RELIABILITY OF SELECTED BIOMETRIC IDENTIFICATION SYSTEMS

Veronika ŠTEKEROVÁ[1]

[1]*Department of Vehicles and Ground Transport, Faculty f Engineering, Czech University of Life Sciences Prague*

Abstract
Biometric identification systems are increasingly being used today. Face recognition biometry is the second most common biometric identification right after the fingerprint recognition. The paper is focused on the reliability of systems in difficult conditions, which were gradually simulated and the time of acceptance or incorrect rejection of the user was measured. Measurements were made in a laboratory environment where two biometric sensors were available.
The results show that the time of acceptance or rejection was to some extent influenced by the users themselves. Users have influenced the system with their reference frame, their position and facial expression in front of the reader. The paper showed these biometric readers are not suitable for areas where difficult conditions can occur.

Key words: *biometrics; face recognition; identification; difficult conditions.*

INTRODUCTION

The face is one of the best known biometric features. It is intuitively used every day without a person realizing that now there is a biometric identification. The ability to respond to facial stimuli is one of the first cognitive functions acquired by newborns (*Rak, Matyáš & Říha, 2008; Eysenck, Michael & Keane, 2010).* It is the most natural and widely used method of identification with a high level of reliability. In fact, the human brain stores the faces of people with whom it comes into contact. However, biometric identification itself is known for over 30 years, although identifying people by recognizing human faces is as old as humanity itself *(Ježek, 1996).*
Due to the development and development of technology, the cost of manufacturing of electronic components is constantly decreasing, making biometric systems affordable. Biometric identification systems are increasingly being used today, in quite common devices such as mobile phones or computers. Due to their high reliability they are not only suitable for smaller or larger companies and corporations, but they are the main domain of the army, securing nuclear weapons, sharply guarded financial sector, stadiums, airport areas, reception of major sites or other significantly guarded places and locations. Governments all over the world demand for biometric security of integrated border protection systems. In the commercial sector, biometric security systems are among the main factors that attract potential clients, as identity protection and cyber-attack prevention are in high demand today (*Drahanský, Orság, 2011).* The aim of this study is reliability of selected biometric identification systems under difficult conditions.

MATERIALS AND METHODS

The whole measurement took place in the laboratory of the department where constant conditions were ensured. Two biometric readers were available in the laboratory to recognize the face-based user. It was a biometric reader Multibio 700 and Aktion AFT-500.

Biometric Reader Aktion AFT-500

Biometric Reader Aktion AFT-500 (Fig. 1) is a terminal with built-in face recognition system, integrated card reader and keyboard. It is a biometric face reader that supports identification (1:N) as well as verification (1:1). The verification method is possible with a combination of RFID card / chip or PIN code. The reader processor has a frequency of 600 MHz. The device is designed with IP54 protection, which allows it to be used outdoors, where higher water contact is expected.

Biometric Reader Multibio 700
This reader, which can be seen in Fig. 2, is elegant, robust, and ergonomic in design, combining face recognition, fingerprinting, and PIN added to the integrated RFID module. It captures the relative position, size and shape of the user's eyes, nose, cheekbones and jaw. The reader enables identification (1:N) and verification (1:1).

Luxmetr - CEM-DT-8809A
Another equipment used is the Luxmeter - CEM-DT-8809A (Fig. 3), which was used to simulate one of the difficult conditions. It is a measuring instrument that measures light intensity. This photometric quantity is defined as the luminous flux that falls on the unit of surface. It can therefore be said that it is the ratio of luminous flux, which is given in lumens and area, which is given in square meters.

Fig. 1 Biometric reader Aktion AFT-500, SOURCE: http://shop.efg.cz/z19476-aft-500
Fig. 2 Biometric Reader MultiBio 700, SOURCE: http://www.zkteco.com/product/MultiBio700_241.html
Fig. 3 Luxmetr - CEM-DT-8809A

The same difficult conditions were simulated for both biometric readers. Both of these readers are located on a panel whose graphical representation can be seen in Fig 4.

