Communications of the Association for Information Systems

FUTURE SECURITY APPROACHES AND BIOMETRICS

Serguei Boukhonine
Vlad Krotov
Barry Rupert
University of Houston
vokrotov@uh.edu

ABSTRACT

Threats to information security are proliferating rapidly, placing demanding requirements on protecting tangible and intangible business and individual assets. Biometrics can improve security by replacing or complementing traditional security technologies. This tutorial discusses the strengths and weaknesses of biometrics and traditional security approaches, current and future applications of biometrics, performance evaluation measures of biometric systems, and privacy issues surrounding the new technology.

Keywords: biometrics, computer security, information security, privacy

I. INTRODUCTION

The idea behind biometrics is not new. Even in ancient Egypt administrative workers used unique body characteristics to identify construction workers and ensure a fair distribution of food. Ashbourn [2000] relates a story about Khasekem, an administrator under the Pharaoh Khaefre, who was responsible for distributing food among construction workers. When giving out food allowances to the craftsmen, he discovered that some of them would attempt to receive their food allowance twice. To prevent future cases of fraud, Khasekem decided to create a profile for each of the construction workers. Besides such basic information as name, age, place of origin, and occupation, each profile included some of the unique physical and behavioral characteristics of the worker. Without the benefit of today's computing power, Khasekem managed to employ biometrics to eliminate what we now call double dipping.

Closer to modern times, Frenchman Alphonse Bertillon proposed a methodology for identifying criminals by anatomical measurements. This methodology, called judicial anthropometry, became popular in Europe and the U.S. In 1823, the research of the Czech Jan Evangelista Purkinje forced the scientific community to accept the idea that fingerprints are unique for each individual. The scientific thinking which emerged during the nineteenth century allowed for the development of real-world applications of fingerprint technology in the beginning of the twentieth century. In 1901 Scotland Yard became the first police force to adopt a fingerprinting system. Fingerprinting technology, now used throughout the world, is the best known example of biometrics. Other types of biometrics were not widely used until the end of the twentieth century when computers and other technologies made new approaches possible.

The tragic events of 9/11 created a new wave of interest in biometrics in the United States and other countries. This revived interest can be attributed to the potential for computer-powered biometric technologies to bring national security to a higher level of effectiveness. In June 2004, The Department of Homeland Security awarded a multi-billion dollar contract for the US-VISIT project to Accenture [eWeek, 2004]. The US-VISIT project involves developing a computer system that uses fingerprints and face recognition to track millions of visitors to the United States. Michael Chertoff, the Secretary of Homeland Security, says that the primary reason behind using biometrics for tighter boarder control is that traditional security approaches do not provide an adequate level of security [Long, 2005]. For Chertoff, "in the area of international travel, biometrics is the way forward in virtually every respect" [Long, 2005].

The UK Passport Service (UKPS) in partnership with several governmental bodies and Atos Origin, a consulting firm, is working on introducing national identity cards (passports) with biometrics features [UKPS, 2005]. A number of other countries are either piloting or planning to introduce National ID cards with biometric security features [Nanavati et al., 2002].

Endorsements of biometric technology by influential organizations, as well as extensive coverage of the technology by the mass-media, may create an impression that biometrics is totally replacing old approaches to security. This is not true, at least at this stage of development of the technology. For biometrics to become commonplace, the technology must be reliable, inexpensive, easy to use, deployable in a variety of environments, and non-invasive. Moreover, the end users of biometric solutions must be educated about the technology and comfortable with the privacy implications of the technology.

A decision to implement biometric security systems must be based on thorough comparative evaluation of biometrics in relation to traditional security approaches. To perform an evaluation, both the basic operating principles of the various biometric solutions and their strengths and weaknesses must be understood. Privacy implications of biometrics are also important when deploying biometric solutions. The purpose of this tutorial is to educate the reader on these (and many other) dimensions.

This tutorial begins with the discussion of numerous security threats faced today by a typical organization. Then we discuss strengths and weaknesses of traditional security approaches in addressing these threats (Section II). Section III begins with an elaborate definition of the term "biometrics" followed by a discussion of some of the fundamental operating principles behind biometric systems. After that we discuss, in detail, each of the main types of biometrics technologies (Section IV). For each of these types of biometrics, we discuss operating principles, advantages and disadvantages, and vulnerabilities to spoofing. The section also looks at some of the less common and emerging types of biometric technologies. In Section V we provide examples of current and future applications of biometric technologies. We look at biometric system performance from both technical and social perspectives in Section VI. The tutorial ends with a discussion of privacy concerns related to biometrics (Section VII) and with implications for research (Section VIII).

PROLIFERATION OF SECURITY THREATS

Even though the current publicity surrounding biometrics can be largely attributed to its recent application in the public sector, biometric security technologies evolved because of the proliferation of computer security threats. It was not until the mid-to-late 1980s that networked computing became sufficiently ubiquitous for penetrations to become a significant problem. The growth of the Internet, e-commerce, and other computer technologies since the 1990s magnified existing threats while giving rise to new classes of threats (Table 1). Driven by these threats, what were then new computer security approaches, such as virtual private networks (VPN) and public key cryptography, gained widespread popularity?

Table 1. Perceived Computer Security Threats Comparison: 1992 Versus 2004

Most severe threats in 1992	**Most severe threats in 2004**	
Natural Hazards	Theft of Proprietary Info	Sabotage
Inadequate control over media	Denial of Service	System Penetration
Weak and Ineffective Controls	Computer Viruses	Abuse of Wireless Network
Hacking	Insider Net Abuse	Telecom Fraud
Access to system by competitors	Financial Fraud	Unauthorized Insider Access
	Laptop theft	Telecom Eavesdropping
		Misuse of Public Web Applications

Reprinted with permission from Computer Security Institute, 2004

Biometric technology, the subject of this tutorial, is an emerging security approach. One of the primary differences between biometrics and some other new computer security technologies is that biometrics is not a pure network security measure. While security measures such as cryptography and VPN are used primarily to prevent unauthorized access to intangible resources, biometrics can be used in both network security and more tangible domains, such as access control and crime/terrorism prevention. Since biometrics can be applied in many domains, the technology can, potentially, become a widely used security approach.

II. TRADITIONAL SECURITY APPROACHES

A number of security approaches have been developed in response to proliferating threats to security. Both traditional and biometric security approaches can be broken down into two general types:

- passive, and
- active.

Passive approaches are like a shield - they protect against a clear and present danger such as a hacker attempting to access a computer system. Traditional security technologies are mostly passive. Active approaches are more like prevention via a preemptive strike, for instance, arresting terrorists before they plant a bomb. One of the traditional ways to search proactively for and identify lawbreakers relies on massive use of manpower such as police on patrol or security guards in casinos watching closed circuit television in the hopes of identifying known cheats. Needless to say, that measure of active security is costly and is not widely used in a commercial environment. Even data mining numerous electronic databases (e.g. in an attempt to detect suspicious activities of a suspect) may be troublesome, since a suspect may use multiple identities.

Another fundamental weakness of traditional security approaches is that they are based on either

- what you *know* (i.e., password or PIN) or
- what you *have* (i.e., keys, cards, etc.), or a
- combination of both (ATM card + PIN) [Ratha et al., 2001].

A fundamental problem with PINs and passwords is that, to be effective, they must be complex. However, complexity of passwords and PINs makes it hard for users to remember them. Because of that, a user may write down his or her password on a note and attach it to the monitor or to the back side of the keyboard. Thus, a strong password policy may not contribute to overall system security [Reid, 2004]. Another fundamental problem with PINs and passwords is that they identify a card rather than its user [Ashbourn, 2000]. In other words, even though a person knows the PIN associated with the card or password associated with the username, that person may not actually be the owner of the card or the authorized user. In addition, passwords are often easy to guess, crack by brute force, or obtain through other means such as social engineering (e.g. an intruder posing as a system administrator calling an employee and asking for the user's network password). Obtaining the card and PIN or the username and password might be difficult, but it is far from impossible. A serious flaw with this possession requirement is that anybody can gain access to a resource if she or he has a security artifact (e.g. a key or a card). Many of the security artifacts can be easily counterfeited [Ashbourn, 2000]. Even sophisticated security mechanisms, such as an ATM card, can be lost, stolen or maliciously taken away and used by an unauthorized person. Thus, card/PIN or username/password combinations provide relatively weak network security. Table 2 provides a brief overview of strengths and weaknesses of traditional security approaches.

Table 2. Traditional Security Approaches

Security Approach	**Strengths**	**Weaknesses**
Lock and key Lock and key is probably the oldest security mechanism used to protect assets	Low cost, simplicity, ease of use, robustness	Can be easily duplicated; not convenient to carry; can be lost or stolen; hard to manage in large organizations
Numeric keypad A security mechanism that requires users to enter a password using a numeric keypad to gain access to a premise or an asset	Easy to use and maintain, robust	Often forgotten; low security
Magnetic stripe card Magnetic stripe card is usually a plastic card with a magnetic strip that contains authentication information. Credit cards are an example of a magnetic stripe card	Low cost, easy to reprogram, easy to manage	Easy to duplicate; sensitive to environment
Punched card Punched card is usually a paper card with holes punched on it to record information, such as access code	Cheap to make and easy to manage	Easy to duplicate; low security
Proximity card Proximity card is a wireless access security device, which opens a premise when being placed in the immediate vicinity of a radio frequency reader that wirelessly reads authentication information from the card	No physical contact—very robust	Expensive and interferes with other electrical devices
Wiegand card [Ashbourn, 2000] Wiegand card employs a unique technology that is used to transmit information between a card and a slot-based reader	Robust and secure; non-contact; can be used in harsh environments	Expensive
Infrared card Bar code information on an infrared card can be read only with the help on an infrared reader – it cannot be seen by a person or copied with a copy machine [ATI, 2004]	Secure, inexpensive	Can be easily duplicated, sensitive to harsh environment
Smart card Smart cards are plastic cards with an embedded microprocessor and/or memory chip used for storing information and providing secure exchange between the card and a reader	Secure; can store a relatively large amount of data	Relatively expensive, requires direct contact, card contacts are sensitive to dust and wear

Adapted from Ashbourn, 2000

III. BIOMETRICS

DEFINITION

Biometrics can be defined briefly as methods for recognizing people based on unique physiological or behavioral characteristics [Ashbourn, 2000; Jain et al., 2000]. Biometrics introduces the third "pillar" of security [Reid, 2004]. Traditional security approaches rest on two pillars: something you *know* or something you *have*. Biometrics authenticates or identifies a person not as much on what she has or knows, but based on something she is (a measurable trait).

