CERIAS Tech Report 2005-22

EXTENDED VERSION: ARE BIOMETRIC TECHNOLOGIES THE WAVE OF THE FUTURE IN HOSPITALITY & TOURISM?

by Matthew Meyers, Juline Mills

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

Extended Version: Are Biometric Technologies The Wave of the Future in Hospitality & Tourism?

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 five 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. 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.

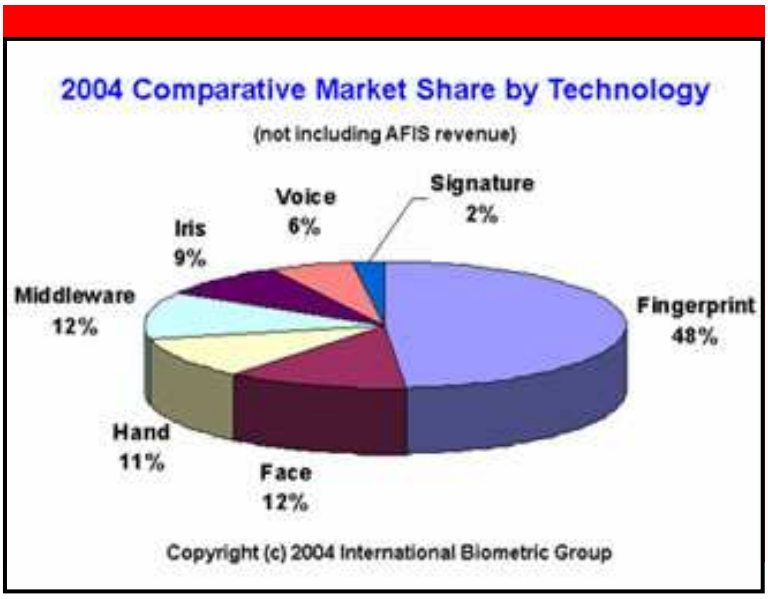

Fig. 1. Market Share Percentage by Biometric (IBC, 2004)

2 Biometric Technologies: A Brief Overview

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

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

Facial recognition can also be accomplished using an overt method as shown in Figure 3. The user poses for the camera and the facial recognition system attempts to identify or verify the individual. If identity or verification is confirmed and the user is authorized the system grants access. For verification, the user would have another form of identification such as a smart card for a one-to-one match instead of one-to-many. The one-to-one matching may reduce the false reject (denies someone actually in the system) and false accept (the system accepts someone not in the system) rate since the facial recognition system is only comparing the images captured to one template rather than the systems entire database for a match. The false reject rate may occur at a high rate, studies have put the range of error from a theoretical 2% to 9% (Lin, et al. 1997) to tested ranges of 22% (Asia Software, n.d.) to 69% (Carney, 2003).

Fig. 3. An individual interacting with a facial recognition system for verification (Cognitec, n.d.)

Although facial recognition is a growing and an improving technology, it may not be reliable enough to be the primary biometric. This is because of the flaws in the current state of facial recognition, and the innate flaws; however, facial recognition may be an excellent secondary biometric in a multimodal approach (Phillips et al, 2002). With facial recognition, several problems arise. First, environmental attributes such as lighting where identification, enrollment, and authentication occur, need to be similar. Furthermore, the camera(s) need to be positioned properly to avoid shadows that may obstruct the face and cannot be exposed to the elements since it could cause degradation of the picture. Additionally, there is the factor that cannot be controlled, the guest, for instance, clothing, stance, and hair may cause the system not to properly identify an individual who is in the system. As in a multimodal approach, fingerprint or iris recognition could be used as the primary biometric with facial recognition as a secondary.

2.2 Fingerprint Recognition

In 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. 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.

While it is theorized that fingerprints are unique, some researchers believe fingerprints may be identical, but the 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. Another problem is that fingerprint quality degrades with age, due to a loss of skin elasticity (Sickler, 2004). 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 geometry has been in use for over 20 years (NCSC n.d.). 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 4.

