Biometric Technologies in Emergency Management: The Case of Hotels

Ahmad Rasmi AlBattat[1]*, Ahmad Puad Mat Som[2]

[1]Department of Tourism Planning, School of Housing, Building and Planning, Universiti Sains Malaysia, Penang, Malaysia, [2]Department of Tourism Planning, Sustainable Tourism Research Cluster, Universiti Sains Malaysia, Penang, Malaysia.

*Email: battat_ahmed@yahoo.com

DOI: 10.18510/ijthr.2014.115

Article History: *Received on 15th Sep 2014, Revised on 18th Oct 2014, Published on 25th Nov 2014*

Abstract

The hospitality industry is susceptible to emergencies and disasters and must be managed in order to mitigate potential impacts. This paper explores biometric technology and their potential usage in the hospitality industry. This paper reviews the viable biometric technologies and further with a discussion of their applications in the hospitality industry to enhance security and increase operational efficiency. Tracking employees and hotel guests may bolster emergency management response time by locating individuals, ensuring secure areas, and aiding individuals in evacuation procedures. In this study, various scenarios in which biometrics can be used are explored. The paper concludes with a discussion on the urgent need for biometric technologies to be installed the hospitality industry to reduce errors and eliminate potential terrorist activities.

Keywords

Hotel, Biometric technology, Emergency management, Mitigation, Planning.

Introduction

Hotel emergencies and safety procedures have become a highly topical issue, especially in the aftermath of several disasters affected hospitality industry in recent decades. Biometric technologies gained high acceptance and recognition through Hollywood blockbuster films, and then the increase of security threats gave this technology widely potential acceptance in science and other research scholars. Meyersa and Millsb (2007) asserted that the service industry could be enhanced by using biometric technologies to improve safety. Installing biometrics in the service industry can reduce the cost, likelihood of guest theft, terrorist activities, and improve operational efficiency and security. Biometric technologies may utilize the safety measurements to identify and verify the human`s identity (Find Biometrics, 2007). The rapidly expanding industry of biometrics changes security from physical access, such as door locks, to security formats such as computer passwords and manual screenings to prevent terrorists and criminals access. Several types of biometrics are now available, and many could be used in the service industry, such as in hotels and aviations. The Economist (2003) mentioned seven biometric technologies in the market that could be used in the service industry (Figure 1). Reports also mentioned that biometrics has experienced exponential growth, since September 11, 2001 until 2007 (Figure 2).

Many companies use biometric technology in addition to standard password systems as a layer of additional identity verification. Some biometrics systems are expensive and sacrifice some measure of personal privacy. To verify personal face, finger, or iris, hotels must have personal data in files in the verification systems, which can be stolen or made public. However, biometric technologies are becoming increasingly popular both as a standalone security system or added security. This study explores four biometric technologies: Face recognition, fingerprint recognition, hand geometry, and iris scan. An overview of these four technologies and potential usage in the hotel industry will be discussed.

Emergency, Disaster in Hospitality, and Tourism

In the last few decades, the tourism industry globally, particularly Southeast Asia, has been subjected to several disasters and emergencies that have caused problems with arrivals and revenue, loss of lives, and multiple challenges to the governments, public, and private sectors (Prideaux, 2004). Emergency situations have been categorized into natural and man-made disasters. Richardson (1993) asserted that man-made disasters are known as socio-technical disasters and have four types: Technical disasters, transport failure, stadia failure, and productivity failure.

Since the 1970s, scholars from a variety of areas adopted different approaches, statistical data, and case studies to determine best practices and management styles when dealing with emergencies (Faulkner, 2001). Specific research was conducted in the tourism industry, including aviation (Henderson, 2008),