Clarke [1999] provides an expanded definition of biometrics: person-identification techniques based on such difficult-to-alienate characteristics as appearance, social behavior, bio-dynamics, natural physiography, and imposed physical characteristics.

- Appearance refers to details of a person's general visual image, such as shape of a face distance between eyes, or height.
- Social behavior can be manifested, for example, through voice particularities and body gestures.
- Bio-dynamics includes the manner in which he or she writes a signature, performs a key-stroke, or moves a mouse.
- Natural physiography refers to such characteristics as skull measurement or fingerprint sets.
- Imposed physical characteristics involve artificial creation of physical characteristics of a person by, for example, implanting a microchip under the skin.

Even though these characteristics provide a precise way of classifying different types of biometrics, biometric types are generally classified based on two generic categories: *physiological* and *behavioral*.

A physiological biometric is a manifestation of some physical trait (e.g. fingerprint pattern or iris pattern). A behavioral biometric can also be based, in part, on physiological characteristics. For example, our voice is influenced, in part, by physical characteristics of the diaphragm. In a similar manner, the length and flexibility of our fingers probably influence, to some extent, our typing pattern. Still a behavioral type of biometric differs from a physiological one. While physiological traits are for the most part determined by Mother Nature, behavioral traits are learned. Thus, the manifestation of behavioral traits involves the application of cognitive processes.

HOW BIOMETRIC TECHNOLOGIES WORK

To discuss biometric technologies, the reader needs to understand the fundamental operating principles behind biometric systems. As in centuries past, biometric technology today relies on two fundamental mechanisms

- authentication and
- identification.

The objective of authentication is to determine if a particular person is who she or he claims to be, for instance to cash a check. Identification systems, by contrast, capture a person's biometric information, say at an airport boarding gate, and then compare it with templates stored in a database looking for a match. Authentication systems often require active participation by the individual.

Authentication Systems

The general process for authentication systems is outlined in Figure 1. The authentication process starts with, for example, an individual inserting a smart or magnetic card into a reader (instead of a card, the user may key in his or her username). If it is a smart card, the reader reads a biometric template from the card. Otherwise, the reader reads the username. Afterwards, the user's live biometric information is captured and compared with the template either read from the smart card or obtained from the database. If the system determines that the individual is who she or he claims to be, access is granted. Otherwise, access is denied. While the authentication process looks like today's common security systems, biometric systems differ in several respects.

1. Biometric information captured from the individual attempting to use the card serves as a means of verifying that the person attempting to use the card is the person to whom the card was issued.
2. People cannot forget biometrics as one might a PIN.
3. Biometrics are unique for each person.

Figure 1 shows the logic of a typical biometric authentication algorithm

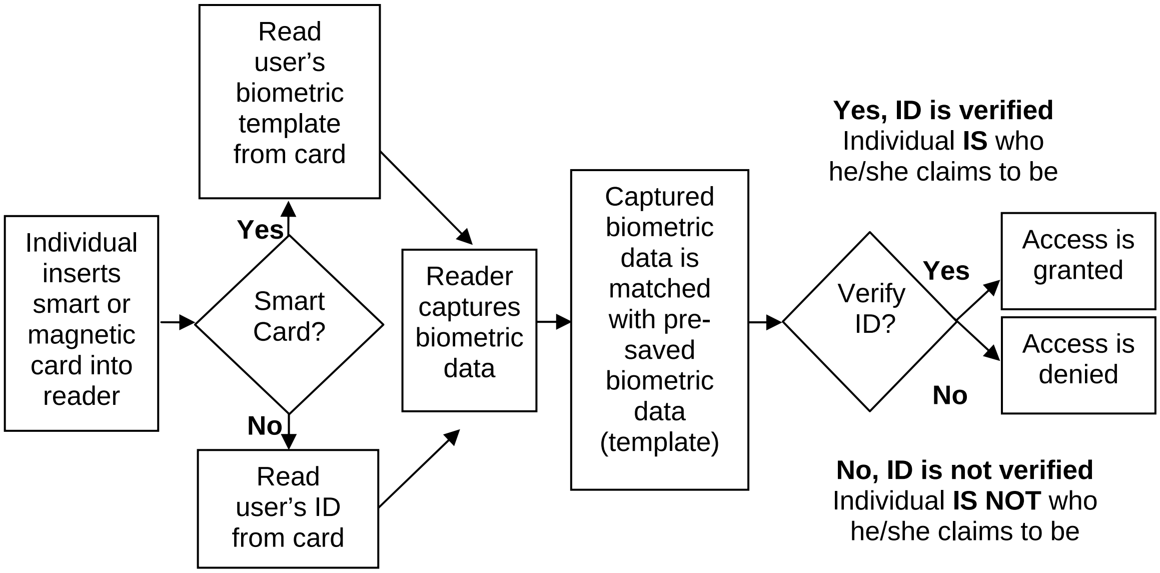
Individual inserts smart or magnetic card into reader
Smart Card?
Yes
Read user's biometric template from card
No
Read user's ID from card
Reader captures biometric data
Captured biometric data is matched with pre-saved biometric data (template)
Verify ID?
Yes
Access is granted
No
Access is denied
Yes, ID is verified
Individual IS who he/she claims to be
No, ID is not verified
Individual IS NOT who he/she claims to be

Figure 1. Biometric Authentication Algorithm

Identification Systems

Identification systems are either passive to the individual (they can be used without the user's knowledge) or are active (they require the individual to provide biometric data, that is they require active cooperation from the user). An example of a passive identification system would be a surveillance system at a stadium entrance that automatically captures face images of entering sports fans with the help of a digital camera. The face images captured are then passed to a computer that attempts to find a face match in a database containing face images of previously arrested violent fans. In this hypothetical example, the "troublemakers" are being identified passively.

An iris recognition system installed near the entrance to an airport is a hypothetical example of an active identification system. A security guard may ask entering passengers to look into an iris recognition device. The iris image obtained is compared with iris images in a database that contains iris images of people with a criminal record or people whose personal background may indicate an inclination to terrorism. If a person is identified as such, more thorough search procedures may be applied to him or her before the person boards a plane. In this hypothetical example, criminals are being identified actively, that is they are made aware of the identification system by being asked for their cooperation. Figure 2 shows the conceptual algorithm behind an identification system.

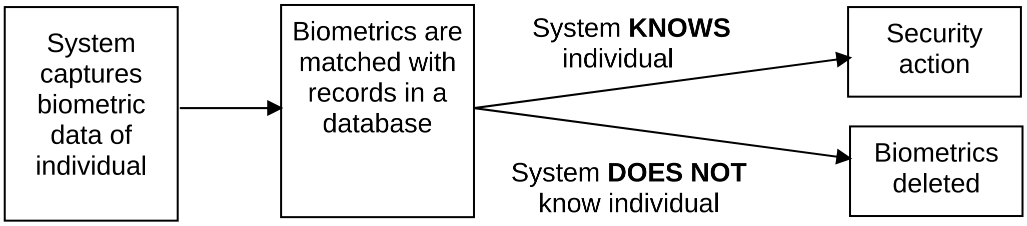
System captures biometric data of individual
Biometrics are matched with records in a database
System **KNOWS** individual
Security action
System **DOES NOT** know individual
Biometrics deleted

Figure 2. Biometric Identification Algorithm

Under the identification algorithms, the individual does not take any intentional actions to identify himself or herself. The biometric data is captured by the system automatically, without the active participation of the user. Then the system uses the database to determine whether the system knows or does not know the individual. The database can consist of biometric data of people who impose a potential public threat (e.g. criminals, terrorists, violent sports fans). The primary task of the system is to try to find a match between the biometric data obtained from the individual and numerous biometric templates stored in the database. For this reason the process of identification is also known as a "one-to-many" comparison [Ashbourn, 2000]. If this type of individual is identified by the system, then action results (e.g. the system notifies the police about the presence of the individual). Otherwise, the captured biometric data is deleted.

IV. TYPES OF BIOMETRIC TECHNOLOGIES

Biometric technologies can be classified according to the input data source they rely on for authentication and identification. Some of the most common body parts that are scanned by biometric systems are hands, faces, and eyes. Voice is also widely used in such applications as automated call centers. Table 3 presents a brief comparative overview of these biometric technology types.

FINGERPRINTING

Operating Principles

The basis for this biometric is that the macro and micro features of each individual's fingerprint are unique [Reid, 2004]. Fingerprints are usually captured with the help of a scanner. The image of a fingerprint can be enrolled and matched using one of the following algorithms: *minutia-based*, *pattern-based*, and *hybrid*. Enrollment is a process of acquiring a biometric image from an individual and storing it as a template in a database for future verification of the user's identity.