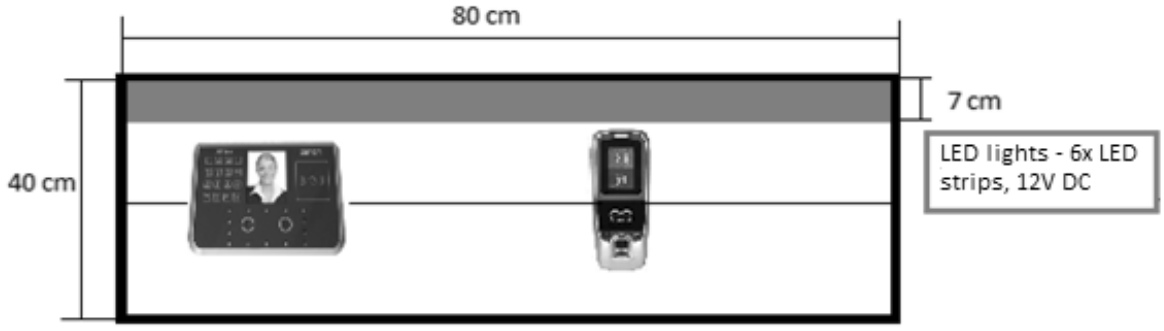

Fig. 4 Graphic representation of the panel

Fig. 5 shows the real photo of the reader panel, which is located in the laboratory. Among other things, the photo and LED strips, which consists of six-meter strips and each of them has 30 high-luminous RGB LEDs - in total, this LED strips 180 has RGB LEDs.

Fig. 5 Panel of biometric readers

Difficult conditions

These are various factors that can occur and affect the reliability of face recognition systems. A total of 11 difficult conditions were tested. Each difficult condition was measured a total of ten times. The following difficult conditions were chosen: brown curly wig, black straight wig, sunglasses, eyeglasses, winter hat, baseball cap, distinctive make-up, soiling with coal, foil scan and artificial light conditions. In one case it will be to ensure the greatest possible darkness and in the second case to ensure as much light as possible, which will be provided by the LED strips. The room will be obscure for the dark.

Measurement procedure

In order to be able to make measurements, it was first necessary to take a user's reference image to create a user profile. A total of 10 people participated in the measurement, namely: 6 men and 4 women. Volunteers were between the ages of 23 and 27.

During the measurement, individual identification times were recorded, for each difficult condition, and any false rejections or false admissions were recorded. All measured times were recorded in pre-prepared tables. Subsequently, the measured data from the tables were analyzed and the FRR was calculated for the individual difficult conditions.

The time of identification was determined for testing, for one identification attempt. This limit was 10 seconds from the start of shooting. If the person was not identified within 10 seconds, the identification was considered unsuccessful. This measurement was then marked with the X symbol in the pre-prepared measurement tables.

First, it was necessary to record each volunteer as a user in the reader and take a reference picture. The reference picture was taken without glasses in normal daylight.

The measurement started with the measurement of the shooting time when the glasses were attached. Next was a measurement with a headgear like a winter hat and a cap. It was used two wigs - black straight with bangs and dark brown curls without bangs. Then followed a scan through the foil. Conversely, for a larger amount of light in the room was used a light in the form of LED strips, which can be controlled by the remote control and adjust its intensity differently. In the end, there was a strong make-up, both for women and men. Rich red lipstick, strong blush and dark blue eyeshadow were used. The last time was measured by the time of scrubbing the face with coal. To obtain reliability data, it was necessary to use a formula that determines the level of false acceptance. This formula is part of one of the two basic types of biometric errors and reads as follows:

$$FRR = \frac{N_{FR}}{N_{EIA}} = \frac{N_{FR}}{N_{EVA}} \quad (1)$$

where *FRR* is False Rejection Rate, N_{FR} is Number of False Rejection, N_{EIA} is Enrolle Identification Attempt.

RESULTS AND DISCUSSION

A total of 2,200 measurements were taken. In order to evaluate the measurement results, it was necessary to first average all the measurement times we obtained, and this is shown in Tab. 1.

