Agronomy Research **15**(S1), 999–1005, 2017

Comparison of reliability of false rejection rate by monocriterial and multi-criteria of biometric identification systems

V. Hartová[1,*] and J. Hart[2]

[1]Czech University of Life Sciences Prague (CULS), Faculty of Engineering, Department of Vehicles and Ground Transport, Kamýcká 129, CZ165 21 Prague, Czech Republic
[2]Czech University of Life Sciences Prague (CULS), Faculty of Engineering, Department of Technological Equipment of Buildings, Kamýcká 129, CZ165 21 Prague, Czech Republic
[*]Correspondence: nverca@seznam.cz

Abstract. Biometric user identification is a highly topical theme these days. The most widespread areas are identification of a person on the basis of fingerprints and identification on the basis of facial features. Testing was performed on the 4 biometric systems. Systems using fingerprint were LA 2000M and iEvo ULTIMATE, and systems disposing even the scan faces were D-Station, IFace 800. Measurements showed that the higher reliability have biometric identification systems which identify the person on the basis of one parameter. From the results it is also seen that sabotage of biometric identification devices that identifies on the the basis of two or more parameters is much simpler than those that identify only using fingerprint or scan of face.

Key words: fingerprint, false rejection rates, false acceptance rates, identification.

INTRODUCTION

At present, identification based on biometric characteristics is being used ever more often. This method of identification of persons is user friendly, as it is not necessary to remember passwords or codes, and there is no need to carry around chips or RFID cards. The development of biometric systems was very extensive in the beginning of this scientific direction, and over time the development of new systems slowed and more attention was paid to the improvement of existing systems. Initially, systems identifying a user were created based on a single feature (fingerprints, face shape, bloodstream and others), while in recent years the trend of combined reading identification devices, e.g. a combination of fingerprint and facial scan, has spread (Rak, 2012; Stroica, 2012; Jazzar, 2013).

One of the most important parameters of biometric identification systems is reliability. These systems are used mainly in places where it is necessary to restrict access to people for whatever reason. We are increasingly seeing cases where these systems were compromised from a security standpoint and an unauthorized user broke into a guarded area. It is therefore important to continuously develop this branch of science by constantly inspecting and testing the correct functionality of existing biometric systems, all whilst designing improvements to existing systems from the obtained results (Jain & Feng, 2009; Yoon et al., 2012).

MATERIALS AND METHODS

Testing was focused on the reliability of dual biometric identification systems in comparison with the reliability of systems that identify only on the basis of one biometric method. Measurements were carried out in the security technology laboratory at the Technical Faculty of the Czech University of Life Sciences in Prague, and the measurements were carried out under laboratory conditions. These conditions are based on standards ČSN EN 50133, ČSN ISO/IEC 19794, ČSN ISO/IEC 19794, ČSN ISO/IEC 27006, ČSN ETSI EN 302 77, as well as on the recommendations of the relevant manufactures.

80 test subjects participated in the measurements. The testing was always done in twenty cycles. The test subjects were 16 women and 64 men aged 21–62. Two devices were selected for the measurements that only identified on the basis of fingerprints (scanner LA 2000M and scanner iEvo ULTIMATE), and two dual systems that identified on the basis of fingerprints and facial features (D-Station and IFace 800). Their basic parameters are shown in Table 1. All of these devices have optic sensors. These systems were selected on the recommendations of the manufacturer. Manufacturers recommend these device to use even in places with difficult conditions.

Table 1. The basic parameters of biometric devices (Information from the datasheet)

LA 2000M	iEvo ULTIMATE	D-Station	IFace 800
			
FRR	FRR	FRR	FRR
< 0.001%	< 0.001%	< 0.001%	< 0.001%
FAR	FAR	FAR	FAR
< 0.00001%	< 0.00001%	< 0.00001%	< 0.00001%
Fingerprint Capacity	Fingerprint Capacity	Fingerprint Capacity	Fingerprint Capacity
8 000	10 000	200 000	2 000
Operating Temperature	Operating Temperature	Operating Temperature	Operating Temperature
0 ~ 45 °C	-20 ~70 °C	-20 ~ 50 °C	0 ~ 45 °C
Matching Speed	Matching Speed	Matching Speed	Matching Speed
< 1sec	< 0.7 sec	< 1sec	≤ 1 sec
Sensor	Sensor	Sensor	Sensor
Optical	Optical	Optical	Optical

