ANNALS of Faculty Engineering Hunedoara
– International Journal of Engineering
Tome XV [2017] – Fascicule 2 [May]

ISSN: 1584-2665 [print; online]
ISSN: 1584-2673 [CD-Rom; online]
a free-access multidisciplinary publication
of the Faculty of Engineering Hunedoara

[1.] Csaba OTTI

THE PAST, PRESENT AND FUTURE OF BIOMETRICS

[1.] Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, HUNGARY

Abstract: Biometric identification is an electronic system used for establishing the identity of people based on their unique biological and behavioural features. Its history started in the past 50 years, the first scientific publication was published in 1963. This article will review the past, with emphasis on the Hungarian respects of the topic, and the directions of the possible future development.
Keywords: biometrics, history

1. INTRODUCTION

The necessity of trustworthy identification of people was a challenge even in the ancient times. Modern age development raised the need for automatic identification and with that, the first operational systems arrived in the 1970-s in the USA. Following this, the areas of deployment, the available technological solutions and devices spread very fast in security and policing.

The next step of development was the commercial deployment in trade and smart devices. It would be very hard to find any adult that has not met biometry in one way or another in the developed societies.

One of the future research directions will be continuous authentication, which can identify any person during their stay in a particular area with requiring only minimal cooperation from them. This mainly has a security benefit, but it serves as a convenience factor as well.

Experience shows that users like technologies, that are contactless and work from afar – or at least they care less about them. In a security respect, they work better against people, who do not wish to cooperate with the system at all.A further tendency is multiple factor authentication, which can circumvent the drawbacks of the traditional technologies.

Automatized, electronic biometric identification has went through a tremendous development in the past fifty years. Policing organizations have an ever bigger need to identify people in a fast and trustworthy way at any given place. Parallel to this, there is a growing demand for identifying users and people accessing facilities at every aspect of life. [1]On the other hand, it can be clearly seen that the user acceptance of the devices and technologies is one of the determining factors regarding the success and usability of such systems.[2]

In security applications, users are much more suspecting and rejecting than in commercial ones, where they can decide whether they want to use biometry and the templates won't leave their possession – and it is convenient to use them. A good example for this is that while general purpose biometrics are rejected by users [3][4], 89% of iPhone users utilise biometry in their devices[1].

The future direction of biometric identification are outlining, biometry is gaining ground, the convenience is becoming ever more important, and instead of discrete identification location solutions, the continuous, behavioural identification methods are spreading.

2. THE HISTORY OF BIOMETRY

The word Biometry stems from the greek „bios" (life) and „metrein" (to measure) phrases. [5]. As the word shows, it deals with measuring parameters connected to life – parameters that are unique to every person and thus identifies said person with certainty.

[1]Source: http://appleinsider.com/articles/16/04/19/average-iphone-user-unlocks-device-80-times-per-day-89-use-touch-id-apple-says, Time of download: 2016. 11. 12.

Bodily feature based identification itself has a long history. It has been used in the ancient Middle- and Far east to establish the identity of people (e.g. by height, weight, special features, etc.) [6].
The first time the Hungarian police used biometric features to solve a crime (in a way that it became known and understood to the general public) was in 1907. An inn at Dános was robbed, burned down, with for people murdered. The utilised biometric feature was the fingerprint, which was found on wine glasses at the crime scene.[7]
One of the first institutionalized use of biometric data (in this case, fingerprints) was their usage in crime registers. In 1903, New York state prisons adopted fingerprint identification to verify the identity of criminals. This solution spread like wildfire among the various penal institutes and police forces. This process culminated in the founding of the fingerprint analysis department of FBI in the 1st July, 1921.

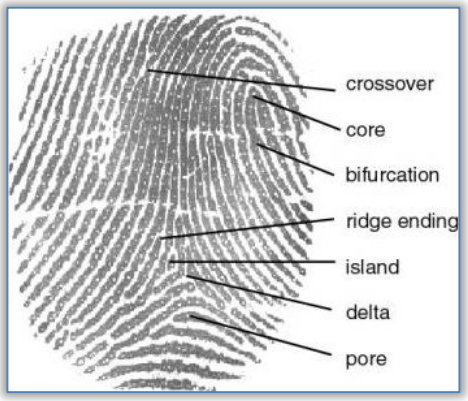

Figure1. Elements of the fingerprint [10]; Source: http://www.barcode.ro/tutorials/biometrics/img/finger3.jpg

