BIOMETRIC SYSTEM IN AVIATION INDUSTRY (FIRST PART)

A REPÜLÉSIPAR BIOMETRIKUS RENDSZEREI (ELSŐ RÉSZ)

ALSHAMAILEH, Lafee[1] – ŐSZI Arnold[2]

Abstract

Due to the increasing demand of public traveling and aviation security after several terrorist attacks and increasing the safety concerns associated with aviation industry, many researches have been carried out in order to develop a secure world-class aviation, since the 9/11 attacks, the air travel system became one of the most high-profile targets for terrorists and it radically effected the mode in which governments cater for high quality security. The Aviation and Transportation Security Act was passed by the American congress to create the "Transportation Security Administration (TSA)" and mandated that federal employees be in charge of airport security screening.

Keywords

Aviation Security, biometrics, Transportation Security Administration, Risk Based Security (RBS)

Absztrakt

A közúti utazás és a légi közlekedés biztonságának növekvő igénye miatt és több terrorista támadás után, valamint a légi közlekedéshez kapcsolódó biztonsági aggályok növelésével számos kutatás készült egy biztonságos világszínvonalú repülés kialakítása érdekében, mivel a légi utazási rendszer a terroristák a 9/11 támadása után az egyik legmagasabb szintű célpontja lett, és radikálisan befolyásolta azt a módot, amellyel a kormányok magas színvonalú biztonságot nyújtanak. Az amerikai kongresszus elfogadta a légi közlekedés és a közlekedésbiztonsági törvényt, hogy létrehozza a „Közlekedésbiztonsági Adminisztrációt" (TSA), és felhatalmazta a szövetségi alkalmazottak felelősségét a repülőtéri biztonsági szűrésért.

Kulcsszavak

Aviation Security, biometrics, Transportation Security Administration, Risk Based Security (RBS)

[1] lafee.alshamaileh@uni-obuda.hu| ORCID 0000-0002-5141-4786 | PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] oszi.arnold@bgk.uni-obuda.hu | ORCID 0000-0001-5988-0143 | adjunct professor/egyetemi adjunktus | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ABBREVIATIONS

US-VISIT: unveiled United States Visitor and Immigrant Status Indicator Technology

DHS: Department of Homeland Security

TSA: Transportation Security Administration

RBS: Risk-Based Security

NSTC: National Science and Technology Council

CAPPS I, II: Computer Assisted Passenger Pre-Screening

IATA: The International Air Transport Association

INTRODUCTION

Biometric technologies offer the future of security technology, but integrating avant-garde technology alone may not automatically solve all expected security problems. Many researches supported by several governments around the world offer an approach that may help to integrate the best solution. Biometric systems are statistical and mathematical methods for data analysis in biological sciences.

Now by the biological characteristics of the body or behavior, such as fingerprint, iris, retina, tone, and signature, the term often applies to the techniques of distinguishing individuals to differentiate a person from the rest of the individual. Europe now leads the world in the use of biometrics, and the largest market is likely to be in Asia, specifically in South Korea and Japan.

Recently, biometric systems and mathematical methods for data analysis in biological sciences have been incorporated in Aviation and Transportation Security Act. [1]

On June 2017, the European Association for Biometrics (EAB) in cooperation with IATA organized a conference to discuss the progressive engagement of biometrics-driven innovations with airlines. Various countries have utilized relevant equipment to register the biometric data of incoming passengers.

Biometric technology must be established and implemented in the least disturbing, most operative manner and in the control of realistic safeguards in order to create the balance between security and privacy.

LITERATURE REVIEW

Biometric System

Recently, biometric systems have been investigated and experienced in many fields, but have only lately entered into the public consciousness because of high profile applications, usage in several media and increased practice by the public in routine activities. The origins of biometrics are provided by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management; "biometrics" is derived from the Greek words "bio" (life) and "metrics (to measure). As per Merriam-Webster dictionary biometrics is defined as the measurement and analysis of unique physical or behavioral characteristics especially as a means of verifying personal identity. Iris images, facial photographs, some types of voice patterns, palm prints, fingerprints andDNAare a small range of recent biological features, commonly referred to as modalities, used to classify individuals [3]. In light of their behavioral and organic qualities, biometricsis a method for the computerized identification of individuals. Face, fingerprints, hand geometry, iris, speech, signature, gait, and keystroke are the most common biometric modalites.[4]

'Biometrics' is described as a process where detectable biological (anatomical and physiological) and behavioral characteristics are based on automated methods of recognizing an individual. In the beginning of the civilization, humans used faces to recognize known (familiar) and unknown (unfamiliar) characters. Face recognition based on geometric characteristics is one of the most accepted methods for identification, since facial features are unique to every human being. Biometric data must be reliable (Safe and operating at a reasonable level of efficiency) and acceptable (non-invasive and socially tolerable) in addition, it must ensure universal, unique, permanent and measurable features.

