11-5-2013

Research Note: Biometric Technology Applications and Trends in Hotels

Anil Bilgihan

Ersem Karadag

Cihan Cobanoglu

Fevzi Okumus
University of Central Florida, Fevzi.Okumus@ucf.edu

Original Citation

11-1-2013

Research Note: Biometric Technology Applications and Trends in Hotels

Anil Bilgihan Dr.
Florida Atlantic University, bilgihan.1@osu.edu

Ersem Karadag
Robert Morris University, karadag@rmu.edu

Cihan Cobanoglu
University of South Florida, cihan@sar.usf.edu

Fevzi Okumus
University of Central Florida, Fevzi.Okumus@ucf.edu

Follow this and additional works at: http://digitalcommons.fiu.edu/hospitalityreview

Research Note: Biometric Technology Applications and Trends in Hotels

Abstract

The purpose of this study is to investigate the biometrics technologies adopted by hotels and the perception of hotel managers toward biometric technology applications. A descriptive, cross sectional survey was developed based on extensive review of literature and expert opinions. The population for this survey was property level executive managers in the U.S. hotels. Members of American Hotel and Lodging Association (AHLA) were selected as the target population for this study. The most frequent use of biometric technology is by hotel employees in the form of fingerprint scanning. Cost still seems to be one of the major barriers to adoption of biometric technology applications. The findings of this study showed that there definitely is a future in using biometric technology applications in hotels in the future, however, according to hoteliers; neither guests nor hoteliers are ready for it fully.

Research Note: Biometric Technology Applications and Trends in Hotels

Anil Bilgihan
Florida Atlantic University

Ersem Karadag
Robert Morris University

Cihan Cobanoglu
University of South Florida

Fevzi Okumus
University of Central Florida

Abstract

The purpose of this study is to investigate the biometrics technologies adopted by hotels and the perception of hotel managers toward biometric technology applications. A descriptive, cross sectional survey was developed based on extensive review of literature and expert opinions. The population for this survey was property level executive managers in the U.S. hotels. Members of American Hotel and Lodging Association (AHLA) were selected as the target population for this study. The most frequent use of biometric technology is by hotel employees in the form of fingerprint scanning. Cost still seems to be one of the major barriers to adoption of biometric technology applications. The findings of this study showed that there definitely is a future in using biometric technology applications in hotels in the future, however, according to hoteliers; neither guests nor hoteliers are ready for it fully.

Keywords: biometrics, hotel, security, technology, guest, privacy

Introduction

Use of recent technological applications can help hotel companies in many areas including marketing, operations, guest services, human resources, information technology and security areas (Crick & Spencer, 2011; Davidson, McPhail, & Barry, 2011; Harrington & Ottenbacher, 2011; Ip, Leung, & Law, 2011; Yoo, Lee, & Bai, 2011). It is even claimed that successful deployment of technological applications can help hotel companies create and maintain a competitive advantage (Bilgihan, Okumus, Nusair, & Kwun, 2011; Okumus, 2013). Currently, biometric technology is one of the novel technologies that can help hotel companies in many areas. For example, biometric technology is now replacing conventional identifications and verification methods in many areas in the business world.

Biometric refers to the use of automated methods to identify a person based on physiological or biological characteristics. Signature verification, fingerprint recognition, iris scanning, hand geometry, vein patterns, voice recognition, and facial recognition are major methods used in biometrics. Biometric technology is a highly effective way to establish identity verification. Therefore, it has emerged as a promising technology for authentication and has already found its' place in the most hi-tech security areas (Bilgihan, Beldona, & Cobanoglu, 2009; Berezina, Cobanoglu, Miller, & Kwansa, 2012; Jackson, 2009: Kim, Brewer, & Bernhard, 2008; Heracleous, & Wirtz, 2006).

Implementation of biometric applications in the hospitality industry is emerging (Jackson, 2009) as such technologies have potential to offer various benefits to hotel operations and the guest experience. For example, in operations it automates employee clock in and clock out, and in terms of guest experiences, it can be embedded in customer relationship marketing systems (i.e. facial recognition of VIP guests when entering to a casino).

Research on biometric context currently focuses on biometric use in security, business, technological and government applications. There are a few studies that investigated biometric technologies from the hospitality industry's point of view (e.g. Bilgihan et al., 2009; Jackson, 2009; Morosan, 2012; Murphy & Rottet, 2009). Previous studies in this area have generally investigated biometric adoption only from the customers' viewpoint. The perception of hotel managers towards biometric technology has not yet been fully investigated. This study aims to fill a gap by examining current and potential future uses of biometric technologies from the managers' point of view.