Tab. 1 Average acceptance times for measurements (sec)

	Aktion AFT-500	**Multibio 700**
Sunglasses	x	x
Eyeglasses	x	x
Cap	1,72	2,2
Winter hat	2,13	1,07
Curly wig	2,18	2,31
Straight wig with bangs	1,93	1,95
Foil	x	x
LED strips	1,29	1,52
Dark	x	x
Soiling with coal	1,51	2,07
Make up	1,49	2,38

As a result of the measurement, the FRR was calculated for each difficult condition. Formula 1 was used to determine this value.

The FRR results for the Aktion AFT - 500 reader are as follows: 100% eyeglasses, 100% sunglasses, 12% cap, winter hat 35%, black bangs 22%, dark brown curly wig 51%, 100% foil, LED strips 0%, dark 100%, soiled face with 3% charcoal and 33% distinct makeup.

The results of the Multibio 700 reader are: prescription glasses 100%, sunglasses 100%, cap 33%, winter hat 44%, black wig with bangs 51%, dark brown curly wig 51%, foil 100%, LED strips 0%, darkness 100%, soiled face with charcoal 28% and distinctive makeup 25%.

Tab. 2 shows the overall error rejection rate for all difficult conditions for each reader.

Tab. 2 Total False Rejection Rate (sec)

	Aktion AFT - 500	**Multibio 700**
N_{EIA}	1100	1100
N_{FR}	556	632
FRR	**51 %**	**57 %**

It has been found that the reliability of readers is relatively low under difficult conditions. Difficult conditions can occur under different circumstances and nowadays biometric readers need to be able to respond. The overall false rejection rate (FRR) was relatively high. This is the frequency of rejection of authorized users. The rate of false rejection does not directly threaten the system's security, but it causes complications to the user and the identification process needs to be repeated or a new identification key generated. The Aktion AFT-500 reader had a FRR of 51% while the Multibio 700 reader had a FRR of 57%. Not only because of the FRR value, but also for its user-friendliness, the Aktion AFT-500 biometric reader was found to be a better choice than the Multibio 700 reader. As a further disadvantage,

the Multibio 700 reader does not even signal when it starts to scan. The Aktion AFT-500 reads that it scans because a square is visible around the face it focuses and detects. The Multibio 700 did not display anything at all, displaying only the quality of the scanned image - if the image quality was not higher than 5, the user was not authenticated at all. Another disadvantage is its very small touch screen, where it was quite difficult to work. From the user's point of view, the Aktion AFT-500 reads better than the MultiBio 700 and can be used as a sound or light signal for MultiBio 700 readers. Fig. 6 shows the rate of mis-acceptance for individual difficult conditions for biometric readers.