Human-to-human identification is also used in behavioral-predominant biometrics such as speaker recognition and gait recognition. Individuals use these traits, somewhat unintentionally, to identify recognized individuals daily. [5] This essential role has gradually become more stimulating as populations have grown.

The National Science and Technology Council acknowledged that automated biometric systems have only become possible over the last few decades as a result of substantial developments in the field of data processing. However, all of these modern computerized systems are based on concepts that were initially been formulated hundreds, even thousands of years ago. [5]

It is a way to create assurance that one is dealing with individuals who are already established (or not known) and therefore fit into a category with certain privileges (or to a group denied certain treats). It depends on the fact that people have different physical and behavioral characteristics.

The Airport Council International (ACI) rely on the importance of having a robust airport position on biometrics and they published a position paper entitled "The Application of Biometrics at Airports" to give a General encouragement for the planning and application of biometrically-enabled border control, passenger simplification and access control systems. [6]

The pioneer biometric system used in Europe is called RAPID, it was used in Portugal for border controlling as each passenger must use electronic passports. Figure 1 Shows Photo of Smart Gate (Facial and Fingerprint) Brisbane International Airport from Frontex, 2010.

First, a photo of the traveler taken at the automated gate and current confirmation in the electronic passport with facial biometrics is processed. Subsequently, the automatic gate will open and the traveler is allowed to enter.

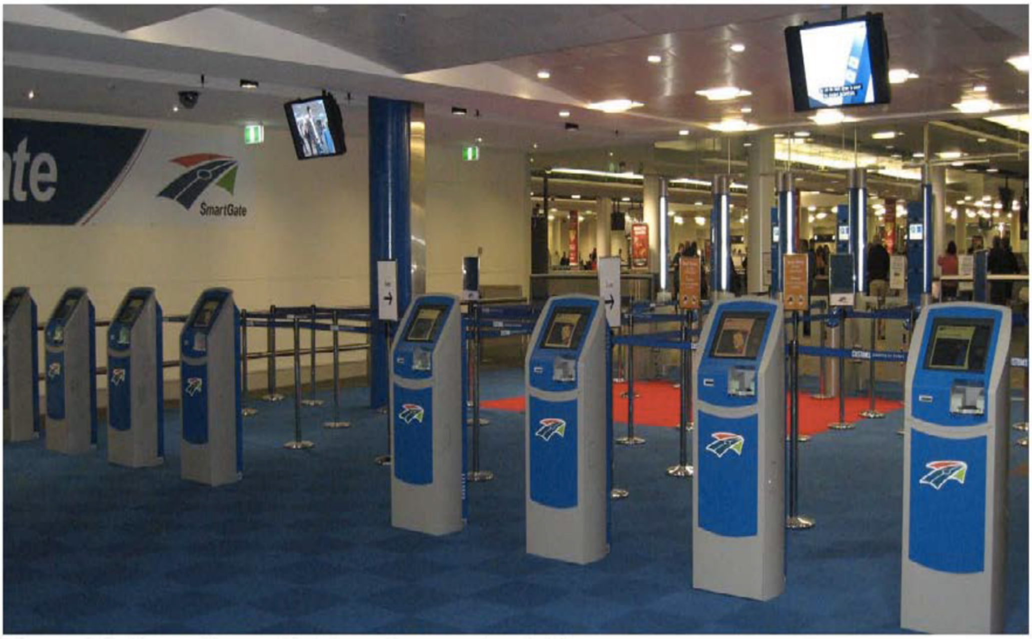

Figure 1: Photo of Smart Gates (Facial and Fingerprint) Brisbane International Airport from Frontex, 2010.

In the Netherlands the Privium system, (Figure 2), is used in as a voluntary option for frequent flyers.

