is to eliminate individuals who apply for duplicate benefits using more than one identity. These individuals can either be detected by the biometric evaluation system, or they can be deterred from applying a second time out of fear of being caught. A biometric screen at enrollment requires a finger image or other biometric information from all adult household members or minor heads of household as a part of the certification process. Use of biometric technology in this way can also ensure that ineligible individuals, such as prisoners, and deceased individuals are not included in food stamp households.

Figure 7. Finger image point-of-sale terminal.[8]

The goal of biometric technology at disbursement is to reduce trafficking or other unlawful uses of benefits by those who are not entitled to receive them. A system designed to meet this goal would incorporate biometric data with an EBT card. When a food stamp client used the EBT card to obtain benefits, he or she would present the biometric information to verify identity and eligibility, using a device like the one shown in Figure 7.

These two applications of biometric identification technology represent considerably different components of the taxonomy of applications of biometric technology described previously. The use of the technology at the point of enrollment requires identification in a non-cooperative, overt, non-habituated, supervised, standard environment. The use of the technology at the point of disbursement requires recognition in a cooperative, overt, habituated, supervised, non-standard environment.

Examples in social service delivery. The major current and projected systems are summarized in Table 1.[9] The table is based on information obtained from the vendors in November 1997. The entries for Texas, Arizona, California, and North Carolina were updated to reflect information presented in the February 1998 issue of the *Biometrics in Human Services User Group Newsletter.* In all cases, the immediate application has been to reduce fraud by identifying duplicate registrations when applicants enroll for General Relief (GR), General Assistance (GA), Temporary Aid to Needy Families (TANF) [formerly Aid to Families with Dependent Children (AFDC)], the Food Stamp Program (FSP), or medical assistance.

[8] From Identicator promotional material [On-line]. Available: http://www.identicator.com/tpt.html.

[9] See Sticha et al. (1999) for a more detailed review of State biometric applications.

Table 1: Fingerprint Systems for Social Services

System	Location	Integrator	Scope	Size of DB
Automated Fingerprint Image Reporting and Match (AFIRM)	Los Angeles County, CA	EDS	Oct 90-Dec 98 GR, TANF, and FSP	750,000
Digital Imaging Program	Connecticut	NBS Imaging	Jan 96-Current TANF and GA ID card issuance	104,000
Automated Fingerprint Image System (AFIS)	New York State	MORPHO	Apr 95-Current GA, TANF, FSP, and others ID card issuance	925,000
Finger Imaging	Suffolk County, NY	NRI	GR: May 94-96 AFDC: 96	GR: 21,000 AFDC: 60,000
Finger Imaging	Nassau County, NY	NRI	GR: Jul 94-96 Coord. With Suffolk County	8,000 (enrolled)
Finger Imaging Project	New Jersey	NRI	GA: Apr 95-Current Newark and surrounding municipalities	22,000
Automated Identification and Match System (AIMS)	Illinois	Printrak	Feb 97-Feb 00 TANF and GA DuPage County and 2 Cook County offices	45,000
Lone Star Imaging System (LSIS)	Texas	MORPHO	Oct 96-Aug 97 TANF and FSP 10 San Antonio offices	120,000
Image Identification System	Massachusetts	Viisage	Mar-Sep 96 TANF ID card issuance	12,000
Finger Imaging	Arizona	MORPHO	Jan 98-Dec 02 TANF and FSP	700,000
Pennsylvania Automated Recipient Identification System (PARIS)	Pennsylvania	To Be Determined	Planned Welfare, FSP, and medical assistance Coord. with electronic benefit transfer	To Be Determined
California Statewide Fingerprint Imaging System (CA SFIS)	California	To Be Determined	Planned TANF and FSP	6.3 million
Biometric Imaging System	North Carolina	To Be Determined	Planned TANF, FSP, and Medical Assistance	To Be Determined

Implementation of the systems includes recertifying current recipients as well as new applicants. Enrollment of the typical client requires five minutes or less. The problem is to assure a consistent flow of current clients while continuing to process new applicants. In the Automated Fingerprint Image Reporting and Match (AFIRM) system, 600,000 clients were enrolled in three months. Using AFIRM staff to monitor the schedule and coordinate rescheduling facilitated the process.[10] In the Lone Star Image System (LSIS) pilot program, the Texas Department of Human Services used temporary staff to assist in the conversion to finger imaging during the first three months of the program.

