Pregledni rad
Primljen: 19. 1. 2016.
Prihvaćen: 29. 6. 2016.

UDK: 351.754/.755:57.087.1
656.7.08
doi:10.5937/nbp1602139T

THE ROLE OF BIOMETRIC APPLICATIONS IN AIR TRANSPORT SECURITY

Smilja Teodorović[1]
Academy of Criminalistic and Police Studies, Belgrade

Summary: As the number of air passengers continues to increase worldwide, so do the security demands and challenges in the air transport industry, particularly in lieu of numerous recent terrorist attacks. One of the essential requirements in fulfilling these needs resides in the accurate and timely identification of passengers and other participants in the air transport flow. Biometrics represents identification of individuals based on their quantifiable biological characteristics in automatic pattern recognition systems and is considered one of the most reliable means for personal identification. It is, therefore, not surprising that biometric technologies have an increasing presence in the air transportation industry. The intent of this review is to familiarize readers with biometric tools aimed at establishing and maintaining high security at airports and during flight, as well as to point out promising emerging biometric applications in the field.

Keywords: biometrics, human identification, airport security.

1 Associate Professor, smilja.teodorovic@kpa.edu.rs

Introduction

Airports represent specific locations, given that they are ports of entry and exit approached with high security, but also ordinary workplaces for airport personnel and ordinary travel zones for frequent travelers.[2] Few millions of passengers pass through airports worldwide daily. For example, the world's busiest airport, Hartsfield–Jackson Atlanta International Airport in the US, handled more than 94,000,000 passengers in 2013.[3] All passengers accessing airport checkpoints and, subsequently their flights, are required to provide a valid identification document (ID). After checked in with the airline, passengers continue through security check point(s), whose intention is to ensure that passengers do not carry dangerous items (weapons, explosives, etc.) that could pose a risk to the integrity of the airport, aircraft, crew and other passengers. This is traditionally done using luggage and passenger screening machines, bomb-sniffing dogs, surveillance camera monitoring, etc.

Yet, despite these safety measures, airports and airlines have become increasingly popular terrorist targets in the past few decades, which, in addition to human fatalities, injuries, panic and psychological consequences, also cause economic damage, and sudden degradation of transportation systems, bringing to attention the issues of transportation networks reliability, emergency response, pre-attack and post-attack counter-terrorism security policies, evacuation strategies, and air traffic congestion mitigation. Furthermore, given that industry experts project 5.9 bn air travelers by 2030,[4] security challenges in the air transport industry are expected to increase.

The central concept in providing collective security to all individuals at airports, as well as protecting aircrafts and airports from unauthorized passengers, outlaws and terrorists, is identification of individuals taking part in the air transport flow. Yet, traditional means of personal identification do not provide the security level that satisfies the current demands in air transportation. Thus, past terrorist actions have increased security efforts globally and reshaped approaches towards airport and airline security, bringing in a new generation of safety measures. Contemporary security measures in large part rely on biometric human identification – human recognition based on their quantifiable *biological* characteristics.

The primary goal of this paper is to acquaint the reader with biometric human identification, innovative approaches related to the employment of biometric technologies in air transportation, as well as emerging technologies and future directions in the field.

2 L.L. Martin, Bombs, bodies, and biopolitics: securitizing the subject at the airport security checkpoint, *Social and Cultural Geography, br 1/* 2010, Abington, p. 17.
3 L. Parks, Points of Departure: The Culture of US Airport Screening, Journal of Visual Culture, br. 2/2007, London, p. 183.
4 http://www.argus-global.co.uk/how-biometrics-help-airports-reach-key-targets.

1. Biometrics 101

Biometrics represents automatic methods for human recognition based on their quantifiable biological characteristics, which can be anatomical (e.g. fingerprint, face, iris), physiological (e.g. heartbeat, brainwaves) and behavioral (e.g. voice, handwriting, gait) (Figure 1). The success of a biological characteristic as a reliable and accurate identifier has been defined by seven parameters: *universality* (trait exists in all individuals in a population), *uniqueness* (trait sufficiently differs among individuals), *permeance* (trait is sufficiently constant over time), *measurability* (trait can be collected, digitalized and further processed), *performance* (recognition accuracy), *acceptability* (agreement of individuals being recognized to present the trait) and *circumvention* (ease of trait forgery).[5] While none of the biological traits score ideally on all seven criteria, nature and requirements of a specific application will dictate the importance of each factor. For instance, if biometric identification is used to restrict access to air traffic control towers to authorized personnel only, low circumvention will have more weight compared to high acceptability in the process of choosing an appropriate biometric trait for this specific application.

Figure 1. *Examples of biometric characteristics: fingerprint, iris, keystroke dynamics, gait, face, ear, hand geometry and signature*

5 R.M. Bolle; S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Norwell, 1998.

Although biometrics is an ancient concept, as demonstrated by 31,000 year old handprints ("signature which cannot be forged") discovered in a French cave,[6] contemporary biometrics represents personal identification in *automatic* biometric systems, developed following the expansion of digital signal processing technologies in the 1960s. An automated biometric system is a pattern recognition system with computer-controlled capture, processing, storage and matching of biometric traits. During registration into a biometric system, a process known as *enrollment*, individual's biometric trait (i.e., fingerprint image) is captured and digitalized by a *sensor*, and further processed to achieve high quality image (Figure 2a). Only reproducible and unique components of a biometric trait (i.e., changes in papillary line patterns, minutiae, in a fingerprint image) are then extracted by a *feature extraction* algorithm, assigned a numerical value (binary vector) and stored as a template in a database. Biometric systems can perform in two modes: *verification* and *identification*. The first entails verification of person's identity - an individual presents themselves to a biometric system via a name, PIN, credit card number, etc., based on which reference template for claimed identity is selected from a database and compared to the presented ("live") biometric trait, known as *query* (Figure 2b). This one-to-one comparison aims to prevent multiple people to use the same identity. On the contrary, identification process begins with immediate biometric trait presentation, capture, processing, feature extraction and template generation. In such a way, query template is compared with all reference templates in an appropriate database (Figure 2c). This one-to-many comparison prevents a single person to use multiple identities.

