CERIAS Tech Report 2005-07

ARE BIOMETRIC TECHNOLOGIES THE WAVE OF THE FUTURE IN TOURISM AND HOSPITALITY?

by Matthew Meyers & Juline E. Mills

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Are Biometric Technologies The Wave of the Future in Tourism and Hospitality?

Matthew Meyers[a]
Juline E. Mills[b]

[a]Center for Education & Research in Information Assurance & Security (CERIAS)
Purdue University, USA

[b]Department of Hospitality & Tourism Management
Purdue University, USA

{mlmeyers, millsje}@.purdue.edu

Abstract

This research endeavor explores four biometric technologies and their potential usage in the tourism and hospitality industry. This paper begins with a review of viable biometric technologies and continues with a discussion of their potential applications to tourism and hospitality businesses. Various tourism and hospitality scenarios in which biometrics can be used are explored. The article concludes with a discussion on the need for additional research on consumer perceptions to assist in answering questions regarding the social and business impact of biometric technologies in tourism and hospitality.

Keywords: biometric, fingerprint recognition, iris scan, hand geometry, facial recognition

1 Introduction

Consumer and management exposure to biometric technologies has been primarily through Hollywood blockbusters such as the numerous *James Bond* films. However, with the growth of security threats the usage of Hollywood 'magic,' so to speak, is becoming more appealing. Biometric technologies may enhance service management by improving security, customer relations, and business management while potentially decreasing costs. Biometrics may reduce costs such as keying, employee and guest theft, and may improve operational efficiency and hotel security. Biometric technologies utilize the measurements or behavioral characteristics of an identifying feature(s) of an individual to automate identification or verification of that person's identity (FindBiometrics, n.d.). Although biometric technologies have been used primarily for physical access, such as door locks, the technology is rapidly expanding to replace some accepted security formats such as passwords for computing devices and manual screening for known terrorists and criminals. While there are numerous types of biometrics, not all are viable based on usability and acquisition of the technology for tourism applications. Currently the market for biometrics is primarily composed of seven biometric technologies as shown in figure 1.

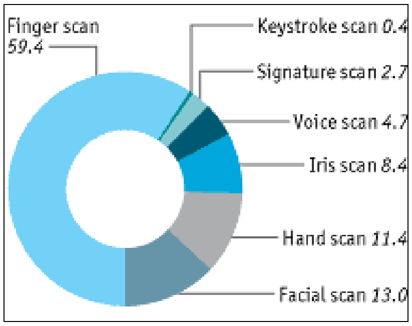

Fig. 1. Market Share Percentage by Biometric (Economist, 2003)

2 Biometric Technologies: A Brief Overview

This article explores four biometric technologies: face recognition, fingerprint recognition, hand geometry, and iris scan. An overview of these four biometric technologies follows.

2.1 Two-Dimensional Facial Recognition

Two-dimensional facial recognition is accomplished using cameras to capture an image and comparing that image to a stored template(s). Templates are data that represents the measurement(s) of an enrollee, used for comparison against subsequent images (National Information Assurance Partnership, 2003), to find the template that is most closely associated to the features captured. These measurements may include the top of the lip, the bottom of the nose, and the distance between the person's eyes. A combination of these measurements among other recognizable facial features may be used. A facial recognition system may work in real-time or capture images to compare to stored templates. Although commercially available since the 1990's, facial recognition has gained attention due to the terrorist attacks of September 11, 2001 (National Center for State Courts (NCSC), n.d.), which resulted in the federal government investing heavily in this technology for passport and border security (Ahlers, 2004).

At Super Bowl XXXV, the Tampa, FL, U.S. Police Department used facial recognition for all attendants to the game at the turnstiles. The Tampa Police had a facial recognition system that processed the images acquired at the turnstiles comparing those images to known criminals and international terrorists (Chachere, 2001). This is in essence a covert method of using biometrics for security purposes since the consumer is not aware that the process is occurring. In another covert method example, taken from a Hollywood blockbuster movie, "*Die Another Day,*" *James Bond* is identified as British Intelligence when his image was acquired using a cellular phone camera and transmitting it to a facial recognition system leading to his capture by the North Koreans. As in *James Bond*, figure 2 shows a female in a crowd being selected and the facial recognition system attempting to identify her as a user. Facial recognition can also be accomplished using an overt method where the user poses for the camera.