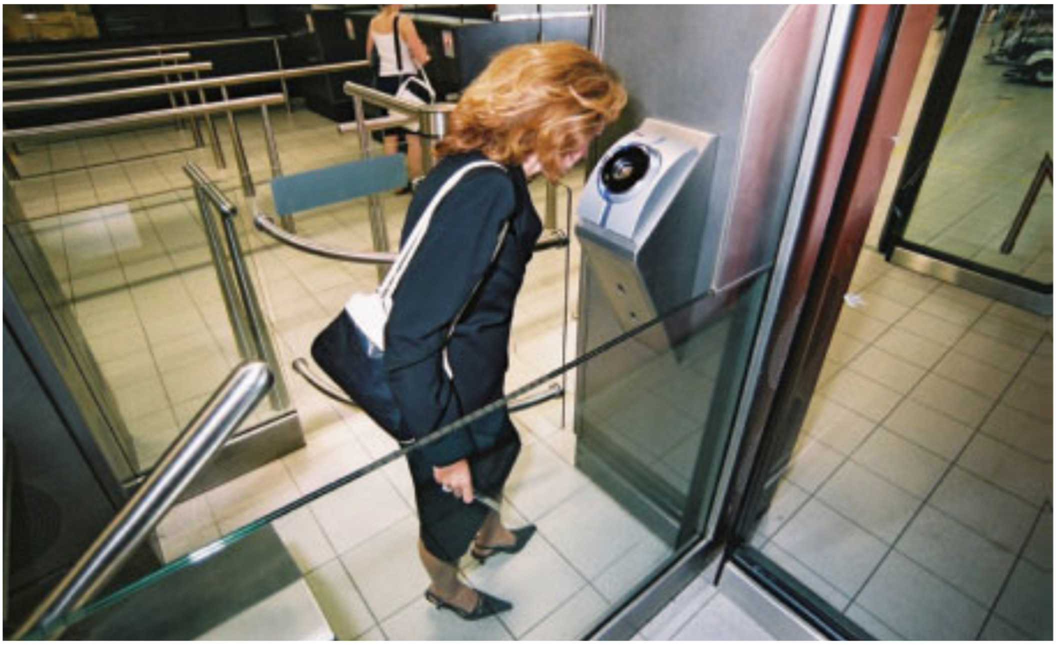

Figure 2: Photo of Privium system in the Netherlands (Iris Scan) from Airport Business, 2009

Let us take Europe as a case. Both passengers entering or exiting the Netherlands are forwarded to a separate border control line where booths accept the Privium smart card as the traveler's biometric data is stored in a smart card and the iris prototype is stored. Iris cameras are used to check the identification of a traveler against an intelligent card. The software has been highly successful in the Netherlands. [7]

Passenger classification may also lead to facilitating the safety protocol in the aviation industry. Poole classified the traveler as the proposed risk-based method in order to affect the concentration on the identification of hazardous persons to (i) low-risk passengers, of whom a great deal is known; (ii) high-risk passengers, based either on lack of awareness or on clear negative information; and (iii) ordinary passengers, mainly infrequent travelers and leisure travelers. [2]

Low-risk travelers are those that have a current federal security clearance or who have been admitted into the Approved Traveler Programme, high-risk travelers are those who do not have a paper trail, so little is understood that the best thing to do is to presume the worst and to perform a comprehensive screening of both the individual and the luggage, and ordinary travelers are those in between the other two risk cats. [2]

This measure would help to improve security monitoring in terminal lobby areas and outside the airport, in ramp areas and across the airport periphery. A different approach to both the screening of travelers and the screening of bags will apply to each category.

Biometric Modalities

There are several known biometric modalities e.g. (face, hand geometry, iris, voice, etc.), see Figure 3, and it is worth mentioning here that there is no biometric modality suitable for all implementations as there are several aspects to take into consideration during the modalities selection and biometric toll such as security risk, location, number of users and the available data. Moreover, it is significant to note that biometric modalities are subject change in the phases of maturity.