The biometric systems revolve around a core biometric verification system which, when deployed by hotels provides best in class security and ease of management in several departments. In some countries, for security concerns and fulfill government requirements, hotels need to keep identity records and/or biometric records of all guests. These records are a great help to law enforcement agencies in case of need. The main concern for the management of any hotel is to offer robust security to its guests, making sure that their stay will be without any problems. To succeed this objective, hotels should deploy a very structured and professional security policy. It should ensure safety of its guests, staff and the estate. However, at the same time, biometrics is a rising and contentious topic in which civil liberties groups declare concern over privacy and identity issues. Biometric technologies may face resistance from managers and customers mainly due to its cost and privacy issues (Blank, 2006). Biometric laws and regulations are in the development process and biometric standards are being tested. Face recognition biometrics have not gotten to the point of fingerprinting, but with constant technological advances and with security threats, researchers and biometric developers will further develop this security technology for the twenty-first century (Osborn, 2005).

Biometric technology may bring several advantages and disadvantages to hotels and its guests. However, there is limited research on the factors that impact utilization of biometric technologies in hotels. For this reason, the purpose of this study is to examine the types of biometric technologies adopted by hotels and the perception of hotel managers toward biometric technology applications. This study uses the perception of hotel managers to assess

the future potential adoptions and barriers of biometric technology applications. More specifically this study attempts to answers the following questions:
1. Which biometric technology applications are used in hotels?
2. What are the purposes of using biometric technology applications in hotels?
3. What are the reasons for not using biometric technologies in hotels?
4. What is the perception of hotel managers who adopt biometric technology applications?

Literature Review

The Modes of Biometrics as a Novel Technology Tool

A biometric system is used in two major ways, which are verification and identification (Jackson, 2009). Biometric systems might seem complex, but all of them tend to use the same three basic steps that are listed below (Sanchez-Reillo, 2000). First phase is "**enrollment**". The first time a person uses a biometric system; it records basic information about the person, such as name or an employee identification number. Later, it captures an image or recording of the person's specific trait, such as fingerprint. The next phase is "**storage**". It refers to storing the information. Most systems do not store the complete image or recording. They instead analyze the trait of people and translate it into a code or graph. Some systems also record this data onto a smart card. The final phase is "**comparison**" where the next time a person uses the system. It compares the trait that the user presents with the information on file. Table 1 shows summarized comparison of the features of biometric technologies (Bolle, Connell, Pankanti, Ratha & Senior, 2004; Harris & Yen, 2002; Jain et al., 2004; Kleist, Riley & Pearson 2005; Woodward, Orlans & Higgins, 2003).

Table 1: Comparison of Biometric Technologies

	Fingerprint	Facial Recognition	Hand Geometry	Iris Scan	Voice Recognition
Accuracy	H	L	M	H	L
Ease of Use	H	M	H	M	H
User Acceptance	M	H	M	L	H
Performance	H	M	M	M	L
Distinctiveness	H	L	M	H	L
Privacy Concerns	H	H	M	H	L
Cost	L	L-M	M	H	L

Note: High, Medium, and Low are denoted by H, M, and L, respectively.

Biometric Technology in the Hotel Industry

Latest security technologies like biometrics, infrared access, smart card access, and custom-made, ID-card printers are available in the market to help hoteliers to enhance safety and security (Oliva, 2003). A survey conducted by Hotel Asia Pacific Magazine and Pertlink, found that one in three hoteliers fear for the safety of their properties. Even more interesting was the fact that nearly 50% of respondents admitted they had not increased investments in security (Hotel Online, 2003). On the other hand, according to a study by Murphy and Rottet (2009) 87.3% of leisure guests are favorably pre-disposed to use biometric technologies for guest services, mostly sport and outdoor activities. This study found that travelers from North America might be more willing than other categories of travelers to use and adopt biometric technologies.

Unlike other conventional identification methods, the personal traits scanned by biometrics are difficult to lose, forget or copy. For this reason, it is considered to be safer and more secure than other conventional methods, such as keys, cards or passwords. For instance, when a hotel guest uses hotel services such as a bar, restaurant or any other paid services, he/she is required to verify his biometric identity by placing their finger on the biometric reader on the Point of Sale System (POS) instead of only their signature. This prevents impersonation and eliminates any possible disputes at the time of final billing regarding the use of these paid services. Beside customer recognition and verification, there are many possible future applications of biometrics, such as keeping time and attendance of employees, Network/Personal Computer (PC) Login Security, and Employee Recognition. Furthermore, research estimates that businesses can save 2.2% of gross payroll annually on average by eliminating buddy punching through the use of biometric technology. The American Payroll Association states that a typical business can save up to $1,000 per employee per year with biometric time and attendance systems (Stone, 2012).

Biometric technology applications that are used in hotels include biometric in-room safes, iris scanning and face recognition systems designed to allow staff and guests access to certain areas (Adams, 2002; Simon, 2004). More recent technologies include face recognition at hotel entrances to identify VIP guests. Usually, hotels do not offer biometric technologies due to reliability, lack of standards (Vijan, 2004), perceived intrusiveness (Singh & Kasavana, 2005), and privacy concerns (Adler, 2008; Kim et al., 2008; Tsai, 2007). On the other hand, it is agreed that biometric technologies can add value to guests' hotel stay experiences (Murphy & Rottet, 2009). In addition, they can help hotels reduce costs and fraud, and increase accuracy in transaction processing (Murphy & Rottet, 2009), while offering users security and convenience (Ives et al., 2005; Jones, Williams, Hillier, & Comfort, 2007).

