Mérnöki Szimpózium a Bánkiban
(ESB 2020)
http://bgk.uni-obuda.hu/esb/2020

Risk management of biometric systems at international airports

[1] Alshamaileh Lafee, [2]Kovacs Tibor

[1]*Doctoral School on Safety and Security Sciences, Budapest, Hungary, lafee.alshamaileh@phd.uni-obuda.hu*
[2]*Institute of Safety and Security Donat Banki Faculty, Budapest, Hungary, kovacs.tibor@bgk.uni-obuda.hu*

Abstract

Either biometric identification refers to the recognition of the figure according to the descriptions. Physically or interactively, biometrics came to change the idea of the personal guarantee from what we own and memorize to what we look like. This paper includes a survey over biometric techniques, tools used in many organizations and facilities generally, and aviation environment specifically. The survey argues the efficiency of biometric tools that we use daily. The survey also seeking for the audiences' opinions about biometric security and its ability to expose theft attacks. The main aim of this paper is to exam the security and efficiency at airports by analyzing the results of the survey to give better understanding to the struggles travelers must face from the moment they enter the airport until they reach to the airplane gate

Keywords: biometrics; security system; airport; risk management; biological; pattern recognition

1 Introduction

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words bio meaning life and metric meaning to measure [1].

Recently, the applications of biometric have started to move to real world applications after many years of developing in the research labs. .Examples of this movement toward using biometric identity in real world applications are the big number of fingerprint sensors and the rapidly increasing interest in iris identification and face recognition as a technology that can be used in access control. Biometric applications are the main block in the developing of security applications in two main fields: the first one is related of protection of critical infrastructure. Surveillance systems and computer vision are the selected technologies to be used in this field. The second one is the Automatic Border Crossing (ABC) systems. Biometric technology is used here to replace police inspection of passports. Facial and fingerprint verification are the main data to be considered in this systems. Using cameras in critical infrastructure like airport is common in both fields to perform face identification. Facial biometry gives the possibility to monitor the object without its awareness, and that is the main advantage of using it over iris identification or fingerprint [2].

2 Risk management

The term of risk management appeared in the ’50s of the last century to describe the effectiveness of acquiring insurance. Focusing on biometric identification the paper proposes risk management of biometric systems in airports. Risk management is directed to avoid adverse situations and minimize the loss of goods. Nowadays the risk is defined as the neutral or negative consequences of events. Sometimes it is defined as positive and negative consequence. Those events can be divided as chance (to get profit and utility) and risk (to get damage and loss). These are called dual events [3].

The recent reports of network security breaches and identity thefts further affirm the fact that a strong authentication method is in the need of nowadays. This has put the focus on biometric security, as it is the only effective way to prove an individual’s identity. Biometric traits are inherent and unique to each individual and comprise physical and behavioral characteristics such as fingerprints, face, iris, voice etc. Therefore, biometric security systems can verify an individual’s identity with utmost accuracy and reliability since biometric traits are part of the individual’s being [3].

3 Biometric systems: theory and practice

Biometric authentication is the process that is used to identify oneself through one’s behavior, anatomy, physiology (for example, through fingerprint or iris), or even vocal patterns [4], To enable future use of one’s biometric image, such image needs to be captured, encrypted and stored [5]. According to research, fingerprints form 52% of biometric systems in the whole world [6]. This popularity of fingerprint biometrics is because of the accuracy of fingerprint images [7]. An edge that the biometric authentication method has over other methods is on its requirement for the presence of the actual use for the verification process to take place [8].

It is expected that the usage of biometrics will grow rapidly in the 21st century, especially in countries such as India, South Africa, and Ghana [9]. These claims are supported by those who [7] support the idea that biometrics will be the ultimate authentication method. The growth in popularity of this technology may be attributed to its provision of a better and reliable access control compared to traditional systems. This assertion is also confirmed by those who state that biometrics improve security control and reduce fraud. Another reason for its growth could be the need to improve safety measures and curb acts of terrorism in public areas, such as airports [9]. For example, in Dubai, the airports have introduced at their border gates an automatic identification system called e-Gates. The system is used to scan facial and iris imprint to authenticate the passengers [10].

