The impact of light conditions on identifying facial features

V. Nídlová[*] and J. Hart

Department of Technological Equipment of Buildings, Faculty of Engineering, Czech University of Life Sciences Prague, Kamýcká 129, 16521 Prague, Czech republic;
[*]Correspondence: nidlova@tf.czu.cz

Abstract. Biometry in the field of identifying people is a highly topical theme these days. The most widespread area is identification of a person on the basis of fingerprints, nevertheless scanners of the bloodstream, iris and retina in particular are undergoing development, as well as identification on the basis of facial features. In the case of scanners which distinguish people according to their face, user problems are appearing. One of these problems is the surrounding environment of the scanner device, in particular light conditions. According to tests, it is necessary to conduct identification of people under laboratory conditions, which is not acceptable from the user perspective. It is essential to consider this problem and to innovate and extend the system for identification on the basis of facial features. It is necessary for the system to react, if possible, with a minimal error rate and within the fastest response time. Through the help of testing light conditions, an improvement was achieved in the capability of identifying facial features, and at the same time a further modification was proposed to perfect the existing technology.

Key words: face, glow, identification, lighting, surrounding environment.

INTRODUCTION

Biometric identification systems are used in various versions, within both commercial and private infrastructure. Their identification was initially predominantly based on the systems of fingerprints, and they were used exclusively in buildings in which high demands were placed on security (chemical laboratories, government organisations, arms industry, etc.). Today, these systems are a part of our society and serve, for example, also for protecting data on flash disks, easier and more secure access to laptop computers, etc. Systems with extend ranges of biometric information focus on various other characteristic attributes of persons. These include, for example, scanners of the retina, iris, bloodstream of the hand, facial features, and last but not least tread.

In various cases, it occurs that the measured values show a relatively high error rate in the acceptance or rejection of a user, even in spite of the fact that the measurement was conducted under laboratory conditions. It is of fundamental importance to focus our attention on this problem and optimise the FAR and FRR values (Rabia & Hamid, 2009). Luminosity is one of the factors that strongly influence the values of FAR and FRR. And all research is based on this aspect.

MATERIALS AND METHODS

According to the recommendation of the manufacturer, tested scanners should be installed at a distance of 3 metres from the opposite window and at a distance of two metres from direct lighting. This lighting should be within the scope of 0–800 lux. Artificial lighting is within this range, for example a 100 W bulb at the distance of 2 m has a lighting intensity of only 35 lux. In the parameters of these scanners, it is stated that they can also be used as outside devices. This information is false, since the conditions of outside lighting are inappropriate for their proper functioning. This is due to the reason that even an overcast winter sky radiates a lighting intensity of 3,000 lux, whilst a sunny summer sky radiates a lighting intensity of up to 100,000 lux. From these values, it is evident that the use of scanners as outside equipment is inappropriate (Tan et al., 2009; Schwartz et al., 2012).

Measurement of the error rate of the systems which use facial features of a person for identification is relatively demanding. First of all, it is necessary to ensure the conditions stipulated by the manufacturer. Upon testing, the distances were set as stated in the instructions. The measuring panel was placed at the height of 1.2 m. Artificial lighting was also ensured at the distance of 2.2 m (Zhang, 2000; Schwartz et al., 2012).

The lighting intensity on the level of the scanning device was 270 lux, on average. The light which fell on the face (refraction from wall) had an average intensity of 70 lux. The scanned persons stood at the distance of 0.5 m from the scanner. A total of 78 subjects were measured, repeated 20 times. The measured persons were 17 women and 61 men within the age range of 22–29 years.

RESULTS AND DISCUSSION

The measurements were conducted on the scanners MultiBio 700 and iFace 302. Both devices are a combination of identification using code, fingerprint and scanning of facial features. The time of scanning the master template for the subsequent identification of persons was measured, as well as the number of erroneous acceptances and rejections of the user, or failure to read the user. The FAR and FRR values were subsequently calculated from these measurements, see Figs. 1 and 2. Fig. 1 shows the values measured on the scanning device MultiBio 700.

The probability of erroneous rejection (Zhang, 2000) on MultiBio 700:

$$FRR = (NFR/NEIA) \cdot 100 \ [\%], \qquad (1)$$

NFR – Number of False Rejections; NEIA – Number of Enrolled Identification Attempts; FRR = (315/1560)·100 [%]; FRR = 20.19%.