Two biometric samples collected from the same person (e.g., voice recording) at different time points cannot be identical, due to differing circumstances during sample acquisition (e.g., landline vs. mobile phone, user's dry throat, wind, background noise), changes in a biometric characteristic of interest (e.g., hoarse voice during a cold, high-pitched voice in excitement) and varying interaction between the user and the sensor (e.g., mouth placement with respect to the phone microphone). As a result, biometric systems make two types of errors in verification mode: 1) False match error (FME), which occurs when an algorithm mistakenly classifies an imposter as an authorized user - for example, an unauthorized user is granted access to a protected transportation facility; 2) False non-match error (FNME), which occurs when an algorithm mistakenly classifies authorized user as an imposter – for instance, a passenger is not matched and has to undergo additional checks. The reduction of either of the errors occurs at an expense of the other, thus setting the threshold level is dependent on the requirements and nature of specific applications - lower FNME results in higher usability, while lower FME is a necessary for high se-

6 According to the International Biometrics & Identification Association document from 2013 "Biometrics and Identity in the Digital World".

curity applications. In the US, Transportation Security Administration (TSA) set qualification rates for FME and FNME to be <1.0%.[7]

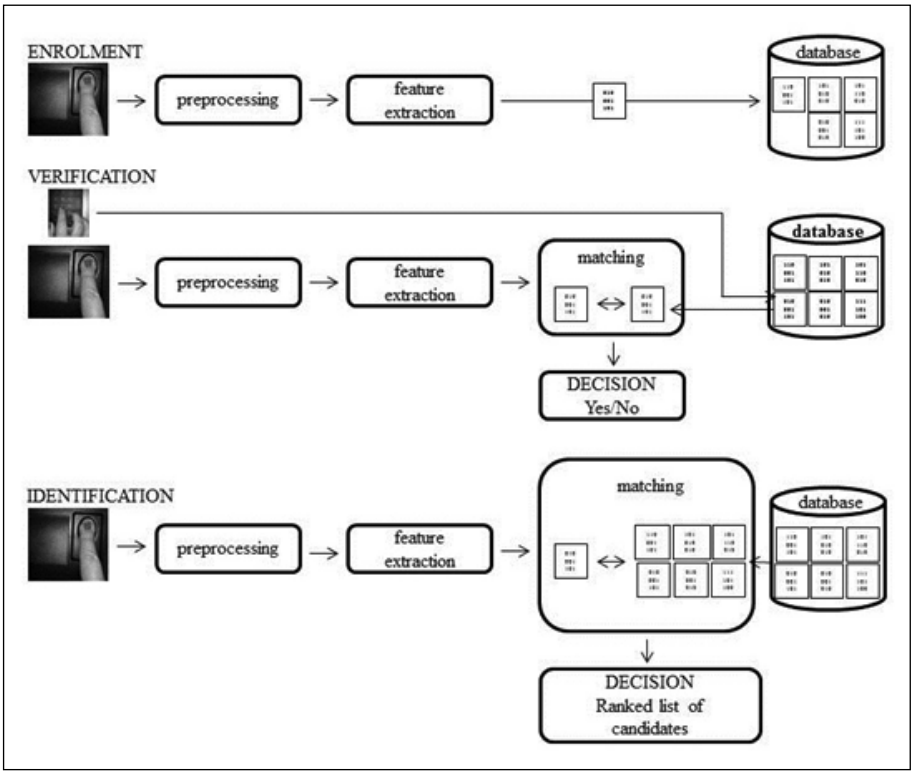

Figure 2. *Schematic representation of processes in a generic biometric system*

Additional errors can occur in biometric systems in both identification and verification modes. Failure to acquire (FTA) error represents users that are unable to provide a usable biometric sample, either because they do not have a biometric characteristic of interest (i.e., mute people) or because it cannot be measured (i.e., severe laryngitis). Failure to enroll (FTE) error occurs when feature extraction cannot occur from previously successfully acquired characteristic (limitations of the technology used). In order to enhance personal identification in biometric systems, a multimodal approach, characterized by

7 R. Lazarick, Biometric Product Qualification Program for US Airport Access Control, *International Biometrics Performance Conference*; 2010, Washington DC.

the use of two or more biometric characteristics simultaneously, has been increasingly implemented.[8, 9]

Biometric identification has found a growing niche in air transportation, as its use at airports and airlines across the globe is on the rise. This is not surprising in the context of national and international security, as it is essential for every government to identify individuals at border crossings.

2. Biometric identification approach to border management at airport

Tightened global security measures coupled with the technology advancements have contributed to a worldwide expansion of biometric passports in 2000s. International Civil Aviation Organization (ICAO) has issued Doc 9303 series on Machine Readable Travel Documents, which provide detailed technical specifications and ISO standards regarding biometric passports.[10] Implemented standards ensure interoperability between countries and passport vendors, as well as increased security. Biometric passports contain an electronic microchip coupled to an antenna, enabling contactless communication between the chip and a reading device. This chip stores data from the information page and biometric information. Three types of biometric identification systems are supported - facial recognition, fingerprint and iris.[11] Facial recognition is a mandatory feature of all biometric passports and it is based on a full frontal (facial) image, while fingerprint and iris are optional. According to ICAO, out of 101 countries which issue biometric passports, 47 use facial image as the only biometric, 51 have opted to include fingerprint recognition, while none of the countries have chosen to store iris image as a secondary biometric.[12]

Individual countries have chosen whether to use either verification, identification or both modules within the electronic border control system. For instance, many airports have opted for automatic security/background checks (identification), while traditional identity check scheme (passport control/im-

8 P. Chawdhry; R.P. Da Silva, Advanced registered traveler paradigm using dynamic risk profile and multimodal biometrics, *IEEE International Conference on Systems, Man and Cybernetics*, 2009, San Antonio, p. 3946.
9 A.Y.J. Nakanishi; B.J. Western, Advancing the State-of-the-Art in Transportation Security Identification and Verification Technologies: Biometric and Multibiometric Systems. *IEEE Intelligent Transportation Systems Conference*, 2007, p.1004.
10 According to the International Civil Aviation Organisation document from 2006 "Machine ReadableTravel Documents Part 1".
11 *Ibidem* .
12 According to the United States Department of State, Bureau of Consular Affairs, Passport Services document "ePassports and Biometrics".

migration officer visually performs facial comparison between the traveler and the digital face photograph in the biometric passport) is still in place of verification. However, in the past years, automated passport control systems have begun replacing traditional passport control desks at international airports in the US, Canada, UK, Netherlands, Estonia, Australia, New Zealand, Abu Dhabi, Japan, etc. E-gates speed up identification time, although issues can also arise (e.g., dirty optical fingerprint reader surface impairs accurate identification).