The procedure for enrollment or recertification begins with the capture of the image of one or two fingers with a scanner and frame grabber. While the scanned image capture is less intrusive than the rolled ten-print images used in law enforcement and does not require a high level of skill, it also yields less information. Because of the limited information the image must have sufficient clarity to enable the extraction of a large amount of information. All of the systems surveyed use a capture device that provides a resolution of at least 500 dots per inch. The grabber should be able to preserve the detail without distortion. Distortion might be a factor when a system includes facial photographs that are enhanced by the frame grabber; finger images should not be enhanced.

The image is next processed to provide measures of a distinctive fingerprint. The selection and combination of these measures for a particular application provide the "art" of the fingerprint applications. All of the systems that have been used in social service delivery apply a computerized process that enters dots at minutiae points (i.e., bifurcations and ridge endings. The minutiae are converted to numerical values based on their position coordinates. The numerical values are then compared with other images in the data base. Certification algorithms for the systems vary in terms of the additional information used to facilitate the comparisons. Options include additional fingerprint data (e.g., number of ridges between pairs of minutiae), filtering based on information not related to the fingerprint (e.g., gender, age, and height), and assignment to bins based on fingerprint characteristics (e.g., loops, whorls, and arches). In large data bases, there are frequently similar fingerprints that require further investigation. This process can be automated (e.g., computerized examination of the full image) or conducted by a human expert.

What Impact Will Large-scale Applications Have on the Cost and Structure of Finger-Imaging Systems?

The results of the finger-imaging systems during the last five years have shown the systems to be effective for the required caseloads. Because of that effectiveness, social service agencies in several States, including California, Texas, and New York, have begun to apply finger imaging to larger client populations. Interviews with manufacturers and integrators uncovered some divergence in projections of the impact on costs and effectiveness of finger-imaging systems for large-scale populations. Only three of the seven vendor representatives responded to this question. One vendor, whose most immediate experience was with a relatively small data base, projected an increase in per client costs in order to achieve an acceptable false match rate. The basis for the projection was that very large applications would probably require more binning and

[10] Dawn Wilder, EDS, personal communication, October 7, 1997.

filtering (and resulting error) than current systems. On the other hand, two other vendors, with immediate experience in large data bases estimated that projected costs would be stable, with savings in technology offsetting increases in personnel costs.

The algorithms in the large applications have been shown to be robust enough to accommodate even larger data bases. For example, the algorithm used in Connecticut's Digital Imaging project is also used by the INS for a data base of one million people, including many who are highly motivated to avoid accurate prints.[11] The algorithm in Texas and California has been implemented in a law enforcement application with over 32 million people.[12] Thus the concern about the need for information beyond the finger image is probably misplaced. Two factors, however, are likely to increase per-client costs in large-scale one-to-many applications. First, the complexity of the matching requirement limits the number of potential suppliers and thereby lowers competition. Second, geographic dispersion may lower the number of clients served by each workstation. For example, in one New York county, clients were clustered so that imaging required one room and two workstations; in another county, the same number of clients were distributed across 100 miles and required eight rooms and eight workstations. In cases where the number of clients is too low to justify a workstation (e.g., 2,000), a combination of live-scan and paper-based images might be considered (New Jersey applied such an approach).