Biometric technologies provide convenience to guests by allowing them to check in/out, access guest areas, and make payments with unprecedented convenience and speed (Morosan, 2012). Although the overall cost of biometric hardware is decreasing significantly, at a hotel's scale, biometric systems represent considerable investments (Kim, 2009). Accordingly, hoteliers need better insights with regards to biometric technologies.

The hotel industry requires an open and friendly environment where customers can come and relax without having to worry about their security. Simultaneously, hotel companies are aware that security is a top concern both to travelers and their establishments. Generally, the hotel industry has long suffered from security breaches, including network and systems security, theft by employees, credit card theft and fraud among many others (Barrier, 2001; Rinehart, 2000). In addition, since 9/11, security awareness has significantly increased in public areas (Bowyer, 2004), such as hotels and airports. Hotel companies feel the pressure to manage risk, loss prevention, and fraud.

Various research firms and industry experts anticipate the growth of the biometric industry to be significant in the near future. A study from Unisys Corporation points out that almost 70% of surveyed consumers are in support of using biometrics as a way of verifying identity, as long as that verification is conducted by trusted organization. The Unisys survey also saw 66% of respondents favoring biometrics as a method of combating identity theft and fraud; the survey compared biometrics in this category to other credential-type methods, including tokens and smart cards. The percentage of support is slightly up over a September 2005 study by Unisys, which was 61% of surveyed consumers favoring biometrics (SecurityInfoWatch.com, 2009). Regardless of the prediction, it is clear that the commercial use of biometrics is expanding worldwide. For example, facial and iris recognition are incorporated into automated teller machines (ATMs); financial institutions use finger scanning to identify clients; and finger geometry is used to control access to major theme parks. Fingerprint applications gaining a significant step in the hospitality areas. For instance, over 20,000 Owens-Illinois employees punch in and out each day using such devices, and more than 30 individuals at Krispy Kreme doughnut shops track their stores' employees in this manner. Likewise, the Decatur Hotel Group in New Orleans started implementing biometrics at its 12 hotels. Aramark Sports and Entertainment Information Technology installed fingerprint recognition systems at its main employee entrances, kitchens, human resources departments, administrative offices and other areas with high visibility (Spence, 2003).

In the past, technology issues in hotels have been handled on a reactive basis, namely after the issue arises. However, recent technology trends have focused on managed services. The managed services proactively monitoring technology can significantly reduce the negative issues that arise when an unexpected problem occurs. Those hotel systems that most effectively use the latest developments in technology will leave their competition far behind them in relation to success in their occupancy and hotel operations (Aronson, 2007). Among all biometric applications, fingerprint-based identification is the oldest method that has been successfully used in numerous applications.

Biometrics and Security in Hotel Companies

Biometric technologies aim to reduce fraud and eliminate risks associated with security (Singhal & Jain, 2011). Recently, airports, financial organizations, police departments, hospitals and businesses of all sizes have been integrating biometric technology applications into their work place. Organizations recognize the potential benefits of investing in biometric technologies (Singhal & Jain, 2011). Hotels may be considered as soft targets due to their nature of being open and accessible to general public (Parton, 2007). For instance, terrorist

attacks on the Grand Hyatt, Radisson SAS and Days Inn hotels in Amman killed 60 people and caused hundreds of injuries. Therefore, security has emerged to be an important issue for hoteliers, particularly at the luxury end of the market. Furthermore, hotels have long suffered from security breaches, including network and systems security, theft by employees, and credit card theft and fraud among many others (Rinehart, 2000). Biometric technologies in hotels can potentially improve room security, control access to restricted areas, and limit access to critical data.

Technology Acceptance Model (TAM)

As with any novel technology, user acceptance of new Information Technology is usually hard to gauge and policies to introduce and ensure adequate and correct usage of such technologies are often lacking (James, Prim, Boswell, Reithel & Barkhi, 2006). Security technologies have extensive applicability to different organizational contexts that may present unusual and varied adoption considerations (James et al., 2006). Technology Acceptance Model (Davis, Bagozzi, & Warshaw, 1989) is the theoretical foundation for most of the research that investigated user acceptance of information technologies. TAM presents the precursors of information system acceptance by providing a basis for tracing the impact of external factors on internal beliefs, attitudes and intentions. The model suggests that actual system use is determined by both perceived usefulness and perceived ease of use of the technologies. Therefore, in order to be used by hotels, the biometric technologies should offer usefulness for both employees and guests and they should be easy to use.