Minutia-based algorithms enroll and match fingerprints based on micro characteristics. Micro characteristics are small details (minutia) of a fingerprint that cannot be seen with the unaided eye. While minutia are classified into formalized categories, they can be seen as tiny "pixels" or groups of "pixels" that comprise an image of a fingerprint. Just like a digital image can be reduced to and analyzed based upon individual pixels, a fingerprint image can also be reduced to "pixels". These "pixels" are building blocks of overall fingerprint patterns. Since minutia-based algorithms

Table 3. Human Body and Types of Biometric Technologies

Body Part	Biometrics Type	How it works	Advantages	Disadvantages	Use Examples
Hands	Fingerprinting (natural physiography)	Uses unique micro and macro features of fingerprints	Easy to use, inexpensive; fingerprints databases are already available	Less reliable than retina or iris scanning	Access control, computer access control
	Hand geometry (natural physiography)	Captures up to 90 unique hand characteristics	Easy to use and inexpensive	Balky and sensitive to environment	Access control, computer access
Face	Face Recognition (natural physiography/appearance)	Face recognition captures characteristics of a face either from video or still image and translates them into digital form	Suitable for identification applications, relatively unobtrusive	Prone to errors caused by environmental influences (e.g. light), and personal changes such as sunglasses, or facial hair.; expensive	Identification (law enforce-ment); identity authentication
Eyes	Iris Scanning (natural physiography)	Captures unique patterns of an iris	Secure, does not need physical contact, non-intrusive	Expensive, sensitive to environmental conditions	High security applications in controlled environments
	Retina Scanning (natural physiography)	Captures unique pattern of blood vessels	Secure and accurate	Expensive; requires perfect alignment - usually a user must look in monocular or binocular receptacle	
Voice	Voice Recognition (social behavior)	Captures unique characteristics of voice	Easy to use and understand, non-intrusive	Sensitive to background conditions such as noises	Automated call centers

Adapted from Ashbourn [2000]

match fingerprints based on a large number of micro characteristics, these algorithms are usually more accurate in the matching process than pattern-based algorithms.

Pattern-based algorithms use both micro and macro features of a fingerprint for matching and enrollment. Macro features are relatively large components of a fingerprint pattern that can be seen with the unaided eye (arches, loops, and whorls). When macro features are used, a larger fingerprint image is necessary (a sufficient number of micro features can be captured with only a portion of a fingerprint image). Authentication based on macro features is usually faster than authentication based on micro features.

Hybrid algorithm leverages the best features of both minutia-based and pattern based algorithm. Thus, hybrid algorithms can provide a middle ground between accuracy of minutia-based algorithm and speed of pattern-based algorithm.

Advantages

Fingerprinting is the most widely used and accepted form of biometrics [Reid, 2004]. Fingerprinting has been used in criminal justice for many decades. As a result, it is based on rigorous procedures developed and verified over the years. Criminologists and the general public accept fingerprinting as a valid form of identification. The popularity of fingerprinting can be also explained by the relative ease with which this biometric is obtained. The computerized procedure for obtaining fingerprints (with the help of a finger scanner) is simple when compared to other biometric procedures, such as iris or retina scans. Another advantage of fingerprint biometrics is that fingerprint scanners are relatively cheap. A fingerprint scanner can be purchased for under $50, while an iris scanner can cost around $1000. Furthermore, fingerprint capture is not sensitive to environmental conditions (such as light) and can be deployed in virtually any environment.

Disadvantages

The three main disadvantages of fingerprint biometrics are the inability to enroll some users, performance deterioration over time, association with forensic applications, and possible short-term changes in a person’s fingerprints [Nanavati et al., 2002].

- *Inability to enroll some users*. A small percentage of the population may not (or may have difficulties with) enrolling in fingerprint systems. Certain ethnic groups (e.g. black and some Asians) and demographic groups (e.g. older people or people involved in manual labor) have less distinct fingerprints, which may prevent them from being enrolled or matched against stored templates.
- *Performance deterioration over time*. Performance of some fingerprint systems is found to drop drastically because of daily wear. The drop in performance can be up to 25% over the span of 6 weeks for some finger-scan technologies.
- *Association with forensic application*. Some individuals feel uncomfortable participating in authentication procedures traditionally associated with criminals.
- *Short-term changes in fingerprints*. Fingerprints of a person performing manual labor which involves damage to the hand’s skin or working with oily substances (e.g. an auto mechanic working without gloves) may change the fingerprints pattern or decrease the readability of the pattern.

Spoofing

In the context of biometric technologies, spoofing is defined as an attempt by an intruder to trick a biometric system into thinking that it is presented with a real biometric feature of an authorized user when it is not.

Finger biometric systems can be spoofed [Reid, 2004]. Table 4 summarizes potential spoofing attacks and ways of mitigating the attacks.

HAND GEOMETRY

Operating Principles

The hand geometry biometric uses the hand’s unique characteristics (e.g. the height and width of the hand and fingers) to authenticate a person. To enroll in the system, a user places his palm on a metallic sheet of the specialized hand geometry device. Cameras acquire the 3D image of the hand and use the image to match with a 3D image of the hand stored at the time of enrollment.

Table 4. Possible Attacks on Finger Biometric System

Possible Attack	Mitigating the attack
Attacking the physical finger After obtaining a fingerprint image, a fake finger can be produced from a number of materials. In an extreme case, a individual's finger can be severed and used for breaking into the system.	• Sensors measuring temperature or detecting pulse can be used to detect whether the finger is "alive" (e.g. measuring temperature or detecting pulse). • Multiple fingers can be used to authenticate a person. Capturing fingerprint images of several fingers without the person knowing is much harder than obtaining an image of just one finger. • Finger biometrics can be used together with passwords or tokens to strengthen authentication.
Using artifacts After a person places a finger on a scanner, the image of the finger can be left on the scanning surface. An intruder can place an object (e.g. a plastic bag with water) on the scanning surface to trick the system into thinking that an actual finger is placed. This spoofing technique is largely based on operating principles of sensors used to capture fingerprint images.	• Software can be used to remember the last finger image scanned. An immediate reoccurrence of the image may signal an intrusion attempt. • A sensor can be used to detect whether the finger is "alive" (e.g. measuring temperature or detecting pulse)
Attacking the communication channel An intruder can use the communication channel between a scanner and network to tamper with the biometric data.	• Continuous monitoring of the connection between the scanner and the network can be used to prevent this type of attack. An interruption in connection may signal an intrusion • Biometric information can be encrypted to prevent eavesdropping • Session keys can be used to ensure that biometric data is not "replayed"
Compromising the template An intruder can break into the system and change the reference template against which newly acquired images are compared.	• Standard information security technologies can be used to protect template data
Attacking the fallback system Occasionally, an authorized user may not have been previously enrolled in the system. Moreover, the system can expect failures from time to time. The fall-back procedure, designed to take care of these situations, can be taken advantage of by an intruder	• The fallback procedures must be designed in a way that foresees possible ways of attempting to trick the system

Adapted from Reid [2004]

Advantages

Hand geometry strengths are[Nanavati et al,, 2002]:

- Hand geometry is able to operate in harsh environments. The technology is not as sensitive to light, dust, or temperature as some other biometric technologies.
- It is a well-established technology. Hand geometry has been used in such applications as access control for many years. A number of vendors already provide reliable hand geometry stations.
- It is relatively non-intrusive. Submitting a hand for measurements is certainly less intrusive than, for example, positioning one's eye for iris scanning.

- Hand geometry is a relatively stable physiological characteristic. Unlike fingerprints, hand geometry is not likely to change significantly in the short term.

Disadvantages

The weaknesses of hand geometry include [Nanavati et al., 2002]:

- The accuracy of hand geometry is inherently limited by the lack of physiological variety in hand geometry characteristics among individuals and by the relatively small number of hand characteristics that can be captured with a hand scan.
- The relative dimensions of hand scan stations limit the scope of potential applications. Hand geometry stations are usually bulky and, as a result, may not be convenient to use in certain applications. For example, it may not be practical to place hand geometry scanning stations near each computer on a corporate network
- The system cannot enroll certain people (e.g. individuals with a crippled arm).

Spoofing

Potential spoofing techniques and mitigation strategies in the case of hand geometry are similar to those discussed for fingerprinting. However, reproducing a hand without the knowledge of the individual may not be feasible. While an intruder can potentially copy a person's fingerprint image from a flat glass surface and construct a finger with the same fingerprint, reconstructing a hand geometry (even with the consent of a user who has access to the system) is much more complex.

FACE RECOGNITION

Operating Principles

The face consists of many distinct micro and macro elements [Reid, 2004]. The macro elements include the mouth, nose, eyes, cheekbones, chin, lips, forehead, and ears. The micro features include the distances between the macro features (or the distances between macro features and reference points) and the size of macro features. In addition, faces, like any body parts, radiate heat. Heat radiation patterns can be captured with the help of infrared cameras and used for authenticating and identifying users. Face images can be captured either "on the spot" through real-time acquisition or by photographs or videos. Four major types of algorithms are used for enrolling and matching a face image:

- *Eigenface*. The staring point of eigenface algorithm is capturing a two- dimensional grayscale image of a face. The unique geometry of the face is then described mathematically and stored as a template. When a reference face image is obtained, it is also transformed into a two-dimensional grey-scale image and then matched against the template.
- *Local Feature Analysis*. The first step under this algorithm is identifying reference points on a face image. A reference point can be a corner of the mouth, an end of an eyebrow, the center of an eye, and many other "face landscape" features. Reference points are detected by analyzing the shading around each feature. For example, the image of one's nose can be surrounded by shadows that can lead the system to identify the face image area as a nose and then locate its central point (the tip of the nose). After all the necessary reference points are identified, the set of reference points is connected with straight lines forming numerous triangles. For example, a triangle can be formed by connecting the centers of eyes with each other as well as the tip of the nose. The angles of the resulting triangles are then measured and recorded in a template. The template is further used for matching newly acquired face images. Needless to say, light conditions severely impact the algorithm.
- *Neural Networks*. A neural network is a computing paradigm that relies on algorithms that imitate the processes of a human brain. In a similar way as our brains learn to

recognize faces, a biometric system can be taught to recognize and differentiate faces [Nanavati et al., 2002]. Neural networks use a wide array of features to determine whether the face image is similar to the one previously stored (template). Each feature "votes" on whether the face is similar or not. A correct vote "raises" the importance of a particular face feature in further matching attempts. Likewise, an incorrect vote lowers the importance of a particular feature as a predictor of whether face images match. Over time, the system learns to recognize faces through this learning process, which is somewhat similar to a trial and error approach. Theoretically, this method can produce greater face recognition success rates in complex environments.