Biometric identity solutions can also be geared towards increasing convenience and speed of low-risk airport passengers, such as frequent flyers enrolled in Privium and SmartGate programs at airports in the Netherlands and Australia, respectively. More recently, a watch-size wearable digital identity solution, based on unique electrical signals from the heart (cardiac rhythm), has been introduced.[13] Virgin Atlantic announced piloting this device, envisioned to allow the enrolled passengers to bypass long waiting lines at airports, allowing them check-in, dropping off their luggage and boarding the plane simply by scanning their wrist.

Importantly, some airports have implemented biometric solutions as part of an immigration procedure. For example, the United Arab Emirates (UAE) launched a nationwide rollout of the "Iris Expellees Tracking and Border Control System" in 2003, with a goal of minimizing illegal immigrants in the country.[14], [15] When an immigrant is to be expelled from the UAE, their iris is scanned at a deportation center and enrolled into a central database operated by the General Directorate of Abu Dhabi Police, Ministry of Interior.[16] Irises of all incoming foreigners with new visas are also scanned upon arrival to one of the eight participating UAE airports and compared against this world's largest iris repository.[17] In such a way, expellees attempting reentry into the UAE with a new identity and fraudulent travel documents can be identified in real time, reportedly in less than 2s. In eight years, almost 350,000 deportees to the UAE have been identified.[18] As in theoretical accuracy performance tests, evaluation of the UAE's iris system demonstrated a lack of FMR, despite 2 tn cross comparisons, due to 'adaptive' decision making process.

13 C.M. Belinda; T. Sugumaran; E. Kannan, iiCardiac rhythm — Biometrie based secure authentication for IEEE 802.15.6, *International Conference on Science Engineering and Management Research (ICSEMR)*, 2014, Chennai, p. 1

14 A.M. Al-Khouri, The UAE Iris Expellees Tracking and Border Control System, *The Future of Secure Documents*, 2004, Florida.

15 M. ALMualla, The UAE Iris Expellees Tracking and Border Control System, *Biometric Consortium Conference*, 2005, Virginia.

16 J. Daugman J; I. Malhas. Iris recognition border-crossing system in the UAE, *Biometrics*, 44/2004, p.49.

17 *Ibidem.*

18 According to Emirates Identity Authority article from 2012 "Iris scan prevented entry of 20,000 deportees into UAE: Director General of Abu Dhabi Police Central Operations".

Office of Biometric Identity Management (OBIM) in the US, former US-VISIT, employs biometrics to establish and verify identities of international travelers holding a non-US passport. Travelers applying for a US visa at their home country are enrolled into a program, by providing digital images of ten fingerprints and a facial digital photograph. At that time their biometrics are compared against "watch lists" of known criminals and suspected terrorists.[19] Following establishment of eligibility to receive a US visa, eligibility to enter the country is determined upon collecting the same biometric data at an arriving airport, verifying that the person entering the country is the same person to whom the visa was issued. This is the largest fingerprint register in the world. Pilot tests at Hartsfield-Jackson Atlanta International Airport and Detroit Metropolitan Wayne County Airport have been made to also implement the system during exiting the US, in order to identify individuals who have overstayed or have stayed illegally in the country.[20] However, these attempts have not resulted in the implementation of the program, mainly due to difficulties in ensuring that the person who presented their biometrics while at exit is actually the person who boarded the plane.[21] Biometric entry and exit immigration systems also exist in Australia, Canada, Bulgaria, Czech Republic, Ireland, France, Latvia, Ghana, The Netherlands, New Zealand, Saudi Arabia, Taiwan, and United Kingdom.[22]

3. Biometric identification of individuals on airport "safe lists" and "watch lists"

As certain areas of every airport, such as warehouses, hangers and the airport apron, are more sensitive, it is necessary to prohibit access of general public to such areas and allow access only to authorized personnel, such as baggage handlers, maintenance workers and truck drivers delivering cargo. Los Angeles International Airport (LAX), for example, issues 60,000 badges annually[23] and has moved from the legacy system (badge number) to fingerprinting. Canadian Air Transportation Safety Administration (CATSA) credentialing system, in place at 29 Canadian airports and based on biometrics, streamlines both badging and background checks, as well as personnel privileges. During the latter process, employees with permission to enter sensitive areas are enrolled into a biometric database, the so called "safe list" and each

19 http://www.immihelp.com/visas/usvisit.html
20 J. Kephart, Biometric Exit Tracking: A feasible and cost-effective solution for foreign visitors traveling by air and sea, *Center for Immigration Studies*, 2013.
21 *Ibidem.*
22 *Ibidem.*
23 R. Garrett, The Credentialing Challenge, Airport Tech, 2014, p. 32.

time they enter the area during their workday their identity is verified via a biometric trait. LAX is currently storing worker iris images for future use, as multibiometric approach, joint use of several biometric traits including fingerprint, iris, hand geometry and vein patterns in this case, is to provide the least error-prone identification. With the same goal in mind, multibiometric system based on gait, voice and face recognition has been developed and pilot-tested for employee authentication in Euroairport in Switzerland, as part of the Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis (HUMABIO) scientific project.[24]