Besides larger individual systems, future applications may enable agencies to be able to share data among jurisdictions that are served by different systems, a vital component for preventing fraud and accommodating a mobile client base. For example, as discussed previously, two finger-imaging vendors have matched files from New York and New Jersey. Three approaches are possible for such cross-checking[13]: (a) exchange hard copies, (b) exchange minutiae files, and (c) exchange raw or compressed images. The feasible exchanges to date have involved images. These exchanges are facilitated by commonality among image capture devices so that all systems work with at least 500 dots per inch resolution. The drawback to wide-spread image exchange relates to the size of files: 160KB uncompressed, about 11KB compressed. Accomplishing matches with such large files requires an off-line approach, transferring to tape or other high density medium. On-line exchanges might be feasible with wide area networks. The International Association for Identification has conducted a proof-of-principle demonstration of image transfer in law enforcement using the Internet (Higgins, 1996).

Exchanging minutiae files may be a more promising approach for social service applications, because of the number of images that must be exchanged, and because social service agencies want to make quick eligibility decisions. However, exchange of minutiae files must overcome the fact that vendors use proprietary formats for minutiae files. Two options to address this issue are possible. First, the various vendor tools might be incorporated into a "super workstation." This option is less likely because it might compromise proprietary processes and impose excessive operator demands. The second approach (recommended by one vendor representative) is to use an established minutiae file format (e.g., the FBI "native mode" format) and develop utilities to write to and read from that format. Further research is required to

---

[11] Wally Briefs, Cogent Systems, Inc., personal communication, August 18, 1997.

[12] Tim Nitzsche-Ruggles & Roger Todd, SAGEM Morpho, personal communication, August 19, 1997.

[13] Tim Nitzsche-Ruggles, SAGEM Morpho, personal communication, August 25, 1997.

develop methods of sharing minutiae data generated by different systems that provide the information required for matching without compromising proprietary algorithms.

4. SYSTEM PERFORMANCE AND EFFECTIVENESS ISSUES

Does the Technical Performance of Finger-imaging Technology Meet the Needs of the Food Stamp Program?

A biometric method used at the time of application to reduce fraud in the FSP must be quick, accurate, resistant to fraud, and acceptable to clients. The need for speed comes from a desire to minimize client burden, and a need to provide expedited benefits in some cases. States have required systems to perform matching in as short a time as five minutes. A false match can also place an unnecessary burden on an applicant or client; consequently, it is imperative that these errors be minimized. It is somewhat less important to minimize the likelihood of a false non-match, because the use of the system would be expected to deter attempted multiple applications more often than it would detect them. However, the likelihood of a false non-match must be low enough for the system to be an effective deterrent to those who might attempt fraud. Of course, the technology will not be effective if it is vulnerable to attempts to change the appearance of a finger image in order to avoid detection of a duplicate applicant. Finally, clients must be willing to provide the biometric information. The following paragraphs discuss technical performance in terms of these requirements. Client acceptability of finger imaging systems is addressed by Sticha et al. (1999).

Assessment of finger-imaging technology (from de Vries, 1996). Finger-imaging technology is one of the most widely used biometric technologies. Existing devices protect against fraud caused by dummy fingers or dead fingers. The equipment operator serves as another protection against attempted fraud. It is easy to use, but, because it is often associated with criminal investigations, there may be some reluctance to use this method in the population. Verification can be made in less than 0.5 seconds, and is based on a finger image template of about 1,000 bytes. Duplicating matching hardware can increase the speed of a one-to-many match, so that the requirements for response timeliness could be met. Fingerprints do not change after adulthood, but may be worn down due to activities involved in plastering, bricklaying, or other occupations that require daily handling of rough material. In addition, the elderly and individuals with very fine fingerprints (including women of Asian descent) may not be able to provide suitable images. The vendors we interviewed asserted that approximately 99% of the population could provide finger images that are of acceptable quality for identification. This estimate has been confirmed by recent data from a finger-image identification system being implemented in the Philippines[14] that indicated 98.7% of individuals could provide an acceptable image for at least one index finger.