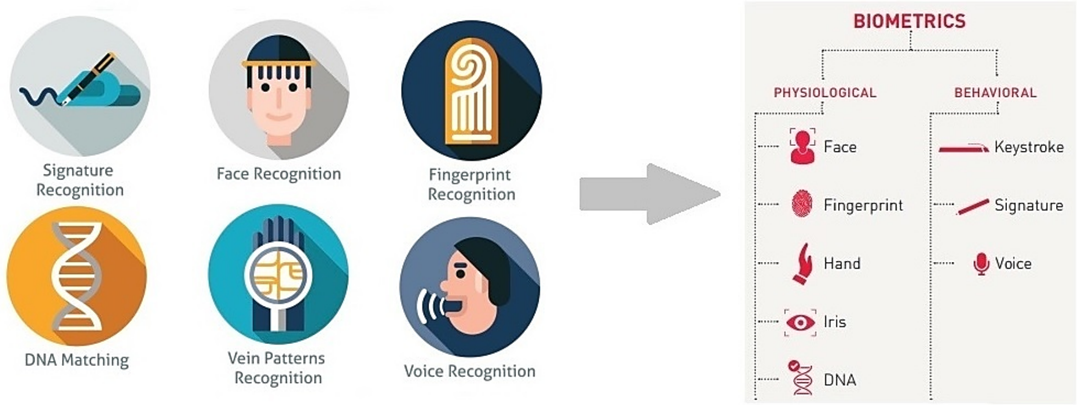

Figure 3: Biometric Modalities

On the other hand, the different sorts of biometric modalities do not all have the same level of consistency. Physiological measurements are usually considered to offer the benefit of remaining more constant during the life of any person. Behaviour-based identification may be affected by stress, which is not true for measurement based on physical features.

TECHNIQUES FOR BIOMETRIC DATA MANIPULATION

Several techniques for biometric data manipulation were listed in the literature such as recognition, pattern categorization filtering, convolution and Fourier transforms. It is favourable that an applied biometric methods be the simplest possible. Some sophisticated decision-making algorithms that are also capable of making errors take the top place of the system, also having an important role in the relationship between a human and a machine. In this section, we consider the verification and identification.

Biometrics is defined in two ways: (i) authentication in this system applies to one biometric and one biometric examination (1:1) to verify that the person is who he says he is. (ii) Recognition relates one biometric to a biometric database (1:N) to find out who the individual is.[8]

Biometric systems have sequences of crucial procedures that have to be accomplished in order to (i) allow a person to use the system and (ii) achieve verification or authentication of a individual's identity. [6]

These vital processes contain:

- Enrolment – the capture of the raw biometric
- Development of a prototype – Preservation of the biometrics by using an algorithm to obtain a model from the input images, which will then enable the image to be matched to others using the same technique. Identification – takes new biometric samples and compares them to saved templates of all enrolled users.
- Verification – takes new biometric samples of a specific user and compares them to old samples taken from the same user.

The concept of a biometric system is summarized by a sequence of measures within a system as a multi-step process, in other words, each individual shows several aspects of himself or herself; after that this aspect is seized by a sensor and transformed into an algorithm model. The registered model is then matched to the reference sample or baseline algorithms saved in system data base. The result of comparison decides the next corresponding response such as entry into a secure structure. Figure 4 shows a schematic diagram for basic biometric system.

The main component of biometric system is sensor in which data will be generated in form of signals such as electromagnetic spectrum.

Biometric data processing techniques in the second part involve different filtering, transformation and pattern recognition algorithms. As a consequence, decision-making mechanisms are used at many phases of the operation of biometric data.

The third component is the hardware platform for the implementation of these techniques. Usually a set of processors are used as a hardware platform for biometric devices and systems.

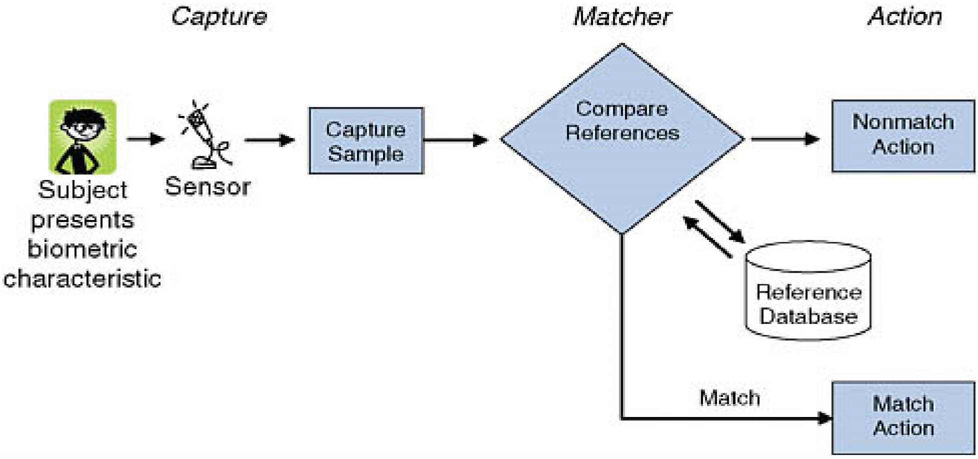

Figure 4: A Schematic Diagram for Basic Biometric System.

