Agronomy Research **16**(S1), 1025–1031, 2018
https://doi.org/10.15159/AR.18.021

Influence of face lighting on the reliability of biometric facial readers

V. Hartová[1,*], J. Hart[2] and P. Prikner[1]

[1]Czech University of Life Sciences Prague, Faculty of Engineering, Department of Vehicles and Ground Transport, Kamýcká 129, CZ165 00 Prague, Czech Republic
[2]Czech University of Life Sciences Prague, Faculty of Engineering, Department of Technological Equipment of Buildings, Kamýcká 129, CZ165 00 Prague, Czech Republic
[*]Correspondence: nverca@seznam.cz

Abstract. At present, there is an increasing need to protect workplace entry and specially guarded premises. In addition to standard access systems on a chip cards are getting to the fore of biometric identification systems such as readers for fingerprint, biometric scans faces and others. Biometric readers face still improve, but still have a lot of blind spots, thanks to which their reliability and user-friendliness decreases. One such problem is the light intensity in the room where the reading device is located. The varying intensity of the light in the room causes a different illumination of the person's face. It emphasizes or suppresses the main points of the face that needed for user authorization, and the whole identification process is prolonged and difficult. The reliability value is significantly different from the value given by the manufacturers. It is very important to highlight on this problem and begin to address it by altering the current production engineering.

Key words: light intensity, measuring, False Acceptance Rate, identification, facial features.

INTRODUCTION

In today's world, an increasing emphasis is placed on securing objects. Quality security is not only about detectors for perimeter and indoor protection, but it is also very important to take care of the security of access systems. At first it used a very simple devices that operate on the principle of a password or pin, then began to use access cards and in recent years the industry has developed so much that for access to protected objects using biometric identification systems. Such systems are many (Jazzaret & Muhammad, 2013).

Most commonly used are systems that use fingerprints to identify people. These systems are quite good enough, but there is still a high chance of their sabotage. In second place are identifying systems based on the geometry of the face. Such systems are financially acceptable, but their reliability is quite a problem. (Di Martino et al., 2016) The first problem is that imitating one's appearance is not difficult, and another problem is that the identification depends on the environment in which the reader works. Although the manufacturer makes recommendations, where he writes about the lighting conditions, the spatial location of the reader, temperature and humidity conditions, etc., but the device is usually installed already in the original space and therefore it is not always possible to fulfill all the recommendations of the equipment manufacturer.

This paper focuses on the issue of the illumination intensity of the room in which the reader is located. It has been found that too high or low light intensity increases the wrong user denial and possible confusion of these users. Appropriate system innovation was needed to increase reliability to an acceptable level (Zou et al., 2010¸ Vinay et al., 2015). By testing, this problem was largely suppressed by adding an additional ice strip to individual biometric identification devices. It is very important to emphasize this problem and begin to address it by changing the current manufacturing engineering. The development of innovation in this area is of great importance. The emphasis is on the implementation of measures that will improve their ability to identify flawless (Ashbourn, 2000; Zhang, 2000; Jain & Feng et al., 2009).

To determine the reliability values of biometric identification systems, the formula for False Acceptance Rate (FAR) and False Rejection Rate (FRR) was used.

MATERIALS AND METHODS

The measurements build upon the previous research which was carried out with 80 participants using the readers MultiBio 700 and iFace 302.

A cohort of 30 participants was chosen for measurements which were repeated 20times. Regarding the face scan it was necessary to observe laboratory conditions, in particular lighting (the lighting required by the manufacturer is in the range of 0–800 lux) for the first measurement, which served as a model standard. A further 20 repeat measurements were performed with the original participants, the room lighting was provided by a dimming reflector. The tests were performed on AFT-500, AccuFACE® EFR-T1, MultiBio 700 and iFace 302 readers, represented in Figs 1 and 2. The light dimmable reflector has been attached to a classical illumination. Testing ranged from 0 Lux values of light intensity up to 1,700 lux value.