Likelihood of identification errors. A recent evaluation of the performance of finger-imaging systems conducted by the National Biometric Test Center (Wayman, 1997) provides both an assessment of system performance under standard conditions (verification of a single comparison) and a procedure to predict performance in other conditions (e.g., one-to-many matching). In this test, four vendors provided matching data from a set of over 8,000 finger

[14] Jim Wayman, National Biometric Test Center, communication to the Biometric Consortium Discussion List, November 18, 1998.

images. The images were collected from adult volunteers; three members of the Philippine Social Security System supervised the collection. The best of these vendors had a single-comparison false match rate of 0.01%,[15] with a false non-match rate of 2%. Other vendors could obtain similar false match rates, but only at the cost of much higher false non-match rates; in fact, the false non-match rate was as high as 20% for one vendor.

The above rates represent the likelihood of an error in a single comparison of two finger images. When biometric systems are used to prevent duplicate applications for benefits from the same individual, the finger image of each applicant must be compared to the images of many other individuals who are already receiving benefits in the program. Usually, images are obtained from more than one finger from each applicant. In such an application, the overall system error rates depend on the number of individuals in the finger image data base, the number of fingers that are imaged for each applicant, the binning and filtering methods that are used, and the criterion for judging that a match has occurred. We applied the procedures developed by the National Biometric Test Center to estimate the system false match and false non-match error rates in the one-to-many matching case. In determining this estimate, we assumed that two fingers were imaged for each individual, and that a match was declared if both of these fingers matched corresponding fingers in the data base; otherwise, a non-match was declared. We further assumed that applicants were categorized by gender, and that right and left fingers were distinguished. The effect of possible filtering errors was not considered. Finally, we assumed that fingerprint type was not used to place images into bins to reduce the number of images searched (i.e., there was no binning).

Based on these assumptions, and on a 0.01% single comparison false match rate, the system false match rate was estimated to be 0.5% for each 1 million individuals in the data base. Thus, in a situation in which 2 million individuals were represented in a finger image data base, 1% of new applicants (not in the data base) would be expected to incorrectly match existing finger images. The system false non-match rate does not depend upon the size of the data base, but it does depend on the number of fingers that are imaged and the criterion for declaring a non-match. Based on the previously stated assumptions and on a 2% single comparison false non-match rate, the estimated system false non-match rate is approximately 4%. This probability can be interpreted as the likelihood that an individual who fraudulently applies for duplicate benefits will not be detected by the system. This rate would be higher if filtering errors were considered. Filtering errors involve misclassifying the gender of an individual, or labeling the left and right fingers incorrectly. The false non-match rate would be substantially higher for those systems with a higher single comparison false non-match rate. For example, for a system with a single comparison false non-match rate of 20%, the highest rate in the National Biometric Test Center assessment, the estimated system false non-match rate is 36%.

System error rates can be improved from the estimated values by using specific procedures that reduce the impact of certain sources of error. For example, using a human minutiae analyst to examine candidate matches may reduce the false match rate. Similarly, the effect of filtering errors on the false non-match rate can be reduced by performing periodic, unfiltered or "cold" searches of the entire data base.

---

[15] This rate represents the minimum false match rate that could be detected with the sample size used.

To What Extent Can Biometric Technology Reduce Fraud in the Food Stamp Program?[16]

The counties and States that have implemented digital-imaging systems in their cash assistance programs typically consider them to be cost effective. Some of the estimated savings are very high: $5 million to $9 million in Connecticut (Mintie, 1997), $66 million in Los Angeles County (Ernst & Young, 1995), and $300 million in New York (Nawrot, 1997). On the other hand, an evaluation of the LSIS by the University of Texas did not find any reduction in cost associated with the pilot program (Schexnayder, Olson, O'Shea, Norris, Schroeder, & King, 1997). Most of these estimates are based on caseload reductions presumed to be fraud related, rather than on identifying people who attempt fraud. Few cases of attempted fraud have been reported: New York State and Los Angeles County – the two largest operational systems – have detected approximately one attempt at fraudulent duplication for each 5,000 cases. This low detection rate is not surprising; it suggests that people realize that there is little chance of fooling the system. The estimates of the level of fraudulent application for all assistance programs without finger images run from less than 2% from the Ernst & Young (1995) finding, to estimates of 10% or higher provided in our vendor interviews. Although these higher estimates have been widely reported, corroborating evidence for them has not been found (GAO, 1994). A survey of clients in Connecticut found that 6% of the clients knew someone who was prevented from cheating due to digital imaging (Connecticut Department of Social Services, 1996).