The use of the first optic sensors was recorded between the 1960s and 1970s. These sensors work on the basis of FTIR – Frustrated Total Internal Reflection technology. This is a laser beam or a thick bundle of optical fibres illuminating the surface of the

finger beds from below, which is placed to the transparent plate of the sensor. The reflected light flux is scanned by the CCD (Charge Couplet Device) element. Papillary lines and furrows determine the amount of reflected light, wherein the ridges reflect more light than the furrows. However, the CCD element does not use the reflection of light from the furrows as a means of evaluation (Rak, 2012; Stroica et al., 2012; Jazzar & Muhammad, 2013).

False rejection rates of a user. Such a situation means that an authorized user is not let into a building via the identification devices. If this happens rarely, the user repeats the entire identification process and is then admitted into the building. False rejection rates of a person can have many causes (incorrectly placed finger on the scanner, wet finger, cold finger, injured finger, dirty finger, etc.). The probability of the false rejection rates of a user can be calculated via the following formula:

$$FRR = \frac{NFR}{NEIA} 100[\%] \quad (1)$$

FRR – False Rejection Rates, NFR – Number of False Rejection, NEIA – Number of Enrolle Identification Attemps (Svozil, 2009).

The measurements were performed both under standard and difficult conditions, focusing on the different types of tests that can arise under realistic conditions. Tests were divided into the following:

- **standard identification –** this identification was carried out on washed, cleaned hands.
- **cold fingers** – it was first necessary to cool the fingers of the test subjects to the same temperature range from 20–25 °C. This was done using ice prepared into moulds. Each mould was treated with waterproof foil in order to prevent dampening the measured finger. This simulated the cold outdoor environment. Each measurement was preceded by a fifteen minute cooling of the finger and then the finger was placed on the surface of the sensor.
- **cooling of a damp finger** – for cooling a damp finger, the measurements were carried out in the same manner as for cooling a dry finger, except for the part with the waterproof foil. During the measurement the finger was cooled directly with the ice. As the ice melted it slightly dampened the skin of the finger. The finger was then not dried, which caused the required wet surface.
- **heated finger** – during this measurement, it was first necessary to determine a method for heating a finger to temperature range from 50–55 °C. Initially, the finger was heated with hot water in a container, but this method was rejected because the water cooled. In order to ensure the same conditions for all of the test subjects, and that the measurement was relevant, a USB (Universal Serial Bus) heater was chosen to heat the finger, to which a digital temperature sensor was attached. The heating temperature was constantly 55 °C, but it is necessary to expect temperature losses during the short movement of the finger from the heater to the sensor of the scanner. That is why the specified temperature range is from 50–55 °C.
- **soaked finger** – soaking of the finger was very important for the testing. Such a case may occur during normal work and domestic situations. The finger beds were soaked using water in a container. The liquid was heated to 40 °C using the USB

heater. Each subject dipped their finger for 20 minutes. After removing the finger from the water bath, it was dried with gauze and tested on the measuring panel.

- **blackened finger** – testing a blackened finger was chosen on the basis of practical experience. Hands are usually not washed before being scanned into the system. Smeared hands are common both at work and in private lives. A black washable marker with incomplete covering was used to simulate blackening and smeared hands. The test focused only on the hue rather than the micro particles of impurities, such as dirt, dust, etc.
- **finger with a layer of glue** – Testing with a layer of glue was selected as a substitute for similar materials such as silicone, adhesives and other lubricants which we encounter in practice in normal life. A thin layer of the glue was applied to the finger and the scan we done after five minutes, during which the glue only partially solidified. After each scan the surface of the scanner sensor was cleaned.
- **finger with a layer of instant glue** – instant glue was selected because it creates a solid hard coating. This coating is transparent and very thin. When the glue is applied and dries, the papillary lines are deteriorated and individual scanners make verifications according to these lines.
- **injured finger** – fingers are injured every day, and it was therefore necessary to also test such cases. The 80 test subjects were asked to evaluate the most common injuries, which included cuts, burnt finger beds and deterioration of the skin from grinding and pressure. These four types of injuries were divided amongst the test subjects.
- **dirty finger (soil)** – dust was used for these measurements acquired from a vacuum cleaner bag. The dust was mixed with peat and the required mixture was created. Each test subject rubbed this mixture between their palms before the measurement was carried out.