Conceptually opposite to "safe lists", recognizing personae non gratae at airports is an imperative. Video surveillance of public airport areas occurs routinely at airports worldwide. Images of individuals from video streams taken by Closed Circuit Television (CCTV) or smart phone cameras can be matched against specific databases in biometric systems. These databases known as "watch lists" contain stored templates of known criminals' and terrorists' facial images. This allows for identification of wanted individuals in a mass, at a distance (few tens of meters) and without their knowledge (covertly). Vendors of such technology claim to have achieved up to twenty simultaneous facial recognitions without delay, as well as up to 1 million identity comparisons per second, resulting in immediate alerts upon occurrence of a positive match.[25] Yet, evaluation of facial recognition technology that took place at the Palm Beach airport[26] at processing "load" of 10,000 images per day, resulted in approximately 50% true positives and an average of three false alarms per hour. False positives, resulting from faces being turned away from the camera, facial expressions, etc., also showed to be high in a test conducted at Boston's Logan Airport in 2002,[27] rendering facial recognition at airports impractical as a stand-alone technology, still requiring human operators. While proponents of implementation of such technologies argue that it represents a proactive crime fighting strategy, opposition warns about rights to privacy (people do not know they are being watched), potentials for abuse (once stolen biometric characteristic cannot be replaced) and risks for total surveillance ("big brother is watching you").

Using human gait as a remote biometric tool during airport surveillance has also been considered as an approach since 2000, when *Defense Advanced Research Projects Agency (*DARPA) in the US launched *HumanID at a Distance* program. Gait is a convenient biometric characteristic, given that it is

24 A. Riera, et al, Multimodal Physiological Biometrics Authentication, objavljano u: *Biometrics: Theory, Methods, and Applications*, 2009, Hoboken.
25 http://www.wavestore.com/technologies/analytics/facial-recognition
26 K.J. Strandburg; D.S. Raicu, Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, 2006, New York.
27 *Ibidem.*

contactless and it can be continuously monitored in real-time at a distance, even with lower-resolution images. Since the early years, much research based on static (i.e., leg length) and dynamic walking parameters (i.e., number of steps per minute), using silhouette-based and model-based approaches, has shown reasonable success of gait to differentiate between individuals.[28], [29], [30] Further research efforts in gait recognition have focused on improving scalability of the initial results, camera viewpoints, effects of walking speed, carrying objects, shoes and clothing on walking patterns, etc.[31], [32], [33], [34] At the National Physics Laboratory, Southampton University, UK, researchers have developed a biometric tunnel with twelve CCTV cameras which allows for automatic gait recognition based on a 3D model of a person's walk.[35] Such technology could help airport authorities identify individuals when walking through a monitored area. Research focusing on detection of concealed load[36] via changes in gait is of particular interest for possible identification of suicide bombers at airports. Researchers at Georgia Tech Research Institute, US have used radar to detect a person walking from ~150m distance wearing a simulated suicide bomb vest.[37], [38] Barki and colleagues have attempted to obtain specific (and changed) walking signatures on a test dataset using an inverse kinematic motion model of lower extremities.[39] A commercial system already widely employed by military in Iraq and Afghanistan[40] uses a combination of video tracking/gait recognition software and radar technology. Gait rec-

28 A.F. Bobick; A.Y. Johnson, Gait recognition using static, activity-specific parameters. Computer Vision and Pattern Recognition, 2001.
29 P.C. Cattin, Biometric authentication system using human gait [PhD Thesis], *Swiss Federal Institute of Technology*, 2002, Zurich.
30D. Voth, You can tell me by the way I walk, *IEEE Intelligent Systems*, br. 1/2003, p. 4.
31 I. Bouchrika; M.S. Nixon, Exploratory factor analysis of gait recognition, IEEE International Conference on Automatic Face and Gesture Recogntion, 2008, p. 1.
32 W. Kusakunniran; Q. Wu; J. Zhang; H. Li, Gait recognition across various walking speeds using higher order shape configuration based on a differential composition model. *IEEE transactions on systems, man, and cybernetics Part B*, br. 6/2012, p. 1654.
33 S. Lombardi, et al, Two-Point Gait: Decoupling Gait from Body Shape. IEEE International Conference on Computer Vision (ICCV), 2013, Washington DC, p. 1041.
34 D. Muramatsu, et al, Arbitrary view transformation model for gait person authentication. IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2012, Arlington, p. 85.
35 L. Middleton, et al, Developing a non-intrusive biometric environment, IEEE/RSJ International Conference on Intelligent Robots and Systems, 2006, Beijing, p. 723.
36 M. Nixon, Gait biometrics, *Biometric Technology Today*, 16/2008, p. 8.
37 T. Barry, Gait Recognition Research Strides Ahead, *Atlanta Business Chronicle*, 2002.
38 R.N. Trebits; G. Greneker Iii: J.L. Kurtz, Very low cost stand-off suicide bomber detection system using human gait analysis to screen potential bomb carrying individuals. *Radar Sensor Technology IX*, 2005, Orlando.
39 G. C. Gilbreath, et al, Extraction of human gait signatures: an inverse kinematic approach using Groebner basis theory applied to gait cycle analysis, *SPIE*, br. 8734/2013.
40 L. Groeger, Army Uses Radar to Spot Suicide Bombers From 100 Yards, *Wired*, 2011.

ognition software detects individuals and tracks them based on their walking style features and physical attributes, locating them even after they have been obscured by crowds and other objects.[41] Low power radar beams repeatedly "inspect" moving subjects in the examined area of interest; reflected beams are then compared to the database of "normal" and "anomalous" responses, determining whether obtained signature corresponds to a person carrying explosive devices or other concealed weapons. Gait recognition software[42] could play a greater role in this system in the future, as researchers are developing tools for analyzing joint movements of walkers, how they correlate with carrying heavy objects, how they change when a person deposits load on the ground, etc.[43] Others have also researched into using knee joint features for biometric identification during airport surveillance,[44], [45] although the scanning technology itself (Magnetic Resonance Imaging – MRI) is not sufficiently rapid for this task at the moment.