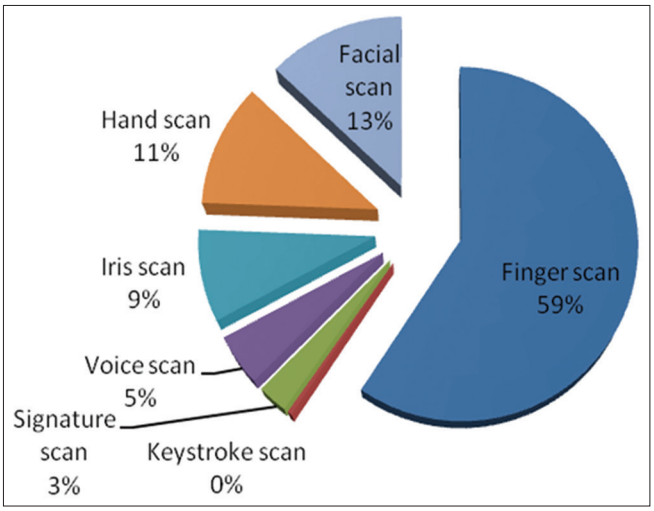

Figure 1: Biometric market share percentage. Source: Economist, 2003

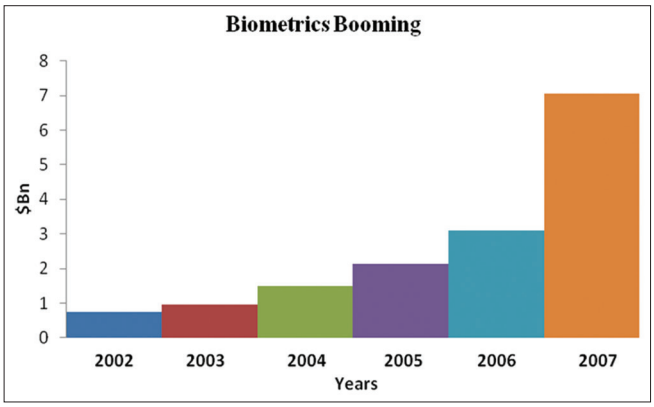

Figure 2: Biometric booming 2002-2007. Source: Economist, 2003

political unrest (Lehrman, 1986), terrorist activities in particular destinations such as Northern Ireland (Witt and Moore, 1992) and Egypt (Aziz, 1995). The Asian financial crisis (Prideaux, 1999) and the event of September 11 generated further studies in all research fields (Pizam, 2002). The range of topics confirms that the tourism industry faces great vulnerability to disasters and emergencies (Santana, 2004). In their book, Faulkner et al. (1998) conclude that tourism is marked by dynamic chaos and turbulence, extracting Faulkner and Russell (1997) who apply the chaos and complexity theories in tourism. They argue that the dynamism of tourism requires a new paradigm, which can accommodate the constant change. Change is evinced in natural and man-made disasters that influence the tourism industry, alongside shifts in demands and product innovation in supply. The matter that leads emphasize the importance of emergency management and preparedness, and devices used to mitigate the effect of any hazard event (Henderson, 2003). This led the researchers to search for why since two decades hotels have not used biometric technology when dealing with guests. Experts argue that it is impossible to use when book the rooms from the websites. However, it could be used in the hotels and resorts, especially when the guest arrived and check-in procedures.

Biometric Technologies: The Current Usage in Tourism and Hospitality

Facial recognition

Facial recognition is accomplished using cameras to capture a person's image and compare with a stored template. Templates are data used to represent the measurements and compare subsequent images (National Information Assurance Partnership, 2003). By using these template systems that include the top of the lip, the bottom of the nose, and the distance between the eyes. This method used commercially since 1990's and gained more attention after September 11 terrorist attacks (National Center for State Courts, 2003). In hospitality Spangler (2004) mentioned that facial recognition was used by the Borgata Hotel Casino in the United States to identify card cheaters and unwanted guests, they used more than 2,000 cameras to compare images of guests with over 1,500 databases (Figure 3).

Fingerprint recognition

The fingerprint is the most commonly known biometric (Jarvis, n.d.). Fingerprint recognition gained popularity based on the assumption that fingerprints are unique, static, and easy to use. The propagation of fingerprint recognition helped in solving