A. Bertillon French police officer designed a way to identify criminals by their various bodily features. Unfortunately, the solution could not be automatized and was rather tedious, and as such, was replaced with a more efficient one. Sir F. Galton and others discovered in 1888, that fingerprints are unique to each person, enabling them for usage in identifying their owner [8].
The first automatization attempt can be credited to Woodrow W. Bledsoe [9], who created a semi-automatic facial recognition system in the 1960s USA, at the request of the government. The operator of the system selected important features on the face for the system (e.g. eyes, mouth, ears, etc.) and the machine calculated the geometric relationships between these points.
Fingerprints are identified by minutiae, which are distinctive topological features on the surface of the fingerprint. The following image shows the type of minutiae:
Naturally, the identification process was not yet automatized, it was done by human experts with the help of magnifying glasses.
The next big step in the history of biometrics was the creation of the identification system and databases supporting the process in the 1960s. The result of this was the first version of AFIS (Automated Fingerprint Identification System) [11].
The first commercially available hand geometry identification system was launched in 1974. This can be called the first truly automatized system that could facilitate identification for the purpose of access control and attendance tracking.[12]This system was deployed in 2008 at Paks Nuclear Power Plant in Hungary.

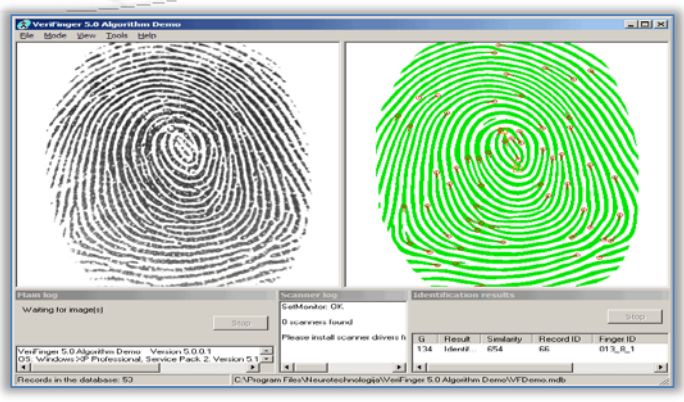
Figure2. The effects of technological development: a fully automated fingerprint recognition system; Source:: http://www.lacp.org/Graphics/fingerprint4.gif

The process continued in 1975, when the FBI launched a project to create a scanner prototype. This system only stored minutiae due to the high cost of data storage equipment. An algorithm was also created – the M40 [13], which was the first operational biometric algorithm ever used by the FBI. Its purpose was that with selecting from the database by user given parameters, it could provide a much smaller dataset for forensic analysts to sift through and perform identification.
In 1985,Drs. Leonard Flom and Aran Safir [14]ophthalmologists discovered that no two identical irises exist. This concept was patented in 1987, and in 1995, an iris scanner prototype was created with the help of Dr. John Daugmann.
In 1987, M. Kirby and L. Sirovich[15]proved that identifying a properly positioned and normalised face requires less than 100 different parameters. This allowed M. Turk and A. Pentlandin 1991 to create the

first algorithm enabling real-time facial recognition.[16] In 2006, the USA introduced biometric passports that stored personal biometric data within an RFID capable chip. [17].The EU allowed this in the same year, and Hungary introduced the new passports in 2009.
The next step in biometric advances was the development of vein scanners by Hitachi. Based on their patent, published in 2009, the first device capable of personal identification was created. It used IR light to penetrate skin and identify the person based on their unique vein pattern. [18]
In 2011, India introduced a mass iris recognition system aimed at making people use their eyes for any matter concerning the state.

3. THE APPLE FINGERPRINT READER

Biometric technologies otherwise known in the security industry did not penetrate general public very well right up until the Apple iPhone 5s was launched. Although, there were prior attempts by other companies to integrate fingerprint readers into laptops and Android based devices, they failed to become widespread. This changed in 2013, when Apple TouchID hit the market. A fingerprint reader was put in place of the physical button, which allowed the user to securely unlock the device. It is important to note, however, that a fallback option must be present as an alternative to the biometric method (which is usually a PIN, password or a pattern lock), so we cannot talk about a truly exclusive application.