Verification or authentication technologies are basically one of the following: (i) things the person knows like a password or (ii) Something the individual has, such as a physical key or cards and the last thing is (iii) Something the individual is or does.

Biometric systems can function without active input, user cooperation, or knowledge that the recognition is taking place. Thus the last one is usually employed with the biometric technologies. However, a biometric system does not store biometric data, as unprocessed or incomplete biometric data cannot be used to conduct biometric contests. The method whereby the biometric data of the user is initially obtained, analyzed, treated and saved in the form of a prototype is called enrollment. [9] So identification follows three phase schemes: data acquisition, techniques, and computing platform.

Creating a biometric system is the implementation of application-specific techniques (methods, algorithms, and programs) using some computing platform.

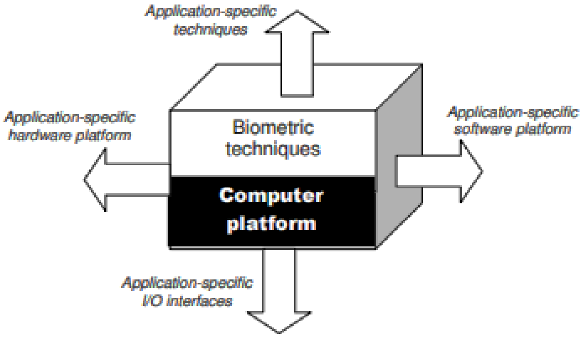
Application-specific techniques
Application-specific hardware platform
Biometric techniques
Computer platform
Application-specific software platform
Application-specific I/O interfaces

Figure 5: Biometric system is an application-specific computer system consisting of the specific-purpose programs and computing platform [9]

Biometrics can be used as uni-biometric to multi-biometric systems. Unibiometric systems make use of a single source of biometric information while multibiometric use several parameters. A multi-biometric system reported by Bartlow and Zekste is illustrated in

Figure 6. It can be seen that the multi-biometric system depend on more than one basis of biometric feedback and can be used to cover lacks from one biometric signal. Debatably, such systems can also provide other sources, such as biographical, traveling document-based, etc. [10]

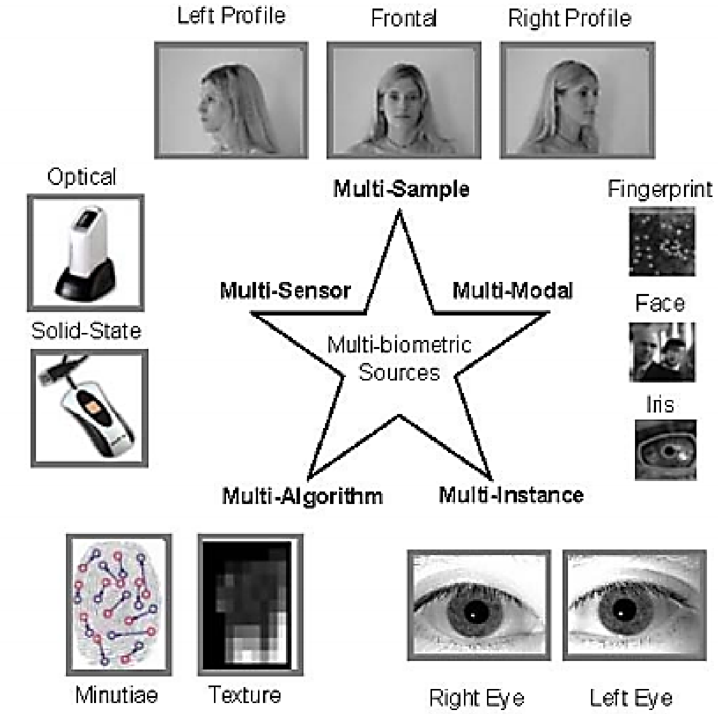

Figure 6 : Multi-biometric system from Bartlow and Zekster, 2009 [10]

Another example of the integration of biometric data is the attack tree presented by Schneier, as he performed a qualitative method to present a security risk analysis. [11] In his model several sorts of biometric approaches are created as shown in Figure 7.