RESULTS AND DISCUSSION

The measurement results clearly show that the use of more modern, dual biometric readers is less secure. It is evident from Fig. 1 that identification is not one hundred percent accurate. Based on the results acquired from the standard identification, the measurements were then expanded to test under difficult conditions.

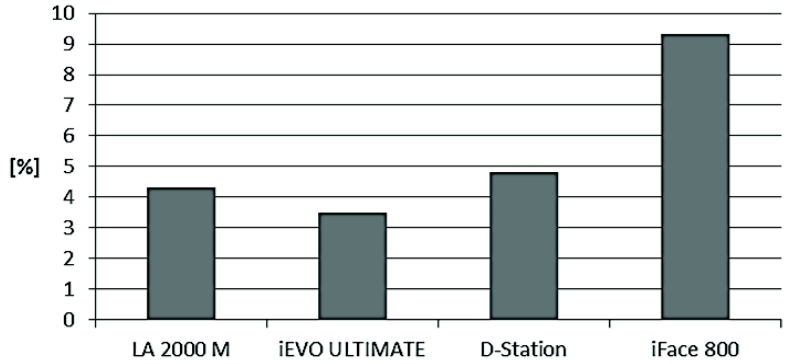

Figure 1. False rejection rates under standard conditions.

Measurement of systems reliability under difficult conditions unequivocally showed that the rate of FRR increased several fold. Fig. 2 shows the average value of errors (FRR) under adverse conditions.

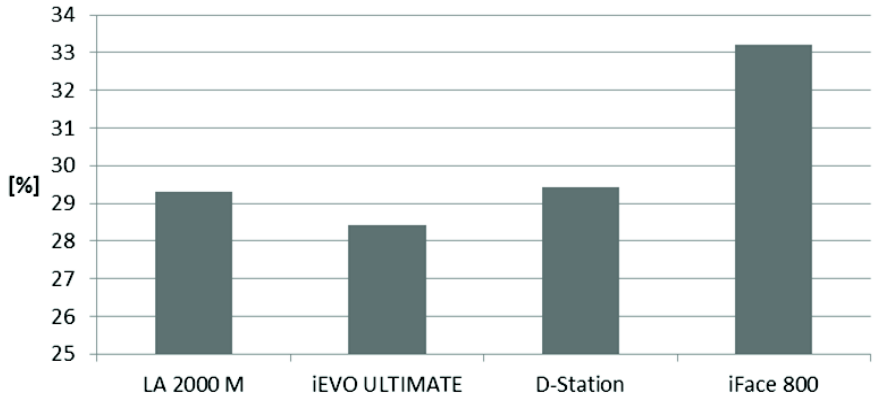

Figure 2. Average false rejection rates of adverse conditions.

Furthermore, using the of chi square test statistical method, a hypothesis was defined regarding whether the results of a standard FRR test on individual readers are consistent with FRR testing under adverse conditions. We will compare the calculated value of the test criterion with the corresponding quartile distribution $\chi 2$ (k - 1), i.e. with three degrees of freedom. For the 5% significance level, we will use $\chi 2$ (1 - α), i.e. quartile $\chi^2_{0,95} = 7.815$. The values of the tested criterion for the individual tests are given in Table 2.

Table 2. Chi square for testing under difficult conditions

	LA 2000M	iEVO ULTIMATE	D-Station	iFace 800	$\sum \chi 2$
cold fingers	0.032609	0.188616071	0.098214	0.006711409	0.3261505
cooling of a damp finger	2.264493	3.135044643	2.545455	0.167785235	8.1127772
heated finger	0.612319	0.251116071	0.207792	0.006711409	1.0779385
soaked finger	2.355978	4.152901786	4.444805	0.184983221	11.138668
finger with a layer of instant glue	2024.479	2534.652902	1858.092	881.9211409	7299.1449
dirty finger (soil)	532.8705	665.1607143	507.858	271.147651	1977.0368

The hypothesis is not rejected in the first and third cases, which means testing using cold fingers and a heated finger. For these statistical results we do not exceed the limits defining the critical field (7.815), and it is found in the field and on the 5% significance level. For tests using a soaked finger, cooling of a damp finger, a finger with a layer of instant glue and a dirty finger (soil), the calculated value of the test criterion exceeds the limit of defining the critical field (7.815), and we reject the hypothesis of the conformity of FRR results under adverse conditions and standard tests.