Presented solutions hold promise in identification of suicide bombers and other terrorists at airports at a safe distance, in a non-invasive, covert manner, before they reach airport perimeters or check points.

4. Biometric profiling approach to airport security

It has been argued that airport *screening* systems tend to have a high probability of false alarms, resulting in wasted time, resources and effort of the government security agencies which implemented the technology, airport security personnel and passengers selected to allegedly carry prohibited items detected by such screening devices.[46], [47] Furthermore, screening is a challenging task, given that it requires probing millions of individuals in search of a few ones with malicious intents, a process which, in addition to implemented technology, also demands difficult decision-making by security personnel. Thus, some argue that airports should focus on passenger *profiling* (or behavioral screening), a risk-based approach for detecting suspicious individuals with hostile thoughts. An Israeli company, WeCU Technologies Ltd., has de-

41 http://www.rapiscansystems.com/en/products/counterbomber
42 K. Nitkin, Walking like a Bomber, *MIT Technology Review*, 2007.
43 B. Siuru, Detecting Suicide Bombers by How They Walk, *ComputorEdge*, 2007.
44 L. Shamir, MRI-based knee image for personal identification, *International Journal of Biometrics*., 2/2013, p. 113.
45 L. Shamir, et al, Biometric identification using knee X-rays. *International Journal of Biometrics*, 3/2009, p. 365.
46 H. Cavusoglu; B. Koh; S. Raghunathan, An Analysis of the Impact of Passenger Profiling for Transportation Security, *Operations Research*, br. 5/2010, p. 1287.
47 http://edition.cnn.com/2008/TECH/12/02/airport.security

veloped a field operational system which is based on audio or visual stimuli specifically designed for relevant target groups, which are expected to elicit a biometric response (conscious or subconscious psychological and behavioral reaction), which can then be captured by hidden cameras and/or concealed sensors either remotely or in an accidental contact.[48] For instance, if a terrorist were to be looking at an airport departures screen and a symbol of his terrorist group appears on the screen, he will exhibit an involuntary reaction, such as increased heart rate, breathing and/or temperature, eye fixation and pupil dilatation, etc. Without interrupting regular flow of airport activities, the company claims to be able to measure up to 14 variables and produce results in approximately 35 seconds, with ~95% success rate in tests.[49] Physiological variables baseline is to be measured initially and again repeatedly following the presentation of "provoking" stimuli. Therefore, anxiousness of nervous flyers and otherwise disturbed passengers is not expected to create significant false positives. Also focusing on passenger's intent, rather than what they are carrying, Suspect Detection System's *Cogito* has been tested in the US and Israel's airports.[50], [51], [52] The system consists of a booth in which a passenger places their left hand on the sensor, wears earphones and sits in front of the screen, answering a set of questions (for instance, "Are you involved in a terrorist activity?"), while their psycho-physiological reaction (i.e., skin electrical conductivity and temperature, left hand and eye movements) is being measured.[53] Designed to catch biometric reactions to specific words, which are compared to passenger's reactions while answering baseline questions, as well as to reactions of a peer group (for example, ten previous passengers), the system is designed to pick up those with criminal and terrorist agendas, rather than generally anxious travelers. After the technology reaches acceptable error rates (some tests indicate 8% FMR and 15% FNMR[54]), it is intended for selected groups of passengers, such as passengers designated as suspicious by officers using The Screening of Passengers by Observation Techniques (SPOT) or travelers flying on known high-risk flights. Future Attribute Screening Technology (FAST) Project[55], [56] in the US envisions following physiological (i.e., eye movement

48 http://www.epicos.com/EPCompanyProfileWeb/GeneralInformation.aspx.
49 D. Rose, 'Are you a terrorist?' The simple question being asked at an airport which could rumble a suicide bomber, *The Mail*, 2010.
50 *Ibidem.*
51 http://www.hash-security.co.il/en/products/sds/
52 J. Karp; L. Meckler, Which Travelers Have 'Hostile Intent'? Biometric Device May Have the Answer, The Wall Street Journal, 2006.
53 http://www.hash-security.co.il/en/products/sds/
54 D. Citron, Brave New World of Biometric Identification, Concurring Opinions, 2013.
55 Lasko L. Privacy Treshold Analysis (PTA). In: Security USDoH, editor. Washington, DC2011.
56 According to the DHS Science and Technology Directorate document from 2011 "Future Attribute Screening Technology".

and blink rate, pupil dilatation, alterations in body temperature), behavioral (i.e., body movements, breathing patterns) and linguistic (i.e., alterations in voice pitch and speech intonation) biometric cues with an idea of predicting future criminal and terrorist actions. The opponents of behavioral approaches designate them *pre-crime* (after a 2002 movie "Minority Report"), too invasive on individual privacy and ineffective for terrorists who take tranquilizers to mask nervous reactions.[57]

Innovative approaches to successful biometric identification with a goal of tightening airport security are continuous. Using a new biometric identifier, eyeball movements when following a stimulus projected on a screen, an Israeli company ID-U Biometrics Ltd., has been field testing their product for detection of ordinary passengers and the ones with hostile agendas.[58],[59] Yet, it is crucial that objective, independent testing and evaluation of biometric system performance is carried out by assessing FNMR, FMR, FTA, FTE and throughput rate. Biometric solutions that pass the evaluation criteria and conform to published standards (if any) can be found on TSA's Qualified Products List (QPL).[60]

5. Biometric identification ensuring during-flight security

Passenger and crew flow through the airport finalizes with boarding the plane and clearly, it is essential to also maintain high level of security during flight. Biometric solutions have been developed to create secure cockpits, which would limit the entrance into the cockpit to authorized personnel only. Recent tragic events on Germanwings flight 9525 emphasize the importance of adequately approaching this issue.