- *Automatic face processing*. This algorithm uses macro face measurements and sizing (e.g. mouth width) to find a match quickly and efficiently. The downside to this algorithm is that facial expressions can impact recognition effectiveness (e.g. a smile would change mouth width).

Advantages

Face recognition's strengths in comparison with other biometrics are [Nanavati et al., 2002]:

- *Ability to leverage existing equipment and imaging processes*. Face recognition systems do not require specialized hardware unlike other biometric procedures. Existing hardware capable of image processing can be used with face recognition software.
- *Ability to operate without physical contact or user complicity*. The facial image of an individual can be acquired in a non-intrusive way even without the user being aware of the procedure. As a result, face recognition systems can operate in surveillance mode. Police, government agents, and casinos use face scans to identify criminals.
- *Ability to enroll static images*. Most biometric systems require several years to deploy, since it takes time to collect biometric data on users. Time delay can be less of a problem in the case of face recognition, since existing sources of facial images of various groups of individuals are collected over time. Departments of Motor Vehicles (DMVs), immigrations offices, and other public agencies collect massive databases of facial images taken in controlled environments.

Disadvantages

Disadvantages of face biometrics include [Nanavati et al., 2002]:

- *Sensitivity to environment.* A number of environmental conditions (e.g. light, background composition, camera position and many other factors) impact system accuracy.
- *Sensitivity to changes in physiology.* Simple changes in physiology (e.g. new hair style, make-up, facial hair, glasses) impact system accuracy significantly.
- *Privacy abuse.* Since a face image can be taken without the user being aware of it, privacy abuse is possible. For example, a face recognition system installed in voting booths in Uganda to prevent voter fraud was found to be highly intimidating to voters [Nanavati et al., 2002].

Spoofing

One of the ways to spoof a face recognition system is to fake a face. A face can be faked by obtaining an image of a person's face (e.g. digital photograph). After an image of an individual's face is captured, the system can be tricked in a number of ways:

- A two-dimensional face image can be presented to a camera. This scam may work for systems that do not use "active eye" recognition or depth recognition. Active eye recognition makes use of reflective nature of the pupil to locate eyes on a facial image. Depth recognition adjusts camera's focal length to capture macro features of a face. If a plain image is presented to the camera, the focal length will be the same for all face features and, thus, the system may be able to detect that it is being presented with a two-dimensional image of the face.

- Systems with active eye recognition can also be fooled with the help of a two-dimensional image. An intruder can cut out the pupil areas in the two-dimensional image and use the image as a mask. In this way, the system is presented with real eyes, while the face as a whole is simply a two dimensional image of the real face. To a certain degree this type of attack is mitigated by requiring the system to detect face movement for authentication. [Reid, 2004]. In this way, a still image not exhibiting any movement will not be interpreted by the system as a real face.

- Another way to spoof a face-recognition system is to replay a previously captured video of an individual's face. The video can be replayed using a laptop or a portable DVD player. In this case, the face can exhibit some degree of movement and the system requiring face movement may be fooled. However, active eye detection may recognize that it is not a real face.

The spoofing techniques discussed above rely on presenting a static image of a face to the system. Even if a recorded video of a face is used, the image can still be viewed as static, since the dynamic characteristics of the face in the video are limited to what was recorded. Thus, a number of challenge and response methods can be used to mitigate this type of attack. An example of a challenge and response method would be asking the individual to blink a random number of times in a particular time pattern. Theoretically, even this challenge and response method can be fooled by creating a complex video model of an individual capable of generating these dynamic face characteristics. However, the model is likely to be prohibitively complex and expensive to generate.

Another potential way of spoofing a face recognition system is to present the system with a face artifact. A face artifact consists of image files that were used by the system during the enrollment process. Theoretically, these files can be fed into the system without the individual undergoing a predetermined face image acquisition process. One of the ways of dealing with this attack is to use encryption to transmit face image data. In this way, it will be difficult if not impossible to intercept face image data and feed it back into the system.

IRIS SCANNING

Operating Principles

The iris exhibits a unique mosaic texture which can be used for identification and authentication. To capture a person's iris, the individual needs to look into a camera. The camera must be positioned appropriately to localize the image of the iris. After the iris image is captured, simple logical operators (XOR and AND) can be used to match the iris image obtained with the one previously stored. As two binary sequences (e.g. 101 and 111 can) can be matched by applying XOR and AND operators to corresponding bits of each binary sequence, the features of a person's iris can be compared to the features of the iris previously stored in a template using similar logical comparison mechanisms.

Advantages

Iris biometrics is probably the most promising biometric trait [Reid, 2004]. Iris scan's advantages over other biometric procedures include:

- The major advantage of iris biometrics is its accuracy. Biometric systems based on iris recognition provide virtually no False Acceptance Rate (FAR) and an extremely low False Rejection Rate (FRR) of approximately 0.2% in three attempts[1] [Reid, 2004]

- The relatively simple matching algorithm based on XOR and AND operators allows for extremely fast matching: fir example, 100,000 matches per second can be carried out even on a 300MHz machine [Reid, 2004].

- Iris texture is a stable characteristic that does not change over time [Nanavati et al., 2002]. Part of this stability comes from the iris's protection by the cornea. The iris is usually not exposed to harsh conditions and does not change with age.

Disadvantages

Disadvantages of iris-scan include [Nanavati et al., 2002]:

- Iris biometric procedures may be difficult to use for some individuals. For an iris to be scanned, a user needs to align a camera with the eye – a procedure that may not be easy for disabled individuals or individuals with poor eye sight.

- Iris-based biometric systems have a propensity towards FRR (Section VI) because the strict positioning requirements may make it difficult to obtain a quality iris image. An authorized user may not be granted access because, with the strict positioning requirements, his or her iris pattern was not scanned properly.

- Iris scans are perceived to be intrusive by a certain percentage of users. There is something about the nature of one's eye as well as its importance in an individual's life that makes users uncomfortable about submitting their eyes to a scanning procedure. Other individuals are worried that the iris scanning camera can damage their eye sight.

- Currently, the market for iris acquisition devices lacks competition or standardization[2]. Only a small number of companies manufacture iris acquisition devices all under the license from Irdian [Nanavati et al., 2002]. Thus, it would be expensive to develop custom security solutions based on iris scanning.

Spoofing

One way to spoof an iris biometric system is to print out a high-quality iris image. The pupil area can then be cut out so that an intruder can present his pupil together with the fake iris to a camera. This spoofing technique may be possible due to the robustness of some systems – they are tolerant to variations in iris image size to loosen strict positioning requirements for iris acquisition. Using this hidden vulnerability, an intruder can print out an iris image sufficiently large to hold it in hands to align it with their pupil. Fortunately, an iris biometric system can be taught to recognize a printed image. No matter how advanced a printing technology is, it uses a particular pattern for drawing lines and filling in spaces with color.

[1] See Section VI for a discussion of FAR and FRR.

[2] While devices from different vendors may use similar algorithms or operating principles, they are not likely to use the same engines. Devices manufactured by different vendors lack common standards, for example for communicating with computers or standard middleware, Implementation may differ both on the device level and at the middleware level.

RETINA SCANNING

Operating Principles

The retina is “the surface on the back of the eye that processes light entering through the pupil” [Nanavati et al., 2002, p. 106]. The retinas of each individual contain unique patterns of blood vessels that can be used for identification. This pattern of blood vessels is a unique physiological characteristic that does not change over time. The process of acquiring a retina image is relatively complex. Since the retina is an internal surface, specialized hardware and camera systems are required for image capture. When the retina is scanned, an individual must gaze directly into the lens of a retina-scanning device, remaining perfectly still. Even a slight movement can nullify the image acquisition process. In ideal conditions, it usually takes 4-5 seconds to acquire a retina image [Nanavati et al., 2002]. The retina biometric is used “exclusively for physical access applications and is usually used in environments requiring exceptionally high degrees of security and accountability, such as high-level government, military, and corrections applications” [Nanavati et al., 2002, p. 106].

Advantages

The retina biometric is highly accurate. Since retina patterns are a stable physiological trait and retina matching algorithms are robust, the retina biometric is highly resistant to false matching [Nanavati et al., 2002].

Disadvantages

The retina scanning procedure is perceived by some users as difficult to use and intrusive [Nanavati et al., 2002]. Similar to iris scans, the retina scan procedure requires some experience and attentiveness from the user. As a result, retina scanning can only be used at present in high-security and low-volume physical access and attendance monitoring applications. Thus, retina scanning procedures may only be appropriate in applications where convenience can be sacrificed for increased security. In addition, some users view the retina scan procedure as intrusive, making users reluctant to submit their eyes to this process.

VOICE RECOGNITION

Operating Principles

The voice is both a physiological and a behavioral biometric [Reid, 2004]. Voice is influenced by physiology. The beautiful sounds that Luciano Povarotti is capable of producing are largely a function of his unique physiology. However, we tend to absorb voice characteristics of people that surround us for a substantial period of time. Our voice also changes depending on social situation – most people probably use different voices when they speak to a telemarketer, a spouse, or a policeman. Our voice also depends on the environment: a stock broker sounds differently at home than on a trading floor (hopefully).

Voice characteristics include pitch, frequency, gain or intensity, short-time spectrum of speech, formant frequencies, linear prediction coefficients, cepstral coefficients, spectograms, and nasal coarticulation [Nanavati et al., 2002]. Many of these characteristics can only be produced by the human voice, which means that even sophisticated audio equipment cannot record and then reproduce these characteristics. However, this restriction does not eliminate the possibility of spoofing based on playback. The possibility of this type of attack can be significantly reduced by detecting some of the voice characteristics.