Malaysians are pioneers of biometric passports [11] (e-passports), which have curtailed the use of false travel passports in Malaysia [11]. Other use of biometric technology includes access to places, such as work or bank premises, and network resources, information protection [1].

4 Examples for some international airports where biometric technology is used

4.1 International Airport Dubai

At Dubai Airport, the passenger is registered for biometric identity inside the UAE. This system is the same system which is used across the federation’s seven emirates: Abu Dhabi, Ras al-Khaimah, Ajman, Sharjah, Dubai, Fujairah and Umm al-Quwain. That can cause another queue at the airport, so there is more point should be added to improve the experience of the passenger. However, the launching of Apple’s new Face ID solution makes registration of mass biometric at the beginning of a passenger’s journey faster than ever before.

The passengers registered into a biometric system that was separated from the main infrastructure. For this trial, they implemented the MFlow system software from Human Recognition Systems (HRS), with hardware in the form of a handheld device from Tascent, which enables the efficient capture of iris, fingerprint, and face biometrics. The data was uploaded into the Cloud, and accessed through a secure database in Dubai [10].

4.2 Heathrow Airport

At the Heathrow Airport after a four-month trial period, air travelers in the UK gave their assent to a biometric security system. The trial used iris and fingerprint scans to screen more than 3000 passengers traveling from and to Hong Kong and Dubai. The goal of this trial was to test the feasibility of the system, which would check the passenger's details against various intelligence databases and, watch lists before allowing them to embark on the flight.

Before boarding the flight, the passenger has to scan his or her passport and right fingers at the self-service kiosk. Then the passenger's biometric details will be compared and if it is validated access will be granted. The enrolment system collected two iris images, ten fingerprints and a facial scan, which digitalized, and after that, it is stored in Radio Frequency Identification Card (RFID). This card was compatible with fingerprint readers installed at the immigration barriers at Heathrow, Dubai, and Hong Kong airports [12].

4.3 Amsterdam Schiphol Airport

A trial of biometric boarding has been started at Amsterdam Airport Schiphol and KLM. This trial will enable passengers to board their flight without the need to show their passport or boarding pass. Instead, passengers board the plane using a special gate that uses the facial recognition technology.

Passengers have to register first in order to board using facial recognition. In the waiting area near the gate, For this purpose a special registration kiosk has been added. In addition, the KLM staff will be ready to offer all the possible help [13].

4.4 Hong Kong airport

In Hong Kong International Airport (HKIA), travelers can use automated e-Security Gates those depend on facial-recognition technology.

Figure 1. E-Security Gate Source: https://www.florasecurity.net/e-gate-system/

Eligible travelers can use the electronic gates to scan boarding passes and their documents. Then these documents will be verified by facial recognition technology using the gates' embedded cameras. However, this process is still done manually by the airport security staff [14].

4.5 Orlando International Airport

Greater Orlando Aviation Authority (GOAA) is the first to deploy fully the U.S. Customs & Border Protection Biometric Entry and Exit Program. At the beginning of 2018, a cooperation between SITA, GOAA and British Airways and Customs & Border Protection (CBP) started to incorporate the US biometric departure check for British Airways customers. The trial's success has prompted the airport-wide implementation of the technology.

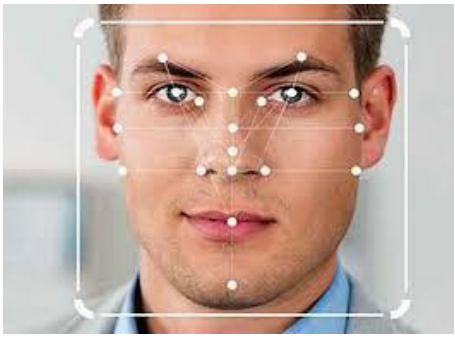

Figure 2. SITA facial recognition system Source: https://americansecuritytoday.com/orlando-airport-implement-100-biometric-exit-sita-see-videos/

Figure 3. SITA Biometric system at Orlando Airport Source: https://www.phocuswire.com/SITA-Orlando-biometric-exit

4.5.1 What is SITA system?

SITA provides IT solutions to airlines, global distribution systems (GDS), major travel management companies, online portals, railway companies and government border-management agencies. While it remains the only provider to deliver an integrated, seamless end-to-end, self-service passenger experience through solutions from check-in (passenger and baggage) to boarding to border security. 1.3 billion passengers have been checked in using SITA's common user terminal equipment (CUTE).

