BIOMETRIC SYSTEMS BASED ON FACIAL FEATURES AND THEIR RELIABILITY

Veronika Hartova, Jan Hart
Czech University of Life Sciences Prague
nverca@seznam.cz

Abstract. Today, user identification based on biometrics is a very topical issue. The most widespread methods of identification include: fingerprints, identification based on face recognition and bloodstream scans. For testing, systems were selected that identify a person based on facial features. Testing showed errors in these readers under both standard and difficult conditions. Difficult conditions that we frequently encounter in everyday life were chosen. In the test of biometric identification systems the probability of erroneous user acceptance and probability of false rejection of the user was calculated and shown graphically. Wrong user acceptance was based on unfavorable conditions. Unfavorable conditions were: pollution with dark oil, pollution with soil, pollution with makeup, pollution with soot, pollution with black coal, pollution with paints. Another problem is the surrounding environment of the scanner device, in particular light conditions. The testing demonstrated that it is necessary to conduct identification of people under laboratory conditions, which is not acceptable from the user perspective. The results of the measurements showed that the measured reliability values do not correspond to those of the manufacturers. It is necessary to adapt and perfect these biometric identification systems for use in industrial areas, as they are often used in these areas as access or attendance systems.

Keywords: facial features, biometrics, systems, reliability.

Introduction

Modern biometric technologies offer an automated method of establishing or verifying the identity of living or dead persons on the basis of measurable and incommutable biometric characteristics. These characteristics are demonstrable, precise and unique for each individual and no confusion is possible. The initial use of these systems was very successful, but only until methods of sabotaging them were discovered. Since then, the focus is on developing safe technologies and when introducing them, measures must be taken to minimise the possibility of sabotaging biometric sensors.

Biometric recognition systems are currently used mainly for identifying persons entering facilities (e.g., nuclear power stations, airports, research institutes, banks, state buildings). Other common use is for recognition of persons (e.g., when searching for specific individuals from wanted persons databases) [1; 2].

One of the frequently-used methods of biometric recognition is identification on the basis of facial features (3D face scan). Systems working on this principle are already available at prices acceptable for the general public and now we can find them both in commercial and state institutions. These systems can be monocriterial or more. In this article we will measure multicriterial systems. The reliability of these readers, which identifying is based on facial features, should be investigated [3; 4].

Materials and methods

Each measurement comprised twenty repeats. 80 persons were measured (16 women and 64 men) with an age range of 21-62 years of age. It was essential to observe laboratory conditions when performing the 3D face scan, especially with respect to lighting (lighting required by the manufacturer is 0-800 lx). The measurements were performed on MultiBio 700 and iFace 302 readers. Both use a combination of recognition on the basis of codes, finger prints and sample facial features. The measurements took place under both normal and impaired conditions.

The number of false acceptances or failure to capture the user was measured. In addition, the degree of confusion between persons was scrutinised, which to a large extent is expressed in the FAR values [2; 4; 5].

Errors in the form of false rejection of the user do not occur with these readers; there just is the possibility that the user is not identified. The time limit for recognition was set at 5 minutes. If the reader does not manage to identify the user within this time limit, the situation is regarded as a false rejection.

The term standard recognition means recognition under laboratory conditions. Values for establishing the functionality and reliability of biometric recognition systems that work on the basis of 3D face scans were collated over the course of 27 months. The two most important values were the time span during which the users were admitted to the facility and the related number of accepted/not accepted (identified, not identified).

Measurement under impaired conditions was intended to simulate situations in dusty operations where smears on faces are common and also work with lubricants and other substances can lead to dirty faces. In everyday life too smears can appear on people's faces, for instance, smeared make-up in the rain.

The measurement was done with a selected group of 20 subjects with five repeat measurements. Black coal, earth, soot, make-up, paint and dark oils were used as soiling.

A hypothesis was set: soiling of the face greatly influences the false rejection rate [1; 3; 6].

For evaluation of the hypothesis a one-sample test of relative frequencies for the parameter π [4].

1. H_0: $\pi_1 = \pi_2$.
2. H_a: $\pi_1 \neq \pi_2$.
3. The level of significance was determined $\alpha = 0.05$.
4. Testing criterion (1):

$$u = \frac{\frac{m}{n} - \pi_0}{\sqrt{\frac{\pi_0 \cdot (1 - \pi_0)}{n}}}, \tag{1}$$

where m – standard identification, percent;
n – 100 %, percent;
π_0 – average values under adverse conditions, percent.

5. Determination of the $u\alpha$ (from statistical tables according to the level of significance) $u\alpha = 1.96$.
6. Critical field.
8. K: ($|u| > u\alpha$).

