Interdisciplinary Description of Complex Systems 21(2), 206-213, 2023

METHODOLOGICAL AND HEALTH REASONS FOR UNSUCCESSFUL BIOMETRIC IDENTIFICATION

Andras Pallagi[1,] * and Aliz Persely[2]

[1]Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

[2]Semmelweis University Doctoral School of Theoretical and Translational Medicine
Budapest, Hungary

DOI: 10.7906/indecs.21.2.10
Regular article

Received: 19 May 2022.
Accepted: 9 February 2023.

ABSTRACT

Nowadays, the use of biometric identification procedures is becoming increasingly widespread making our lives more convenient and safer at the same time - due to their uniqueness.- from mobile phones through access control systems to the official use of biometric identifiers.

However, proper identification can be hampered by a number of errors, when either an incorrectly chosen method or even the health condition of the person may cause a problem.

Our research examined the main causes of failed identification procedures through examples. The obtained result can provide guidelines for the selection of the optimal identification methodology and determine their development directions.

KEY WORDS

biometrics, identification, twin research

CLASSIFICATION

ACM: I.2, I.5

JEL: O33

PACS: 42.30.Sy

*Corresponding author, η: pallagi.andras@uni-obuda.hu; +36 703837237;
OE-BDI office, Nepszinhaz str. 8, H – 1081 Budapest, Hungary

INTRODUCTION

Biometrics, as a term, derives from the combination of the Greek words "bio" – life and "metric" – i.e. the measurement of the physiological characteristics of an organism. In our present case, this living entity is a human, whose biometric characteristics are the basis of determining their identity. Thus, biometric identification is a process that requires an automatic technique that measures and records a person's unique physical characteristics and behavioural traits, and uses them for identification and authentication purposes. Biometric recognition may be used for the purpose of personal identification, where the biometric system identifies the person by searching for a match in the whole registered data file, and it may be used for verification purposes, when the system authenticates a person based on previously recorded and stored samples.

BIOMETRIC IDENTIFICATION

Biometric identification methods can be divided into two groups based on the individual biological or behavioural characteristics that differ from person to person:

BIOLOGICAL CHARACTERISTICS

- skin pattern: fingerprint, palm print, footprint,
- hand and face geometry (2D, 3D),
- vascular/vein network (typically: palm, wrist, finger),
- facial features, facial thermal image,
- iris and retina pattern,
- fragrance, the combination of body fluids,
- heart rate,
- DNA genotype, white blood cell antigen.

BEHAVIOURAL CHARACTERISTICS

- voice,
- walking, posture,
- handwriting,
- typing dynamic, habits.

The identification and measurement process consists of the following steps:

1) The sensor detects the required biometric sample from the person.
2) From the whole sample, the program highlights the characteristic (identifiable) features.
3) The comparison algorithm compares a detected sample with samples pre-recorded in its database and evaluates it.
4) The comparison generates an identification response, i.e., a match or no match.

Four specific characteristics can assess the efficiency and reliability of identification systems:

- False Rejection Rate (FRR),
- False Acceptance Rate (FAR),
- Crossover Error Rate (CER),
- Failure to Enroll Rate (FER).

An erroneous denial is when the access control system denies access to an authorized user. There are several possible reasons, such as incorrect sampling or even a timeout for sample evaluation. In case of false acceptance, the algorithm identifies unauthorized persons as

authorized, which may be due to sample tampering or incorrect algorithm assessment. The same error rate has been introduced for the objective comparison of different types of identification systems. The crossing error rate describes the point where FRR and FAR are equal, thus describing the overall accuracy of the biometric system. Below the probability of a coverage error, it shows us the number of chances that someone will fall out of the biometric measurement.

The most important of the above mentioned four characteristics is the FAR index, which shows us the proportion of wrongly identifying an unauthorized person as eligible.

FAR indicators of some biometric systems (informative, device-specific data) [1]:

- voice identification, voice analysis: 200 … 1 000: 1;
- face recognition (2D, 3D): 2 000 … 10 000: 1;
- hand geometry analysis: 10 000 … 100 000: 1;
- vein network identification: 100 000 … 1 000 000: 1;
- fingerprint identification: 100 000 … 1 000 000: 1;
- iris, retinal examination: 10 000 000: 1.