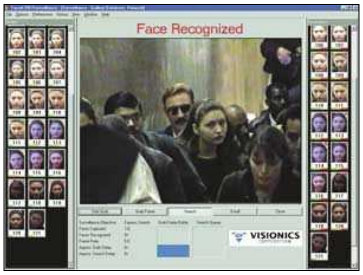

Fig. 2. Facial Recognition System Software by Visionics (Kroeker, 2002).

2.2 Fingerprint Recognition

Fingerprint recognition is the most commonly known biometric (Jarvis, n.d.). The popularity for the usage of fingerprint recognition is based on the assumptions that fingerprints are unique, static, are easy to use, and are acquired using an array of methods. The proliferation of fingerprint recognition has aided in solving and providing evidence for criminal cases in the United States and Europe. Fingerprint recognition is "the use of the ridges and valleys found on the surface tips of a human finger to identify an individual" (Biometrics Institute, n.d.). Fingerprint recognition is accomplished by placing a finger on a scanning device that acquires an image of the fingerprint and stores it under a selected template for later usage. Fingerprint recognition may be accomplished using one-to-one or one-to-many matching. One-to-one matching compares the image to one template while one-to-many compares the image to all stored fingerprint templates. In yet another Hollywood blockbuster taken from the movie "*The Bourne Identity*," actor Matt Damon, places his hand on a fingerprint scanner at a bank for identification. In a matter of seconds, the bank confirms his identity and provides access to his safety deposit box.

While it is theorized that fingerprints are unique, some researchers believe fingerprints may be identical, but this probability is extremely low (approximately 10^{97} power) (Association of American Law Schools, 2002; Coghlan and Randerson, 2004). Since fingerprints are theoretically unique, the technology is reliable enough to do one-to-many searches, eliminating the need for a pin number, password, or data card. Another advantage to the technology is the ease of usage and the ability for long life spans of the templates since fingerprints do not change drastically in short periods. However, there are possible problems with fingerprint recognition. It is possible to 'steal' an individual's fingerprints by lifting them (Waldman et al., 2004), but this risk may be mitigated by using devices that attempt to detect if the finger is 'live' (live testing tries to detect if the submitted biometric is from the owner and not a reprint or fake). For instance, if the scan of the fingerprint is too rich in features it may be a reprint or fake. Fingerprint quality also degrades with age, due to a loss of skin elasticity. It is also possible to wear off fingerprints, this is common with manual laborers, potentially causing the guests or user to not be accepted or recognized by the fingerprint recognition system (Walsh, 2004).

2.3 Hand & Two-Finger Geometry

Hand and finger geometry is primarily used for verification utilizing measurements such as, three dimensional shape, size, and angles in conjunction with a pin number or data card for a one-to-one match. The security of hand and two-finger geometry is unique in that the user presents the pin number or data card and must squeeze the pins as shown in figure 3.

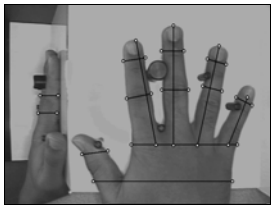

Fig. 3. Top-view of Hand Geometry and Measurements Being Obtained (Ross et al., n.d.).

There are several advantages to hand and finger geometry such as the minute amount of personal data collected, durability in varied environmental conditions, reliability, and speed of processing user verifications. Hand and finger geometry are perceived as less invasive in respect to privacy since the measurements taken are not unique. Hand and finger geometry may have limitation problems depending on implementation procedure, such as large populations that may require additional information for verification. In large populations placing a hand or two-fingers on a device and squeezing raises concerns over the sanitation of the instrument and the transference of bacteria. Potential problems may arise due to the template needing to be updated frequently to adjust for body changes such as weight. Furthermore, jewelry, hand injuries, and clothing may alter the acquired image causing the system to reject a legitimate user.