The estimates of deterrence are based on reductions in caseload. One precaution in interpreting these estimates is to avoid the assumption that people who fail to appear for digital imaging have submitted fraudulent applications or have dropped out of the social service system. Data collected by Connecticut, for example, show that a substantial proportion of the clients who discontinued benefits when the requirement for finger imaging is introduced reapplied after several months, a phenomenon known as recidivism (Connecticut Department of Social Services, 1997). The fact that these clients reapplied indicates that their cases were not fraudulent duplicates and that the reduction of these cases should not be considered a benefit of finger imaging. Consequently, caseload reduction estimates should be adjusted for recidivism to ensure that the estimates of caseload reduction do not confound reduction of fraud with general effects of recertification (which detects changes to family and employment circumstance), improved economic climate, and other welfare reform initiatives. The evaluation of LSIS by the University of Texas considered the influence of such factors by including control groups of offices that do not use a finger image system Schexnayder, et al, 1997).

In addition to meeting the fraud deterrence mandate, the implementation of digital imaging systems can have significant benefits for the administration of a State's social service program. The vendor representatives we interviewed identified three possible benefits. First, the fingerprint information can eliminate or reduce State administrative errors, such as inadvertent new case identification numbers (e.g., through an error in entering a Social Security number). Besides saving time to correct the problem, this protection prevents the issuance of duplicate benefits until the problem is identified. Second, the data base facilitates the tracking of clients who move to a different office within a jurisdiction, substantially reducing paperwork and protecting against duplicate certification. Third, the conversion of selected services can be the catalyst for

[16] Sticha et al. (1999) provide a more thorough discussion of this topic.

automating a variety of social services, with the finger image data serving as the basis for integrating the various services.

How Can Policy Determine the Effectiveness of Biometric Technology?

The technical capabilities of the biometric identification system interact with policy decisions to produce overall system performance. In verification systems, policies regarding what actions to take when non-matches occur can have an impact on system error rates, client satisfaction, and probabilities of detecting fraud. Allowing multiple attempts to obtain a match will lower the false non-match rate substantially, and raise the false match rate slightly. Policies for overriding the biometric for individuals who cannot provide the biometric information will affect client satisfaction as well as the likelihood that the system will actually eliminate fraud. In verification systems used to disburse social benefits, policy must consider due process as well as client satisfaction.

For identification systems used at the time of enrollment, the policies regarding who should be exempted from biometric requirements might affect the likelihood of catching fraudulent attempts to obtain duplicate benefits. Exemptions are required for those who are missing fingers or who cannot provide an image with sufficient quality for identification. In addition, temporary exemptions are needed for individuals who cannot provide an image due to injury or system failure. Exemptions may be allowed for other reasons, depending on agency policy. For example, exemptions may be given to individuals who are certified outside of the office or who have a religious objections to finger imaging. It is the use of these latter types of exemptions that might affect the ability of the system to reduce duplicate participation fraud. Sticha et al. (1999) describe the exemption policies of States that have implemented biometric systems in their assistance programs, and report that State representatives favor a more restrictive exemption policy.

REFERENCES

Bahuguna, R. D., & Corboline, T. (1996). Prism fingerprint sensor that uses a holographic optical element. *Applied Optics, 35,* 5242-5245.

Beale, A. (February 20, 1997). *Facial thermogram system*. Paoli, PA: Unisys Corporation.

Beckwith, B. (November 1997). Illinois biometric identification demonstrations. *Biometrics in Human Services User Group, 1(6).*

Broderick, J., Morrey, B., & Fischer, C. (1997). Network authentication solution. *Info World Electric* [On-line]. Available: http://www.infoworld.com/cgi-bin/displayTC.pl?/970616comp.htm.

Chandrasekaran, R. (March 30, 1997). Brave new whorl: ID systems using the human body are here, but privacy issues persist. *Washington Post,* p. H1.