One of the possible scenarios, proposed in SAFEE program, is that an access to the cockpit is regulated by a fingerprint or another biometric scanner. In such a way, a biometric characteristic being presented live could be matched against a crew database created for each flight. In addition to this, a camera linked to a video display inside the cockpit would allow the pilot or the co-pilot to inspect whether a crew member is attempting to enter the cockpit alone or if they are in duress. Importantly, data of possible imposters would be stored for later evaluation. Additional proposals include surveillance of passengers by cameras and microphones for possible suspicious behavior.

57 S. Weinberger, Terrorist 'pre-crime' detector field tested in United States, *Nature*, 2011.
58 D. Rose, *Opus citatum*.
59 L. Sandhana, Eyeball This: Biometrics That Track the Way You See, *Fast Company*, 2010.
60 Accpording to Biometric Technology Today article from 2007 "TSA announces qualified product list".

However, if an intruder were to reach the cockpit and attempt hijacking the plane, continuous or on-demand biometric authentication, rather than conventional, one-time-only biometric approaches, could serve as an anti-spoofing strategy. Researchers have been developing such biometric system, which is based on distinctive alpha and beta brain wave patterns recorded by an electroencephalogram (EEG).[61], [62] Pilot's EEG would thus be stored in a database during enrollment, and brain wave patterns during flight would continuously be compared to the stored template, verifying the assigned pilot is truly operating the plane.[63] In case of a non-match due to the changes in brain wave patterns, the system would block the control panel for further use by a hijacker. Although this emerging technology is promising, additional research, as well as adequate testing and evaluations are yet to be carried out.

Conclusion

Automatic biometric identifications represent a contemporary approach to addressing modern day security demands in air transportation. Yet, the expectation of "one fits all" solution is likely far-fetched. For example, it has been noted that long term use of cytostatic capecitabine may cause loss of usable fingerprints for identification.[64] Thus, for such patients, as well as for individuals missing an arm, reference templates cannot be generated in biometric systems based on fingerprints. Generally speaking, it is not very likely that a single approach will be satisfactory for airport security and airline safety needs. As a result, quest for biological traits that could serve as biometric characteristics, is continuous. These can be either biological characteristics with previously unknown biometric potential, or biological traits which have long been known to have biometric value, but could not previously be adequately measured or processed. Yet, routine employment of such technologies is not typically quickly around the corner, given that it is necessary that they undergo

61 I. Nakanishi; S. Baba; S. Li, Evaluation of Brain Waves as Biometrics for Driver Authentication Using Simplified Driving Simulator. International Conference on Biometrics and Kansei Engineering (ICBAKE), 2011, Takamatsu, p. 71.
62 I. Nakanishi; H. Fukuda; S. Li, Biometric verification using brain waves toward on-demand user management systems, *The 6th International Conference on Security of Information and Networks*, 2013, New York.
63 D. DiSalvo, Using The Power Of Brain Waves To Prevent Car And Plane Hijackings, *Forbes*, 2013.
64 M. Wong; S.P. Choo; E.H. Tan, Travel warning with capecitabine, *Annals of Oncology*, 20/2009, p. 1281.

standardization and objective evaluations by independent bodies.[65, 66] Further, biometric systems are not attack-free. For instance, Galbally and colleagues proposed that an iris image can successfully be reconstructed from binary templates and used to trick iris recognition system.[67] To that end, much effort is made towards developing superior sensors and algorithms, multibiometric approaches, as well as anti-attack software for diverse attack scenarios.[68]

Opponents of the technology warn that its use is controversial, not always accepted by the public and, in some countries, not properly regulated by law. It has been argued that a concept in which a government or a private airline company handle and manage individual's most private possessions (their own body parts), which, if stolen, misused or manipulated in some other way cannot be replaced, is non-ethical and violates one's rights to privacy. However, the question is whether the right to individual privacy comes before collective security in the air transportation context. In addition, it should be noted that obtaining a biometric passport and participating in the air transport flow are voluntary activities and not government-mandated. These arguments constitute important factors when considering the principle of proportionality in air transportation biometrics.

Acknowledgments

During the preparation of this manuscript S.T. was supported in part by the Serbian Ministry of Education, Science and Technological Development Project No. TR34019 and the EU Commission project AREA, Contract No. 316004.

References

1. Al-Khouri AM, The UAE Iris Expellees Tracking and Border Control System. The Future of Secure Documents, Florida, USA, 2004.
2. ALMualla M, The UAE Iris Expellees Tracking and Border Control System, *Biometric Consortium Conference*, Virginia, USA, 2005.

65 V. MacLeod; B. McLindin, Methodology for the Evaluation of an International Airport Automated Border Control Processing System, objavljeno u: *Innovations in Defence Support Systems -2. Studies in Computational Intelligence*, Springer Berlin Heidelberg, 2011, p. 115.
66 C. Wilkinson; E. Rao, Airport access control standards, *Security Technology*, 2003, p. 305.
67 J. Galbally, et al, From the Iriscode to the Iris A New Vulnerability of Iris Recognition Systems. *Black Hat USA*, 2012, Las Vegas.
68 J. Galbally; S. Marcel; J. Fierrez, Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition, *IEEE Transactions on Image Processing*, br. 2/2014, p. 710.