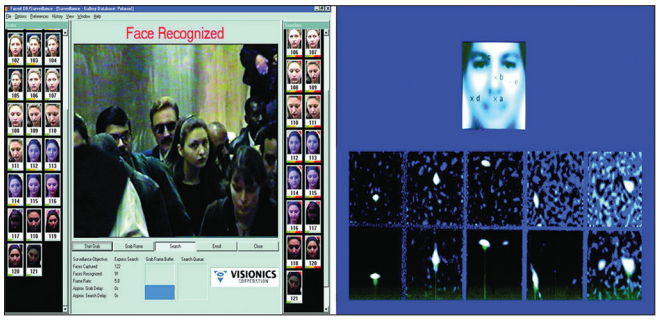

Figure 3: Facial recognition system software. Source: Kroeker, 2002

and providing evidence for criminal cases around the world. The Biometric Institute (n.d.) defined it as "the use of the ridges and valleys found on the surface tips of a human finger to identify an individual." By placing a finger on a scanning device, that acquires an image of the fingerprint, it is then stored for future use. The Waldorf Towers Hotel in New York City installed a fingerprint recognition system for in-room safes in November 2003 from Elsafe, the global market leader in in-room security. Hospitality Upgrade (2003) explained the goal of the installation by providing additional guest security and loss prevention efforts. By placing the finger on the scanner A LED light would flash to indicate successful enrollment and the safe can then be used (ElSafe, n.d.) (Figure 4).

Hand and two-finger geometry

Hand and two-finger geometry are used primarily to verify utilizing measurements such as three dimensional size, shape, and angles in conjunction with a pin number for a one-to-one match. This geometry is unique in that the person presents his pin number or data card with squeezing the pins (Figure 5). Since 1995, Disney World theme parks, in Orlando, FL, United States utilized this solution (Davis, 1997) in order to increase the security of annual membership passes for individuals over the age of 10 (Levin, 2001). Hence, the need arises to use a durable, reliable, and quick solution like finger geometry system. Wayman (2000) claimed that since the implementation, Disney has had over 20 million transactions.

Iris recognition

The National Center for State Courts (N.D.) theorized in 1930's that iris patterns were unique and defined it as recognition use feature patterns of the iris for recognition. By capturing an image of the iris, that image is processed that image using the system, which takes a hundred of points of the iris and compares it to the database for identification. The system is very easy to use; it involves looking into the camera for a few seconds while the system captures the iris. The iris recognition system did not require any additional identification cards. The system is reliable and fast enough to do one-to-many match with a high probability, it can ever detect colored contacts, eye surgery, and monitors pupil movement to enhance security. A summary of the pros and cons of the discussed biometrics is presented in Table 1.

Discussion

The theories of disaster management assume that events move through several stages of actions until they reach the final

Table 1: Summary of biometric technologies

Biometric	Pros	Cons
Face recognition	• Can be used covertly • Easy to use • Dual purpose – can be used as a security camera	• Environmental conditions can greatly affect matching • Personal features can result in high failure rates
Fingerprint	• Easy, fast, reliable, and well known • One-to-many matching • Long life span • Suitable for many environments	• Degradation of fingerprint: elderly, manual labor, drying of hand, cut • Requires physical interaction • Not suitable for all environments
Hand geometry	• Minimal privacy concerns • Fast and reliable • Hard to produce	• Not static • Awkward and obtrusive • One to one matching
Iris	• Easy, fast, and reliable • One-to-many matching • Multi-purpose • Longest life spam	• Environment attributes may cause the camera to not acquire the image