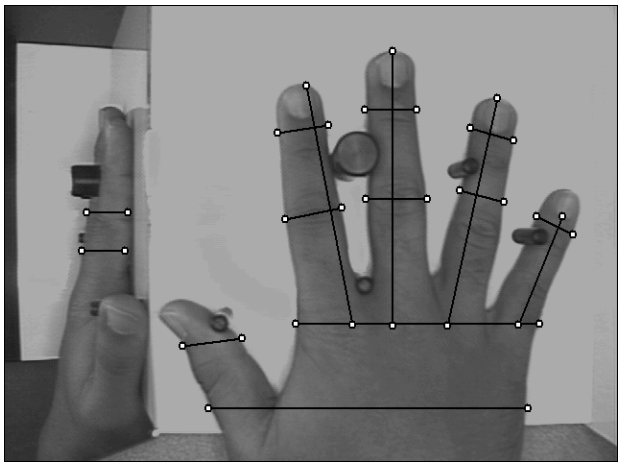

Fig. 4. Top-view of Hand Geometry and Measurements Being Obtained (Ross et al., n.d.).

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 the blood vessels in the back of the eye that are visible via the retina and the iris pattern were unique (NCSC n.d.). The theories of these scientists were correct as both iris and retina scans are now acceptable forms of biometric technologies. Retina scan recognition is not utilized in commercial entities and not publicized when and if used for government purposes. 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 other irises for identification. 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.

A user would typically stand approximately 12 to 24 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 5 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.

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 one-to-many matching ability eliminates the need for a pin or smart card device as would be needed with hand geometry. Furthermore, the life span of the iris is almost a lifetime, as the iris does not normally alter after two years of age reducing the enrollments by a customer over a time span compared to other biometric technologies. Iris recognition is 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 is not invasive and does not require full user cooperation or physical contact, as the customer may be up to 24 inches away from the camera. This also allows iris recognition cameras to be dual purpose, though they may not be as efficient as normal surveillance cameras due to positioning. Moreover, the iris images may be processed later, giving iris recognition the ability to be overt and covert, although the covert method is more difficult since the iris needs to be captured in high quality for analysis.

For example, the Afghan woman pictured in National Geographic in 1985 and than after the US invasion of Afghanistan was pictured again and identified as the previous person by iris recognition (Newman, n.d.). Iridian Technologies, the company that holds the patent for the iris recognition algorithm, was asked by National Geographic to identify the Afghan woman from a picture in 1984 to one in 2002. Iridian took digital images of the two pictures and ran it through their software to compare the iris features. After comparing the iris images, Iridian concluded that the eyes were indeed

the same. The probability of error that those two eyes were not the same is one in one hundred million, leaving little doubt that it is in fact the same person pictured in 1984 and 2002 (Iridian, n.d.).

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. By using iris recognition the company was also able to monitor the health and safety of employees while they were underground. The results were positive, as the iris system exceeded expectations. The other advantages found were: users could wear full equipment (masks and sunglasses), accurate record of personnel for emergency management, real-time response to attempts to circumvent security, time keeping, and real-time work time of employees for safety assessment. The mining company found that the cameras were able to work in low light conditions, after midnight, however, they had problems with glare from the sun

in the morning, and positioning of the cameras was important to minimize this problem.

Fig. 5. A Scientist at Celex Labs Using an Iris Camera with Eye Gear (Argus, n.d.).

2.5 Signature Verification

Signature verification is the comparison of characteristics such as speed of stroke, pressure of writing utensil on certain points, and length of characters (findBiometrics n.d.). The software to allow signature verification was developed in 1994 by CyberSign and became mainstreamed in 1996 (CyberSign, n.d.). To make document signature verification more efficient, devices verify if the signature matches the signature on file for an individual. The security of signature verification is fairly strong as it is difficult to replicate the measurements acquired and compared to, for instance, even if the signature looks identical, it may still fail if processes by a signature verification system. For the security and convenience, signature verification may be useful for billing and internal document control. This could allow restaurants

to function at the status quo, by having the customer sign for a billing statement when using payment methods besides cash by implementing digital signature pads. This could permit the restaurant, if applicable, to have biometric enabled technology to help mitigate the risk of fraudulent charges by verifying that the signature is the authorized signature for that billing profile (Sternberg n.d.).