The voice can be captured using the existing infrastructure, such as a phone or a microphone connected to a computer. Some of the voice interpretation algorithms include [Reid, 2004]:

- *Fixed phrase verification*. Under this algorithm, an individual is both enrolled and identified based on a single phrase. The enrollment phrase is matched with the phrased obtained from the individual during the identification procedure simply by comparing the wave forms of each of the two phrases.

- *Fixed vocabulary verification*. A user is enrolled and identified based on a limited vocabulary of words. A random sequence of words is generated for the user to pronounce aloud. After the individual pronounces these words (e.g. “one, two, four, seven”), each word is matched with the word previously recorded from the individual. After that, a composite match score is generated based on the extent to which individual words match.
- *Flexible vocabulary verification*. Under this algorithm, an individual can use any word from a given lexicon. During the enrollment process, an individual is asked to repeat a series of words from the lexicon. The set of words pronounced during the enrollment process must cover all the phonemes (the vocal building block of each word) of every word in the lexicon. During the authentication process, the user is asked to speak a word or a number of words from the lexicon. The words are broken down into phonemes and then matched with the previously stored phonemes to authenticate the user.

Advantages

The advantages of voice biometric are [Nanavati et al., 2002]:

- *Ability to leverage existing hardware infrastructure*. Voice can be recorded using phones or by simply attaching a microphone system to a computer. An organization can theoretically get by without purchasing expensive specialized hardware. Furthermore, automated telephone systems are now ubiquitous. These existing technologies can be leveraged for creating security applications.
- *Resistance to imposters*. Some voice characteristics are difficult to fake even using high-end audio systems. Systems based on voice biometrics can potentially be more secure than even some finger-scan systems.
- *Non-intrusiveness.* The voice scanning procedure is perceived to be less intrusive than scanning of iris, retina, or even finger.

Disadvantages

The disadvantages of the voice biometric include [Nanavati et al., 2002]:

- *Voice is subject to numerous distortion factors*. First of all, the type of hardware used to record one’s voice can have a significant impact on the quality of the obtained voice sample. For example, the microphones used in phones are not of a high quality. But even if high-end voice recording equipment is used, it may still be hard to obtain a quality voice sample. A user may not know, for example, how to hold and position the microphone properly. Voice can be distorted or masked by background noise. Finally, users may unintentionally vary their voice characteristics.
- *Perception of low accuracy*. After watching too much TV, some people believe that their voice can be faked by a skillful impressionist. As was mentioned previously, some voice characteristics cannot be reproduced artificially even using sophisticated audio equipment for recording and then playback. Although voices can be faked, it is not as easy as some think.
- *Large template size*. When compared to other types of biometrics, voice templates require a lot of storage space. While finger or iris templates usually occupy up to 1K of memory, voice templates can occupy 10K or more.

OTHER TYPES OF BIOMETRIC TECHNOLOGIES

In addition to the major techniques listed in Table 3, biometric techniques include vein pattern scanning, detection of individual scent, measurement of earlobes, facial thermogram procedures, analysis of individual keystroke dynamics, signature verification, and gait recognition [Ashbourn, 2000; Delac and Grgic, 2004; Jain et al., 2000; Monrose and Rubin, 2000; Nanavati et al., 2002; Schneier, 1999]. These methodologies, described in Table 5, are less developed and are not widely used at present.

Table 5. Less Developed Biometric Applications

Biometric Type	**Description**
Vein Pattern Scanning **(natural physiography)**	The vain pattern on the back of the hand and wrist is scanned while the user grips a bar within a specialized scanning device. Commercial applications based on this biometric are already available in ATM banking.
Scent **(natural physiography)**	Since each object distributes an odor that is based on the object's chemical composition, identifying individuals based on their unique scent patterns may be possible. However, there are many unanswered questions, such as how unique individual scent is and whether the scent can be captured easily by specialized equipment.
Measurement of earlobes **(natural physiography)**	While it is possible to identify unique geometrical characteristics of an earlobe, the procedure is likely to be inconvenient and is not likely to be more accurate than measuring other body parts.
Facial thermograms procedures **(natural physiography)**	The face below the skin emits unique infrared patterns that can be captured by a specialized scanning device. While the technology is highly accurate, its high cost is probably the main factor preventing the emergence of commercial applications.
Keystroke dynamics **(bio-dynamics)**	Keystroke dynamics is a behavioral characteristic. Individual keystroke dynamics, such as speed of typing, pauses between words, and intervals between individual characters, could potentially provide on-going identity verification rather just one-time verification at the beginning of a computer session.
Signature Verification **(bio-dynamics)**	A signature is a behavioral characteristic. Signature verification is based not only on the appearance of the signature, but also on signature dynamics: the pressure applied to the pen, the speed at which individual pen stroked are executed, the overall time it takes an individual to reproduce his or her signature, and other characteristics.
Gait Recognition **(bio-dynamics)**	Rhythmic patterns associated with walking stride can be potentially used in surveillance. However, many principal questions remain unsolved in relation to how this biometric methodology might be implemented.

SOME PROMISING EMERGENT BIOMETRIC TECHNOLOGIES

Emerging technologies include instant DNA testing and brain wave scanning. In 10 to 20 years these technologies may present a practical and more reliable alternative for instant identity verification.

Instant DNA Testing

Instant DNA testing could be used for both authentication and identification. Currently, DNA testing is extremely accurate but requires specially equipped laboratories, rigorous procedures, and takes time. It is extensively used for both identification and authentication purposes in law enforcement but currently is not a practical option for real time security applications. However, scientists at Northwestern University claim they developed an instant DNA identification technique which will eventually be built into a handheld device [Connor, 2002].

Brain Wave Scanning

Brain wave scanning is a promising technology. Neuroscientist Lawrence Farwell, who is now associated with Brain Fingerprinting Laboratory, invented a technique he calls Brain Fingerprinting ® (brain wave scanning).

Brain Fingerprinting® can detect information stored in one's brain based on electrophysiological manifestation of information processing in the brain [Brain Fingerprinting Laboratories, 2005]. Information processing occurs in response to certain type of meaningful stimuli. An electrical brain wave known as P300 is emitted by the brain when an individual is exposed to particularly meaningful or noteworthy stimuli. For example, when an individual is shown a picture of the gun she used to kill her husband, the P300 wave is likely to be emitted. However, when the individual is shown a picture of a random gun, the P300 wave is not likely to be emitted. The picture of a random gun is not as meaningful to her as the picture of the gun actually used in the crime. Brain Fingerprinting can also be used for identifying individuals who are likely to pose a terrorist threat. A suspected individual would be shown a series of pictures presumably familiar to terrorists such as weapons while his brain is being scanned. If the suspect sees a familiar object (for example, a picture of a bomb) his brain may emit a P300 wave. If this happens, the investigators may have grounds to believe that the individual participated in a terrorist attack. The Brain Fingerprinting technique has already been used in the courtroom to help to establish the innocence or guilt of suspects.

"Brain fingerprinting" can also be used for identity verification. An individual might be shown a series of unique pictures that would be not be seen by anyone else (e.g. randomly generated by a computer) and asked to memorize them. In the process of authentication, these pictures could be shown again to the individual. Only the authorized person's brain would emit the right response (of course, given that the individual does not have disabilities preventing him from storing and retrieving information from memory).

V. CURRENT AND FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGY

On the most abstract level, biometric applications can be divided in three categories [Nanavati et al., 2002]:

- *Logical Access*. Biometrics can be used to control access to data or information (intangible resources). This group of applications can be referred to as *network security applications*.
- *Physical Access*. Biometrics can be used to control access to tangible resources or premises.
- *Identity Verification*. Biometrics can be used to verify the identity of an individual or check his or her identity against other data.

On a more practical level, applications of biometrics can be divided into forensic, civilian and commercial applications [Jain et al., 2000]. As presented below in Table 6, each of these broad categories has a number of concrete applications.

Table 6. Applications of Biometric Technologies by Sector

Law Enforcement	**Civilian**	**Commercial**
Criminal investigation Corrections monitoring Surveillance Terrorism prevention	National ID Driver's license Voting and Voter Registration Welfare disbursement Immigration control	PC/Network Access Physical Access Control Time and attendance ATM Transaction Security Surveillance Background check

LAW ENFORCEMENT

The history of using biometrics for forensic applications is long and rather glorious. In essence, forensic applications of biometric technologies aim at identifying or verifying identity of a suspect, detainee, or individual in a law enforcement context [Nanavati et al., 2002]. “Over the past 25 years, automated fingerprint searches against local, state, and national databases, as well as automated processing of mug shots, have become pervasive criminal identification applications, used around the world” [Nanavati et al., 2002, p. 152]. Numerous other types of biometric technologies are currently used in law enforcement and crime prevention (Table 7).

Table 7. Applications of Biometric Technologies in Law Enforcement and Crime Prevention

Biometric Type	Applications	Agencies
Fingerprint	PC/Network Access	Most state identification bureaus Many police departments FBI INS
Retina	Identification of prisoners in jail	Cook County, Illinois, Sheriff's Office
Iris	Identification of prisoners in jail	Lancaster County, PA Sarasota County, FL
Face	Searching mug shots Surveillance video cameras Driver's licenses Driver's licenses	Los Angeles County, Sheriff Newham, England police West Virginia Illinois
Hand	Prisoner identification Probationer monitoring Border control	Federal and state prisons 3 Minnesota prisons New York City corrections INS
Voice	Border control Probationer monitoring	INS Some corrections agencies

Reprinted with permission from Coleman [1999]

A relatively new forensic application of biometrics is using face recognition for active surveillance. Face recognition systems allow law enforcement agencies to increase surveillance, tracking, and apprehension of criminals. For example, in 1998 Newham, a borough in London, installed 250 surveillance cameras to feed information to the FaceIt® Surveillance system [Identix Inc., 2000]. The system continuously matches the images of people captured by the surveillance cameras with a database of suspects and known criminals. If a match is found, the system alerts law enforcement agencies about the match. Robert Lack, Newham's Security and Operations Manager, credits the system with 40% crime reduction in the borough [Identix Inc., 2000]. However, the exact procedure for assessing effectiveness of the system was not reported.