Figure3. The Apple TouchID sensor; Source: http://cdn2.knowyourmobile.com/sites/knowyourmobilecom/files/6/25/touch-id.jpg

4. STADIUM ACCESS CONTROL SYSTEM IN THE GROUPAMA ARENA

One of the most relevant applications of biometrics in Hungary is the vein scanner system installed at the Groupama Arena in 2014. Its main purpose to make visiting football matches more secure and family friendly by locking hooligans out and also filter out anybody avoiding ticket purchases. This system uses a two-factor authentication: fans own an RFID card which holds the user ID, based on which the system selects the relevant user from the database. The template is then matched against the sample the user provides to verify the identity of the cardholder. The development[2]was made with devices manufactured in Hungary that use Fujitsu sensors at their core.

Figure4. The Hungarian solution; Source: http://kep.index.hu/

Fan groups, however, were not keen on this idea. As of the 2016 September standing in this issue, they attack the operator from multiple directions. In April 2016 the Authority for Equal Treatment issued a decree that the practice does not restrict any rights.
In 2014, the Társaság a Szabadságjogokért (a non-profit organisation) attacked the practice at the Alkotmánybíróság (AB)[3] on behalf of a football fan. The problem lies within the handling method of the biometric data[4], as it is held– although anonymously – in a central database. At the request of the AB, the NAIH[5]performed an analysis, which concluded that the solution endangers the users, as any abuse of the database would allow for acquisition of personal data, and also, users might get monitored without their knowledge or consent.
With the decision of the AB, a strong precedent might be set regarding the storage and usage of biometric data, which will affect the future of biometric system. It will determine which systems can be operated and what technologies must be used to minimize the possible harm to the users.

5. THE NEW HUNGARIAN PERSONAL IDENTIFICATION CARD[6]

Hungary issued personal ID cards capable of holding biometric data in 2016. It is a basic credit card format plastic card, but with an RFID antenna and a memory chip. The ID card can hold fingerprints,

[2]http://index.hu/sport/futball/2014/07/30/venaszkenner/
[3]Constitutional court – the highest authority court in Hungary
[4]https://www.dropbox.com/s/c0dt2rt1fyjkg64/NAIH-2016-1729-2-V-1m.pdf?dl=0
[5] National Data Protection Authority
[6]http://nol.hu/belfold/tul-okos-aza-uj-szemelyi-igazolvany-1584895

social security numbers, tax ID numbers and any penalties afflicting the particular person (like travel restrictions). The system conforms with the data protection questions as the template is stored on the card itself. In 2016, Ghana announced that they will be using biometrics to verify voter identity in the parliamentary elections.

6. WINDOWS HELLO [19]

With the first Anniversary Update of Windows 10, a new identification system was introduced to unlock the computer, log in and identify accounts. The service is called Windows Hello and it allows for PCs to use a lightweight, native biometric solution.

The system supports multiple technologies, and currently works on PCs and Surface devices with built-in fingerprint readers, but the list will expand continuously in the future.

The biometric template in this case is stored on the user device and identification is performed locally. [20]The solution is not compulsory, the user can use any former login solution as well. Note, that by biometric template, the system means a code that was created from the presented sample. Microsoft says that they never save any actual biometric sample.

7. THE FUTURE

Traditional biometric solutions are not unerring and several factors rose during their use that may be avoided with the technology of the future.

1. Traditional technologies require serious will from the user to cooperate with the system[7].[21]A solution for this is to expand the range of identification, for example, with camera systems.
2. Multi-factor authentication can circumvent the shortcomings of the individual technologies and make the usage of the systems much easier.
3. An attacker, if able to pass through discrete identification locations may move freely within a facility or network. Behavioural biometrics analyse people real time, and can force the users to re-identify themselves if any suspicion rise.

One direction of development is to use behavioural biometric identification methods. These generally deal with unique features which can be analysed without cooperation from the user. Examples to these technologies are signature identification, keystroke identification or gait analysis.[22]

Figure5. Example for motion and gait based identification; Source: http://i.kinja-img.com/gawker-media/image/upload/t_original/19fh0dw40y2xypng.png

Motion and gait based systems can work by several ideas. The first – and commercially more feasible – solution is video based. In this case, the gait and movement of the person are recorded by cameras and software based analysis determines the identity. [23]

Another possible solution is to use sensors on the user (e.g. an accelerometer) which are generally available in one or more smart devices already held by the user. [24]

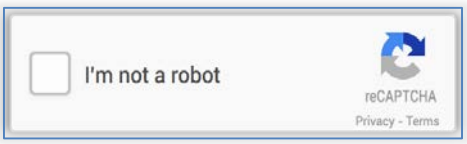

Figure 6. Google reCaptcha interface; Source: https://upload.wikimedia.org/wikipedia

Gesture based identification is another type of behavioural biometrics. This is most feasible with touchscreen devices. Algorithms analyse the characteristics of the motions of the user fingers (such as length, strength, direction of strokes), which are unique to every user.