Connecticut Department of Social Services (1996). *Connecticut survey of clients who have just been digitally imaged for AFDC* [On-line]. Available: http://www.dss.state.ct.us/faq/disurvey.htm.

Connecticut Department of Social Services (1997). *Recidivism study* [On-line]. Available: http://www.dss.state.ct.us/ faq/distudy.htm.

de Vries, E. (1996). *Comparison of biometric identification methods* [On-line]. Available: http://www.and.nl/id/gen_biom.html.

Dugas, Christine (May 15, 1996). Credit-card fraud is put to the test. *USA Today.*

Ernst & Young (1995). *Los Angeles County DPSS AFDC AFIRM program* (Annual Progress Report, May 1, 1994 - April 30, 1995).

Falbo, J. (March 1995). Signature verification. *Proceedings of the Biometric Consortium 7th meeting.*

Higgins, A., & Nichols, J. (October 1994). A software-only voice verifier. *Proceedings of the Biometric Consortium 6th meeting.*

Higgins, P. T. (1996). *Cross-jurisdictional use of AFIS Systems* [On-line]. Available: http://www.iaibbs.org/afispr97.htm.

Holmes, J. P., Wright, L. J., & Maxwell, R. L. (June 1991). *A performance evaluation of biometric identification devices* (SAND91-0276). Albuquerque, NM: Sandia National Laboratories.

Hopkins, R. (1997). *The use of fingerprinting in large-scale identity systems—technical paper 2.* Middlesex, UK: IBM.

Klett, J. (April 1997). Thermal imaging fingerprint technology. *Proceedings of the Biometric Consortium 9th meeting.*

Lee, Y. K., Woodley, J., & Hopkins, R. (1997). *Benchmarking very large civilian AFIS applications—technical paper 3.* Middlesex, UK: IBM.

Mansfield, A., & Roethenbaugh, G. (1998). *1998 Glossary of biometric terms* [On-line]. Association for Biometrics and International Computer Security Association. Available: http://members.aol.com/afb31/af00001.htm.

Maxfield, M., & Allin, S. (April 1995). *The income and eligibility verification system (IEVS) targeting demonstration: Findings and guidelines for State food stamp IEVS programs, final report.* Washington, DC: Mathematica Policy Research, Inc.

McManus, K. (May 6, 1996). At banks of future, an eye for an ID. *Washington Post,* p. A3.

Miller, B. (February 1994) Vital signs of identity. *IEEE Spectrum*. pp. 22-30.

Miller, B. (March 1995). Biometric technology: The state of the biometric market. *Proceedings of the Biometric Consortium 7th meeting.*

Mintie, D. (1997, March). Report from Connecticut. *Biometrics in Human Services User Group* [On-line], *1*. Available: http://www.dss.state.ct.us/faq/bhsug03.htm.

Nawrot, R. (1997, March). New York update. *Biometrics in Human Services User Group* [On-line], *1*. Available: http://www.dss.state.ct.us/faq/bhsug03.htm.

Phillips, K. (March 26, 1997). In-your-face security. *PC Week.*

San Jose State University (1996). *Biometrics research: A taxonomy of applications* [On-line]. Available: http://www.engrresearch.org/biometrics/taxonomy.htm.

Schexnayder, D., Olson, J., O'Shea, D., Norris, D., Schroeder, D, & King, C. (1997). *Lone Star Image System evaluation: Final report.* Austin, TX: Center for the Study of Human Resources.

Sidlauskas, D. (February 1994). Hand: Give me five. *IEEE Spectrum*, pp. 24-25.

Sinton, P. (April 11, 1997). ATM cash for your eyes only. *San Francisco Chronicle.*

Sticha, P. J., Thomas, D., Zamberlan, C., & Gribben, M.A. (1999). *Use of biometric identification technology to reduce fraud in the Food Stamp Program: Final report.* Arlington, VA: R. Lewis & Co., Inc.