3. Rosenblatt, D: Behavioral screening - the future of airport security? [online], available at: *http://edition.cnn.com/2008/TECH/12/02/airport.security/* (15/12/2015)
4. T. Barry: Gait Recognition Research Strides Ahead [online], available at: *http://www.bizjournals.com/atlanta/stories/2002/04/22/focus4.html* (15/12/2015)
5. Belinda, CM; Sugumaran, T; Kannan, E, iiCardiac rhythm — Biometrie based secure authentication for IEEE 802.15.6., objavljeno u: *Proceedings of the 2014 International Conference on Science Engineering and Management Research (ICSEMR)*, IEEE, Chennai, India, 2014.
6. Bobick, AF; Johnson AY, Gait recognition using static, activity-specific parameters. Computer Vision and Pattern Recognition, objavljeno u: *Proceedings of the 2001 IEEE Computer Society Conference on 2001*, CVPR 2001, vol. I, Kauai, HI, USA, 2001.
7. Bolle, RM; Pankanti, S; *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, Norwell, MA, USA, 1998.
8. Bouchrika, I; Nixon, MS, Exploratory factor analysis of gait recognition, objavljeno u: *8th IEEE International Conference on Automatic Face & Gesture Recognition*, IEEE, Amsterdam, Netherlands, 2008.
9. Cattin, PC; *Biometric authentication system using human gait*, PhD Thesis., Swiss Federal Institute of Technology, Zurich, 2002.
10. Cavusoglu, H; Koh, B; Raghunathan, S; An Analysis of the Impact of Passenger Profiling for Transportation Security, *Operations Research*, vol. LVIII, br. 5/2010
11. Chawdhry, P; Da Silva, RP, Advanced registered traveler paradigm using dynamic risk profile and multimodal biometrics, objavljeno u: *2009 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, San Antonio, TX, USA, 2009.
12. Citron, D: Concurring Opinions [online], available at: http://concurringopinions.com/archives/2013/08/brave-new-world-of-biometric-identification.html (15/12/2015)
13. Daugman, J; Malhas, I; Iris recognition border-crossing system in the UAE, *International Airport Review*, br. 2/2004, Russell Publishing Ltd, Brasted, UK.
14. DiSalvo, D: Using The Power Of Brain Waves To Prevent Car And Plane Hijackings [online], available at: *http://www.forbes.com/sites/daviddisalvo/2013/09/21/using-the-power-of-brain-waves-to-prevent-car-and-plane-hijackings/* (20/12/2015)

15. Galbally, J; Marcel, S; Fierrez, J; Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition, *IEEE Transactions on Image Processing*, vol. XXIII, br. 2/2014
16. Galbally, J; Ross, A; Gomez-Barrero, M; Fierrez, J; Ortega-Garcia, J; From the Iriscode to the Iris A New Vulnerability of Iris Recognition Systems, objavljeno u: *White Paper for Black Hat USA 2012*, Black Hat USA, Las Vegas, USA, 2012.
17. Garrett, R, The Credentialing Challenge, objavljano u: *Airport Tech*, p. 32, 2014.
18. Gilbreath, GC; Barki, A; Kendricks, K; Tuttle, RF; Bunker, DJ; Borel, CC, et al, Extraction of human gait signatures: an inverse kinematic approach using Groebner basis theory applied to gait cycle analysis, *Proceedings of SPIE*, vol. 8734, 2013, SPIE, Bellingham, WA, USA.
19. Global, A: How Biometrics Help Airports Reach Key Targets [online], available at: *http://www.argus-global.co.uk/how-biometrics-help-airports-reach-key-targets* (15/12/2015)
20. Groeger, L: Army Uses Radar to Spot Suicide Bombers From 100 Yards [online], available at: *https://www.wired.com/2011/07/army-uses-radar-to-spot-suicide-bombers-from-100-yards/* (20/12/2015)
21. Immihelp: US Visit-Entry/Exit System [online], available at: *http://www.immihelp.com/visas/usvisit.html* (20/12/2015)
22. Karp, J; Meckler, L: Which Travelers Have 'Hostile Intent'? Biometric Device May Have the Answer [online], available at: *http://www.wsj.com/articles/SB115551793796934752* (20/12/2015)
23. Kephart, J: Biometric Exit Tracking: A feasible and cost-effective solution for foreign visitors traveling by air and sea [online], available at: http://cis.org/biometric-exit-tracking-feasible-and-cost-effective (15/12/2015)
24. Kusakunniran, W; Wu, Q; Zhang, J; Li, H; Gait recognition across various walking speeds using higher order shape configuration based on a differential composition model, *IEEE transactions on systems, man, and cybernetics Part B (Cybernetics)*, vol. XLII, br. 6/2012, IEEE Systems, Man, and Cybernetics Society
25. Lasko L, Privacy Treshold Analysis (PTA), *Security USDoH*, 2011, Washington, DC.
26. Lazarick R, Biometric Product Qualification Program for US Airport Access Control, *International Biometrics Performance Conference*, 2010, National Institute of Standards and Technology

27. Lombardi, S; Nishino, K; Makihara, Y; Yagi, Y; Two-Point Gait: Decoupling Gait from Body Shape, objavljeno u: *2013 IEEE International Conference on Computer Vision (ICCV)*, IEEE Computer Society Washington, Sydney, VIC, USA, 2013.
28. Ltd. WT: WeCU Technologies Ltd. [online], available at: *http://www.epicos.com/EPCompanyProfileWeb/GeneralInformation.aspx* (15/12/2015)
29. MacLeod, V; McLindin, B; Methodology for the Evaluation of an International Airport Automated Border Control Processing System, objavljeno u: *Innovations in Defence Support Systems -2. Studies in Computational Intelligence*, vol. 338, Springer Berlin Heidelberg, 2011.
30. Martin, LL; Bombs, bodies, and biopolitics: securitizing the subject at the airport security checkpoint, *Social & Cultural Geography*, vol. XI, br. 1/2010.
31. Middleton, L; Wagg, D; Bazin, A; Carter, J; Nixon, M; Developing a non-intrusive biometric environment. Intelligent Robots and Systems, objavljeno u: *2006 IEEE/RSJ International Conference*, IEEE, Beijing, China, 2006.
32. Muramatsu, D; Shiraishi, A; Makihara, Y; Yagi, Y; Arbitrary view transformation model for gait person authentication, objavljeno u: *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, IEEE, Arlington, VA, 2012.
33. Nakanishi, AYJ; Western, BJ; Advancing the State-of-the-Art in Transportation Security Identification and Verification Technologies: Biometric and Multibiometric Systems, objavljeno u: *2007 IEEE Intelligent Transportation Systems Conference*, IEEE, Seattle, WA, USA, 2007.
34. Nakanishi, I; Baba, S; Li, S; Evaluation of Brain Waves as Biometrics for Driver Authentication Using Simplified Driving Simulator, objavljeno u: *2011 International Conference on Biometrics and Kansei Engineering (ICBAKE)*, IEEE, Takamatsu, Kagava, 2007.
35. Nakanishi, I; Fukuda, H; Li, S; Biometric verification using brain waves toward on-demand user management systems, objavljeno u: *Proceedings of the 6th International Conference on Security of Information and Networks*, ACM New York, NY, USA, 2013.
36. Nitkin, K: Walking like a Bomber [online], available at: *https://www.technologyreview.com/s/407189/walking-like-a-bomber/* (20/12/2015).
37. Nixon, M; Gait biometrics, objavljeno u: *Biometric Technology Today*, 2008.
38. Parks, L; Points of Departure: The Culture of US Airport Screening, *Journal of Visual Culture*, vol. 6, 2/2007, SAGE, Los Angeles, London, New Delhi, Singapore
39. Riera, A; Soria-Frisch, A; Capparini, M; Cester, I; Ruffini, G; Multimodal Physiological Biometrics Authentication, objavljeno u: *Biometrics: Theory, Methods, and Applications*, Hoboken, NJ, 2009.

