Agronomy Research **13**(3), 786–791, 2015

Reliability of biometric identification using fingerprints under adverse conditions

V. Nídlová[1,*] and J. Hart[2]

[1]Czech University of Life Sciences Prague (CULS), Faculty of Engineering, Department of Electrical Engineering and Automation, Kamýcká 129, CZ-16521 Prague, Czech republic; [*]Correspondence: nidlova@tf.czu.cz
[2]Czech University of Life Sciences Prague (CULS), Faculty of Engineering, Department of Technological Equipment of Buildings, Kamýcká 129, CZ-16521 Prague, Czech republic

Abstract. Biometric user identification is highly topical these days. The most well-represented method is fingerprint identification, to which this study is also dedicated. However, we cannot forget other methods such as scanning the bloodstream, retina and iris, facial recognition, etc. Four reading devices were tested in this study. Tests were carried out both under standard and adverse conditions. Adverse conditions included situations such as cold finger, cooled damp finger, heated finger, soaked finger, finger with a layer of instant glue, and dirty finger (soil). All tests performed under adverse conditions simulated realistic industrial plant environments. The results of the measurements showed that the measured reliability values do not correspond to those claimed by 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.

Key words: biometrics detector identification systems, fingerprints, user's false rejection.

INTRODUCTION

Nowadays, there are many methods by which persons at a workplace can be identified. These include identification based on entering a password or numerical code, as well as chip systems and identification (ID) cards. All of these methods are transferable in a certain way. Biometric identification systems have been developed as the safest method for entering protected buildings. These systems make identifications on the basis of the unique biometric characteristics of an individual (Jain et al., 1997).

Biometric systems are used not only as identification systems serving for entry into guarded buildings (access systems), but also as attendance systems. It is very important to be aware of the fact that such systems are used in numerous jobs. They can be found in the banking sector, medical sector and automobile industry, steelworks and in a number of other fields. This is where the issue of their reliability becomes important. Every manufacturer specifies for each scanner the percentage of erroneous acceptance and refusal of the user, but the question is under what conditions? For attendance systems, verification occurs under standard conditions, wherein, for example, fingerprint-based identification requires the verified parts of the finger to be free of

impurities. But when these systems are used as access systems, there is a risk of a decrease in reliability. One example of such risks is their use in industrial areas, where absolute cleanliness of the palm and fingers cannot be expected (Lourde & Khosla, 2010). For these reasons, a number of measurements were carried out, which indicate the need to improve the biometric identification systems, if they are used under more adverse conditions.

MATERIALS AND METHODS

The testing focused on the reliability of the selected biometric identification system under adverse conditions. 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 included 16 women and 64 men aged 21–62. Two devices were selected for the measurements that only identified on the basis of fingerprints (scanner TAC-05 MFF and scanner F7), and two dual systems that identified on the basis of fingerprints and facial features (Multibio 700 and IFace 302).

All tested biometric systems had an optic sensor. 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 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 (Hlaváč & Šonka, 1992; Jain et al., 1999).

Erroneous rejection of a user 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. Erroneous rejection 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 erroneous rejection of a user can be calculated using the following formula (Ashbourn, 2000; Rak et al., 2012):

$$\mathrm{FRR} = \frac{\mathrm{NFR}}{\mathrm{NEIA}} . 100\ [\%] \tag{1}$$

where: FRR – False rejection of a user; NFR – Number of False Rejections; NEIA – Number of Enrollee Identification Attempts.

The measurements were performed both under standard and adverse 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 and cleaned hands. Based on the results acquired from the standard identification, the measurements were then extended to tests under adverse conditions;
- **cold fingers** – it was first necessary to cool the fingers of the test subjects to the same temperature range of 20–25 °C. This was done by using ice prepared into moulds. Each mould was covered 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;
- **cooled damp finger** – for cooled 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 of 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 temperature losses are expected during the short movement of the finger from the heater to the sensor of the scanner. That is why the specified temperature range is 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 fingers 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;
- **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 it dries, the papillary lines deteriorate, while individual scanners make verifications according to these lines;
- **dirty finger (soil)** – dust acquired from a vacuum cleaner bag was used for these measurements. The dust was mixed with peat to prepare the required mixture. Each test subject rubbed this mixture between their palms before the measurement was carried out.

The values stated by manufacturers were identical for all of the tested scanners, namely FRR ≤ 1%.

Table 1 displays the percentage of reliability of individual types of biometric identification systems for standard and adverse conditions.

Table 1. Percentage results of user's false rejection under standard and adverse conditions

Condition	TAC-05, %	F7, %	IFace 302, %	Multibio 700, %
Standard identification	2.00	7.50	9.00	9.50
Cold finger	2.75	8.25	9.15	9.75
Cooled damp finger	5.25	10.35	12.25	10.75
Heated finger	1.00	6.75	7.50	8.25
Soaked finger	5.00	13.25	14.50	10.25
Finger with a layer of instant glue	96.75	99.75	99.75	99.50
Dirty finger (soil)	49.19	57.63	65.00	60.00

RESULTS AND DISCUSSION

The measured values proved that identification based on fingerprints is imperfect under more adverse conditions. Four scanners from various manufacturers were tested: two multi-functional scanners combined with a detection function of characteristic facial features, and two normal scanners that evaluated only fingerprints.