United States General Accounting Office (1994). *Food assistance: Potential impacts of alternative systems for delivering Food Stamp Program benefits* (GAO/RCED-95-13). Washington, DC: Author.

United States General Accounting Office (1995). *Electronic benefits transfer: Use of biometrics to deter fraud in the nationwide EBT program* (GAO/OSI-95-20). Washington, DC: Author.

United States General Accounting Office (1997). *Food stamps: Substantial overpayments result from prisoners counted as household members* (GAO/RCED-97-54). Washington, DC: Author.

United States General Accounting Office (1998a). *Food stamp overpayments: Households in different States collect benefits for the same individuals* (GAO/RCED-98-53). Washington, DC: Author.

United States General Accounting Office (1998b). *Food stamp overpayments: Thousands of deceased individuals are being counted as household members* (GAO/RCED-98-53). Washington, DC: Author.

Visionics Corporation (October 31, 1997). *Sentri commuter lane on the US/Mexico border with FaceIt technology is now operational* [On-line]. Available: http://www.faceit.com/pr/sentri.html.

Wayman, J. L. (September 1997). Large-scale civilian biometric systems—issues and feasibility. In *CTST '97: The art of implementation* (conference proceedings). Bethesda, MD: CardTech/SecurTech, Inc.

Westin, A. F. (1996). *Public attitudes toward the use of finger imaging technology for personal identification in commercial and government programs* [On-line]. Available: http://www.nrid.com/privacy.html.

Wing, B. (1997). A report on biometrics at the U.S. Immigration and Naturalization Service (INS). *Proceedings of the Biometric Consortium 9th Meeting.*

APPENDIX A.

INTERVIEW GUIDE FOR FINGER-IMAGING INTEGRATORS AND MANUFACTURERS

Interview Guide for Finger-Imaging Integrators and Manufacturers

Introduction: The purpose of this interview is to gather information that will help people in the USDA Food and Consumer Service initiate and monitor finger-imaging applications to reduce fraud in the Food Stamp Program. While our immediate interest is the Food Stamp Program, all applications of finger imaging to enroll clients and disburse benefits in social services are relevant.

1. We understand that your company is a key component for the _____ system in [State or County].
    - 1a. Is that correct?
    - 1b. What is your company's role in that system (e.g., integrator, manufacturer, combination)?
    - 1c. What is the scope of the system (review data from table)?
        - 1c1. Programs served (e.g., AFDC, GA, FS)?
        - 1c2. Size of the data base?
        - 1c3. Include registration and point of sale verification?
    - 1d. Are you involved in other current systems (review data from table)? [We would like to consider the (pick one) system as the point of reference and note where the other systems differ.]

Image Capture

2. What capture device is used?

3. What criteria did you consider in deciding whether to build or buy the device?

4. What technology does the device incorporate (e.g., flat scan, holographic, thermal)?

5. How reliable is the capture device?
    - 5a. How often does the device need to be maintained?
    - 5b. What is the mean time between failures?
    - 5c. What is the mean time to repair?

6. How many finger images per client are captured? Does the technology put any limits on this number?

7. Is there a provision to alert registration personnel that the quality of an image is inadequate and needs to be rescanned?

8. How often do clients need to have a finger rescanned?

9. What training is given to registration personnel for operating the image capture device?

10. What percentage of the population cannot give a reliable finger image?
    - 10a. What population segments do these people represent (e.g., elderly, occupations)?
    - 10b. Are there any procedures that can aid identification of such people?

Image Processing (Assuming flat image)

11. What hardware is used for image processing (e.g., frame grabber)?

12. What criteria did you consider in deciding whether to build or buy the device?

13. How reliable is the processing hardware?
    - 13a. How often does the hardware need to be maintained?
    - 13b. What is the mean time between failures?
    - 13c. What is the mean time to repair?

14. What criteria were applied in the selection of the processing algorithm?

15. What is the average number of minutiae identified for an image?

16. Does the processing algorithm include fingerprint data in addition to bifurcation and ridge endings (e.g., ridge direction, ridge counts)? If so, what characteristics?