The probability of erroneous acceptance (Zhang, 2000) on MultiBio 700 is determined by the relationship:

$$FAR = (NFA/NIIA) \cdot 100 \; [\%],$$ (2)

NFA – Number of False Acceptances; NIIA – Number of Imposter Identification Attempts; $FAR = (76/1560) \cdot 100 \; [\%]$; $FAR = 4.87\%$.
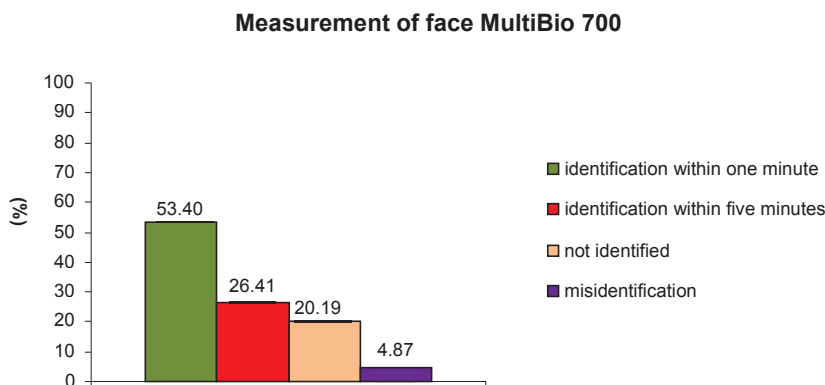
Measurement of face MultiBio 700

Figure 1. Identification capability of the MultiBio 700 biometric device.

Fig. 2 shows the measurements on the iFace 302 scanner, on which the resulting values were even less acceptable in comparison with the previous reader. A mere 53.4% of users were successfully read into the system and admitted into the building. Also, the value of more than 26% for both scanners, meaning successful identification taking up to 5 minutes, is highly uncomfortable from the user perspective.
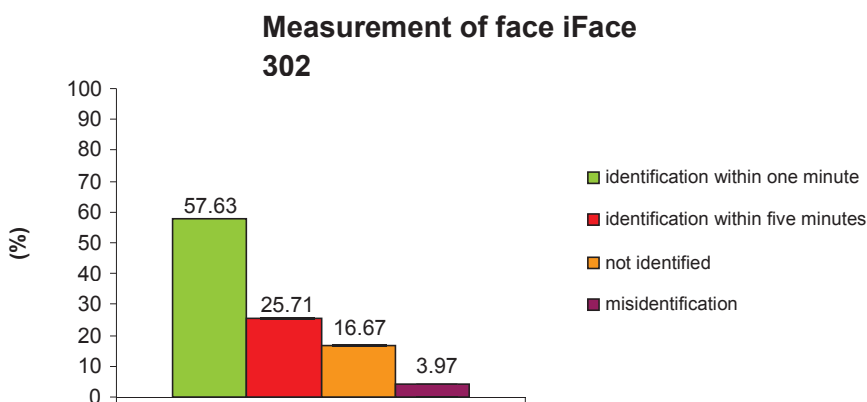
Measurement of face iFace 302

Figure 2. Identification capability of the iFace 302 biometric device.

The probability of erroneous rejection (Zhang, 2000) on iFace 302:

$$FRR = (NFR/NEIA) \cdot 100 \, [\%],$$

$FRR = (260/1560) \cdot 100 \, [\%]; FRR = 16.67\%.$

The probability of erroneous acceptance (Zhang, 2000) on iFace 302 is determined by the relationship:

$$FAR = (NFA/NIIA) \cdot 100 \, [\%],$$

$FAR = (62/1560) \cdot 100 \, [\%]; FAR = 3.97\%.$

From the calculations and their graphic expression, we can see that the percentage of erroneous rejections of users slightly exceeds the percentage of erroneous acceptances. However, both of these values are highly discomforting, and it is necessary to consider whether it is appropriate to use these systems for granting entry into important buildings. From the measured results, it is evident that it is continuously necessary to improve systems for identification on the basis of facial features.