In 2002, Mercedes-AMG a division of DaimlerChrysler was looking for a solution to optimize and control internal documentation processes. Initially the company looked at a pin and password solution for encryption but felt it would still be insecure due to incidents such as social hacking (social engineering). Mercedes-AMG came across SignDoc, a system that digitally records and encrypts signatures into a document and compares them against a stored signature to verify the authenticity. This is accomplished using one-to-one matching since the system compares the signature in question to the signature stated to be compared to and not all in the database. Mercedes-AMG implemented this system for legal purposes, such as test clearances, inspection reports, garage acceptances, and applications for orders and vacations. Mercedes-AMG expects an increase in reliability of a document since the system can show when and who signed or modified a document. Furthermore, additional benefits will be realized from reduced costs associated with printing, storage, and time. Additionally, many users are habituated from usage, for instance, many department stores have electronic signature pads that capture the signature for receipts. Signature verification is the same process for the user as shown in figure 6 the user signs on the

electronic pad, which then appends their signature onto the document in digital format (SoftPro, n.d.).

Fig. 6. A person signing on a digital pad for signature verification (SoftPro, n.d.).

Although signature verification may be appropriate for documentation, it may not be practical for physical access control. The first problem is that people may not sign with a digital pen the same as with traditional pen and paper. The second problem is feasibility; imagine signing a pad next to a door to gain entry. The time required to sign a pad that may be awkward to use and have the signature verified may take longer than a customer would prefer to spend waiting. Additionally, signatures tend to vary throughout ones life, making the age of the template possibly minute, resulting in the need for repeat enrollments to the system. 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 – also can be used as a security camera	• Environmental conditions can greatly effect matching • Personal features can result in high failure rates
Fingerprint	• Easy to use • Well known – Acceptability • One to Many Matching – Uniqueness • Fast • Long life span • Suitable for many environments	• Degradation of fingerprints: elderly, manual labor, drying of hands, cuts • Requires user physical interaction • Not suitable for all environments
Hand Geometry	• Minimal privacy concerns • Fast & Reliable • Hard to reproduce	• Not static – body features may change • Awkward to use • Obtrusive • One to One Matching
Iris	• Fast & Reliable • One to Many Matching • Easy to use • Non-obtrusive • Dual Purpose – can be used as a security camera and for facial recognition • Longest life span	• Environmental attributes may cause the camera to not acquire the image • Possible privacy issues

Biometric	Pros	Cons
Signature Verification	• Easy to use • Reliable • Help mitigate risk of signature fraud	• Electronic signature pads can be awkward to use • Can be reproduced • Not one to many matching under normal circumstances

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

3.1.1 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.

3.1.2 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 7. 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. 7. Demonstration of the Elsafe Infinity Biometrics Fingerprint Safe (ElSafe, n.d.).

In addition to safety deposit boxes, door locks are also commercially available with fingerprint recognition scanners as shown in figure 8. The hotel guest would place their enrolled finger on the scanning device, located towards the top of the lock. If the finger is valid, (matches appropriate fingerprint stored in the database) the door would unlock allowing the guest to enter the room.

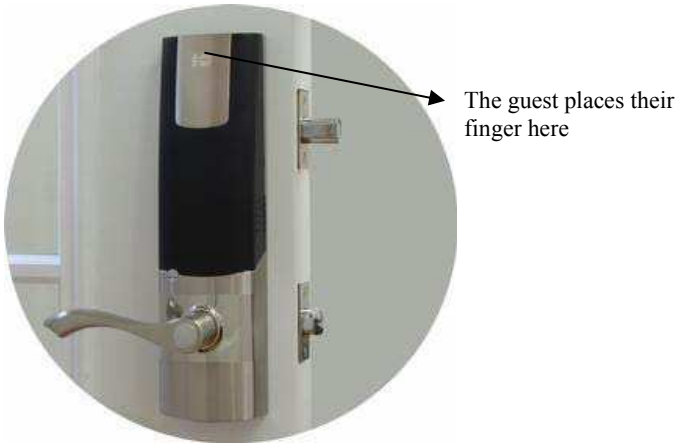

Fig. 8. A biometric enabled door lock (ArrowVision, n.d.).