2.4 Iris Recognition

In the 1930's to 1940's ophthalmologists theorized that iris patterns were unique (NCSC, n.d.). Iris recognition is the use of the feature rich patterns of the iris for recognition. The system patented by Irdian Techologies Inc. captures an image of the iris then processes that image using Iridian's algorithm which takes hundreds of points of the iris and compares them to others irises for identification. A typical user would stand approximately 12 inches from the camera, wait a few seconds for the system to capture their iris, as well as identify and grant access where appropriate (Argus, n.d.). In figure 4 from Celex labs, the user looks at the camera with a lab mask on and is able to be identified and permitted into the laboratory. In "*X-Men*" actor Patrick Stewart, accesses Cerebro, a special machine, to find other mutants by using his iris. The iris recognition system did not require any additional identifiable information such as a data card; hence, the iris system was identifying him in a one-to-many manner. Similarly, in *"Minority Report,"* actor Tom Cruise is automatically identified where ever he walks after a camera 'scans' his iris.

For corporate security purposes, many private companies prefer to remain anonymous but are willing to discuss their usage and experiences with biometric technologies. For example an anonymous mining company in New South Wales Hunter Valley near Sydney, Australia had a problem controlling employees, contractors, and visitors based on operational and safety procedures. After conducting research on ways to improve their operations the mining company went with an iris recognition solution. By implementing the system the company was able to locate and track the number of employees and contractors on duty. In addition, the company was able to improve scheduling procedures thereby ensuring that properly trained individuals were in appropriate locations as needed. The company using iris recognition was also able to monitor the health and safety of employees while they were underground.

Fig. 4. A Scientist at Celex Labs Using an Iris Camera with Eye Gear (Argus, n.d.).

Iris recognition is reliable and fast enough to do a one-to-many match with a high probability that there will be no duplicates. The span of the iris is almost a lifetime, as the iris does not normally alter after two years of age reducing the number of needed enrollments by a customer. Iris recognition may be able to detect colored contacts, eye surgery, and perform a 'live' test by monitoring pupil movement to enhance the security and reliability of the system. Additionally, iris recognition may not be invasive and does not require full user cooperation or physical contact. Although iris recognition is robust and reliable, it has drawbacks as do the other technologies. The primary drawbacks to iris recognition are environmental attributes. For example, lighting conditions may distort the image. Furthermore, some individuals are not be keen to the idea to have their iris used for identification purposes due to privacy and medical concerns. A summary of the pros and cons of the discussed biometrics is presented in table 1.

Table 1 Summary of Discussed Biometric Technologies

Biometric	**Pros**	**Cons**
Face Recognition 2-D	• Can be used covertly • Easy to use • Dual Purpose –can be used as a security camera	• Environmental conditions can greatly effect matching • Personal features can result in high failure rates
Fingerprint	• Easy, Fast, Reliable, & Well known • One to Many Matching • Long life span • Suitable for many environments	• Degradation of fingerprints: elderly, manual labor, drying of hands, cuts • Requires physical interaction • Not suitable for all environments
Hand Geometry	• Minimal privacy concerns • Fast & Reliable • Hard to reproduce	• Not static • Awkward & Obtrusive • One to One Matching

Biometric	Pros	Cons
Iris	• Easy, Fast, & Reliable • One to Many Matching • Multi Purpose • Longest life span	• Environmental attributes may cause the camera to not acquire the image

3 Exploration of Biometric Technology Usages in Tourism & Hospitality

Are tourism and hospitality businesses embracing biometrics? Some current examples of how biometric technologies are being utilized in tourism and hospitality follow.

3.1 Current Uses of Biometric Technologies in Tourism and Hospitality

Facial Recognition. In hospitality, the Borgata Hotel Casino & Spa in Atlantic City, NJ, U.S. implemented a facial recognition solution to help identify card cheaters and unwanted guests. At Borgata, surveillance is carried out using approximately 2,000 cameras to compare images of guests to a database of over 1,500 in an attempt to identity card cheaters and unwanted guests (Spangler, 2004). This facial recognition is most likely accomplished in a manner similar to the Super Bowl example. Images of guests are captured and then processed for identification, though not all will be done in real-time. At the Borgata, the card cheat and/or unwanted guest would not be identified if they are not in the database or the image acquired does not have enough similarities to any stored templates.