In the wake of the September 11, 2001 attacks, the United States government began exploring biometrics technologies for use in preventing acts of terror. Biometrics is one of the technologies currently used by the Department of Homeland Security to identify people who might be a threat to national security.

CIVILIAN APPLICATIONS

National ID

Using biometrics for national IDs and driver licenses provides a more reliable way of identifying individuals [Schimke et al., 2005]. Additional benefits of this application of biometrics include prevention of duplicate identities and faster processing of transactions requiring individual identification [Nanavati et al., 2002]. Jurisdictions in the Unites States including Illinois, Georgia, and West Virginia either deployed or are planning to deploy identification programs based on biometrics. Such countries as Argentina, El Salvador, Panama, Bolivia, Argentina, Nigeria, Germany, Korea, and the United Kingdom are either experimenting or already using biometric information with national IDs, to some extent.

Driver's License (DL)

In the Unites States, the driver license is the most widely used form of personal identification. People fake DLs not so much to be able to drive a car, but to commit other forms of fraud, such as passing bad checks, committing credit card fraud, illegally purchasing alcohol and tobacco, and stealing others' identity for all kinds of purposes. Because of that, the United States is seeking new ways to control the issuance of DLs and, thus, strengthen the reliability of this form of identity [Coleman, 1999]. A number of states use fingerprinting to verify the identity of DL recipients. West Virginia was the first state to apply facial recognition to DLs. The major goal of this application is to prevent people from obtaining an extra DL for use as a fake ID.

Voting and Voter Registration

Voting and voter registration is an extremely important procedure and must be protected against possible fraud. Biometrics can help achieve this goal [Nanavati et al., 2002]. Mexico is using facial recognition to prevent voting fraud. Face biometrics was also used in Uganda's 2001 election for the same purpose. However, the technology encountered some degree of hostility from voters in Uganda – voters felt that face recognition compromises the anonymity of the voting process.

Welfare Disbursement

Biometrics are used in government benefit programs for two purposes: to ensure secure transfer of funds to eligible recipients and to prevent "double dipping" – the fraudulent practice where an eligible recipient receives governmental support more than once [Coleman, 1999]. Table 8 briefly describes the use of biometrics for authentication of welfare recipients in the United States in 1998.

Immigration Control

After the 9/11 attack, the U.S. government began using biometrics in hopes of preventing terrorists from entering the United States and for overall tighter control of visitors to the United States. Everyone entering the United States with a visa must now permit fingerprints and photographs to be taken and scrutinized by the U.S. Customs Service [BBC News, 2004]. It is estimated that the system will generate around five million gigabytes of biometric data per year [Betts, 2003]. While this enormous amount of data may certainly contribute to terror prevention, it also creates several technical problems. A system with this much data requires ultra-fast

Table 8. Biometric in Welfare Distribution (1998 Data)

State	Biometric Type	Benefit	Year Began
AZ	Fingerprints	AFDC (Aid For Dependent Children), food stamps	1998
CA	Fingerprints, hand geometry	AFDC, GA (General Assistance), food stamps	1991
CT	Fingerprints	AFDC, GA	1996
IL	Fingerprints, retina	AFDC	1996
MA	Fingerprints, face	AFDC, GA, food stamps	1996
NJ	Fingerprints	GA	1995
NY	Face, signature fingerprints	AFDC, GA, food stamps	1995
TX	Fingerprints	AFDC, food stamps	1996
NC	Fingerprints, face	AFDC, food stamps, medical	1998

Reprinted with permission from Coleman [1999]. This data is the latest available to the authors.

database and networking technologies to ensure that travelers entering the U.S. are processed without significant delays.

COMMERCIAL APPLICATIONS

Table 9 gives a brief overview of actual applications of various types of biometrics. The list provided in Table 9 is by no means comprehensive – it focuses on some of the main trends in commercial application of biometrics.

PC/Network Access

Biometrics can be used to complement or replace traditional login/password combination for access to computers and networks. One of the advantages of using biometrics for PC/Network access is that biometrics are believed to be more secure than traditional PC/Network security measures, such as passwords or tokens. Another advantage of biometrics over traditional security approaches in the area of PC/Network Access is convenience. Biometrics alleviates the burden of remembering different login/password combinations for accessing intangible assets. Moreover, swiping a finger to access a computer is more convenient than typing in a username and a password.

Physical Access

Better security and convenience are also important factors in implementing biometric technology for controlling access to facilities and other tangible resources. Again, swiping a finger on a finger scan or submitting one's face to the face-scan procedure may be more convenient than using keys or magnetic cards. Physical access artifacts can be lost, stolen, or misplaced, causing inconvenience for employees. Moreover, some employees share their access artifacts with others, which can create additional security vulnerability for the company. However, it always takes time for employees to absorb a new technology. Biometric access systems are likely to result in a higher failure rate when compared to, say, keys. Reported cases describe employees smashing a biometric device in despair after several unsuccessful attempts to access a premise.

Time and Attendance Monitoring

Using biometrics in time and attendance applications can mean better convenience for employees and better fraud protection for the employer. "Buddy punching", a situation where an employee "clocks in" for his or her buddy, is relatively common. When, a finger is used for clocking in, an employee must lend a finger to the "punching buddy". This may not be worth even a year's pay.

ATM Access

ATMs are important nodes in the financial network of many countries. ATM security can be strengthened with the help of biometrics. Currently, a number of banks and other financial institutions around the world use various forms of biometrics (e.g. hand vein scanning) for ATM access [Asawa et al., 2005]. Still, using biometrics with ATM access is not common. Since ATMs are used on a large scale by diverse populations, a number of issues must be resolved before ATM biometrics becomes a commonplace. For example, when Citibank experimented with using biometrics as an authentication tool in ATMs [Mearian, 2002], the company encountered serious difficulties and decided that they were not ready to implement the technology. Apart from the numerous technical difficulties that usually accompany any emerging technology, implementing biometric identification in ATMs required substantial startup resources to capture customers' biometric information and educate the public on how to use ATM biometric identification

Table 9. Commercial Applications of Biometrics[3]

Biometric Type	**Application Type**	**Companies**
Fingerprint	Network/ PC Access	The city of Oceanside, California; Credit Union Central, British Columbia; The Guardian Life Insurance Company of America, USA
	Physical Access/ Time and Attendance	Hermes Pension Management Limited, UK; Credit Suisse, Switzerland; Shell Petroleum, UK; Fujitsu, UK; O'Rourke Construction Company, UK
	POS	A number of small companies in the United States use BioPay – an automated terminal where purchases can be paid for by scanning a finger (instead of swiping a credit card or paying cash)
	ATM	Purdue Employees Federal Credit Union, IN
	Wireless Security	HP manufactures iPAQ PDAs with fingerprint biometric access protection
	Background Check	Aramco Saudi Arabia National Oil Company; Melon Bank, USA; ING Direct, USA
Hand	ATM	Japanese banks used hand vein recognition technology from Fujitsu to enhance ATM security
	Physical Access	Disney World: gate access to attractions; San Francisco International Airport: hand geometry is used to control access to restricted areas
	Time and Attendance	McDonald's uses fingerprinting to prevent "buddy punching" among its restaurant employees in Venezuela
Retina	Physical Access	Retina scanning is used for physical access control in organizations requiring highly secure environment, such as power plants and some research labs
	POS	Venerable Bede School, UK: retina scan for library check-out and cafeteria payment
Iris	Physical Access	Vertical Screen; North Florida Medical Centers; Nine Zero hotel, Boston: retina scanning for room access for some of its luxury suits
	POS	The Charlotte/Douglas International Airport, NC and the Flughafen Frankfort Airport, Germany: iris scan for streamlining boarding of frequent fliers
Face	Physical Access	Berlin Airport, Germany
	Surveillance	A number of casinos in the United States, Canada, Puerto Rico and Aruba use face surveillance solution from Biometrica Systems to identify unwanted patrons
Voice[4]	PC/Network access	BMC Software: password reset over the phone; INTRUST bank: internal wire transfers
	Physical access	City of Baltimore: evening and weekend access to five city main buildings
	Telephone security	University of Maryland, College Park: toll-free long distance lines for faculty and staff; GTE TSI: speaker verification as a part of the wireless security program
	Time and attendance	SOC Credit Union: Time and attendance monitoring of part-time employees; Salvation Army: time and attendance monitoring of workers
	Transaction Security	Glenview State Bank: transfer of money between accounts for customers; Home Shopping Network: automated product ordering over the phone

[3] This table was compiled from numerous online and offline sources.
[4] This section adopted from Markowitz [2000]

Transaction Security

Biometric technology can be used to strengthen transactions conducted from remote locations (e.g. via a phone, Internet, or Intranet). The biometric, such as voice recognition or fingerprinting, can be used to complement or replace traditional authentication mechanisms. For example, voice recognition is already used to authenticate a customer wishing to perform a financial transaction over the phone [Markowitz, 2000]. In a similar manner, fingerprints can be used to authenticate a person during e-commerce transactions.

Surveillance

Using biometrics (mainly face recognition) is a relatively new application. A number of casinos around the word use automated face surveillance systems to identify unwanted customers (e.g. customers who were previously caught cheating or causing some trouble). One of the advantages of this application is that the procedure is not intrusive and can be used without significant (if any) cooperation from casino patrons. Another advantage of this system is that it frees up staff resources to some extent, since security guards can spend less time attempting to identify troublemakers. However, the effectiveness of such systems in recognizing unwanted customers is still not proven.

Background Check

Many organizations cannot afford to hire employees with questionable backgrounds. Biometrics (usually fingerprints) can be used to check the background of potential employees. This system may not require a significant amount of time to get off the ground, since numerous digital fingerprint databases of criminals exist. A software application can be installed on the top of one of these databases to get the system working.