It is worth noting here that the sophistication of the biometric authentication approach from (single/multi) factor monomodal to (single/multi) factor multimodal biometric authentication methods, a higher security advantage is produced. [12]

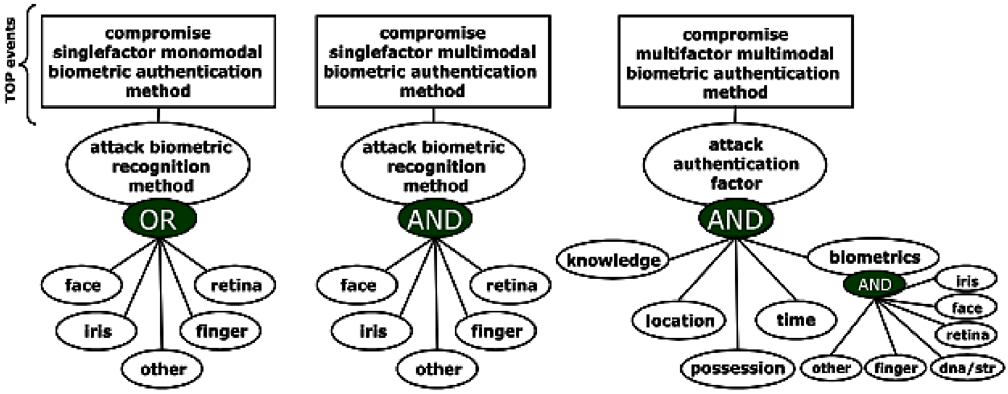
TOP events
compromise singlefactor monomodal biometric authentication method
attack biometric recognition method
OR
face
retina
iris
finger
other
compromise singlefactor multimodal biometric authentication method
attack biometric recognition method
AND
face
retina
iris
finger
other
compromise multifactor multimodal biometric authentication method
attack authentication factor
AND
knowledge
biometrics
AND
iris
face
retina
location
time
possession
other
finger
dna/str

Figure 7: General attack trees for (single|multi)factor (mono|multi)modal biometric authentication methods. [11]

Merging several biometric data is used to increase system precision.

Population base, reduction of failures to enroll

In any biometric system there are a number of issues that should be considered, in particular:

Acceptability, which determines the degree to which individuals are able to accept the use of a specific biometric identifier (characteristic) in their everyday lives. Efficiency, which can relate to many factors: (i) The accuracy and the speed of the recognition achieved. (ii) The specifications of the needed resources. (iii) The organizational and environmental factors.

After contemplating security risk of biometric verification strategies, scientists have come to more secure and dependable prototypical research arrangements like the one presented by Hong and Jain, with multimodal biometric strategies (biometric combination procedures) [13] and with multifaceted multimodal biometric validation techniques by Br¨omme and his co-worker. [12]

An example of High-Level Component and Process Model for Integrated Security Risk Analysis of Biometric Authentication Technology is introduced by Eric P. Haas [12] As shown in Figure 8, his model is applicable for several researches and models such as the one published by Schneier, as he presented attack trees, a general attack tree for different types of biometric methods can be constructed showing a security risk analysis in a qualitative way, [11] and the one published by Leveson for safety analysis technique of fault trees. [14]

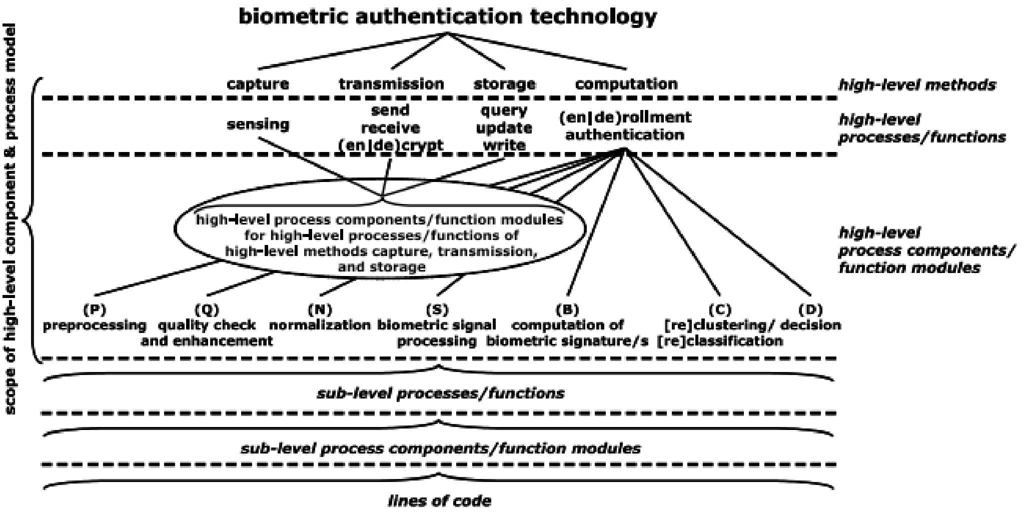
biometric authentication technology
capture
transmission
storage
computation
high-level methods
sensing
send
receive
(en|de)crypt
query
update
write
(en|de)rollment
authentication
high-level processes/functions
high-level process components/function modules for high-level processes/functions of high-level methods capture, transmission, and storage
high-level process components/ function modules
(P) preprocessing
(Q) quality check and enhancement
(N) normalization
(S) biometric signal processing
(B) computation of biometric signature/s
(C) [re]clustering/ [re]classification
(D) decision
sub-level processes/functions
sub-level process components/function modules
lines of code
scope of high-level component & process model