3.1.3 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 9 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). There are several advantages to hand geometry such as the minute amount of personal data collected, robustness, reliability, and speed. Hand and two-finger geometry are perceived as less invasive in respect to privacy since the measurements taken are not unique, hence the need for the one-to-one match in combination with a pin number or data card. Similar to the current username/password combinations for computers the same is for hand geometry as the pin number or data card is the username and the hand is the password.

Fig. 9. Two-finger Geometry System Implemented by Disney Inc. (Levin, 2001).

3.1.4 Iris Recognition

Frankfurt International Airport launched a six month test project, Automated and Biometrics-based Border Control, using iris recognition. The program allows passengers to expedite the security process by having a biometric enabled passport. The passenger would approach the iris recognition system as seen in figure 10 (AP, 2004). First the passenger slides their passport through a device that extracts their template. The passenger then looks into the camera and waits approximately three seconds while the system verifies their identity. The program was running in terminal 1 and successfully enrolled over 9,000 passengers (Frankfurt Airport, 2004). Due to the success the program has been extended for an additional 12 months.

Fig. 10. German Interior Minister Schily using the iris recognition system at Frankfurt International (Lohnes, 2004).

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 misusage 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 numerous 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. Due to secure perception and possibly the lack of awareness (tracking of financial transactions) of the technology guest spending may 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. Table 2 is an abbreviated version of how biometrics may be applied to hospitality and tourism industry.

Table 2 Possible Biometric Usages in Hospitality

Procedure	Current Process	Biometric Process
First time check-in	A template/profile is created for the guest with required information. Once complete the hotel employee issues a key for access to the room(s) and hotel facilities.	A template/profile is created or modified with required information. A biometric is acquired of the guest for access to hotel facilities.
Return guest check-in	The guest checks-in at the appropriate location. However, information is typically stored from the previous visit to speed up the check-in process.	The guest check-in at the appropriate location and uses their biometric to pull-up the profile and reservation. The hotel employee confirms the check-in and room. It may be possible to implement self check-in kiosks, where the guest would interact with a system for automated check-in.
Employee assistance with luggage	The guest uses a key card or key to enter the room. The hotel employee may have a key or request the key to open the door for the guest.	The guest uses their biometric to enter the room. The hotel employee may have temporary access to the room or request the guest to open the door.
Check-in Via Hotel Shuttle	Some hotels are using wireless technology to do remote check-in of guests while in transit to the hotel. However, key cards are not issued until the guest arrives to the hotel.	The hotel could fully check-in guests using a biometric in transit to the hotel such as a portable iris or fingerprint recognition device.

Procedure	Current Process	Biometric Process
Check-Out	The guest check-out process is normally accomplished in two ways. The guest uses an interactive system via the television and leaves the keys in the room or the guest goes to the appropriate location in the hotel and does a check-out at that location.	The guest check-out process would be similar but using biometrics to assure it is the individual responsible for payment of the room.
Hotel Parking	The guest receives a permit or stub for self-parking or valet parking of their vehicle. For valet parking, the guest leaves a car key with the hotel employee.	The guest parks their vehicle and is only able to leave and/or enter the facility using their biometric. The valet parking is done using a biometric rather than a stub, and may have a biometric enabled storage box for keys to reduce liability.
Exercise Facilities: Ex: Fitness Centers, Aquatic Facilities, Tennis, Racquetball, & Basketball Courts	The guest enters the fitness center using their key or the hotel may have an open door policy.	The guest would use a biometric device to identify for access to the exercise facilities. The biometric device may have information pertaining to age and other factors that may result in a guest being denied permission for entry. If the guest meets the hotel requirements to use the facility access would be granted.