Methodology

A descriptive, cross sectional survey was developed based on extensive review of literature (Jackson, 2009; Kim, Brewer, & Bernhard, 2008) and expert opinions. The population for this survey was property level executive managers in the U.S. hotels. For this purpose, the members of American Hotel and Lodging Association (AHLA), the largest organization that represents American Hotels, was selected as the target population for this study. In the AHLA Database, there were 46,498 members from all over the world. All members that are outside of the United States were deselected from the database. This left 30,924 members and 26, 841 hotels in the database. The executive managers of all these hotels were listed in an Excel spreadsheet alphabetically. Limiting the number of the managers to one thousand, was deemed to be sufficient to get the perceptions for the purpose of this study, a random number was generated by using RAND function. Then, these managers were re-sorted based on this random number. The top 1000 managers that had an email address were selected as the sample for this study.

The survey instrument consisted of four sections: 1) biometric technology applications used; 2) reasons for using and not using biometric technology applications; 3) perceptions about biometric technology applications as adapted from Kim et al (2008) and 4) demographics of the respondent and characteristics of the hotel.

Findings and Discussions

Out of the 1000 email invitations sent, 255 valid responses were collected with a 25.5% response rate. Of the participants, 68% of the respondents were male while 32% were female. About 32% of the respondents had a bachelor's degree while 23.4% had a master's degree, 14.3% had some college degree. Thirty-two percent of the respondents were owners, 28.6% were general manager, 10.4% were sales and marketing managers. The sample used in this study represents US hotel manager demographics (Nebel et al., 1995). In terms of the hotels that the respondents worked for, 39.5% were mid-priced properties, 30.3% were upscale, 13.2% were luxury, and 10.5% were budget and economy hotels. About quarter of these hotels had less than 50 rooms, another quarter had 51-100 rooms, 18.2% had 101-200 rooms, and 13.2% had 201-500 rooms. About 37% of the hotels were in business more than 20 years, 26.7% for 11-20 years, 20% for 6-10 years, 12% for 1-5 years and 4% for less than 1 year.

The first research question of this study aimed to investigate the type of biometric technology applications used in hotels. Table 2 shows the current uses of biometric technologies in hotels. Out of the 255 respondents, only 21 of them (8.2%) reported that they use some kind of biometric technology in their hotels. The adoption level of biometric technologies was low as expected given the novelty of the technology. According to the study findings, among the hoteliers that use a biometric technology application, the most common biometric application used in hotels is fingerprint scanning (42.9%). The main reason of this finding might be the fact that a greater variety of fingerprint devices are available than for any other biometric (Liu & Silverman, 2001). As the prices of these devices and processing costs fall, using fingerprints for user verification may gain wider acceptance. Fingerprint devices were followed by hand geometry and palm print scanning (28.6%) and signature recognition (14.3%), face recognition (14.3%). Iris scanning and voice recognition were found not to be used in hotels. Iris scanning compared to most of the other tools has a relatively lower ease of use (Liu & Silverman, 2001).

Table 2: Current uses of biometric technology applications in hotels

Biometric Application	Frequency	%
Fingerprint scanning	9	42.9%
Face recognition	3	14.3%
Hand geometry and palm print scanning	6	28.6%
Iris scanning	0	0.0%
Voice recognition	0	0.0%
Signature recognition	3	14.3%
Total	21	
N=255		

The second research question of this study aimed to investigate the purposes of using biometric technology applications in hotels. It was found that the most frequently reported reason for using biometric technology applications in hotels is employee attendance tracking (71.4%), followed by door lock (14.3%) and hotel security (14.3%). McIntosh (2009) reported

that employee attendance tracking systems are used to help reduce hourly payroll costs, prevent unauthorized overtime and stop timecard misuse such as buddy punching. Hotel workers are usually paid on an hourly basis (Krause et al., 2005); therefore, it is explicable that hotels prefer to deploy biometric technology applications for employee attendance tracking. This finding suggests that the participating hotels adopted biometric technologies mostly for operations and managing cost, not for the guests.

Table 3: The purpose of using biometric technology applications in hotels

Purpose	Frequency	%
Employee attendance tracking	15	71.4%
Door lock	3	14.3%
Hotel security	3	14.3%
Total	21	

With regards to the third research question that examined the potential reasons for not using biometric technologies in hotels, it was found that a high majority of hotels (91.8%) do not utilize a biometric application. As noted in Table 4, the most frequently reported reason for not using a biometric application in a hotel was the unfamiliarity with the technology (42.3%). It appears that hoteliers simply do not know enough about the biometric technology applications and their potential advantages. The reason behind this might be the fact that the hotel industry is usually slow in accepting technological changes (Donaghy et al., 1997). Accordingly, biometrics vendors are advised to introduce their biometric technology applications and their advantages for the hoteliers. The second most reported reason was the lack of need (39.7%), followed by the cost (28.2%). As Polemi (1997) highlighted earlier, most of the biometric systems are expensive and this puts a barrier in the expansion of the biometric market. About 3% reported other reasons such as "too soon for guests to accept", "limited application and interface", and "legal issues".