Fingerprint Recognition. The Waldorf Towers are utilizing fingerprint recognition for in-room safes. In November 2003, Elsafe, the global market leader in in-room security, installed their one-millionth fingerprint biometric enabled safe in the presidential suite at the Waldorf Towers, New York City, NY, U.S. The goal for the installation of this safe was to provide additional guest security and to assist with the hotel's loss prevention efforts (Hospitality Upgrade, 2003). The guest would need to place their thumb on the scanner as shown in Figure 5. A LED light would flash indicating that enrollment was successful. At that point the guest may add additional room occupants or begin using the safe (ElSafe, n.d.).

Fig. 5. Demonstration of the Elsafe Infinity Biometrics Fingerprint Safe (ElSafe, n.d.).

Two-Finger Geometry Recognition. In tourism, Disney World theme parks in Orlando, FL, U.S. have utilized a finger geometry solution since 1995 (Davis, 1997) to increase speed of admittance and security of annual and seasonal membership passes for individuals over the age of 10 (Levin, 2001). Disney needed a solution that was durable, intuitive to the user, reliable, and quick, they found this in the finger geometry system by BioMet. The finger geometry system as shown in figure 6 has instructions on usage. The guest places their fingers in the appropriate locations between the pegs while inserting their seasonal or annual membership card in the slot provided to verify in a one-to-one match that the person accessing the system is probably the holder of the membership. The intent of this system is not to deny customers from entering; to achieve this goal Disney set the threshold to fail a user very low. The implications of this is that users may be accepted who are not valid. Since the implementation, Disney has had over 20 million transactions with finger geometry (Wayman, 2000).

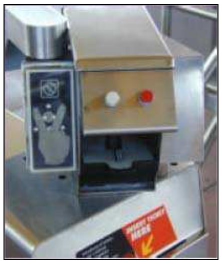

Fig. 6. Two-finger Geometry System Implemented by Disney Inc. (Levin, 2001).

3.2 Potential Uses of Biometric Technologies for Tourism and Hospitality

Although there are examples of biometrics being utilized by tourism and hospitality its usage is at best minimal and often by well-established prominent organizations with a large revenue base. However, could the usage of biometric technologies in tourism and hospitality increase?

Consider the following hypothetical scenario: You are a guest at MLM Golf Resort, the tourist destination of the future. You check-in to the hotel upon arrival by providing the required information for the reservation system and placing your finger on a scanner that captures your fingerprint while a camera captures your facial characteristics and iris pattern. The front desk employee who checked you into the hotel informs you that the only key needed for your room and hotel facilities is your finger and iris. Following check-in, you proceed to the elevator and use your finger to access the VIP floor where your room is located. The door to your room is equipped with an iris recognition scanner that captures your iris and identifies you after glancing at the camera allowing you to open the door. After viewing your room you decide to park your vehicle and get your luggage. Pulling up to the entry gate for parking you notice a fingerprint scanner to enter and leave the parking premises. You place your finger on the scanner and the gate opens allowing you to park your vehicle without the need for a paper ticket stub. While at the hotel, you use the business center and access a computer to read your email using your registered fingerprint. The computer pulls up a unique profile that allows you to have personalized settings each time you use any computer with this company.

In the afternoon, you decide to use the exercise facilities provided by the hotel and gain access by using your iris. On the way back to your room, you purchase a soft drink from a vending machine using your iris. For dinner, you go to the MLM Silver Spring Restaurant & Bar and verify your age thereby allowing you to purchase and pay for alcohol using your fingerprint. Afterwards, you go to a show in the hotel and pay for your ticket, and subsequently beverages and souvenirs with your fingerprint. Returning to your room for the night you turn on the television and order a pay-per-view movie using your finger that simultaneously authorizes that you are of legal age to purchase the movie and completes payment for the movie. Throughout your stay, the hotel staff continuously greets you by name using facial recognition. When you check out you place your finger on a scanner to accept all charges. Reflecting on your stay you realize that you did not have to track any keys, cards, or paper ticket and the housekeeping staff never knocked on your door. You also realize that you spent more money then expected as it was more difficult to keep track of purchases as with your credit cards. Is this the hotel of the future?