Procedure	Current Process	Biometric Process
Business Centers	The guest enters the business center(s) and utilizes equipment available, typically with no tracking of how the guest is using the equipment.	The guest would utilize equipment by identifying with a biometric device attached to the equipment. For example, a guest would access a computer by using their biometric feature, which then accesses a unique profile that can allow auditing of what the guest is doing with hotel equipment.
Restaurant, Shopping, and Entertainment Billing	The guest may pay with their room number and name or acceptable payment methods such as local currency and credit cards. If payment were done via room number or credit card the guest would sign a receipt.	The guest may pay with their registered biometric or traditional payment methods. This may reduce time spent for the billing/payment phase and reduce fraudulent transactions. This will also allow the hotel to track guests to potentially improve marketing and overall business management.
Bars & Entertainment Age Verification	The guest is asked to present identification to confirm that they are of legal age to purchase alcohol or participate in entertainment functions that have a minimum age requirement.	The guest would identify with a biometric device with their registered biometric feature for age verification. This may reduce the liability to the hotel for underage consumption and participation in entertainment. Not all attendees will be in the biometric system, the hotel may require enrollment or use the current process in conjunction with biometrics.

Procedure	Current Process	Biometric Process
In-Room Features: Pay-Per-View, Phone Usage, Safes	The guest makes phone, orders pay-per-view movies via cable/on-screen service, and may have electronic or safes at the front desk. It is not typical for hotel rooms to have automatic environmental controls.	The guest would identify with the biometric devices to ensure A. that the guest is of age depending on the movie, and B. that the guest is utilizing the phone. This may reduce the amount of fraudulent complaints and usage of in-room features. Additionally, biometric safes can help reduce liability.
Special Events	Guest may be manually verified for special event admission.	Guests residing at the hotel may enter special events using their registered biometric for identification and authorization for the events. This may speed up the processing of attendees for events. Attendants without a registered biometric may be manually verified or enrolled into the biometric system.
Security & Theft	Security services may be present in hotels utilizing physical appearance and cameras for security. Physical access to rooms and facilities may be secured by electronic keys.	Security services may be able to locate known criminals and terrorists by increased surveillance in-real-time on when guests and employees are on the hotel premises. This may help in emergency situations such as evacuations. Physical access to rooms and facilities would be secured via biometric technologies. This may reduce theft by guests and employees.

Procedure	Current Process	Biometric Process
Employee & Guest Management/Tracking	Hotels may track guest purchases and complaints. Hotels may also have a general idea where employees and guests are in the facility but generally not exact positions.	The hotel may track guest purchases, and complete profiles unique to each guest. Additionally, the hotel may do real-time tracking of guests to know proximity of guest location. For employees the hotel may use this for time management, tracking, performance evaluations, and security to try and prove who was in a room at what point and the duration of time spent in the room.
Hotel Room Cleaning	Housekeeping cleans a room and updates the reservation system stating the status of the room.	Housekeeping could notified in real-time updates of the room status and know when a guest is in a room rather than disturbing a guest which, may save time and increase customer satisifaction.
Employee Computer/Networks Access	Employees use userid and passwords for computer and local and remote network access.	Employees would use their registered biometric for userid and password for local and remote network access. This eliminates lost passwords which may reduce workload and costs for the IT department.

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 primary biometrics 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. In respect to the other technologies discussed it may be feasible to implement a multi-modal approach. For instance, facial recognition and iris recognition can be combined into one system where both biometric features are extracted from the same device. Another usage could be the multi-modal approach of fingerprint recognition and signature verification for receipts. 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.

5 References

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

Anonymous, Interview conducted on July 15, 2004. The company wishes to maintain anonymity.

Anonymous. Pool Drowning. Hotel Security Report April 2001. The articles goes over the nine misdemeanors the prosecutor could sue the hotel. The hotel had very few security measures.

Asia Software. The Art of Identification. Available Online: http://asia-soft.com/frs/en/products/prod_dem.asp

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

Associated Press. Frankfurt Airport introduces iris scan for border control. February 2004. Available Online: http://www.usatoday.com/travel/news/2004-02-16-german-scan_x.htm

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

ArrowVision. ArrowVision Adds Tracking Function to Popular Biometric Door Locks. Available Online: http://www.marketwire.com/mw/release_html_b1?release_id=71707

Blando, Sal. Protecting Hotel Guests and Assets During Very Special, Special Events. Hotel Security Report. February 2001 Page 8-9.