Results and discussion

Figures 1 and 2 show the percentual representation of recognitions in separate time intervals. The penultimate column of the graph shows the user false rejection rate – FRR, which is stipulated to occur upon exceeding 5 minutes per attempt at recognition. The last specified value in the graphs represents user false recognition (false acceptance rate – FAR). This value appears on the graph to give the results more relevance and is taken from the total number of attempts at recognition. Fig. 1 shows measurements taken on the MultiBio 700 reader. 53.40 % of users were successfully enrolled into the system and were let into the facility. Also the value for both readers of just over 26 % successful recognitions within 5 minutes is very inconvenient for the user.

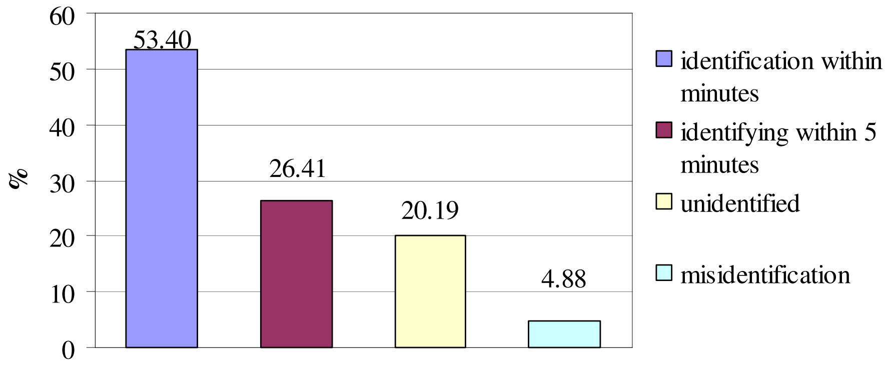

Fig. 1. **Recognition capability of MultiBio 700 biometric device**

Fig. 2 shows measurements taken on the IFace302 reader, and they are even less acceptable than those on the previous reader. Only 57.63 % of the users were successfully enrolled into the system and were let into the facility. Also the value for both readers of just over 25 % successful recognitions within 5 minutes is very inconvenient for the user.

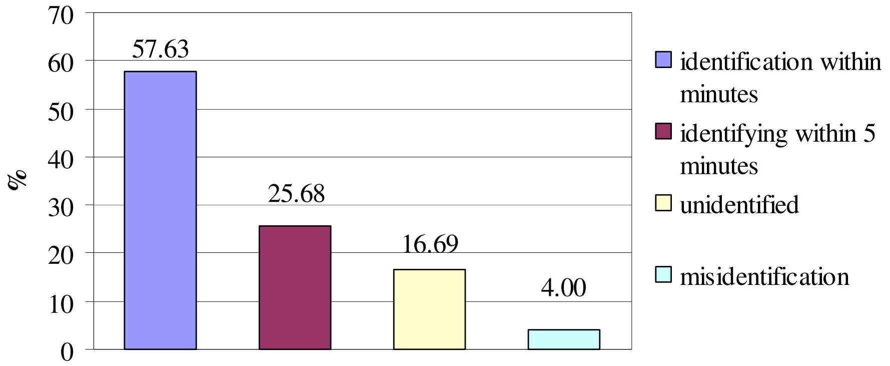

Fig. 2. **Recognition capability of IFace 302 biometric device**

The calculations and the graphic expression thereof tell us that the percentage of false user rejections exceeds the percentage of false user acceptances by about 10 %. However, these values are extremely worrying and the question should be asked as to whether these systems are suitable for entrance security at important facilities. The results of our readings clearly demonstrate that with recognition systems based on facial features there is still considerable room for improvement.

Subjects with prominent facial features were no problem to identify. However, in contrast to standard recognition, the false rejection rate rose with the remaining subjects, see Table 1.

Table 1

Percentual user acceptance with SD face readers with dirty faces

Type of dirt	IFace 302 – testing, %	Multibio 700 – testing, %
Standard identification	84	79
Dark oil	81	76
Soil	79	75
Makeup	78	76
Soot	54	47
Black coal	48	52
Wall paint	38	46

During scanning, some confusion of the users arose. This situation arose with 13 tested subjects. These subjects were confused with each other. The most frequent cases of confusion applied to these 4 men in Fig. 3. In the separate photos you can notice the common features these men share. We have assigned numbers one to four to the men – from left to right.

1 2 3 4

Fig. 3. **Most frequently confused users**

Men 1, 2 and 3 have a very similarly shaped eyes, 1, 3 and 4 have similar shape of the face. Subject 1 and 3 have the same shaped chin. The men in photos 3 and 4 have similarly shaped eyebrows.