VI. BIOMETRIC SYSTEM PERFORMANCE

TECHNICAL PERSPECTIVE

Computer-powered biometrics is still an emerging technology. Because computer-enabled biometrics is not mature, organizations considering using the technology need to assess its performance before proceeding with implementation. Performance of a biometric security system can be evaluated in terms of its accuracy, storage requirements, and speed [Jain et al., 2000].

FNR and FMR

Mistakes are always possible in biometric systems. The system can accept an impostor as a valid individual (a false match) or reject a valid individual (a false no match) [Jain et al. 2000]. These types of mistakes constitute two important variables for assessing system performance: False No Match Rate (FNR) and False Match Rate (FMR). These two variables are correlated negatively. Indeed, if the system is designed to operate at a high level of accuracy, even a slight interference (such as dust, or light conditions,) may result in the system not recognizing a valid individual. Conversely, a system which operated at a lower level of accuracy may accept an imposter as an authorized individual, making the system more vulnerable to intrusion. This limitation makes it necessary to seek a balance in the level of accuracy along the Receiver Operating Characteristics (ROC) line (Figure 3). The ROC represents an estimation model for system accuracy in a given test environment [Jain et al. 2000].

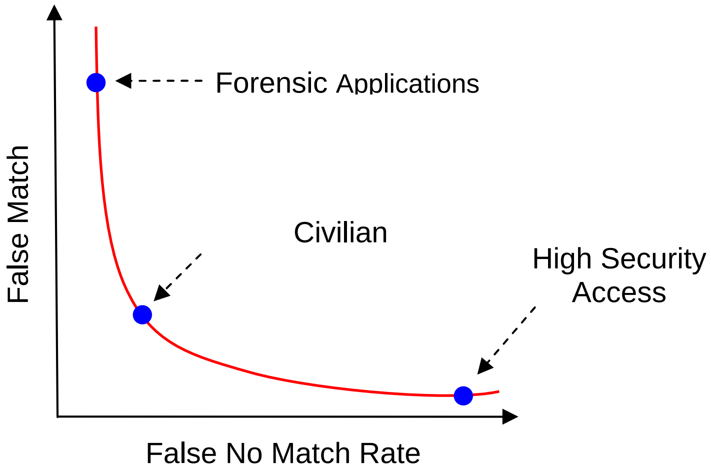

Figure 3. Receiver Operating Characteristics [Jain et al. 2000]

FTE

Another measure of performance of biometric systems is Failure to Enroll Rate (FTE) [Navati et al., 2002]. FTE can be defined as "the probability that a given individual will be unable to enroll in a biometric system" [Navati et al., 2002, p. 33]. The two major reasons for FTE are:

1. An individual's biometric characteristics may be insufficiently distinctive or replicable. For example, older people or people whose work involves manual labor may have more "blurry" fingerprints, making it difficult for the system to enroll them.

2. The design of a biometric system (e.g. its ergonomics) can make it difficult for certain groups of people to enroll. For example, the study by UKPS [2005] found biometric data (face, iris, and fingerprint) from younger or healthy individuals results in more accurate authentication when compared to biometric data obtained from older or disabled individuals. In the study, the 55+ age group found it more difficult to position themselves for fingerprint enrollment than the 18-54 age group.

Moreover, the study found that it is harder for the system to record fingerprints of individuals with large fingers (e.g. overweight individuals). Iris enrollment success for participants under 60 was higher than those above 60. As a group, enrollment success for disabled participants was lower, with 0.62% of disabled participants failing to enroll in any of the biometrics (face, iris, or fingerprint). Table 10 summarizes the comparative FTE rate for "quota participants" (a representative sample of 2000 people drawn from the UK population) and "disabled participants" (750 individuals with some form of disability).

Storage and Other Technical Requirements

Biometric technologies require more storage, bandwidth, and processing power than traditional security technologies. Storing digitized human body patterns requires more computer memory than is required, for instance, for storing passwords (Table 11). A system that uses text for profiling users generates only a fraction of the five petabytes that would be generated by the same number of users in the US-VIST system, where each entrant to the U.S. submits his or her fingerprints and his or her face image.

Table 10. Comparative FTE Rates

Biometric Type	**FTE (Quota Participants)**	**FTE (Disabled Participants)**	**Additional Considerations**
Face	0%	2%	Maintaining the correct position for facial biometric enrollment was a problem for some disabled participants with physical impairment or learning disabilities
Iris	10%	39%	Asian and white participants had lower FTE than black participants. Participants under 60 years of age had lower FTE than participants over 60 years
Fingerprint	0%	4%	Participants with a learning or physical disability had higher FTE than other disabled participants and quota participants

Adapted from UKPS [2005]

Table 11. Comparative Template Size for Biometrics

Biometric Type	Voice	Signature	Face	Iris	Finger	Retina	Hand Geometry
Template Size (bytes)	2,000-10,000	1,500	1,300	512	250	96	9

Adapted from Nanavati et al. [2002]

In addition to storage requirements, transferring scanned biometrics requires expanded network bandwidth. Moreover, the computer processing power requirements for matching a user name and a password with a particular record in a database of logins and passwords are not nearly as high as for applying complex pattern recognition algorithms to biometric input. These increased requirements for computer processing capacity are closely related to system speed. Unless sufficient computer resources are provided, a biometric system does not function at an acceptable performance level.

SOCIAL PERSPECTIVE

In addition to purely technical criteria for evaluating system performance, social factors can also play a big role in the overall system effectiveness. System evaluation measures on the human side involve acceptability and circumvention [Jain et al., 2000]. Acceptability is the extent to which people are willing to accept a biometric solution in their daily lives. It can be argued that acceptability consist of two sub-factors: intrusiveness and ease of use. Some of the scanning techniques may be invasive and troublesome, which may cause end-user resistance. Circumvention refers to how easy it is to fool a system through fraudulent means. People may not be willing to sacrifice their privacy knowing that systems can be easily spoofed. Acceptability and circumvention is not only about subjective human perceptions. Users' perceptions towards the system will determine whether the system is used effectively (or used at all).

VII. PRIVACY ISSUES

Each type of biometric provides irrefutable proof of one's identity [Jain et al., 2004]. A biometric is not a login/password combination that can be easily modified. A biometric is not an ID that can be nullified in case of theft and then reissued. A person has only one instance of each biometric trait and will never have a new one. Once a user submits his or her biometric to a system, the user is in the system for good. Because of that, users are concerned about the privacy aspects of biometric technology [Jain et al., 2004]:

- Will this undeniable proof of identity be used to track the individual beyond his or her interaction with a system requiring the user's biometric information? Moreover, can this type of tracking be carried out without the individual being aware of it?
- Is it possible that biometric data will be used for unintended purpose? For example, the fingerprints obtained from individual for access control can be matched with the fingerprints in a database of criminals.
- Will the biometric data be used to cross-link independent records from the same person (e.g. health insurance and grocery shopping)?

Individuals are concerned that with the help of biometric technologies, his or her privacy will be compromised. Altman [1975, p.24] defines privacy as "…the selective control of access to the self," while Mason [1986] looks at privacy as the extent to which an individual is required to reveal information about himself or his association with others. One of the crucial questions related to privacy is "what things can people keep to themselves and not be forced to reveal to others?" [Mason, 1986, p. 5].

In light of the above definitions, biometrics-based identification technologies, such as facial recognition, appear to pose a great privacy risk. A security camera does not ask for consent before capturing an image. Control over personal information is therefore weakened. Agre [2003], a strong opponent of facial recognition, presents a comprehensive list of arguments against its widespread adoption and use:

> *… automatic face recognition in public places, including commercial spaces such as shopping malls that are open to the public, should be outlawed. The dangers outweigh the benefits…The potential for abuse is astronomical. Pervasive automatic face recognition could be used to track individuals wherever they go… The information from face recognition systems is easily combined with information from other technologies. Among the many "biometric" identification technologies, face recognition requires the least cooperation from the individual… The technology is hardly foolproof…Among the potential downsides are false positives, for example that so-and-so was "seen" on a street frequented by drug dealers… Yet the conditions for image capture and recognition in most public places are far from ideal. Shadows, occlusions, reflections, and multiple uncontrolled light sources all increase the risk of false positives… Face recognition is nearly useless for the application that has been most widely discussed since the September 11th attacks on New York and Washington: identifying terrorists in a crowd…* [5]

While identification systems invoke Orwellian or, more currently, Minority Report images of a total surveillance society, authentication systems pose a threat of their own. Schneier [1999], a well-known cryptologist and computer security expert, warns:

> *Biometrics don't handle failure wel…, Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation.*

Indeed, an individual only has one set of fingerprints. Once someone's fingerprints are stolen, they are stolen for life. No governmental agency can annul your old fingerprints and issue you new ones. The dilemma here is that biometrics can help prevent identity theft but can also,

[5] Reprinted with permission from Philip Agre

simultaneously, complicate the problem of identity theft, as argued by Schneier in the quote above.

Still, many in the biometrics industry believe that properly deployed biometrics will increase privacy, since if an individual's biometrics are known, no other information such as race, gender, or social security number is required. Moreover, it can be argued that privacy threats come not as much from the nature of the technology itself, but rather from the particular way in which the technology is applied and from the system design used to support the applications [Nanavati et al., 2002]. This sentiment is not limited to the biometrics industry. The well-known sociologist Amitai Etzioni [1999] believes that benefits of privacy should be weighed against its costs and that biometric technologies may bring about huge benefits to consumers and businesses as well as enhance privacy. Etzioni [1999] believes Big Brother fears are overstated. He believes that new identification technologies do not control individuals – totalitarian governments do. Thus,

> *"Strengthening the foundations of civil society is the best defense against totalitarianism, not trying vainly to return the genie of biometrics into the bottle from which it already has escaped."* Etzioni [1999[.