40. Rose, D: 'Are you a terrorist?' The simple question being asked at an airport which could rumble a suicide bomber [online], available at: *http://www.dailymail.co.uk/home/moslive/article-1336571/Terrorism-Can-really-stop-bomber-asking-Are-terrorist.html* (20/12/2015).
41. Sandhana, L: Eyeball This: Biometrics That Track the Way You See [online], available at: *http://www.fastcompany.com/1706811/eyeball-biometrics-track-way-you-see* (15/12/2015).
42. Shamir, L; Ling, S; Rahimi, S; Ferrucci, L; Goldberg, IG; Biometric identification using knee X-rays, *International Journal of Biometrics*, vol. I, 3/2009.
43. Shamir, L; MRI-based knee image for personal identification, *International Journal of Biometrics*, vol. V, 2/2013.
44. Siuru, B; Detecting Suicide Bombers by How They Walk, *ComputorEdge*, 2007.
45. Strandburg, KJ; Raicu, DS; *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer US, 2006.
46. Systems, R: CounterBomber [online], available at: http://www.rapiscansystems.com/products/counterbomber (15/12/2015)
47. Trebits, RN; Greneker Iii, G; Kurtz, JL; Very low cost stand-off suicide bomber detection system using human gait analysis to screen potential bomb carrying individuals, objavljeno u: *SPIE Proceedings Radar Sensor Technology IX*, vol. 5788, Orlando, Florida, USA, 2005.
48. Voth, D; You can tell me by the way I walk, *IEEE Intelligent Systems*, vol. XVIII, br. 1/2003.
49. Wavestore: Facial Recognition [online], available at: *http://www.wavestore.com/technologies/analytics/facial-recognition* (12/12/2015)
50. Weinberger, S; Terrorist 'pre-crime' detector field tested in United States [online], available at: *http://www.nature.com/news/2011/110527/full/news.2011.323.html* (20/12/2015).
51. Wilkinson, C; Rao, E; Airport access control standards, objavljeno u: *2003 Proceedings IEEE 37th Annual 2003 International Carnahan Conference on Security Technology*, IEEE, 2003.
52. Wong, M; Choo, SP; Tan, EH; Travel warning with capecitabine, *Annals of oncology: official journal of the European Society for Medical Oncology*, vol. XX, 7/2009.
53. (SDS) SDSL: Suspect Detection Systems LTD [online], available at: *http://www.sdscp.com/* (20/12/2015)

BIOMETRIJSKE APLIKACIJE U BEZBEDNOSTI VAZDUŠNOG TRANSPORTA

Smilja Teodorović
Kriminalističko-policijska akademija, Beograd

Sažetak: Sve veći broj putnika u vazdušnom saobraćaju, kao i sve učestaliji teroristički napadi, povećavaju bezbednosne zahteve i rizike u avio-industriji na globalnom nivou. Jedan od osnovnih uslova za povećanje bezbednosti jeste mogućnost precizne i brze identifikacije kako putnika, tako i drugih učesnika u saobraćajnom toku. Biometrija je oblast koja se bavi identifikacijom pojedinaca na osnovu njihovih merljivih, bioloških (anatomskih, fizioloških i ponašajnih) karakteristika u automatskim informacionim sistemima i smatra se jednim od najpouzdanijih pristupa za utvrđivanje identiteta. Stoga ne čudi što su biometrijske tehnologije danas sve prisutnije u avio-industriji.

Cilj ovog rada je da upozna čitaoce sa dostupnim biometrijskim alatima koji se koriste za postizanje i održavanje visokog nivoa bezbednosti u vazdušnom saobraćaju. Autorka najpre daje pregled biometrijskih identifikacija koje se vrše na vazdušnim graničnim prelazima – aerodromima. U ovom kontekstu su, pored biometrijskih pristupa koji se koriste kao pooštrene mere bezbednosti, takođe obrađene i tehnologije koje imaju za cilj da povećaju brzinu prelaska granice i udobnost putnika niskog rizika, poput putnika koji često putuju (*frequent flyers*). Autorka dalje predstavlja načine na koje se, pomoću biometrijskih identifikacija, obavlja kontrola pristupa autorizovanih zaposlenih određenim zonama aerodroma, kao i provera prisustva osoba za kojima se traga. Kako skrining sistemi na aerodromima mogu imati visoke stope lažnih uzbuna, a sam proces skrininga predstavlja izazov, budući da zahteva proveru miliona pojedinaca u potrazi za svega nekoliko njih sa zlim namerama, autorka diskutuje o profilisanju putnika (bihevioralni skrining), kao savremenom pristupu identifikaciji pojedinaca na aerodromima, koji je u povoju, i koji je zasnovan na automatskom, biometrijskom prepoznavanju sumnjivih individua. Konačno, autorka predstavlja biometrijske aplikacije za identifikaciju pojedinaca tokom leta, koje se razvijaju u cilju obezbeđivanja putnika, posade i letelice.

Ključne reči: biometrija, identifikacija pojedinaca, bezbednost na aerodromu.