Hypothesis: soiling of the face seriously influences the false rejection rate.

1. Statistical calculation for Multibio700 biometric system

H_0: $\pi_1 = \pi_2$,

H_a: $\pi_1 \neq \pi_2$.

A significance level has been set at: $\alpha = 0.05$.

Testing criterion (1):

$$u = \frac{\frac{79}{100} - 0.62}{\sqrt{\frac{0.62 \cdot (1 - 0.62)}{100}}} = 3.5 \cdot$$

Setting $u\alpha$ (from statistical tables, according to the significance level): $u\alpha = 1.96$.

Critical field:

K: ($| u | > u_\alpha$)

K: ($| 3.50 | > 1.96$)

H_0 is rejected → soiling of the face in general greatly influences the user false rejection rate.

2. Statistical calculation for IFace302 biometric system

H_0: $\pi_1 = \pi_2$,

H_a: $\pi_1 \neq \pi_2$.

A significance level has been set at: $\alpha = 0.05$.

Testing criterion: u = 84100−0,630,63. (1−0,63) = 4.35.

Setting uα (from statistical tables, according to the significance level): $u\alpha = 1.96$.

Critical field:

K: ($| u | > u_\alpha$)

K: ($| 4.35 | > 1.96$)

H_0 is rejected → soiling of the face in general greatly influences the user false rejection rate.

In view of the results of the one-sample relative frequency test performed with IFace302 Multibio700 readers, the hypothesis is rejected.

The matter of reliability of biometric systems that identify on the basis of face recognition is also being addressed by Di Martino, Luis D. et al. in their article “Face matching with an a contrario false detection control”, where they pointed out the existence of two identical templates. Thanks to this, the reliability of the systems should increase distinctly. Also, in their article “Beard tolerant face recognition based on 3D geometry and color texture”, the authors Abate, Andrea F. et al. talk of the technology for recognition on the basis of facial features, where color texture was used in combination with 3D geometry as an innovation for increasing reliability. Constant innovation of these systems is important for increasing reliability, which, as can be seen in the results of the scans, is not user friendly [8; 9].

Conclusions

The measurements show that reliability of the tested facial recognition systems differs from the values cited by the manufacturers. With such readers there are many aspects that can influence their reliability. One of these are light conditions, another is make-up in women or moustache or beard in men; they are also very sensitive to face soiling and other circumstances. These readers can recognise a person both by fingerprints and by facial features. The question is whether or not the manufacturers concentrated more on the fingerprint option than on facial recognition capabilities. The results clearly show that the existing systems need more testing and improvement to make it possible to rely fully on the technology and to avoid unwanted confusion of persons that can lead to admission of unauthorized persons into restricted areas. It should also be borne in mind that companies will want to use these systems in industrial environments where soiling and dust nuisance is common. The results indicated that the readers cannot deal with this type of problem and perform false recognitions or else recognition does not come about at all.

Acknowledgements

It is a project supported by the IGA 2016"The University Internal Grant Agency" (Innovation of systems for verification of a person according to his characteristic).

References

1. Rak R., Matyáš V., Říha Z. Biometrics and identity of man – in forensic and commercial applications, 2008, 664 p. (in Czech)
2. Yoon S., Feng J.J., Jain A.K., Altered Fingerprints: Analysis and Detection. IEEE Transactions on pattern analysis and machine intelligence, 2012, pp. 451-464.
3. Jazzar M.M., Muhammad G. Feature Selection Based Verification/Identification System Using Fingerprints and Palm Print. Arabian journal for science and engineering, 2013. pp. 849-857.
4. Svozil L., Aspects of biometric identification of persons using facial recognition. bachelor thesis, Univerzita Tomáše Bati ve Zlíně. 2009 (in Czech)
5. Stroica P., Vladescu M. Implementation of a multiple biometric identification system based on face, fingerprints and iris recognition. Advanced topics in optoelectronics, microelectronics, and nanotechnologies VI., 2012
6. Jain A.K., Feng J.J., Latent Palmprint Matching. IEEE Transactions on pattern analysis and machine intelligence, 2009. pp. 1032-1047.
7. Abate A.F., Ricciardi S., Sabatino G., Tucci M. Beard tolerant face recognition based on 3D geometry and color texture, 11th International Conference on Distributed Multimedia Systems, 2005. pp. 202-207.
8. Di Martino L. , Preciozzi J., Lecumberry F. , Fernández A. Face matching with an a contrario false detection control, 2016. vol 173. pp. 64-71.