Though the above example may sound like a Hollywood movie, the application of biometrics in the hotel sector and tourism is indeed viable. Biometric technologies have the potential to enhance security and increase operational efficiency. With regards to security fingerprint and iris recognition, may enable the hotel to assist local and federal agencies combat crime and terrorism with watch lists (Chin, 2003). For example, the government may send out fingerprints of terrorists to the hotel to add to their fingerprint database that will ‘red flag’ the terrorist if they attempt to check-in to the hotel. In addition, logs created by biometric recognition systems will help prove culpability and assist with tracking possibly reducing theft by employees and guests as well as mis-usage of hotel property (Ginn, 2001; Tinari 2003). The tracking of employees and guests may bolster emergency management response time by locating individuals on the premises and ensuring areas are secured and clear. For instance, in a fire it would be easier to locate individuals aiding in evacuation procedures.

Biometric technologies may improve information technology (IT) security while reducing IT costs. Cyber crime incidences using hotel computers may be reduced by having unique guest accounts rather than the current anonymous access structure in place in some hotels. Furthermore, the guest and employee biometric would become the password eliminating the need to change passwords. This may also permit increased security on corporate networks for remote information distribution. Additionally, operational efficiency can also be improved. For instance, housekeeping may be more efficient by knowing guest entry and exit to rooms in real-time and transmitted using portable communications to visually show housekeeping vacant rooms. This same device may also allow housekeeping to update the status of rooms to improve turnaround time of rooms. Likewise, time management and record keeping of employees can be tied into the biometric system to eliminate redundant systems while increasing the security and reliability of employee time cards. Furthermore, financial transactions occurring would be more secure and may reduce disputes over charges and fraudulent transactions. Guest spending may also increase through biometric being used as a payment method. For instance, when credit cards were originally implemented there was an increase in spending by consumers, resulting in a corresponding increase in the profitability of credit card companies. Through biometric technologies, a hotel company may be able to improve their competitive advantage by offering distinguishable services, thereby increasing guest loyalty and satisfaction as well as attracting new guests.

4 Conclusion and Recommendations

One of the constant discussions in tourism and hospitality management centers on the integration of technology within the workplace where IT is available to employees and guests anywhere and anytime in the facility. Technology is seen as an enabler to improving guest services and employee productivity. However, despite this talk many tourism and hospitality organizations have yet to achieve full IT capabilities throughout the organization. Additionally, some have at times been plagued by what is known as the “chauffeur problem” where Chief Information Officers make IT recommendations without directions from other department managers. It is estimated that US companies, in particular, waste more than $130 billion on inappropriate technology annually (Hopkins and Kessler, 2002).

Through the exploration and examination of biometrics literature, two of the discussed biometrics seem the most viable for tourism and hospitality operations -- fingerprint and iris recognition. These two biometrics are the most reliable, accurate, easy to use, have the longest life spans, and perform one-to-many matches. However, before the chauffer drives away, so to speak, further research needs to be conducted on social and business impacts of biometrics in tourism and hospitality. Moreover, tourism and hospitality companies must have a clear and logical approach for usage and implementation of biometric technologies. For instance, if the goal of the company is to improve service management then the company must determine if biometrics may enhance areas such as IT integration, internal business practices, customer relations and employee efficiency. Although a biometric solution may be profitable or practical on paper, it is vital to determine if guests are willing to use the technology, which may differ by location due to cultural and social practices. Further, tourism and hospitality companies need to be acutely aware of any privacy, guest perceptions, attitude towards, and trust factors that may surround the usage of biometric technologies. Moreover, corporate responsibility and ethical usage of the information obtained from biometrics may influence guest willingness and perception to use the technology. Currently, ‘shades of gray’ exist on whether biometric technologies violate consumer privacy. Privacy may be a tough obstacle for companies to overcome, particularly since this technology is not widely used in consumer markets. Therefore, research is needed to determine guest privacy and attitude concerns toward biometric technologies and methods to mitigate perceived perceptions that may hinder utilization of biometric technologies. In closing, biometric technologies may be the wave of the future in tourism and hospitality. The possibilities that the technology brings to the tourism and hospitality industry are numerous as this article only presents a glimpse of what may be done with the technology as the potential extent of their usage is bound only by management’s imagination. Though biometric technologies may appear promising tourism and hospitality businesses must proceed with caution when deciding to use biometrics to avoid contributing to the $130 billion a year of wasted capital spent on information technology.