Table 4: Reasons for not using biometric technology applications

Reason	Frequency	%
Too expensive	66	28.2%
There is no need	93	39.7%
Not familiar with technology	99	42.3%
Privacy issues	18	7.7%
Other	7	3.0%

N=234

In order to investigate the perceptions of the hotel managers, mean and standard deviation of biometric technology perception statements was calculated (See Table 5). The Cronbach's alpha score was calculated to measure the reliability of this scale as it was used for the first time in this study and the items were created from the literature. The Cronbach's

alpha was .83, suggesting that the scale is reliable based on the suggested thresholds by Hair et al. (1998). As presented in Table 5, the respondents agreed that fingerprint door locks would be more convenient than electronic key-based door locks (M=3.64). Similarly, respondents agreed that fingerprint door lock would be more secure than keycard lock (M=3.61) and it will keep hotels more secure (M=3.52). Although not strongly, the participants agreed that those biometric technologies would result in faster service. The respondents slightly disagreed that using biometric technologies in hotels at this time is not a good idea. Similarly, they had privacy concerns over the use of biometric technology applications in hotels. This finding confirms the previous studies as biometric technologies often conflict with personal privacy issues (James et al., 2006). The tradeoff between maintaining a desired level of security while maintaining a sufficient level of privacy for an individual is a challenge that the hoteliers need to tackle.

Table 5: Biometric technology perception statements

Statement	Mean	s.d.	Mean df
A biometric fingerprint door lock will provide my customers with more personal convenience than a keycard lock.	3.64	1.13	1.28*
A biometric fingerprint door lock will keep my customers' room more secure than a keycard lock.	3.61	1.09	1.13*
A biometric technology will keep my hotel property more secure.	3.52	1.05	1.08*
Biometric technology will protect my customers from identity thefts (because fingerprints are encrypted and stored in a safe way).	3.30	1.09	1.04*
Biometric technologies will give my customers faster service.	3.01	0.99	0.72*
Using biometric technologies in my hotel is a good idea.	2.96	1.08	0.70*
I have no privacy concerns about using a biometric technology in my hotel.	2.74	1.26	0.84*

N=225
1=Strongly Disagree 5=Strongly Agree
* α=0.05 level

A t-test was conducted to understand if there is a significant difference in the biometric technology application perceptions between hotels that had a biometric technology application and hotels that did not. As expected, in all perception statements, the hotels that utilized a biometric technology application agreed significantly more (α=0.05 level) with the statements than the hotels that did not. Therefore, it can be claimed that if hotels are familiar with the biometric technology, they are more likely to believe that it can be beneficial for the company. Hotels that already deployed biometric technologies believed that such technologies

would protect customers from identity thefts, make the property more secure and it will be convenient for the customers. Moreover, they believed that such technologies could lead to faster service (e.g. payment via fingerprint). Hotel managers who had experience and essential knowledge about biometric technologies believed in the positive consequences of using the systems compared to managers that were unfamiliar with such technologies. This finding is consistent with Broadbent et al. (2009) as they found out that lack of familiarity with technology could be a reason for people feeling uncertain about technologies. Consistent with the study findings of Koenigsfeld, Youn, Perdue and Woods (2012), it is perhaps important to educate and train managers so they can evaluate the hotel company's technology needs and recommend appropriate technological applications.

The questionnaire also included an open-ended question to capture the opinions of hotel managers about biometric technologies. The respondents' statements were content analyzed and according to the findings from their statements, the respondents were mainly concerned about the acceptance of biometric technologies from consumers' end. For example, one respondent stated, "*I am concerned about guest acceptance of the technology*". Similarly, another respondent noted, "*The guest will have to demand in order for this to work. With a key it is simple, just give the key. I am not sure if guests will like the hotel collecting the fingerprints from them. We have a hard time getting them to give their Driver License. How to prevent the theft of the finger print data?*" Another respondent stated *"I suspect guests may have an issue, particularly in these days of increased government activity and shows like CSI. I think other technologies such as cell phone and RFID may be better accepted for hotel door lock schemes*". In a similar vein, another respondent indicated that "*As long as it is not a commonly established standard to take guests' biometric measures, it will be difficult to convince a guest and get the trust from him to leave the biometric data with the hotel*". Another theme emerged from the qualitative findings was privacy. Several respondents agreed that their guests insist on privacy. The following statement by one of the respondents can summarize this theme "*Our guests do insist on privacy, and they might find fingerprinting to be invasive.*"

A number of respondents further claimed that biometric technology would be useful for in-room safes. Therefore, this may present opportunities for in-room safe vendors. Some of the respondents highlighted the reliability of the biometric technologies: "*While the technology seems like a good idea, my main concern would be the reliability. We already deal with key issues (dead keys, dead locks).*" A number of respondents were aware of integration of biometric technologies with customer relationship marketing. For example, one of them stated that "*employees use more than guest use but with guest use could create more Customer Management Relationships…*"

Several respondents admitted that they had limited knowledge of biometric technologies, "*I would like to know more about biometric locks that are easily programmable, especially for any new construction we might take*". The respondents were familiar with biometric technologies for employee tracking, however, they were not aware of guest technologies. One respondent stated "*we use biometric technology only for attendance tracking, but using it for room security is a good idea that I would like to pursue*". Finally, a very high majority of the respondents commented about the cost of biometric technologies. Comments on this issue were similar to the following statement: "*cost to implement this technology and technical support might be more than we are willing to spend at this time*".