Figure 8: High-Level Component & Process Model for integrated Security Risk Analysis of Biometric Authentication Technology [12]

Figure 8 shows that the security attacks on biometric technology can be classified using three specific categories:

- Sensor abuse (copy, falsification, similarity attacks),
- attacks on data exchange (replay attacks) and
- Attacks on the servers (integrity attacks).
- Software attacks and thus provides a clear understanding of the biometric processes used in bio-authentication technology. [15]

RISK BASED SECURITY “APPROACH”

Modern risk analysis frameworks for bio-authentication technologies are limited to admission and identification/verification procedures with bio-algorithms primarily considered to be running as part of the system with no clear indication of how they operate.

US-VISIT Program stated that the core of any biometric identification system is the database, which has all the previously stored biometric characteristics for base comparison. [16] Data base life-cycle can be divided into four phases: (i) collection, (ii) use, (iii) disclosure, processing, and (v) retention-destruction. [16]

Governments follow many protocols to keep these data in high privacy level as there are many arguments from civil libertarians regarding the accumulation of such personal data and numerous citizens are anxious about governmental intrusion which cause a little discomfort for the individual. For instance, the DHS Chief Privacy Officer claimed that if the databases were combined, the government would enforce strict regulations on which agencies could use traveler information and how it could be accessed." [17]

The literature point to the risk-based security agenda for aviation passenger screening which has been adopted by the TSA for many different exploratory pilot programs in 2011. Taken into consideration, these risk-based methodologies will improve checkpoint efficiency while decreasing aviation customer waiting time.

The aim of the second part of Biometric Systems in Aviation is to review governmental programs, which have combined biometrics into their Airport's security measures to develop the Efficiency and sustainability. This review enables us to have a background on how to integrate biometrics into the current Risk-Based Security Aviation Passenger Screening Program. Biometric technologies are a fundamental part of the improvement of more suitable and ensured travelers procedure frameworks. However, these developments are declined in many cases. There is an essential requirement for data sharing on optimized practices and lessons learned in order to have the compounded configuration. A case study will be implemented in the second part of Biometric Systems in Aviation as an example of the usage of biometric systems in airport security. This case study took place in the USA discussing the Engineering structure of their biometric systems and how it contributes to making the out of the best results. In the USA, the Transportation Security Administration (TSA) coordinates capricious safety efforts, both seen and concealed for top-notch administration. Integrating biometric frameworks is one of TSA service.

Combining productive biometric innovation that approves a person's identification will restore the skillfulness of the screening framework since biometrics offers more predominant security and availability than conventional methodologies of individual identification. Thus, Biometrics are features that can supplant or improve existing technologies. This paper will give an overview on how biometrics can lift key features of the passengers processing at the airport's terminals and it will discuss the massive numerous new opportunities emerging from improved biometric innovations and strategies, intelligent utilization of organized information and modern public/private organizations. Finally, new models for airport security and biometrics will be reviewed with actual experiments for well-known contributors in the aviation industry.

CONCLUSION

This paper has presented several aspects for biometric modalities and biometric systems used in airport security. Presently biometric technology is swiftly improving, but it is not fully mature and in some cases it does not operate in the proper way.

In terms of sensibleness, the improvements obtained by biometric technology as it now stands do not offer the gains in security that are expected with the corresponding invasion of privacy that occurs when biometric technology is implemented.