SITA also provides air-ground communications over an integrated network of more than 1,100 VHF data-link ground stations across more than 160 countries. It ensures 13,500 aircrafts are connected using SITA's aircraft communication services with 100 million type-B messages carried per day, 4.6 million flight plans delivered a year.

4.5.2 Entry and exit process:

The facial recognition verification process takes less than two seconds, with a 99 per cent match rate. CBP chose a facial biometrics system because it seamlessly integrates into the airport's current verification processes. By comparing the photographs of travellers with those that are already on file in Department of Homeland Security (DHS) holdings, no new data is required.

The exiting process is prior to boarding: CBP generates biometric templates of the historical images (including passport and visa photos) of travelers for a given flight and temporarily stores them in the Virtual Private Cloud. Each traveler approaches the departure gate during boarding to stand for a photo, which is captured by a camera operated by airlines/airport authorities.

The matching service verifies the traveler's identity by comparing the best photo taken prior to boarding to the historical images in the CBP database. Once verified, the passenger can board.

British Airways is said to have boarded flights of almost 240 passengers in around 15 minutes. The technology means passengers just need to look at the camera, no need to present boarding passes or passports at the gate. The system makes passenger boarding quicker and easier, while it also incorporates the new secure biometric exit checks [15]

4.6 Shannon Airport

Shannon Airport in Ireland has deployed biometric facial recognition technology to speed up its security screening process. Shannon Airport, which is operated by Shannon Airport Authority, is located on the west coast of Ireland 24km north of Limerick city. Last year, more than 1.75 million passengers passed through the airport.

Using the facial recognition technology, the security personnel at the airport verify passengers by matching them to the documents they are presenting [16]

4.7 Ottawa Airport

To enter Canada through the Ottawa International Airport, travelers will use biometric kiosks. Instead of the paper customs forms those were used previously, the kiosks will be used to process new arrivals to the country. After disembarking, travelers will use the kiosks in order to enter their personal details, and then the kiosks will scan their faces and compare the images against those in their passports. Nowadays much of the process can be done on the plane by using a mobile app, proceeding to upload the data to the kiosks upon arrival [17]

4.8 Atlanta airport

In Atlanta's Hartsfield-Jackson International Airport, Delta Air Lines launched what it called America's first "biometric terminal". This technology was initially used at boarding gates. On Nov 29, 2018, it opened the nation's first curb-to-gate biometric terminal, which is expected to improve aviation security and keep moving travelers faster by taking only 2 seconds for screening. This program uses facial recognition technology in order to check-in pass through board flights and security without having to scan boarding documents or a passport in all of the airport's international terminals. This camera-based system compares scans of travelers' faces to a database of verified ID photos curated by US Customs and Border Protection (CBP) with a 98% success rate. For the busiest airport in the world, like Atlanta, it saves 9 minutes for the boarding process, which the time that the passengers will not be spending in lines in waiting to board the aircraft. Besides, to saving time, it makes airports and air travel safer in an era when aviation systems are targeted often by criminals and terrorists. [18]

5 Results

We can see from these examples that facial recognition is the most biometric system and it is used in many airports, and some cases it can be used along with fingerprint and iris, that we summarized in this table:

In addition, we can notice that iris is not that common and usually it is not used alone. As it is shown in table only Dubai International Airport is used the all three biometric systems together.