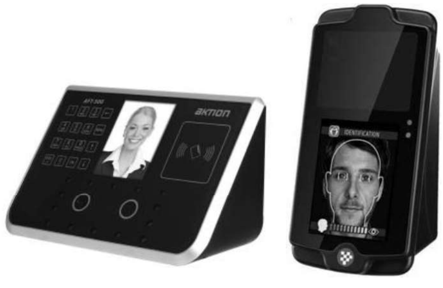

Figure 1. AFT-500 and AccuFACE® EFR-T1.

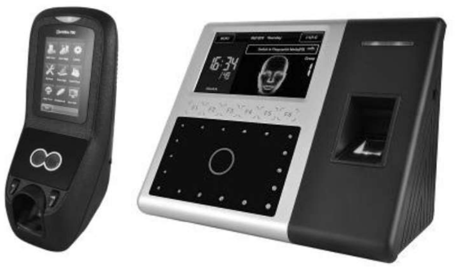

Figure 2. MultiBio 700 and iFace 302.

The measurement was primarily focused on false user acceptance. False acceptance of a user means that an unauthorized person is admitted to a particular premises. The admittance of an unauthorized person can happen in two ways, namely through a reading device error, when a person in question has no intention of criminal activity, while the other way consists in intentionally causing the door to open with certain intents in mind (trespassing, theft and other offenses. The offender has more than one possibility of outsmarting the biometric identification system. One of them is to cause a shortcircuit of the reading device without subsequent alarm activation (most of the identification systems are connected to the switchboard of Intrusion and Hold-up Alarm Systems.) Another way is to adjust your visage in a way that is as close as possible to one of the eligible users (Rak, et al., 2012; Jazzar & Muhammad, 2013).

$$FAR = \frac{N_{FA}}{N_{IIA}} \cdot 100\ (\%) \qquad (1)$$

FAR – False Acceptance Rate; N_{FA} – Number of False Rejection; N_{IIA} – Number of attempts by unauthorized persons to identify.

In addition, testing was aimed at a false denial of the user, and in the case of these readers a threshold for user denial was set for 2 seconds. Facial-identifying readers can not reject the user, only the user can accept, so it is necessary to set a limit. This limit is the value the manufacturer gives as the value at which the identification is to take place.

$$FRR = \frac{N_{FR}}{N_{EIA}} \cdot 100\ (\%) \qquad (2)$$

FRR – False Rejection Rate; NFR – Number of false rejection; NEIA – Number of Enrolle Identification Attemps.

A measurement panel was set up and all the measured readers were attached to it – see Fig. 3. First it was necessary to download individual users to each biometric system. All the tested readers have the same software and downloading was carried out in the same manner. First, each user was assigned his/her ID (identification number), next their fingerprints were taken (scanning the same finger 3times) and after that a 3D face model example was downloaded. The readers' voice application gave the users instructions on how to turn their heads (Abateet al., 2005, Stroica & Vladescu, 2012).

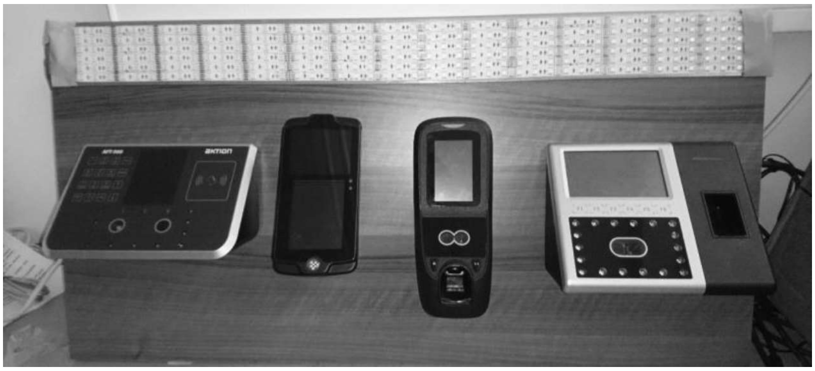

Figure 3. Measuring panel.