17. What data are stored (e.g., minutiae, image, both)?
    - 17a. How many bytes are required to store the data?
    - 17b. What data are compressed?

18. Are applicants issued identification cards that include finger-image data for verification of benefit transfers?

Image Matching (Assuming flat scan)

19. What hardware is used for matching?

20. What criteria did you consider in deciding whether to build or buy the matching hardware?

21. How reliable is the matching hardware?
    - 21a. How often does the hardware need to be maintained?
    - 21b. What is the mean time between failures?
    - 21c. What is the mean time to repair?

22. What criteria were applied in the selection of the matching algorithm?

23. Does the system use the same matching algorithm for both certification and verification?

24. Does the matching algorithm classify cases based on fingerprint characteristics (e.g., loops, whorls, and arches)? If so, what characteristics are considered?

25. Does the matching algorithm filter applicants on characteristics that are not related to the fingerprint (e.g., gender, age, height)?
    - 25a. What characteristics?
    - 25b. How reliable is the assignment of characteristics?

26. What is the maximum size of the data base that the matching algorithm can accommodate?

27. Is there any information on the accuracy of the system (e.g., benchmark studies during procurement, system accuracy tests after initiation)?
    - 27a. Verification at point of sale (1-1 match).
        - 27a1. What data base was used to test the system's accuracy (e.g., size, number of duplicate images, quality of images)?
        - 27a2. How many tries were included to establish false match and false non-match rates? How many fingers were imaged?
        - 27a3. What is the false match rate?
        - 27a4. What is the false non-match rate?
        - 27a5. (If images compressed, 17b) Did the test include compressed images?
        - 27a6. Did the false match and false non-match rates change as applicants and operators became more experienced with the system?
    - 27b. Certification at time of enrollment.

    [Same follow-up questions as 27a, but add the following.]
        - 27b7. How large was the data base against which images were matched?
    - 27c. Are there reports of the test methods and results we can obtain?

28. Does the matching procedure consider data from other jurisdictions?
    - 28a. If not, could the procedure incorporate data from other jurisdictions?
    - 28b. What characteristics are needed for systems to cross jurisdictions?

Overall System

29. How many were enrolled in the startup?
    - 29a. How long did the startup enrollment take?
    - 29b. How many enrollment sites were involved?

30. Does the algorithm include expert review of possible matches?
    - 30a. How is the expert review conducted (e.g., automated or human)?
    - 30b. What percentage of cases require expert review?
    - 30c. Does the matching protocol generate a candidate list? If so, what is the typical size of the list? What proportion of cases include more than five candidates?

31. How long does enrollment require (from image capture to certification/flag for further review)?
    - 31a. For average enrollment?
    - 31b. If the enrollment requires expert review?

32. (If system includes ID card) How long does it take to verify a client's identity when benefits are transferred?

33. Do you have any information about how applicants react to finger imaging?
    - 33a. At registration?
    - 33b. (If system includes ID card) At benefit transfer?

34. How many duplicate registrations have been found?
    - 34a. How many have been fraudulent?
    - 34b. How many duplicates could have been found with a computer search on name and social security number?

35. (If system includes ID card) How many non-matches have been found at points of transfer? How many were fraudulent?

36. What impact did the enrollment have on the number of applicants (e.g., fewer than expected enrolled)?

37. Does the sponsor consider the program to be cost effective?
    - 37a. What is the basis for the conclusion (e.g., fraud reduction, efficiency compared to manual enrollment)?
    - 37b. What is the current cost per scan (including procurement of equipment, training and installation)?
        - 37b1. For certification at enrollment.
        - 37b2. For verification at benefit transfer.
    - 37c. What trend do you anticipate in regard to cost?

38. Is there any scenario where the system would be susceptible to fraud?

39. What modifications would be required to extend this system to a regional or national application?

40. We are familiar with finger-image applications for social services in the following systems (review list from table). Are you familiar with other systems we should consider? (Name of point of contact.)

41. Are you developing any other applications that may be relevant for the Food Stamp Program?