H0: The value of FRR of readers LA 2000 M and iEVO ULTIMATE (monocriterial readers) is the same as D-Station P (2) = 0.00127 and IFAC 800 (readers combined). Statistics was performed separately so that the results was relevant and so that each monocriterial reader was compared with each reader combined. They were used two-sample paired t-test with a fixed level of significance 0.05. Achieved statistical significance for two-sided test P (2) was for readers LA 2000 M and D-Station P(2) = 0.00127, for LA 200 M and iFace 800 P(2) = 0.000642, for iEVO ULTIMATE and D-Station P(2) = 0.000115 and for iEVO ULTIMATE and iFace 800 P(2) = 0.000528, which is in all cases less than the determination level of importance, and we therefore reject the hypothesis.

It is unnecessary to continue to develop new devices and new biometric methods unless the reliability of existing systems is improved. It is important for new systems to avoid the errors of the existing systems. These issues are also discussed by the author Yoon, who in his article 'Altered Fingerprints: Analysis and Detection', refers to the possibility of sabotaging systems through the creation of a synthetic fingerprint, etc. He also modifies the algorithm in order to be immune to this sabotage. In contrast, author Jain focused on the development of a new device for identification of a person. As a unique characteristic, he chose the entire surface of the palm. Compared to a small fingerprint, minutiae are more clearly visible on entire surface of the palms. The tests showed that the new device operates with 78% reliability, and it can thus be tested in practice (Jain & Feng, 2009; Yoon et al., 2012). Similar testing indicates Veronica Nídlová just right for readers destined into normal environments. (Nídlová, 2015)

Before purchasing an access biometric identification system, it is necessary to consult with professionals in the field and pay attention to the reliability of individual biometric systems. It is important to understand what areas or information we want to protect, and to adapt the choice of the biometric identification device with regard to this.

CONCLUSIONS

Today, the reliability of biometric identification systems is a very current issue. The measured values show that the first two scanners that identify a person solely on the basis of a fingerprint are much more reliable than dual scanners.

These results: for readers LA 2000 M and D-Station P(2) = 0.00127, for LA 200 M and iFace 800 P(2) = 0.000642, for iEVO ULTIMATE and D-Station P(2) = 0.000115 and for iEVO ULTIMATE and iFace 800 P(2) = 0.000528 show that the combined biometric identification systems are less reliable and can therefore not be recommended for practical use. It is necessary to continuously improve these systems in order to get closer to the values given by the manufacturers. The value of erroneous acceptance given by the manufacturers for all of the tested readers is ≤ 0.0001%, and the value of false rejection ratesof a user is ≤ 1%. When comparing these values with the values obtained from the standard measurements, it is evident that in dual systems the value of reliability decreased by almost 10%, which is very user-unfavourable.

ACKNOWLEDGEMENTS. It is a project supported by the CULS IGA TF 2016 'The University Internal Grant Agency' (2016:31150/1312/3110).

REFERENCES

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

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

Nídlová, V. & Hart, J. 2015. Reliability of Identification Based on Fingerprints in Dual Biometric Identification Systems. *Applied Mechanics and Materials* **752–753**, 1040–1044.

Rak, R., Matyáš, V. & Říha, Z. 2012. Biometrics and identity of man – in forensic and commercial applications, 664 p. (in Czech).

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

Svozil, L. 2009. Aspects of biometric identification of persons using facial recognition. *Bachelor thesis*, Univerzita Tomáše Bati ve Zlíně. (in Czech)

Yoon, S., Feng, J.J., & Jain, A.K. 2012. Altered Fingerprints: Analysis and Detection. *IEEE Transactions on pattern analysis and machine intelligence*. 451–464 p.