The readers are equipped with two cameras scanning the user's face at a specific angle. If the cameras get the required values, they will create a picture and store it. Already during the scanning of the model/template it is necessary for the scans to reach minimally 95% correspondence with the first scan. This means a match at the points which developers determined to be the points of reference (tip of the nose, nose width, distance between eyes, facial bones, mouth shape, chin and more). It was the matching of the individual snaps which were scanned in gradual steps, which extended the time needed for creating of example models.

When testing the readers, a series of measurements was performed at each light intensity. The individual luminous intensities were 0 lux, 45 lux, 160 lux, 400 lux, 725 lux, 1,150 lux and 1,700 lux.

After that LED lighting was attached to the measurement board, made up of six rows of LED tape which contained 270 LEDs.

These additional LEDs have been used to increase the reliability of biometric identification systems. Again, a set of tests was performed on the same counts as the previous measurements, except that the reader had an additional white LED light.

RESULTS AND DISCUSSION

First, measurements were made of the number of received users by each biometric systems. A total of 600 measurements were made for each light intensity and for each biometric identification system. Seven different luminous intensities were determined. These intensities were set from 0 lux to 1,700 lux. These values correspond to the values measured in individual rooms in different businesses that did not want to be published for security reasons. The graphs in Figs 4 to 7 show the measured values, where at each luminous intensity there are 4 levels of acceptance / rejection of the user. According to the legend of the chart, it is obvious that it is a borderline and so identification within 3 seconds, within 5 seconds, within 10 seconds and over 10 seconds. 10 seconds have been set limit for user identification. Anything over 10 seconds has already been taken as a wrong user denial. The first two readers AccuFace and AFT 500 are modern biometric identification systems that are in the middle price range. According to distributors and manufacturers are statistically one of the most used in Europe. The first two levels of the chart are decisive for the system owner. Both the AccuFace reader and the AFT reader make it clear that they are encircling the gaus curve. Highest reliability have systems from 1,150 lux up to 160 lux. If the intensity is too high or too low, there is a significant decrease in reliability. At values of 45–0 lux, it is clear that the integrated illumination with red LEDs is inadequate.

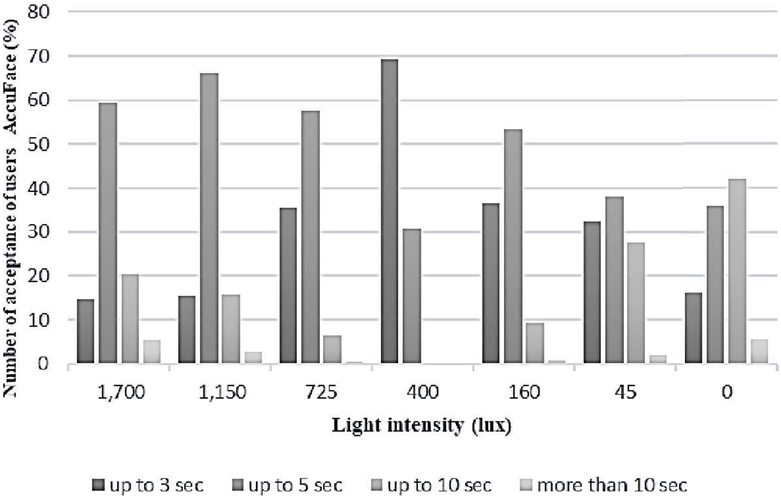

Figure 4. False Rejection Rate AccuFace.

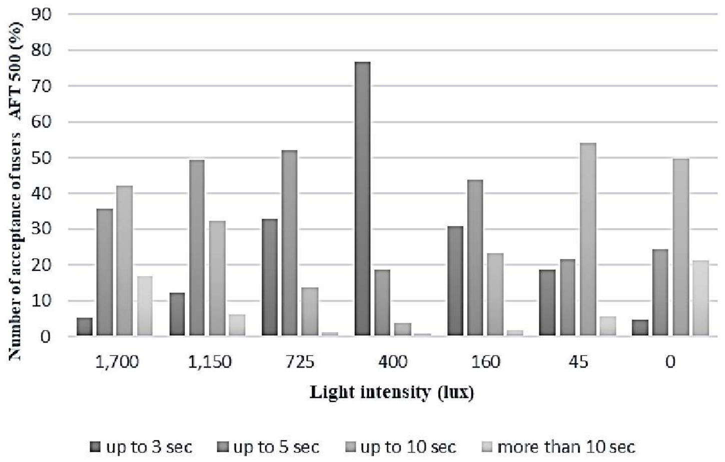

Figure 5. False Rejection Rate ATF 500.