Table 1. Comparing the used biometric systems between different airports

Airport	Facial recognition	Fingerprint	Iris
International Airport Dubai	Used	Used	Used
Heathrow Airport	Unused	Used	Used
Amsterdam Schiphol Airport	Used	Unused	Unused
Hong Kong airport	Used	Unused	Unused
Orlando International Airport	Used	Unused	Unused
Ireland's Shannon Airport	Used	Unused	Unused
Ottawa Airport	Used	Unused	Unused
Atlanta Airport	Used	Unused	Unused

Source: Author own edit

6 Conclusion

The need for security is something that nowadays matters to all of us in the different fields and environments in which we are involved on a daily basis. This is possible thanks to the use of a biometric identifier for each passenger whose information is stored in a private and secure database and that will allow them to access all airport services and even pay in the stores attached automatically to their profiles. By digitizing this information, trends and behaviors of users can be analyzed to improve their future experience.

Airport operators and airlines are adding biometrics to boarding passes or frequent-flier cards to improve security or streamline the traveling process. Most countries are starting to include biometric data (usually digital photographs and fingerprints) in passports and identity cards. It is likely that, soon, every traveler will encounter biometric systems at every stage of travel. If this happens, such systems must not only support their stated security aims, but travelers must be able to interact with them and find the user experience acceptable.

7 References

[1] Riley, C., Buckner, K., Johnson, G., & Benyon, D. (2009). Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & SOCIETY, 24(3), 295–306. https://doi.org/10.1007/s00146-009-0218-1

[2] IEEE statistical signal processing workshop (SSP12). (2011). IEEE Transactions on Multimedia, 13(5), 1180. https://doi.org/10.1109/tmm.2011.2167469

[3] IEEE Transactions on Control Systems Technology publication information. (2004). IEEE Transactions on Control Systems Technology, 12(1), c2. https://doi.org/10.1109/tcst.2004.825379

[4] Alterman, A. (2003). ``A piece of yourself'': Ethical issues in biometric identification. Ethics and Information Technology, 5(3), 139–150. https://doi.org/10.1023/b:etin.0000006918.22060.1f

[5] Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 90–98. https://doi.org/10.1145/328236.328110

[6] Milasinovic, N. (2016). Polymers in criminalistics: Latent fingerprint detection and enhancement: From idea to practical application. Nauka, Bezbednost, Policija, 21(3), 133–148. https://doi.org/10.5937/nabepo21-11888

[7] NEC develops acoustic ear biometrics. (2016). Biometric Technology Today, 2016(4), 12. https://doi.org/10.1016/s0969-4765(16)30069-8

[8] US to get biometric exit system in 2018. (2016). Biometric Technology Today, 2016(3), 12. https://doi.org/10.1016/s0969-4765(16)30053-4

[9] Arutyunov, V. V., & Natkin, N. S. (2010). Comparative analysis of biometric systems for information protection. Scientific and Technical Information Processing, 37(2), 87–93. https://doi.org/10.3103/s0147688210020012

[10] M.K, N., & Ramayah, T. (2017). Trust in Internet Banking in Malaysia and the Moderating Influence of Perceived Effectiveness of Biometrics Technology on Perceived Privacy and Security. Journal of Management Sciences, 4(1), 3–26. https://doi.org/10.20547/jms.2014.1704101

[11] Sasse, M. A. (2007). Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems. IEEE Security & Privacy Magazine, 5(3), 78–81. https://doi.org/10.1109/msp.2007.69

[12] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20. https://doi.org/10.1109/tcsvt.2003.818349

[13] Sutrop, M., & Laas-Mikko, K. (2012). From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. Review of Policy Research, 29(1), 21–36. https://doi.org/10.1111/j.1541-1338.2011.00536.x

[14] Farrell, S. (2016). How airports can fly to self-service biometrics. Biometric Technology Today, 2016(1), 5–7. https://doi.org/10.1016/s0969-4765(16)30016-9

[15] Maguire, M. (2009). The birth of biometric security. Anthropology Today, 25(2), 9–14. https://doi.org/10.1111/j.1467-8322.2009.00654.x

[16] Canada tests biometrics and blockchain as airports worldwide extend biometric use. (2018). Biometric Technology Today, 2018(2), 11–12. https://doi.org/10.1016/s0969-4765(18)30026-2