Conclusions and Recommendations

This study aimed to examine the type of biometric technologies adopted by hotels and the perception of hotel managers toward use of biometric technology applications in hotel companies. The findings of this study suggest that there definitely is a future in using biometric technology applications in hotels in the future. However, according to study findings neither guests nor hoteliers are fully ready for using such applications. The most frequent use of biometric technology application is fingerprint scanning. It is known that "buddy-punching" in which someone clocks a friend in for work signing in is a significant problem in the hotel industry. Biometric technology applications may help hotels save an average 2.2% of gross payroll annually by using such fingerprint terminals to clock in and out. In tight economic times, such a saving may be substantial. Biometric application vendors may propose hotels to use fingerprint devices in attendance tracking. This way, hoteliers would be introduced to the biometric technology with a solid return on investment. Subsequently, other uses of biometric technology applications can be introduced.

According to the study findings, the main reason for not using a biometric application in hotels in the unfamiliarity with the technology by hotel managers and owners. It appears that hoteliers do not have much knowledge about such applications and their potential advantages. Cost of these applications appears to be another major barrier to adoption of biometric technology applications. Vendors should provide solid case studies that show the return on investment on the use of biometric technology applications in hotels. It will help information technology managers secure funding for this investment.

Hoteliers seem to have significant privacy concerns about the use of biometric technology applications in hotels. One can claim that even though security problems exist with current technologies such as keycard locks or paying with credit cards, when a keycard or credit card is stolen, they can be replaced easily. However, when biometric information of a guest or hotel staff member is stolen, replacing it may be impossible. Unless vendors prove and convince hoteliers and guests that the biometric technology applications are 100% safe, it seems that the adoption rate may suffer for some time. The study findings also support this statement in that if hotels use a biometric technology application, the managers' perceptions towards it are more positive than managers whose hotels do not have a biometric technology application. In this regard, vendors may create a business model where they can install biometric technology applications in hotels free of charge for a limited time. This will allow the hotel managers to see the benefits first hand.

Potential uses of biometric technologies in the hotel industry are endless. For example, casinos have already adopted this system. For example, Bally's uses biometric recognition to solve business problems at the point of play. Their system passively identifies players at the game and tracks their activities; further the system is connected with customer relationship marketing and provides input for the system. Such systems can also be linked to any existing lists of excluded players, enabling instant messages to be sent to security when they enter to the property, similarly it could identify VIP guests. Another application might be validating employee identity before allowing entry to gaming devices.

Biometric technologies have also tremendous opportunities for chain hotels since once the guest checks in to the property, the system remembers guest preferences from hotel-to-hotel in locations across the world and they could open their assigned guestroom with only one time registration to the system. Furthermore, as Wang (2012) suggests biometrics

technologies provide solutions to forgotten and stolen password issues. Hotel employees can use biometric technologies to reduce the time spent on password-related problems.

The study findings suggest that hotel managers still have limited knowledge about biometric technologies. However, it is also found that the hoteliers that adopt such technologies are aware that biometric technology applications can play a role in their operations and investments into this area will bring potential benefits. Biometrics in the US lodging industry is still in the early stage as only the minority of hotels have adopted biometric technologies. Continued privacy concerns, unfamiliarity with the technology, limited need, and the high installment costs seem evident for slow adoption.

There is potential for biometric technology usage in other hospitality industry segments. For instance, airlines are sensitive to physical access because of security concerns. Thus, biometrics can be used in access control to provide more security and quicken the check-in processes (Wang, 2012). Aviation transportation in the USA has been using biometric technologies to verify and authenticate the identities of both passengers and employees. The Federal Aviation Administration (FAA), the Department of Homeland Security (DHS), and the Transportation Security Administration (TSA) have been investigating the use of biometrics for security, which includes access control to secure areas of an airport and identifying travelers, control of people moving into or out of protected areas such as physical buildings and information systems (Wang, 2012). Furthermore, restaurants can benefit from biometric technologies. Many point-of-sale systems are integrated with fingerprint scanners for user sign-in and out. Such method eliminates the need for employees to carry the magnetic swipe cards and remember a password.