Fig. 1 shows that the average value of false rejection of user under adverse conditions for all biometric readers greatly exceed the value specified by the manufacturer. All producers specify that the value of the false rejection of user is less than 1%. All the tested systems were intended for outdoor use. Therefore, they should have succeeded well in the performed tests. It is important to point out that the measurement showed that the type of adverse conditions is very important. From Table 1 it is evident that when papillary lines are better visible, the error value is lower. It would be useful for producers to take these measurements into account.

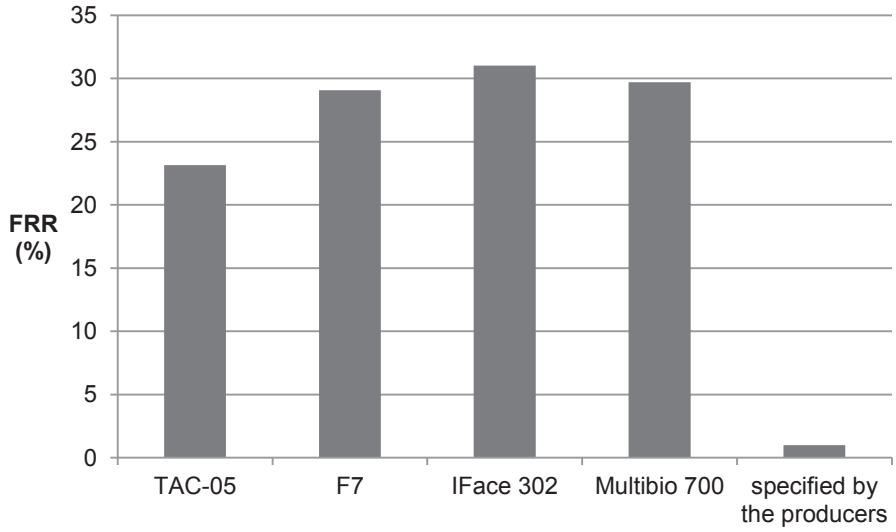

Figure 1. Graphical comparing of the average values of the false rejection of users under adverse conditions for each tested biometrics system and specified by the producers under standard conditions.

The measurement results clearly show that the use of more modern, dual biometric readers is less secure. From the author's point of view, it is unnecessary to continue developing 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 (Yoon et al., 2012). 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 et al., 2009).

Based the acquired values, it is possible to recommend the users to consider whether the rate of reliability of these systems is sufficient for the protection of their spaces before using the biometric identification systems. It should also be considered that the biometric systems should be combined with other entry protection options such as PINs, ID cards, passwords or the possibility of interconnection with security systems (Straus & Porada, 2007; Heřman et al., 2008).

CONCLUSIONS

The values stated by manufacturers were identical for all of the tested scanners, namely FAR $\leq$ 0.0001% and FRR $\leq$ 1%. For systems that only work with fingerprints, these values were on average lower than those of combined detectors, which shows that when two technologies are combined, some component is always slightly suppressed.

When acquiring a biometric identification system, it is first necessary to consider how important access protection is for the given organization or institution, as individual devices vary within an extensive price scale. For attendance or security for a normal company, a better-quality fingerprint scanner would be sufficient; this type of identification is very fast, but very simple falsification of prints is a problem. For stronger protection, it is suitable to use systems tested both under laboratory and normal conditions, the result of which are satisfactory for the user. The measurements proved error rates and deficiencies in four of the frequently used fingerprint identification systems.

The measurements carried out show that the reliability of scanners is lower than stated by the manufacturer, and that is why biometric identification systems are rather often used as attendance systems. However, companies that use such systems as access systems should be aware of the fact that what they want to protect with them is not fully safe. For biometric systems used to protect entry, users should utilize their alternative entry possibilities, for instance identification based on biometric data in combination with a password, access card or chip, wherein both types of data would be necessary for entry.

ACKNOWLEDGEMENTS. This is a project supported by the IGA 2015 The University Internal Grant Agency (Inovace systémů pro verifikaci člověka dle jeho charakteristických rysů).

REFERENCES

Ashbourn, J. 2000. Biometrics. Advanced Identity Verification, Springer-Verlag, London.

Heřman, J. 2008. . Electrical and telecommunications installations, Verlag Dashöfer, Prague.

Hlaváč, V., Šonka, M. 1992. Computer Vision, Grada, Prague.

Jain, A.K., Hong, L., Pankanti, S., & Bolle, R. 1997. An identity-authentication system using fingerprints. *Proceedings of the IEEE* **85(**9), 1365–1388.

Jain, A., Bolle, R., Pankanti, S. 1999. Biometrics. Personal Identification in Networked Society, Kluwer Academic Publishers, Norwell, Massachusetts, USA.

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

Lourde, M. & Khosla, D. 2010. Fingerprint Identification in Biometric Security Systems. International *Journal of Computer and Electrical Engineering* **2**(5), 852–855.

Rak, R., Matyáš, V., Říha, Z. 2012. Biometrics and personal identity in forensic and commercial applications, Grada Publishing, a.s., Prague.

Straus, J, & Porada, V. 2007. Frensic biomechanical application in criminalistic. In Forensic Science International.

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