In addition to the aforesaid, the efficiency of biometric systems can be measured by the following seven essential criteria [2]:

1) Universality: Every individual accessing the application should possess the trait.
2) Uniqueness: The given trait should be sufficiently different across individuals comprising the population.
3) Permanence: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.
4) Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.
5) Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
6) Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
7) Circumvention: This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioural traits.

TECHNICAL AND METHODOLOGICAL REASONS FOR IDENTIFICATION FAILURE

Most biometric identification systems in use today typically use a single biometric feature to establish identity (i.e. they are unibiometric systems). It is essential to know the vulnerabilities and limitations of these systems. Below are some of the challenges that biometric systems often face.

THE DETECTED DATA IS NOISY, INCORRECT

The scanned biometric data will be noisy due to inadequate data collection or minor differences in the biometric feature. Such a discrepancy could be a damaged or bloated fingerprint. Due to extreme weather conditions, the evaluation of the venous map may also be incorrect.

INVOLVEMENT ERROR

There may be cases where the identification system is unable to obtain the biometric data required for identification from the user. For example, lesions in the iris or fingerprint due to disease cannot be identified. The conditions and rules must be established under which these persons may also be included in the identification system.

UPPER LIMIT OF IDENTIFICATION ACCURACY

The matching performance of a one-factor authentication system cannot be improved indefinitely. During identification, it compares templates made from predefined sample parts with the perceived biometric feature, but there is also an upper limit to using a sample that can be recognized based on the templates.

The number and complexity of each sample depend on the biometric feature. For example, fingerprints have far fewer template patterns than irises.

ATTACKABILITY

Many physical and behavioral biometric features are attempted to be falsified and copied. Fingerprints and palm prints are reproduced on a silicone-based surface. An IR photo can be used to create a device that deceives venous scanners. Behavior, gait, and speech imitation may also be part of the attacks.

To minimize the challenges outlined above and the associated errors, and to maintain the trust of those involved in the identification, we should strive to select the appropriate identification system. The following parameters must be considered when choosing the optimal biometric identification system:

- operating temperature, humidity, dust content,
- number of users, religious, ethnic composition,
- identification time,
- the working environment of the persons to be identified,
- simple integration with existing systems,
- the cost of the system.

It is essential to consider the operating temperature and humidity range specified in the manufacturer's instructions to use the identification devices properly. In some cases, environmental dust limits are also set. Ignoring the operating parameters, in most cases, increases the identification time and the FRR.

The number of individuals to be identified and their religious and ethnic composition are essential considerations in selecting the appropriate system. The throughput of the identification system should be designed depending on the number of people. The religious habits of some individuals may make biometric identification impossible. For example, Muslim women wear the niqab and burqa, which partially or wholly cover the face.

Identification time is also an important parameter when selecting a biometric identification method.

Rapid identification is not required in cases where individuals need to be identified infrequently or in small numbers. Where a large group needs to be identified, identification time can be a very important consideration to avoid congestion. For example, when changing shifts in large companies, the goal is to direct the crowd to the exits at the same time as fast as possible. In such cases, a palm vein scanner or facial recognition system may be a good solution.

The last parameter contains a description of the user's work environment. There are a number of work environment parameters that can impair the efficiency of biometric identification. This can be the case with a wet work environment, which causes the fingers and palms to become damp and swollen.

For example, the fingerprints of people who fold paper temporarily disappear, as the folds wear off. There are chemicals that also temporarily destroy fingerprints (instant glue, acids).

HEALTH REASONS FOR IDENTIFICATION FAILURE

Our research also examined biometric identification errors deriving from the users going through identification procedures. In addition to individual behaviour, we have identified health reasons that make clear or impede clear biometric identification. The list does not include injuries caused by accidents.

HEALTH CAUSES THAT IMPEDE RECOGNITION OF IRIS AND RETINA

- Aniridia, i.e. an eye without an iris. It occurs in one in every 50 000 to 100 000 newborns.
- Ptosis is known as the sagging of the upper eyelid and the patient usually complains of visual and cosmetic damage. It may be congenital or acquired, or it may be of neurogenic, myogenic, aponeurotic, mechanical, or traumatic origin.
- Endophthalmitis is defined as an inflammation of the inner coats of the eye. If not properly treated or neglected, it may even require the surgical removal of the eyeball.
- Cataracts, also known as cloudy lens. The lens is positioned behind the iris.
- Trichomegaly, i.e. abnormally long eyelashes. Eyelash trichomegaly can have several different causes. These causes can include both genetic inheritance and environmental causes (such as side effects of certain drugs).