A more basic version of this technology is Google ReCaptcha, which protects websites from bots. The technology [25]uses the gestures – along with other parameters – to determine whether the visitor is a human or a program. If there is sufficient data to verify identity, clicking the checkbox will automatically

[7]The will to cooperate with the system is a that describes the willingnes of the user to position the sample such that it conforms with all the requirements of the device to perform successful identification.

solve the challenge. If not, then the program will present a picture puzzle that is only solvable by humans (e.g. select a type of animal out of 9 images).
With the help of the solution, the required willingness expected from the user can be lowered along with the complexity of the task. With the proper amalgamation of the technologies, Continuous Authentication can be realized[26], which would allow to identify a person continuously as long as they stay within a location.

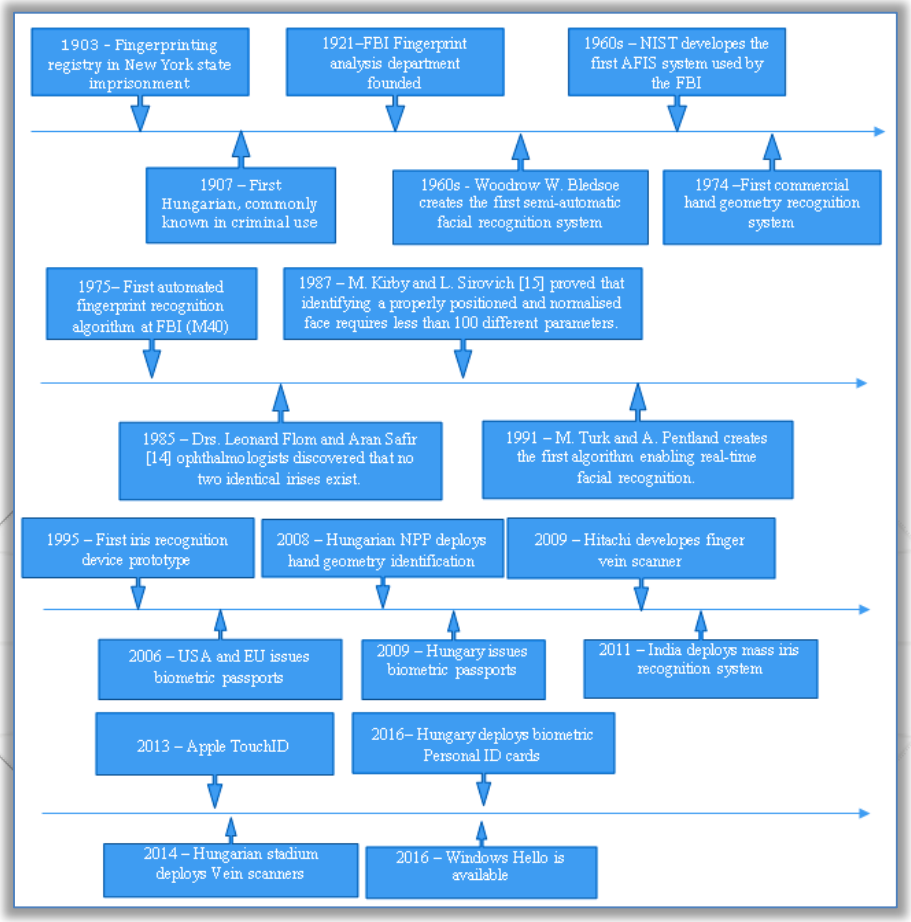

Figure 7. The timeline of biometrics

8. CONCLUSION

By studying the history of personal identification, we can see that with the increasing risk factors and the secure and convenient solutions offered, biometry found its way into the lives of the general public. It is a real possibility and requirement for automated systems in the near future to identify users with a very high degree of confidence and in real time.
Biometry has already spread wide with the help of smart mobile devices and it increases acceptance significantly.
Beyond this, the general directions of development can be determined, and continuous, automated authentication methods that use multiple modalities seem to be the ones with the brightest future.