References

Association of American Law Schools. (2002) Expert *Opinions on Identity.* Retrieved from http://homepages.law.asu.edu/~kayed/talks/se-aals-02/p1-notice.htm

Ahlers, M. (2004). Officials *expect biometric passports next year.*

Argus Solutions. (N.D.) *Mining Case Study*. Retrieved from http://www.argus-solutions.com/pdfs/mining_study.pdf

Argus Solutions. (N.D.) *Laboratories Case Study*. Retrieved from http://www.argus-solutions.com/pdfs/laboratroeis_study.pdf

Biometrics Institute. (N.D.) Working Definitions Retrieved from http://www.biometricsinstitute.org/bi/types.htm

Chin, J. (2003). *Lessons Learned From 9/11 By NYC Hotel Security: A Model For Other Cities.* Hotel/Casino/Resort Security. March. pp 10.

Chachere, V. (2001). *Snooper Bowl?* Retrieved from http://abcnews.go.com/sections/scitech/DailyNews/superbowl_biometrics_010213.html

Coghlan, A. & Randerson, J. (2004). *Investigation: Forensic evidence in the dock.* Retrieved From: http://www.newscientist.com/news/print.jsp?id=ns99994611

Davis, A. (1997). *The Body As Password*. Retrieved from http://www.wired.com/wired/archive/5.07/biometrics.html?pg=2

Economist, The Print Edition. (2003). *Prepare to be Scanned*. Retrieved from http://www.economist.com/science/tq/displayStory.cfm?story_id=2246191

ElSafe. *Infinity Biometrics*. (N.D.). Retrieved from http://www.elsafe.com/page?id=456 & http://www.elsafe.com/binary?id=29450

FindBiometrics. (N.D.) *Glossary* Retrieved from http://www.findbiometrics.com/Pages/glossary.html

Ginn, D. (2001) *Hotel Group Uses New Technology To Protect Guests And Their Assets.* Hotel Security April pp. 1-2

Hospitality Upgrade (2003). Retrieved from http://www.hospitalityupgrade.com/__852568890071b5b7.nsf/0/08b538906813c0b085256c8e00508e3e?OpenDocument&Highlight=0,biometric

Hopkins, J., Kessler, M.(2002) *Companies Squander billions on tech* USA Today.

Jarvis, Angela. (N.D.) *Facial Recognition, Retinal Iris Scans, DNA, Fingerprinting, Brain Printing, Ear Matching, Smart Cards …. What's Next?* Retrieved from http://www.forensic-evidence.com/site/ID/ID_Biometric_jarvis.html

Kroeker, K. (2002) Graphics and Security: Exploring Visual Biometrics. IEEE Computer Graphics & Applications. Vol. .22. pp. 16-21.

Levin, G. (2001) *Real World, Most Demanding Biometric System Usage*. Biometric Consortium 2001. Retrieved from http://www.itl.nist.gov/div895/isis/bc2001/FINAL_BCFEB02/FINAL_4_Final%20Gordon%20Levin%20Brief.pdf

National Center for State Courts . (N.D.) Retrieved from http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

National Information Assurance Partnership, (2003). *US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments*, v1.0. pp. 15

Ross, A., Jain, A., Pankanti., S. *Capturing Hand Geometry and Extracting Features*. (N.D.) Retrieved from http://biometrics.cse.msu.edu/hand_proto.html

Spangler, T. (2004) *Face Invaders*. Ziff Media. pp. 3

Tinari, M. (2003) *Reducing Lawsuit Vulnerability of Your Hotel Parking Areas: Advise From a Legal Expert.* Hotel/Casino/Resort Security September. pp 3-4.

Waldman, Scheuermann, Eckert. (2004) *Protected Transmission of Biometric User Authentication Data for Oncard-Matching.* ACM Symposium on Applied Computing. pp 425-426

Walsh, L. Departing (2004) *Grandmother Leaves No Fingerprints*. Post-Gazette. Retrieved from http://www.post-gazette.com/pg/04168/332692.stm

Wayman, James. (2000) Retrieved from http://www.biomet.ch/aboutus.htm