Source: Meyersa and Millsb, 2007

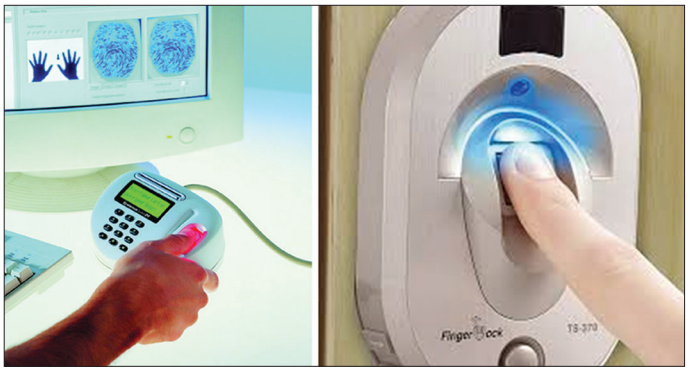

Figure 4: Facial recognition system software. Source: Kroeker, 2002

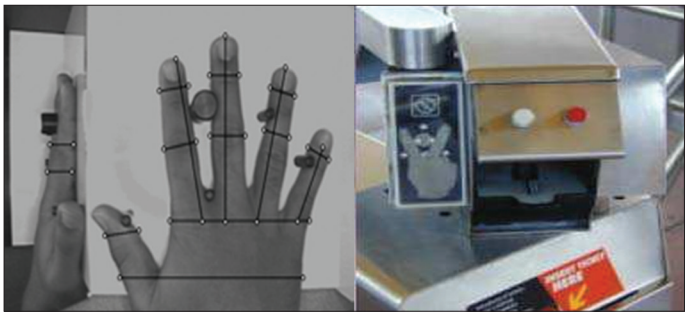

Figure 5: Hand and two finger geometry measurements. Source: Ross et al., n.d

disaster. Turner (1976) identified seven stages and four stages by Fink (1986). These stages can be summarized into three broad stages of pre-disaster, disaster, and post-disaster. Faulkner (2001) presented a tourism disaster management framework, presenting elements related to pre-event, prodormal, emergency, intermediate, long term/recovery, and resolution stages. The conceptualization would be appropriate to hospitality studies after some modifications to the process proposed by Henderson (2003) mentioned in Figure 6.

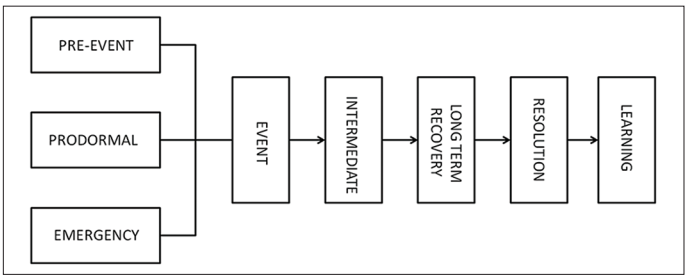

Figure 6: Stages in hotel disaster management. Adopted from Henderson, 2003

A pre-event stage, when hotels can implement preventive measures to ensure maximum safety and security, should be the ongoing standard practices in the hospitality industry. Biometric technologies can increase emergency preparedness and security, and reduce the chance terrorists have of using false names and stolen passports to check-in the hotels and pursue their terrorist activities. Guests have to spend some time in the reception area to complete the check-in procedures and sign some forms. This is enough time to check all guests using biometric technologies. Hotels may use face recognition, fingerprints, and iris recognition to identify the passport holder who wants to check-in, which give more accurate, reliable, and perform one-to-many matches. Governments should use these biometric technologies when issuing passports and uploading them onto the Interpol network, and in connecting it with all related organizations, hotel companies, and airports.

Cassedy (1991) clarified that tourism and hospitality organizations have been already displayed their plans and prepared themselves for disasters and emergencies; while, aviation's must plan for emergencies and install necessary technologies to secure passengers and crew (IATA, 1998). Experts in disaster management, stress the necessity of establishing a task force to recognize potential terrorist zones, devise preventive measures, and formulate copying policies when dealing with disasters. Biometric technology may be the wave of future security to hospitality and tourism companies. Furthermore, biometric technologies and its usage may exceed the experts' imagination.

Considering all scenarios, as a guest in a hotel or resort upon arrival you check-in by providing you essential information and

placing your finger on a scanner that capture your fingerprint while a camera captures your facial image and iris pattern. The hotel employee informs you that the only key you required to use the room and hotel facilities is your finger and iris. After check-in, guest may proceed to the elevator using his finger to access the floor where his room located. The room door is equipped with iris scanner that captures his iris and identifies that he is the same user for the room the matter will allow him to open the door. After viewing the room, guest may decide to park his rented car by placing his finger on the scanner to open the parking gate, which allows him to park his car without the need for a paper ticket. After having some rest guest decide to use the business center to check his mails, he can simply access the computer using his registered fingerprint. In the evening, guest may decide to use the gym facilities and have access by his iris. On the way back to his room, guest may but soft drink from vending machine using his iris.

The application of biometrics in the hotel and tourism is indeed viable. Biometric technologies have the potential opportunity to enhance safety and security and increase efficiency. With regards to fingerprint, face recognition, and iris recognition, may provide a good opportunity to assist local and federal agencies to prevent crime and terrorism (Chin, 2003). For example, the federal government related agencies may send biometric data of terrorists to the hotel and tourism agencies to add to database that will "red flag" the terrorist if they attempt to check-in to the hotel or resort. In addition, loge created by biometric recognition systems will help assist with tracking and reducing theft by employees and guests, as well as misusage of a hotel property (Tinari, 2003). The tracking of guests and employees may help emergency management response time by locating individuals on the premises and ensuring areas are secured and clear. For instance, in the case of fire emergency it will be easier to locate individuals aiding in evacuation procedures.