REFERENCES

[1] Transportation Security Administration: "49 U.S. Code § 114 - Transportation Security Administration | US Law | LII / Legal Information Institute". Law.cornell.edu. Retrieved 2016-08-08..

[2] Őszi Arnold, Kovács Tibor: „Theory of the Biometric-based Technology in the field of e-commerce” Óbuda University – CINTI 2011 – 12th IEEE International Symposium on Computational Intelligence and Informatics, 2011. nov. 21-22. ISBN: 978-1-4577.

[3] National Research Council of the National Academies. Biometric Recognition Challenges and Opportunities. Research Report, Engineering and Physical Sciences, National Academy of Sciences, Washington: National Academy of Sciences, 2010..

[4] B. a. I. M. N. S. a. T. C. W. N. 2. National Science and Technology Council. Biometrics in Government Post 9/11. Report.

[5] ACI World Headquarters • Geneva • Switzerland, The Application of Biometrics at Airports, http://www.aci.aero/media/aci/file/free%20docs/aci%20biometric%20position%20final.pdf.

[6] Accenture, "Insights into Automated Border Clearance." Accenture: High performance. Delivered. Chicago, IL: Accenture, 2010.

[7] Poole, Jr., Robert W. "Airport Security: Time For a New Model." Policy Study 340. Los Angeles, CA: Reason Foundation, January 2006..

[8] Center for Army Lessons Learned (CALL). Commander's Guide to Biometrics in Afghanistan. Vols. 11–25. For Leavenworth, KS: CALL, 2011..

[9] Svetlana N. Yanushkevich and Anna V. Shmerko ,Fundamentals of Biometric System Design: New Course for Electrical, Computer, and Software Engineering Students, 2009, ISBN: 978-0-7695-3754-2 doi>10.1109/BLISS.2009.27.

[10] Bartlow, Nick and Zekster, Gregory. "Holistic Evaluation of Multi-Biometric Systems." BRTRC, October 2009..

[11] Schneier, "Attack trees," Dr. Dobb's Journ. of Softw. Tools, vol. 24, no. 12, 1999..

[12] Eric P. Haas, Back to the Future - The Use of Biometrics, Its Impact of Airport Security, and How This Technology Should Be Governed , Journal of Air Law and Commerce Volume 69 2004..

[13] L. Hong and A. K. Jain, Multimodal Biometrics, in: Jain, Bolle, and Pankanti (eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Press, 1999..

[14] N. G. Leveson, Safeware - System Safety and Computers, Addison-Wesley, 1995.

[15] Bundesamt f¨ur Sicherheit in der Informationstechnik (BSI): Vergleichende Untersuchung biometrischer Identifikationssysteme - BioIS, Bonn, Germany, 2000.

[16] US-VISIT Program, Increment Privacy Impact Assessment, Dec. 18, 2003.

[17] Press Release, ACLU, supra note 180..

[18] Ross, Prabhakar & Jain, An Introduction to Biometric Recognition, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004, supra note 125.

[19] Chris McGinnis, Biometrics boom at the airport,2018, https://www.sfgate.com/chris-mcginnis/article/Delta-other-airlines-bring-biometrics-to-more-12782175.php, Published 11:20 am, Monday, March 26, 2018.

[20] The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3": "The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3" . 9-11commission.gov. Retrieved 2016-08-08..

[21] 2. US-VISIT Data Sheet www.dhs.gov/us-visit.

[22] ACI Media Releases, 2015, http://www.aci.aero/News/Releases/Most-Recent/2015/02/09/Antoine-Rostworowski-joins-ACI-World-as-Director-of-Facilitation-and-IT..

[23] ACLU conference, https://www.aclu.org/other/secure-flight-compared-capps-ii.

[24] BIOMETRICS | SECURITY // JUL 2014, Improving airport security and immigration pain points with a risk-based approach, automation and more choice, http://www.futuretravelexperience.com/2014/07/improving-airport-security-immigration-pain-points-risk-based-a.
[25] US-VISIT FACT SHEET, findBiometrics.com, at http://www.findbiometrics.com/Pages/feature%20articles/usvisit.html, 2004.

Other sources:
https://www.theverge.com/2018/3/9/17100314/british-airways-facial-recognition-boarding-airports
International Journal of Network Security, Vol.2, No.1, PP.52–63, Jan. 2006 (http://isrc.nchu.edu.tw/ijns/)