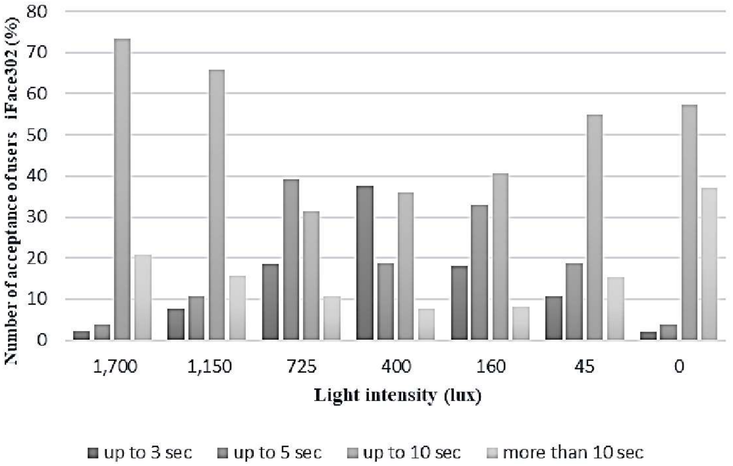

Figure 6. False Rejection Rate IFace302.

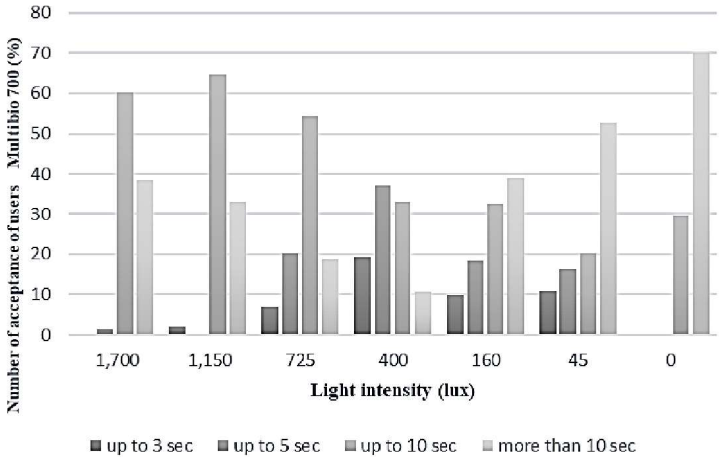

Figure 7. False Rejection Rate Multibio 700.

The IFace 302 and Multibio 700 readers have charts with the same waveform, with worse measured values. These readers are most commonly used in the Czech Republic. It belongs to a lower price category and is gradually changing for newer technologies. The graphs show that the technology of biometric face readers is still evolving and improving.

The second step was measured incorrect user acceptance. Fig. 8 shows that the highest error rate was achieved at luminous intensities of 1,150 lux and above and 46 lux and below. The optimum luminous intensity was 400 lux for all readers.