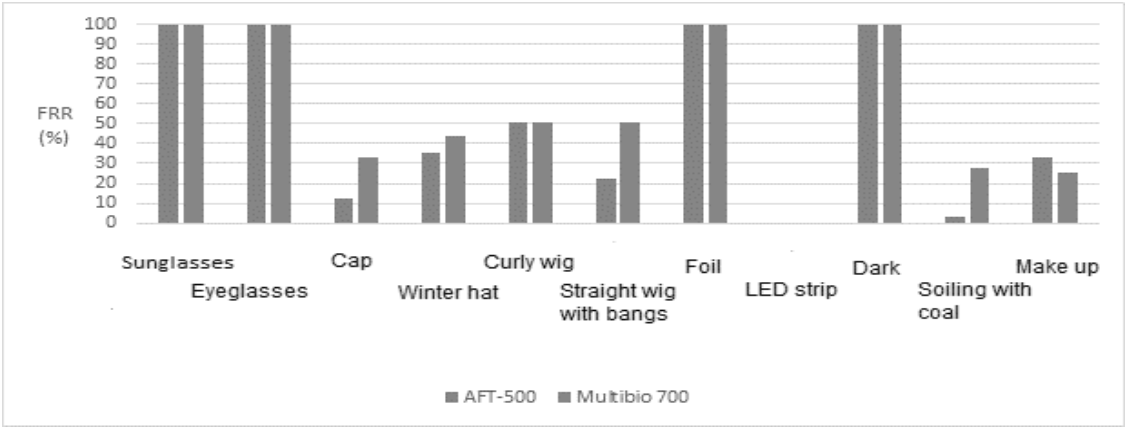

Fig. 6 FRR for individual difficult conditions for biometric readers

Technavio is predicted to grow by more than 79% by 2021 to further enhance security, mainly because the technology based on biometric identification becomes affordable.
Due to the low reliability of biometric readers, it is advisable to provide them with a more appropriate recognition algorithm. This problem could be solved by face recognition based on dictionary learning *(Liao & Gu, 2019).* Dictionary learning plays an important role in sparse representation based face recognition. In their paper, they propose a face recognition algorithm based on dictionary learning and subspace learning.
Facial recognition is a challenging task, *Abudarham N., Shkiller L., Yovel G.,* comes with a study where they use reverse engineering to discover which facial features are critical to familiar face recognition. As a result, they propose a new framework that assumes a similar perception of all faces and integrates knowledge and perception to take account of the excellent human knowledge of familiar faces.
Toshiba has developed face recognition software, as face recognition technology is used in a wide variety of applications, including identifying individuals in video surveillance systems used in public spaces, identifying airports and financial institutions, and marketing activities to identify personal attributes such as age, gender, or expression. Toshiba has more than 20 years of experience in face recognition technology and achieves excellent face recognition results. Among other things, it has a high processing speed and has also received excellent feedback.

CONCLUSIONS

Biometrics is an area where new technology is constantly developing. Recently, this is a security method that ensures a high level of security, and that is why this type of security is being sought and is becoming more and more used. It is important to keep in mind that it is a matter of protecting property or just taking an attendance system to select a suitable reader. This research means that it should be used in common commercial spaces
This research shows that the selected biometric readers are not suitable for use in more demanding areas and shows that the reliability of biometric systems under difficult conditions is low.
These readers are suitable for environments where they do not experience difficult conditions - for example use in attendance systems in companies. These biometric readers are not suitable for property security.

ACKNOWLEDGMENT
This study was supported by Department of Vehicles and Ground transport at Czech University of Life Sciences, Faculty of Engineering.

REFERENCES

1. Aburddarham, N., Shkiller, L., & Yovel, G., 2019, Critical features for face recognition. *Cognition, 182*, 73-83.
2. Biometrics in 2018: For ever more secure security. Retrieved from http://www.businessit.cz/cz/biometricke-prvky-v-roce-2018-pro-stale-dokonalejsi-zabezpeceni.php.
3. Digital luxmetr CEM DT-8809A. gme.cz. Retrieved from https://www.gme.cz/digitalni-luxmetr-cem-dt-8809#product-detail
4. Drahanský, M., Doležel M., & Orság, F. (2011). *Biometrie* . Brno: Computer Press. ISBN 978-80-254-8979-6.
5. Eysenck, M., W., & Keane, M., T. (2010). *Cognitive psychology: a student's handbook.* 6th ed. New York: Psychology Press. ISBN 978-1841695402.
6. Ježek, V. (1996). *Systémy automatické identifikace: aplikace a praktické zkušenosti*. Praha: Grada. ISBN 80-7169-282-4
7. Liao M. & Ge, X., (2019), Face recognition based on dictionary learning and subspace learning. *Digital Signal Processing, 90*, 110-124.
8. Putting More Than Just a Name to a Face. Retrieved from https://www.nec.com/en/global/solutions/safety/face_recognition/
9. Rak, R., Matyáš, V., Říha, & Z. (2008). *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada. Profesionál. ISBN 978-80-247-2365-5.
10. The Rise of Biometric Security. Retrieved from http://www.fastlane-turnstiles.com/press-releases/biometric-security/

Corresponding author:
Ing. Veronika Štekerová, Department of Vehicles and Ground Transport, Faculty f Engineering, Czech University of Life Sciences Prague, Kamýcká 129, Prague, Czech Republic, stekerova@tf.czu.cz