Like any other study, this study has some limitations. This study employed the members of American Hotel and Lodging Association that had email addresses. This limitation may have resulted that some members that did not have email addresses were excluded. Future studies can examine the reasons for not accepting biometric technologies in hotels, for example possible studies might use Technology Acceptance Model to understand the roles of perceived ease of use and perceived usefulness on adopting biometric technologies. This research should open doors for future research. First, future studies are advised to develop theoretical models and test them empirically. TAM would be a suitable model to test biometric technology adoption in the lodging industry. Second, future studies should investigate the biometric technology adoption from the guests' point of view. Future research should consider potential safety/security strategies, and ethical aspects surrounding information securitization of biometric technologies in the lodging industry. Finally, future studies may utilize semi-structured interviews and Delphi method (Paraskevas & Saunders, 2012; Sobaih, Ritchie, & Jones, 2012) to collect data from hotel managers and guests to solicit their opinions about utilizing such technologies in hotel companies.

References

Adams, B. (2002). Hotels slow to embrace biometric security. *Hotel & Motel Management, 217*(8), 46 - 54.

Adler, A. (2008). Biometric systems security. In A. K. Jain, P. Flynn, & A. A. Ross (Eds.), *Handbook of biometrics* (pp. 381-402). New York, NY: Springer.

Aronson, M (2007). Effective use of Technology is Key to Success. Retrieved on January 15, 2010. from: *http://www.hotelworldnetwork.com/meeting-tools/effective-use-technology-key-success*.

Berezina, K. Cobanoglu, C., Miller, B., & Kwansa, F. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. International Journal of Contemporary Hospitality Management, 24 (7), 991 – 1010.

Barrier, M. (2001). Unmasking hotel fraud. Internal Auditor, 58(2), 26-32.

Bilgihan, A., Beldona, S., & Cobanoglu, C. (2009). The Adoption of Fingerprint Payment Technology Mechanisms at the Customer End. Paper presented at the Information and Communication Technologies in Tourism 2009: Proceedings of the International Conference in Amsterdam, The Netherlands, 2009.

Bilgihan, A. Okumus, F. Nusair, K., & Kwun, D. (2011). Information Technology Applications and Competitive Advantage in Hotel Companies, Journal of Hospitality and Tourism Technology, 2 (2), 139-153.

Blank, C. (2006). Is Biometric Technology For You? Hotel and Motel Management. 221 (14) 130-131

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., & Senior, A.W. (2004). Guide to biometrics. New York: Springer-Verlag.

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. Technology and Society Magazine, IEEE, 23(1), 9-19.

Broadbent, E., Stafford, R., & MacDonald, B. (2009). Acceptance of healthcare robots for the older population: Review and future directions. International Journal of Social Robotics, 1(4), 319-330.

Crick, A. & Spencer, A. (2011). Hospitality quality: new directions and new challenges, International Journal of Contemporary Hospitality Management, 23 (4), 463 – 478.

Davidson, M., McPhail, R., & Barry, S. (2011). Hospitality HRM: past, present and the future", International Journal of Contemporary Hospitality Management, 23 (4), pp. 498 – 516.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management Science, 35(8), 982-1003.

Donaghy, K., McMahon-Beattie, U., & McDowell, D. (1997). Implementing yield management: Lessons from the hotel sector. International Journal of Contemporary Hospitality Management, 9(2), 50-54.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate Data Analysis. (5ᵗʰ Ed.). Upple Saddle River, New Jersey: Prentice Hall.

Harris, A.J., & Yen, D.C. (2002). Biometric authentication: Assuring access to information. Information Management & Computer Security, 10(1), 12-19.

Harrington, R. & Ottenbacher, M. (2011). Strategic management: An analysis of its representation and focus in recent hospitality research", International Journal of Contemporary Hospitality Management, Vol. 23(4), pp. 439 – 462.

Heracleous, L., & Wirtz, J. (2006). Biometrics: the next frontier in service excellence, productivity and security in the service sector. Managing Service Quality, 16(1), 12-22.

Hotel Online (August, 2003). Assessing Hotel Security HOTEL Asia Pacific Magazine/Pertlink Re-Issue Hotel Security Checklist, retrieved on: January 14, 2010 from: http://www.hotel-online.com/News/PR2003_3rd/Aug03_HotelSecurity.html

Ip, C., Leung, R. & Law, R. (2011). Progress and development of information and communication technologies in hospitality, International Journal of Contemporary Hospitality Management, 23(4), 533 – 551.

Ives, R. W., Du, Y., Etter, D. M., & Welch, T. B. (2005). A multidisciplinary approach to biometrics. IEEE Transactions on Education, 48(3), 462-471.

Jackson, L. A. (2009). Biometric technology: the future of identity assurance and authentication in the lodging industry. International Journal of Contemporary Hospitality Management, 21(7), 892-905.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. Circuits and Systems for Video Technology, IEEE Transactions, 14(1), 4-20.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. Journal of Organizational and End User Computing (JOEUC), 18(3), 1-24.

Jones, P., Williams, P., Hillier, D., & Comfort, D. (2007). Biometrics in retailing. International Journal of Retail and Distribution Management, 35(3), 217-222.