Biometric technologies may improve information technology (IT) security while reducing IT costs. Biometric technologies may reduce cyber-crimes using hotel computers, by having unique guest accounts rather than anonymous access. Furthermore, the employees and guest biometrics would become the password, eliminating the need for changing passwords. This may improve operational efficiency and increase security. Housekeeping may be more efficient by knowing the guest entry and exit real time, and then show the vacant rooms by using portable devices to update the room status. Record keeping of employees can be tied into the biometric system to eliminate redundant systems, increasing the security and reliability of employee time cards. Biometric technologies may improve competitive advantage by offering distinguishable services, thereby increasing guest loyalty and satisfaction, as well as attracting new guests.

Conclusion

Hotel emergencies and safety procedures have become a highly topical issue in recent years; biometric technologies gained high acceptance and consideration with the growth of security threats spread to technology, science, and other research scholars. Several types of biometrics are now available on the market, and many could be used in the service industry such as hotels and resorts. Man-made disasters affected the hotel industry known as socio-technical disasters that can occur in four types: Technical disasters, transport failure, stadia failure, and productivity failure. As mentioned by many scholars, disaster management can be categorized into three major stages: Pre-disaster, during disaster, and post-disaster. Hotels may implement preventive measures to ensure maximum safety and security. Biometric technologies may be used as the ongoing, standard practices in the hospitality industry to increase the preparedness and security, reducing the chance of terrorists using fake passports to check-in and pursue their terrorist activities. Governments may use biometrics when issuing passports and upload it on the Interpol network, and then connect it with all related organizations, hotels, tourism companies, and airlines.

Further research needs to be conducted on the impact of biometrics in hotel and tourism industry. Hospitality organizations may have a logical approach for implementing biometric technologies to improve service quality, customer relation, and employee efficiency. Further, hospitality organizations should be aware of guest's privacy, attitude toward, and trust factors that may surround the use of biometric technologies. Privacy may be an obstacle for organizations to overcome, particularly since this technology is not widely used in customer markets.

Acknowledgments

The authors would like to extend their appreciation to the Universiti Sains Malaysia (USM) for the Research University Grant under the Sustainable Tourism Research Cluster (STRC) entitled "Tourism Planning" [Grant No. 1001/PTS/8660013], and for USM Fellowship Scheme which made this study possible.

References

[1] *Aziz, H. (1995). Understanding attacks on tourists in Egypt. Tourism Management, 16(2), 91-95.*

[2] *Biometric Institute. (N.D). Working Definitions. Available from: http://www.biometricsinstitute.org/pages/about-biometrics.html. Retrieved 27.03.2014.*

[3] *Cassedy, K. (1991). Crisis Management Planning in the Travel and Tourism Industry: A Study of Three Destination Cases and a Crisis Management Planning Manual. San Francisco: Pacific Asia Travel Association.*

[4] *Chin, J. (2003). Lessons learned from 9/11 by NYC hotel security: A model for other cities. Hotel/Casino/Resort Security. March, 10.*

[5] *Davis, A. (1997). The body as password. Available from: http://www.wired.com/wired/archive/5.07/biometrics.html?pg=2. [Last accessed on 2014 Mar 25]*

[6] *Economist. (2003). The print edition: Prepared to be scanned. Available from: http://www.economist.com/scince/tq/displayStory.cfm?story_id=456, http://www.elsafe.com/binary?id=29450. Accessed 27.03.2014.*

[7] *ElSafe. (N.D.). Available from: http://www.elsafe.com/page?id=456, http://www.elsafe.com/binary?id=29450.*

[8] *Faulkner, B. (2001). Towards a framework for tourism disaster management. Tourism Management, 22(2), 135-147.*

[9] *Faulkner, B., Laws, E., & Moscardo, G. (1998). Embracing and Managing Change in Tourism: International Case Studies. London: Routledge.*

[10] Faulkner, B., & Russell, R. (1997). Chaos and complexity in tourism: In search of a new perspective. Pacific Tourism Review, 1(2), 93-102.