A measurement was also conducted on the error rate of existing systems without an LED chiaroscuro, and with a chiaroscuro via a LED diode. The measurement was conducted on 78 subjects and with 20 periods. The measurement was completed after the elapse of one minute from the beginning of scanning at the latest. From the results presented in Fig. 3, it appears that the additional chiaroscuro of the LED diode accentuates the contours of the face and thereby increases the effectiveness of reading facial features, accelerating user identification.
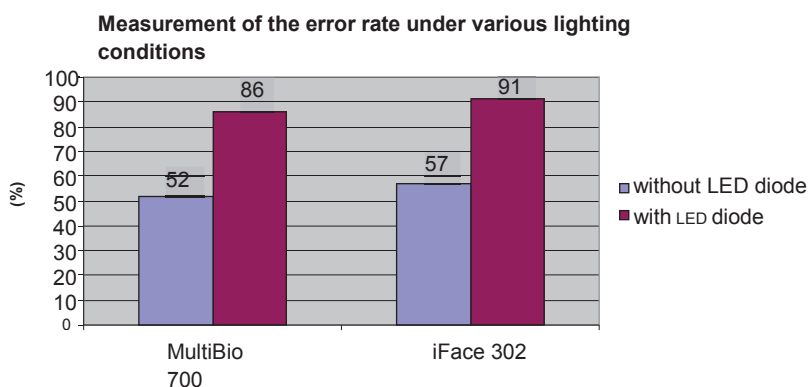

Figure 3. Identification capability under various lighting conditions.

The same photographs are show on Fig. 4. On the right side, there is photography with LED illuminator and on the left side without LED illuminator. The figure shows that the LED illuminator identification points are more visible. Due to this phenomenon, the success of correct identification is increased, as is evident from Fig. 3.
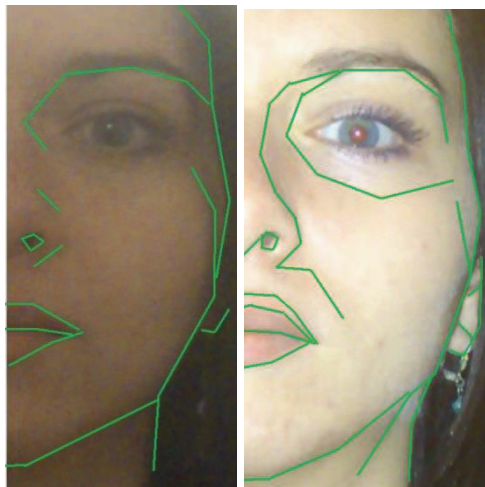

Figure 4. Identification capability under various lighting conditions.

DISCUSSION

Upon purchasing a biometric identification system, it is first of all necessary to consider how important the guarding of access is for the organisation or institution in question, since individual devices vary considerably in terms of price. For monitoring attendance or safeguarding a regular company, a higher quality fingerprint scanner is sufficient. This identification is very quick; the problem resides in very easy falsification of fingerprints. For superior protection, it is more appropriate to use systems which are tested in both laboratory and in regular conditions. These systems include, for example, readers of the iris, retina, bloodstream of the hand, etc. It is naturally mainly at the discretion of each company as to how much it intends to invest in protecting access and data. The measurements demonstrated an error rate and deficiencies of the two systems for reading facial features, and the only question is whether these deficiencies are a common feature of these biometric access systems.

CONCLUSIONS

The measured values demonstrated that identification on the basis of facial features is very imperfect. Two scanners from different manufacturers were tested, and the results were very similar. The determined error rate values in the case of both erroneous acceptance and erroneous rejection of the user were around 5%, which is a relatively high risk for the protection of valuable information and items.

Thanks to the conducted tests, modifications have been developed, which partially eliminate certain deficiencies of the tested systems. It was determined that with the help of a chiaroscuro the contours of the face are accentuated and sharpened better than with the existing systems, which do not have a chiaroscuro. It is necessary to constantly continue the development and innovations of biometric identification systems, since the present state is not yet error-free.

REFERENCES

Rabia, J. & Hamid, R.A. 2009. A survey of face recognition techniques. *Journal of Information Processing Systems* **5**(2).

Schwartz, W.R., Guo, H., Choi, J. & Davis, L.S. 2012. Face identification using large feature sets. IEEE Transactions on Image Processing **21**, 2245–2255.

Tan, X., Chen, S., Zhou, Z.-H. & Liu, J. 2009. Face recognition under occlusions and variant expressions with partial similarity. IEEE Transactions on Information Forensics and Security **4**(2), 217–230.

Zhang, D.A. 2000. Automated Biometrics Technologies and Systems. 137–158, 325 ISBN 0-7923-7856-3.