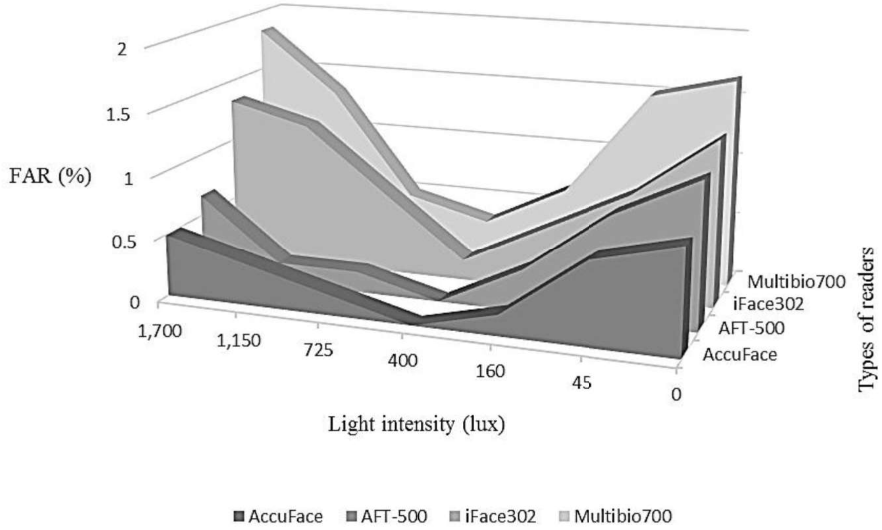

Figure 8. False Acceptance Rate.

As a countermeasure to increase reliability, another series of measurements was made, but this time with an additional panel LED white light. In all cases, the values have improved almost by half. And so the reliability reached an acceptable level. The question of the intensity of the room has not yet been dealt with by anyone else.

The authors Bourlai, T. and Hornak, L.A. in their article Face recognition outside the visible spectrum, highlight the issue of exposure, examining the reliability of systems in low light conditions or at night. Where they point to the different wavelengths and functionality of the systems in the balance sheets.

CONCLUSIONS

Measurement has shown that the intensity of light in the room in which biometric identification systems are located is very important. Too high and low light intensity values reduce the reliability of these systems. Manufacturers declare that the reliability values should be up to 1%, but the graphs could even see values around 30%, which is very unacceptable to the user. It was important to make countermeasures to increase the value of reliability for individual readers to a user-friendly value. This was aided by an additional white LED LED strip. Erroneous acceptance and false rejection values improved by an average of half by adding this additional device. This development area needs to be further deepened and addressing new innovations in these systems. Accesses to protected objects should not be underestimated.

ACKNOWLEDGEMENTS. It is a project supported by the CULS IGA TF 2015 '*The Study of Alternative Energy Resource Utilisation Under Rural Conditions*' CZU 2017:31150/1312/3122.

REFERENCES

Abate, A.F., Ricciardi, S., Sabatino, G. & Tucci, M. 2005, Beard tolerant face recognition based on 3D geometry and color texture, In: *11th International Conference on Distributed Multimedia Systems,* pp. 202–207.

Ashbourn, J. 2000, Biometrics. Advanced Identity Verification, In: *Springer-Verlag*, London, pp. 266–268.

Di Martino, L., Preciozzi, J., Lecumberry, F. & Fernández, A. 2016. Face matching with an a contrariofalse detection control, vol. **173**. pp. 64–71.

Jain, A.K. & Feng, J.J. 2009. Latent Palmprint Matching, In: *IEEE Transactions on pattern analysis and machine intelligence,* pp. 1032–1047.

Jazzar, M.M. & Muhammad, G. 2013. Feature Selection Based Verification/Identification System Using Fingerprints and Palm Print. In: *Arabian journal for science and engineering* pp. 849–857.

Rak, R., Matyáš, V., Říha, Z. 2012. Biometrics and identity of man in forensic and commercial applications. Praha: Grada Publishing, a.s. (in Czech).

Stroica, P. & Vladescu, M. 2012. Implementation of a multiple biometric identification system based on face, fingerprints and iris recognition. In: *Advanced topics in optoelectronics, microelectronics, and nanotechnologies VI.*

Vinay, A., Vinay, S. & Shekhar, K.N., Balasubramanya, M. & Natarajan, S. 2015, Face Recognition Using Gabor Wavelet Features with PCA and KPCA - A Comparative Study. In: *Procedia Computer Science* **57**, 650–659.

Zhang, D.A. 2000. Automated Biometrics. Technologies and Systems, In: *Kluwer Academic Publishers*, Boston, pp. 137–158.

Zou, W., Pong, C. & Yuen 2010. Discriminability and reliability indexes: Two new measures to enhance multi-image face recognition. In: *Pattern Recognition* **43**, 3483–3493.