[11] Find Biometrics. (2007). Biometric Sensors and Detectors. Available from: http://www.findbiometrics.com/solutions/biometric-sensors-detectors/. Accessed 27.03.2014.

[12] Fink, S. (1986). Crisis Management: Planning for the Inevitable. New York, NY: American Management Association.

[13] Henderson, J. (2003). Communicating in a crisis: Flight SQ 006. Tourism Management, 24(3), 279-287.

[14] Henderson, J. (2008). Managing crises: UK civil aviation, BAA airports and the August 2006 terrorist threat. Tourism and Hospitality Research, 8(2), 125-136.

[15] Hospitality Upgrade. (2003). Available from: http://www.hospitalityupgrade.com/__852568890071b5b7.nsf/0/08b538906813 c0b085256c8e3e?OpenDocument& Highlight=0,biometric. [Last accessed on 2014 Mar 23].

[16] IATA. (1998). Crisis Communication Manual. Monreal: Air Transport Association.

[17] Jarvis, A. (N.D). Facial recognition, retinal iris scans, DNA, fingerprinting, brain printing, ear matching, smart cards. What's Next? Available from: http://www.forensic-evidence.com/site/ID/ID_Biometric_jarvis.html. [Last accessed on 2014 Mar 09].

[18] Kroeker, K.L. (2002). Graphics and security: Exploring visual biometrics. Computer Graphics and Applications, IEEE, 22(4), 16-21.

[19] Lehrman, C.K. (1986). When fact and fantasy collide crisis management in the travel industry. Public Relations Journal, 42(4), 25-28.

[20] Levin, G. (2001). Real World, Most Demanding Biometric System Usage. Paper presented at the Biometric Consortium.

[21] Meyersa, M., & Millsb, J.E. (2007). Are biometric technologies the wave of the future in tourism and hospitality? CERIAS Tech Report 2005-07. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086.

[22] National Center for State Courts. (2003). Biometric Facial Recognition. Available from: http://www.ctl.ncsc.dni.us/biomet%20web/bmfacial.html. Accessed 27.03.2014.

[23] National Center for State Courts. (N.D.). Available from: http://www.ctl.ncsc.dni.us/biomet%20web/BMFacial.html, http://www.ctl.ncsc.dni.us/biomet%20web/BMIris.html. Retrieved 28.03.2014.

[24] National Information Assurance Partnership. (2003). U.S. Government Approved Protection Profile - U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0. pp. 15. Available from: https://www.niap-ccevs.org/pp/PP_BVM_MR_v1.0/. Accessed 27.03.2014.

[25] Pizam, A. (2002). Tourism and terrorism. International Journal of Hospitality Management, 21, 1-3.

[26] Prideaux, B. (1999). Tourism perspectives of the Asian financial crisis: Lessons for the future. Current Issues in Tourism, 2(4), 279-293.

[27] Prideaux, B. (2004). The need to use disaster planning frameworks to respond to major tourism disasters. Journal of Travel and Tourism Marketing, 15(4), 281-298.

[28] Richardson, B. (1993). Why we need to teach crisis management and to use case studies to do it. Management Learning, 24(2), 138-148.

[29] Ross, A., Jain, A., & Pankanti, S. (N.D.). Capturing hand geometry and extracting features. Available from: http://www.biometrics.ese.msu.edu/hand_proto.html. [Last accessed on 2014 Apr 17].

[30] Santana, G. (2004). Crisis management and tourism. Journal of Travel and Tourism Marketing, 15(4), 299-321.

[31] Spangler, T. (Producer). (2004) Face Invaders, Ziff Media, pp.3, access date 27 March 2014.

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

[33] Turner, B.A. (1976). The organizational and interorganizational development of disasters. Administrative Science Quarterly, 21(3), 378-397.

[34] Wayman, J. (2000). Available from: http://www.biomet.ch/aboutus.htm. [Last accessed on 2014 Mar 07]

[35] Witt, S.F., & Moore, S.A. (1992). Promoting tourism in the face of terrorism: The role of special events in Northern Ireland. Journal of International Consumer Marketing, 4(3), 63-75.