HEALTH REASONS THAT MAKE FINGERPRINT RECOGNITION IMPOSSIBLE:

- severe hand eczema, also known as hand dermatitis, is a common disease. Genetics o contact allergens or irritating substances play a role in "triggering" this form of eczema [3].
- fingerprint smoothness. One of the side effects of paclitaxel and capecitabine for the treatment of cancer is the smoothing of fingerprints [4].

HEALTH REASONS THAT MAKE FACIAL GEOMETRY AND VEIN RECOGNITION MORE DIFFICULT:

- facial nerv paralysis, such as stroke or Bell's palsy,
- side effects of Botox treatments.

HEALTH REASONS FOR THE UNRECOGNIZABILITY OF SPEECH/VOICE:

- changes in sound characteristics due to Parkinson's disease [5],
- speech may change due to diseases affecting the sound-producing organs (throat, mouth, nose).

CAUSES OF DNA IDENTIFICATION ERRORS

- after a bone marrow transplantation, the sequence of the donor DNA will also be detectable, distorting identification,
- nearly identical DNA sequence of monozygotic twins (the difficulties with monozygotic twins are covered in the next section) [6].

ANOMALIES IN THE BIOMETRIC IDENTIFICATION OF TWINS

Authentication of identical twins might be the most challenging area in the biometrical field Therefore, the number of twins studies have been increased to achieve better methods. It is well-known that monozygotic twins share almost 100 % of their genetical background, but not only their genes are closely the same, they also have great similarity in phenotypical appearance. However, there are differences between them, which are mostly caused by epigenetics and environmental factors [6]. A previous study revealed that false accept rate for the recognition of monozygotic twins might be 2-6 % [7].

Literature data in biometrical identification of the monozygotic twins is mostly about face recognition, fingerprint and palmprint matching, iris and retina recognition, speaker recognition and handwriting. However, the need of proper detection initiated more studies to be conducted about multimodal matching systems [7-9].

Fingerprints are known to be personally unique, the ridges are formed during fetal development and they remain the same across the whole lifespan, unless skin damage occurs. Previous studies confirmed that fingerprint class, ridge width, depth and separation are significantly shared by monozygotic twins. Although they show huge similarities compared to fraternal twins, they also have minor differences, and this way, monozygotic twins can be distinguished by their fingerprints, especially when they are using and rotating both thumbs [8, 10]. It was observed by Kong et al. that the palm print of identical twins have correlated characteristics, and the discrimination is possible [8].

The patterns of irises were also found to be similar and reliable sources of identification [8].

The voice recognition of twins has also been studied, because the sounds are assumed to be same due to for example their anatomical resemblance [8].

The accuracy of recognizing images of monozygotic siblings is the most problematic part, because by manual face detection it was around 78,82 %, in a study where features like moles, scars, freckles were used for the correct answers. Currently, however, automatic face detection processes are quite promising and show better results. [8]

Multimodal studies are emerging in the field of biometric twin examinations. Sun et al. observed the recognition of iris, fingerprint and face patterns. They found that only some or none degradation in performance was shown when using the iris and the fingerprint, but there were difficulties when only the face matchers were regarded [8].

Priya et al. found in their multimodal study that the accuracy of matching was 93,62 % using only fingerprints, 95,2 % using only lip prints and 91,27 % using facial patterns, while the combination of these three methods altogether meant 93,36 %. [9] Combining facial recognition and skin surface texture analysis can increase the accuracy by 20 to 25 % [8].

MULTIMODULAR IDENTIFICATION SYSTEMS

Multimodular identification systems have been developed to increase the level of security. However, the individual parameterizability and fine-tuning of the system identification methodologies can eliminate the identification difficulties associated with technical or health reasons in one-factor identification systems. Using properly defined rules, individuals who have been excluded from single-factor systems can also be included in the identification.

The multimodular identification system can use:

- only biometric identification,
- biometric and knowledge-based identification
- biometric and object-based identification.