References

[1.] Csaba Otti, „Why does it fail to operate?," FIKUSZ, 2016
[2.] M. M. Dillon, „User acceptance of new information technology: theories and models.," Annual Review of Information Science and Technology, %1. kötet31, pp. 3-32., 1996.
[3.] F. B. H. S. Suplicz Sándor, „Írisz felismerésen alapuló beléptetı rendszer által keltett attitődök és averzív reakciók vizsgálata.," in 6. Nemzetközi Mechatronikai és Biztonságtechnikai Szimpózium, Budapesti Műszaki Főiskola, 2006.
[4.] K. T. Földesi Krisztina, Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendsze-rek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára, Securinfo, 2015.
[5.] D. K. Tibor, Szerző, Biometrikus azonosítás. [Performance]. Óbudai Egyetem Bánki Donát Gépész- és biztonságtechnikai kar, 2015.
[6.] B. József, A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelı hatása a határ- és közbiztonság alakulására, Budapest, 2013, p. 75.

[7.] F. Krisztina, PhD Értekezés, Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2017.
[8.] K. N. A. R. Anil K. Jain, „50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," Pattern Recognition Letters, p. 6, 2016.
[9.] D. R. J. J. J. Jigar M. Pandaya, „A Survey of Face Recognition approach," International Journal of Engineering, %1. kötet3., %1. szám1., pp. 632-365, 2013
[10.] K. J. S. P. Salil Prabhakar, „Learning fingerprint minutiae location and type," Pattern Recognition, %1. kötet36., %1. szám8., p. 1847–1857, 2003.
[11.] E. T. C. L. W. Michael D. Garris, „NIST Fingerprint Evaluations and Developments," Proceedings of the IEEE, %1. kötet94., %1. szám11., pp. 1915-1926, 2007.
[12.] Csaba Otti, „Comparison of hand geometry and fingerprint based identification," in Proceediengs of the 3rd international conference and workshop Mechatronics in Practice and Education, MECHEDU 2015, Subotica, Serbia, 2015.
[13.] J. Loudermilk, Szerző, The FBI Fingerprint Program. [Performance]. FBI, 2016
[14.] S. Leonard Flom, „Iris recognition system". Amerikai Egyesült Államok Szabadalom száma: US 4641349 A, 3 február 1987.
[15.] L. S. a. M. Kirby, „Low-dimensional procedure for the characterization of human faces," Optical Society of America, %1. kötet4., %1. szám3., pp. 519-524, 1987
[16.] P. M. Turk, „Eigenfaces for Recognition," Journal of Cognitive Neuroscience, %1. kötet3, %1. szám1, pp. 71-86, 1991.
[17.] M. C. J. O. Jeffrey Stanton, „ICAO and the Biometric RFID Passport: History and Analysis," Syracuse University, School of Information Studies, Syracuse, NY 13244
[18.] N. T. M. Naoto Miura, „Personal identification device and method". Amerikai Egyesült Államok Szabadalom száma: US 7526111 B2, 28 április 2009.
[19.] M. Support, „What is Windows Hello?," Microsoft, 29. szeptember 2016. [Online]. Available: https://support.microsoft.com/en-us/help/17215/windows-10-what-is-hello. [Hozzáférés dátuma: 10 november 2016].
[20.] Microsoft, „Windows Hello and Privacy," Microsoft , 2016. [Online]. Available: https://privacy.microsoft.com/en-us/windows-10-windows-hello-and-privacy. [Hozzáférés dátuma: 10 11 2016].
[21.] Csaba Otti, „Classification of biometric access control systems based on real-time throughput," in Proceedings of Fifth International Scientific Videoconference of Scientists and PhD. students or candidates, Bratislava, 2015.
[22.] P. Kenneth Revett, Behavioral biometrics, A remote access approach, United Kingdom: Wiley, 2008.
[23.] C. C. R. D. L. S. Benabdelkader, „Person Identification Using Automatic Height and Stride Estimation," IEEE International Conference on Automatic Face and Gesture Recognition, 2002.
[24.] M. O. N. C. B. P. a. B. C. Derawi, „Unobtrusive User-Authentication on Mobile Phones using Biometric GaitRecognition," Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010.
[25.] Google, „Google reCAPTCHA," Google, [Online]. Available: https://www.google.com/recaptcha/intro/index.html. [Hozzáférés dátuma: 10 11 2016].
[26.] X. G. Liang Wang, Behavioral Biometrics for human identification: Intelligent applications, Hershey - New York: IGI Global, 2010.
[27.] C. C. Club, „Chaos Computer Club breaks Apple TouchID," 2013.
[28.] T. Matsumoto, Szerző, Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies. [Performance]. 2002.