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

Carney, William. Scenario Test of Facial Recognition for Access Control. 2003 International Conference on Emerging Technologies. Available Online: http://www.rfbinternational.com/papers/Carney.pdf

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

Cognitec. Available Online http://www.cognitec-systems.de/products-entry-a.htm

Cybersign. Available Online: <http://www.cybersign.com/about.htm#history >

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

findBiometrics (N.D). Understanding Signature Verification, Available online: http://www.findbiometrics.com/Pages/signature%20articles/signature_1.html

Frankfurt International Airport. Iris recognition program for border controls continues. October 2004. Available online: http://www1.frankfurt-airport.com/cms/default/dok/30/30179.iris_recognition_program_for_border_cont.htm

Gill, Moon, Seaman, Turbin. Security Management and Crime in Hotels. International Journal of Contemporary Hospitality Management 2002. Page 62. The article describes the two main types of fraud, one being false guest theft reports. With electronic keys the rate of reports decreased because of accountability.

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

Hill, Sean. Security For The New Casino. Hotel/Casino/Resort Security February 2003 Page 5. SGA Corporation is trying to deal with underage gambling and drinking by implementing machines to read the bar codes on the back of identification cards. Though this is good, additional measures may be taken with the usage of biometrics.

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.

Hudak, Richard. Laptop Thefts Loom As A Major Hotel Security Problem. Hotel Security Report July 2001. This article discusses the cost of laptop theft and the growing percentage particularly from guest rooms.

Iridian. National Geographic's Afghan Girl Positively Identified By Iris Recognition. Available Online: http://www.iridiantech.com/news.php?page=1&rel=031802

Iridian Technologies. Selected Case Studies. Available Online: <http://www.iridiantech.com/solutions.php?page=2>

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

Kontzer, Tony. Hilton Makes Check-In Easier. Information Week. June 8, 2004. Hilton has implemented kiosks to check-in and has stated there is great success and continues to implement the kiosks. Available Online: <http://www.informationweek.com/story/showArticle.jhtml?articleID=21402089&tid=16028>

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

Lin, Shun-Hung, Kung, Sun-Yuan. Face Recognition/Detection by Probabilistic Decision-Based Neural Network. IEEE Transactions on Neural Networks. January 1997.

Lohnes, Thomas. Frankfurt Airport introduces iris scan for border control. February 2004. Available Online: http://www.usatoday.com/travel/news/2004-02-16-german-scan_x.htm

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
http://ctl.ncsc.dni.us/biomet%20web/BMHand.html#history
http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.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

Newman, Cathy. A Life Revealed. Available Online: http://magma.nationalgeographic.com/ngm/afghangirl/

Paraharm, Arias, Prado. New Luxury Hotels: Upscale Security Ideas That Can Be Applies To Average Properties. Hotel Security Report. December 2001. Pages 8-10. This articles describes security measures for spa/fitness centers including height restrictions and how the hotels try to enforce the requirements.

P. JONATHON PHILLIPS, PATRICK GROTHER, ROSS J. MICHEALS, DUANE M. BLACKBURN, ELHAM TABASSI, MIKE BONE. Face Recognition Vendor Test 2002.

Pinto, Toni. Good Basic Security At New JFK Hotel Promotes Guest Feeling of Safety. Hotel/Casino/Resort Security January 2003 Page 4. The article goes over key points for increasing parking security to make customers feel more secure which in turn increases customer satisfaction.

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

Sickler, Nate. An Evaluation of Fingerprint Quality Across an Elderly Population vis-à-vis 18-25 Year Olds.
SoftPro. Case Study: Innovative Signature Verification to optimize processes in the automotive industry.
Spangler, T. (2004) Face Invaders. Ziff Media. pp. 3
Sternberg, Barbara. Employee Fraud: Protecting Your Bottom Line. Available Online: http://www.igin.com/Landscaping/fraud.html
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
World Airline News. New Airline Kiosks Minimize Airport Time For Business Travelers. Nov. 10, 2000. This article describes the new kiosks for self check-in at the airport and the result of higher customer satisfaction and lower costs to the airlines. Available Online: <http://www.findarticles.com/p/articles/mi_m0ZCK/is_45_10/ai_66894566>