Still, privacy concerns must be addressed and those concerns seem only likely to increase with the future adoption of technologies such as DNA fingerprinting. The biometrics industry and privacy advocates both favor adoption of comprehensive regulations to prevent possible biometric abuses and protect privacy and civil rights while allowing the industry to develop. They disagree, however, on the source of those regulations. Many privacy advocates favor government regulation, contending that industry self-regulation will fail. Clarke [2004] laments "…self-regulation means protection of the sheep by the wolves; and funnily enough the wolves pay more attention to their own objectives than to those of the sheep."

VIII. IMPLICATIONS FOR RESEARCH

Biometrics is an evolving technology. Because of the technology's relative immaturity, numerous challenges must be overcome in system performance, user acceptance, technology diffusion, system security, and privacy among others. These problems call for a multidisciplinary research approach.

The solution to the challenge of biometric system performance may lie in Computer Science and Engineering. While some types of biometric technologies (e.g. fingerprinting) achieved levels of performance which make these applications acceptable for everyday use, many other types of biometric technologies need performance improvements to become viable security solutions. The focus of research on improving the performance of biometric systems is likely to be in the computer infrastructure associated with biometric solutions and algorithms and methods of biometric technologies.

User acceptance of biometric technology and diffusion of biometrics within organizations and countries are other potentially fruitful avenues for research. Even the most reliable, efficient, and productive technology can do little for an organization unless users adopt the technology. Adoption of biometric technology may be influenced by both objective (e.g. the speed at which biometric devices authorize an individual) and subjective factors (e.g. attitudes and perceptions towards the new technology).

A number of factors can prevent biometrics from being adopted by organizations and counties. For example, using biometrics as a security tool may require substantial modifications of the computer infrastructure used to support the technology. Moreover, diffusion of biometric technologies may require modification or even total reengineering of both technical and managerial security procedures currently in place in organizations. These issues clearly lie within the domain of Information Systems research.

Information security and privacy in the context of biometric technology may influence user acceptance of biometrics and diffusion of the technology. Technical and managerial (in the case of security) and legal (in the case of privacy) research may find solutions that will minimize the negative impact of security and privacy concerns on the adoption and diffusion of biometric technologies.

IX. CONCLUSION

Biometrics relies on a body of knowledge developed over centuries. Advancements in computer technology brought biometrics to a higher level of effectiveness, allowing for use of the technology in a variety of security applications. In many ways, biometrics is more reliable than traditional security approaches. However, a number of unresolved issues (such as privacy concerns and relatively high cost of large-scale biometric solutions) often make biometrics a less attractive alternative in comparison with traditional security measures. Advances in computing technology and related areas of research gradually allow for better processing of biometric information. As businesses gain more experience in deploying biometric security measures, biometrics should become a major security technology in the years ahead.

ACKNOWLEDGEMENTS

We thank Blake Ives, C. T. Bauer Chair in Business Leadership at the Department of Decision and Information Systems and Director of the Information Systems Research Center at the University of Houston, for his insightful comments and suggestions, which were indispensable in preparing this paper. We also thank Andy Schwartz, currently on the MIS faculty at the Louisiana State University, for his part in preparing a previous version of this paper for presentation to the Information Systems Research Center at the University of Houston.

Editor's Note: This article was received on December 2, 2004. It was with the authors for 10 months for 2 revisions and was published on _______, 2005.

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Agre, P. (2003) "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places", http://polaris.gseis.ucla.edu/pagre/ bar-code.html(current Sept. 24, 2004).

Altman, I. (1975) *The Environment and Social Behavior*, Monterey, California: Brooks/Cole

Asawa, T., A. Ohta, and T. Ando "Promoting Universal Design of Automated Teller Machines (ATMs*)", Fujitsu Scientific and Technical Journal*, (41) 1, pp. 86-96

Ashbourn, J. (2000) *Biometrics: Advanced Identity Verification*, London, UK: Springer-Verlag

ATI Access Technologies International (2004) http://www.atiaccess.com/

BBC News (2004) “US Fingerprint Foreign Visitors”, http://www.news.bbc. co.uk/2/hi/ americas/3367893.stm (current Sept. 24, 2004).

Betts, M. (2003) “The Almanac: Storage Briefs”, Computerworld.com, http://www.computerworld. com/databasetopics/storage/story/0,10801,87153,00.html (current Sept. 24, 2004)

Clarke, R. (2004), Interview, http://www.biometricsinstitute.org/bi/passprot/ clarkeinterview1.htm (current Sept. 24, 2004).

Clarke, R. (1999). “Introduction to Dataveillance and Information Privacy, and Definitions of Terms”, http://www.anu.edu.au/people/Roger.Clarke/DV/ Intro.html (current Sept. 24, 2004).

Coleman, S (1999) “Biometrics in Law Enforcement and Crime Prevention”, A Report to the Minnesota Legislature, Center for Applied Research and Policy Analysis, http://www.metrostate.edu/slc/pdf/biometrics.pdf (current June 15, 2005).

Computer Security Institute (2004) “CSI/FBI Computer Crime and Security Survey”, http://www.gocsi.com/forms/fbi/pdf.jhtml (current Sept. 24, 2004).

Connor, S. (2002) “Instant DNA Fingerprinting Turns Sci-Fi into Reality”, http://www.nanotechnology.northwestern.edu/press/independent%20february%202002.PDF (current Sept. 24, 2004).

Delac, K. and M. Grgic (2004) “A Survey of Biometric Recognition Methods”, *46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June*, Zadar, Croatia.

Etzioni, A. (1999) “Biometrics Are Coming! Biometrics Are Coming!” SpeakOut.com, http://speakout.com/activism/opinions/3808-1.html(current Sept. 24, 2004).

eWeek (2004) “Accenture Lands High-Tech Border Security Contract”, http://www.eweek.com/article2/0,1759,1607036,00.asp (current Sept. 24, 2004).

Identix Inc. (2000) “Tony Blair Gets a First Hand Look at Faceit® Surveillance System at Newham”, http://www.shareholder.com/identix/ReleaseDetail. cfm?ReleaseID=53283 (current Sept. 24, 2004).

Jain, A., L. Hong, and S. Pankanti (2000) “Biometric Identification”, *Communications of the ACM,* (43) 2, pp. 91-98.

Jain, A., Pankati, S., Prabhakar, S., Hong, L., Ross, A., Wayman, J. (2004) “Biometrics: A Grand Challenge Seen Spurring Biometrics”, *Proceedings of International Conference on Pattern Recognition*, Cambridge, UK.

Long, G. (2005) “Get Used to Biometric Tests, U.S. Tells Travelers”, *Computerworld.com*, http://www.computerworld.com/databasetopics/data/story/,10801,102079,00.html Current June 15, 2005).

Markowitz, J.A. (2000) “Voice Biometrics”, *Communications of the ACM*, (43)2, pp. 66-73.

Mason, R.O. (1986) “Four Ethical Issues of the Information Age”, *MIS Quarterly,* (10) 1, pp. 4-12.

Mearian, L. (2002) “Toppling the PIN: Banks eye biometrics for ATM access”, *Computerworld.com,* http://www.computerworld.com/securitytopics/security/story/0,10801,67314,00.html (current Sept. 24, 2004).

Monrose, F. and A.D. Rubin (2000) “Keystroke Dynamics as a Biometric for Authentication”, *Future Generation Computer Systems*, (16), pp. 351-359.

Nanavati, S., M. Thieme, and R. Nanavati (2002) *Biometrics: Identity Verification in a Networked World,* New York, NY: John Wiley & Sons, Inc.

Reid, P. (2004) *Biometrics For Network Security,* Upper Saddle River, N.J.: Prentice Hall PTR

Ratha, N.K., J.H. Connell, and R.M. Bolle (2001) “Enhancing Security and Privacy in Biometrics-Based Authentication Systems”, *IBM Systems Journal*, http://www.research.ibm.com/journal/sj/403/ratha.html (current Sept. 24, 2004).

Schimke, S., S. Kiltz, C. Vielhauer, and T. Kalker (2005) “Security Analysis of Biometric Data in ID Documents”, *Proceedings of SPIE/IE2005*

Schneier, B. (1999) “The Uses and Abuses of Biometrics”, *Communications of the ACM,* (42) 8, p. 136.

United Kingdom Passport Service (UKPS) (2005) “Biometric Enrollment Trial”, http://www.homeoffice.gov.uk/docs4/UKPS_Biometrics_Enrolment_summary.pdf (current Sept. 24, 2004)

Verton, D. (2004) “Office Building Managers Eye IT-Based Access Control Tools”,*Computerworld.com*, http://www.computerworld.com/industrytopics/ financial/story/ 0,10801,67360,00.html (current Sept. 24, 2004)

Vijayan, J. (2004). “Corporate America Slow to Adopt Biometric Technologies”, *Computerworld.com*,http://www.computerworld.com/hardwaretopics/hardware/story/ 0,10801,95092,00.html (current Sept. 24, 2004)

LIST OF ACRONYMS

ATM	Automatic Teller Machine
DNA	Deoxyribonucleic Acid
FMR	False Match Rate
FNR	False No Match Rate
FTC	Federal Trade Commission
PIN	Personal Identification Number
ROC	Receiver Operating Characteristics
VPN	Private Networks
UKPS	United Kingdom Passport Service

ABOUT THE AUTHORS

Serguei Boukhonine is a doctoral student at the Department of Decision and Information Sciences, Bauer College of Business, University of Houston. His research interests include strategic information systems, biometrics, human decision making, and computer education.

Vlad Krotov is a doctoral student at the Department of Decision and Information Sciences, Bauer College of Business, University of Houston. His research interests include strategic information systems, e-commerce, RFID (and other auto-identification technologies), and wireless/mobile technologies.

Barry Rupert is a former partner with Accenture. He is currently a doctoral student at the University of Houston.

Communications of the Association for Information Systems

ISSN: 1529-3181