The most common multimodular identification systems based on biometric characteristics only:

- fingerprint and finger vein recognition system,
- hand geometry and hand vein network recognition system,
- facial geometry and facial venous recognition system,
- face and write recognition system,
- face and ear geometry recognition system.

Biometric identification and knowledge-based combined identification systems:

- finger or palm print and pin code,
- voice and password phrase (for example, telephone-based authentication),
- face/iris and pin code.

In the case of biometric identification and object-based combined identification systems, the object is typically an access card or token. In many cases, the HASH code generated from the holder's biometric characteristics is stored in the access card's chip portion. Typically, the following combined systems are developed:

- fingerprint or palmprint and access card,
- palm vein and access card (e.g., in stadiums, in sports facilities).

Many other combinations are possible, but in most cases the above combinations are used to reduce the cost of installing the system.

CONCLUSION

According to our research, the majority of misidentifications were due to a poorly chosen biometric identification system. Neither the health status of the user group nor the installation environment of the system was taken into account. In the examined one-factor access control systems, there were identification points where the system operator preferred to turn off biometric identification because of the high reading time. We have experienced a loss of trust in the identification system due to a series of false rejections.

Where multimodular identification (both biometric or biometric-card) is used, it is possible to define and/or rules. This will allow better parameterization of the identification system and reduce the rate of false rejections.

Observations on monozygotic twins have highlighted that most one-factor identification systems are not able to adequately handle nearly identical biometric features. In this regard, we recommend the development of detection resolution.

The present research will be continued in two separate directions. It will further investigate the biometric identification anomalies associated with monozygotic twins, and determine the basic system requirements that will help to select the optimal access control system.

ACKNOWLEDGEMENTS

The research on which the publication is based has been carried out within the framework of the project entitled " How do we imagine? About cobots, artificial intelligence, autonomous vehicles for kids". Project no. MEC_N-141290 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the MEC_N funding scheme (affiliation: NextTechnologies Ltd. Complex Systems Research Institute).

REFERENCES

[1] Fialka, G. and Kovács, T.:*The vulnerability of biometric methods and devices.* Annals of the Faculty of Engineering Hunedoara **14**(3), 45-48, 2016,

[2] Jain, A.K.; Flynn, P. and Ross, A.A., ed.: *Handbook of biometrics*. Springer Science & Business Media, 2007,

[3] Lee, C.K., et al.:*Fingerprint changes and verification failure among patients with hand dermatitis.* JAMA Dermatology **149**(3), 294-299, 2013, http://dx.doi.org/10.1001/jamadermatol.2013.1425,

[4] Azadeh, P., et al.: *Fingerprint changes among cancer patients treated with paclitaxel.* Journal of Cancer Research and Clinical Oncology **143**(4), 693-701. 2017, http://dx.doi.org/10.1007/s00432-016-2314-1,

[5] Hashiyada, M.: *DNA biometrics*. IntechOpen, 2011,

[6] Holmes, R.J.; Oates, J.M.; Phyland, D.J. and Hughes, A.J.: *Voice characteristics in the progression of Parkinson's disease.* International Journal of Language & Communication Disorders **35**(3), 407-418, 2000, http://dx.doi.org/10.1080/136828200410654,

[7] Bowyer, K. W. and Flynn, P. J.: *Biometric identification of identical twins: A survey*. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, Niagara Falls, pp.1-8, 2016, http://dx.doi.org/10.1109/btas.2016.7791176,

[8] Shalin, E.S.; Bino,T.; Kizhakkethottam, J.J. and Kizhakkethottam, J.J.: *Analysis of effective biometric identification on monozygotic twins*. In: 2015 International Conference on Soft-Computing and Networks Security (ICSNS). IEEE, Coimbatore, pp.1-6, 2015, http://dx.doi.org/10.1109/icsns.2015.7292444,

[9] Lakshmi Priya, B. and Pushpa Rani, M. :*Authentication of Identical Twins Using Tri Modal Matching.* In: 2017 World Congress on Computing and Communication Technologies (WCCCT). IEEE, Tiruchirappalli, pp.30-33, 2017, http://dx.doi.org/10.1109/wccct.2016.17,

[10] Rahat, M.A., et al.: *Monozygotic and dizygotic twins differences in fingerprint patterns of swat district*. Advancements in Life Sciences **7**(4), 232-236, 2020.