Kleist, V.F., Riley, R.A., & Pearson, T.A. (2005). Evaluating biometrics as internal control solutions to organizational risk. Journal of American Academy of Business, 6(2), 339-343.

Kim, J., Brewer, P. & Bernhard, B. (2008). Hostel Customer Perception of Biometric Door Locks: Convenience and Security Factors. Journal of Hospitality & Leisure marketing, 17 (1-2), 162-183.

Koenigsfeld, J., Youn, H., Perdue, J. & Woods, R. (2012). Revised competencies for private club managers. International Journal of Contemporary Hospitality Management, 24 (7), 1066-1087.

Krause, N., Scherzer, T., & Rugulies, R. (2005). Physical workload, work intensification, and prevalence of pain in low wage workers: results from a participatory research project with hotel room cleaners in Las Vegas. American Journal of Industrial Medicine, 48(5), 326-337.

Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27-32.

McIntosh, D. B. (2009). Biometrics–a fad or the future? Biometric Technology Today, 17(5), 9-11.

Morosan, C. (2012). Theoretical and Empirical Considerations of Guests' Perceptions of Biometric Systems in Hotels. Journal of Hospitality & Tourism Research, 36(1), 52-84.

Murphy, H. C. & Rottet, D. (2009). An Exploration of the Key Hotel Processes Implicated in Biometric Adaption. International Journal of Contemporary Hospitality Management, 21(2), 201-212.

Nebel, E. C., Lee, J. S., & Vidakovic, B. (1995). Hotel general manager career paths in the United States. International Journal of Hospitality Management, 14(3-4), 245-260.

Okumus, F. (2013). Knowledge Management through Information Technology in Hospitality Organizations. Journal of Hospitality and Tourism Technology, 4 (1), 64-80.

Oliva, R (2003). Scratching the Surface: Slowly but Surely, Hotels Implement New Security Technology. Hotels, Retrieved on January 18, 2010, from: http://www.hotelsmag.com/article/364465-Scratching_The_Surface.php

Osborn, A. (2005). Biometrics history -- Looking at Biometric Technologies from the Past to the Present, Retrieved on January 12, 2010, from: **http://www.video-surveillance-guide.com/biometrics-history.htm**

Paraskevas, A., & Saunders, M. (2012). Beyond consensus: an alternative use of Delphi enquiry in hospitality research, International Journal of Contemporary Hospitality Management, 24 (6), 907 – 924.

Parton, H. (2007). Guard Duty. HotelManagement-Network.com. Retrieved February 13, 2013 from: http://www.hotelmanagement-network.com/features/feature1019/

Polemi, D. (1997). Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable. Reported prepared for the European Commission DG

XIIIC, 4.

Rinehart, G. (2000). Biometric payment: The new age of currency. Hospitality Upgrade, pp. 114- 116.

Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (2000). Biometric identification through hand geometry measurements. Pattern Analysis and Machine Intelligence, IEEE Transactions, 22(10), 1168-1171.

Simon, H. (2004). Company seeks public acceptance for iris biometrics in posh hotel. Aviation Weeks Homeland Security and Defense Report, 3(32), 4.

Singh, A. J., & Kasavana, M. L. (2005). The impact of information technology on future management of lodging operations: A Delphi study to predict key technological events in 2007 and 2027. Tourism and Hospitality Research, 6(1), 24-37.

Singhal, R., & Jain, P. (2011). Biometrics: Enhancing Security. Asian Journal of Computer Science and Information Technology, 1(3), 89-92

SecurityInfoWatch.com (2009). Study: Biometrics Gaining Acceptance among Consumers. Retrieved on January 16, 2010, from: *http://www.securityinfowatch.com/printer/1282404*

Sobaih, A., Ritchie, C., & Jones, E. (2012). Consulting the oracle?: Applications of modified Delphi technique to qualitative research in the hospitality industry, International Journal of Contemporary Hospitality Management, 24 (6), 886 – 906.

Spence, B. (2003). How Biometric Terminals can Reduce payroll Costs, Paytech, January, 2003.

Stone, A. (2012). Biometric scanners help restaurants take bite out of attendance fraud. Retrieved March 20, 2013, from http://www.bizjournals.com/columbus/print-edition/2012/02/24/biometric-scanners-help-restaurants.html?page=all

Tsai, R. C. (2007). Biometrics in the private sector: Trends and case studies. In W. S. Coats, A. Bagdasarian, T. J. Helou, & T. Lam (Eds.), The practitioner's guide to biometrics (pp. 139-146). Chicago, IL: American Bar Association.

Vijan, L. (2004). Corporate America slow to adopt biometric systems. Computer World Magazine, 38(32), 32-34.

Woodward, J.D., Orlans, N.M., & Higgins, P.T. (2003). Biometrics. New York: McGraw-Hill/Osborne.

Yoo, M. Lee, M., & Bai, B. (2011), Hospitality marketing research from 2000 to 2009: Topics, methods, and trends, International Journal of Contemporary Hospitality Management, 23(4), 517 – 532.