Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

RESEARCH ON FACE RECOGNITION SYSTEMS IN TERM OF THEIR RELIABILITY AND CREDIBILITY

SULOVSKA, K[aterina] & KOVAC, P[etr]

Abstract: *The biometric systems are part of our everyday lives. Many of us are in touch with them every day in order to carry out our work. However, we are unaware about their important qualities: reliability and integrity. Those qualities may in many cases affect our satisfaction with these tools and their eventual deployment to designated areas. This article presents the results of the research on facilities available to the general public, and confronts the reliability and the speed of the device presented by the manufacturer.*

Key words: *biometric systems, face recognition, system evaluation, reliability, FAR and FRR*

1. INTRODUCTION

The security issues in companies and the public sector is often inflected topic. This is due to the fact that the risk of not only terrorist attacks rises every day and we want to protect our assets. The face recognition systems are one of the possibilities that can help us protect the selected area. Hovewer, the selection of the best biometric system from many is not so easy. We must always take into account the place of deployment, the number of users, and the working conditions of the system. It is also necessary to consider the system data reported by the device manufacturer. These systems mostly cannot work under common conditions as well as specified by the manufacturer. For that reason, each device should be tested to obtain real data. This paper deals with the analogous testing procedure on the face recognition systems under common conditions as these systems covers c. 12 % of the biometric system market (see. Fig. 1). The results will be later confronted with data obtained from newer types of the same device and software, which will give us the idea of advancement in the face recognition field.

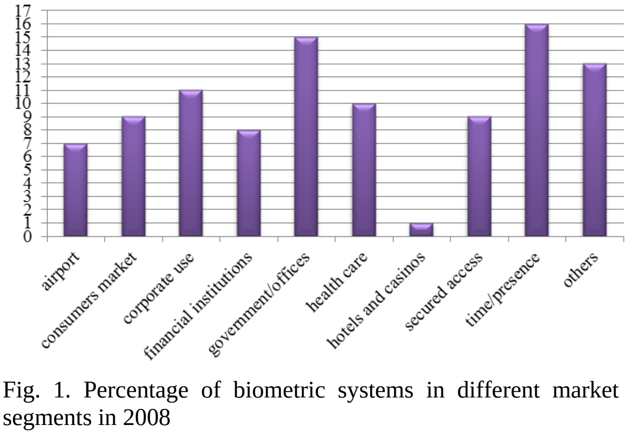

Fig. 1. Percentage of biometric systems in different market segments in 2008

2. SYSTEM SELECTED FOR TESTING

For the purposes of this research, the face recognition system A4 VisionAccess by the Canadian company Bioscrypt, Inc. was chosen. This biometric system was introducen in 2007, consisting of two main parts: the Enrollment station (desktop computer, 3D EnrolCam), and the FaceReader (3D FaceReader Optical Unit, FaceReader Controller, Easy Install Box). Another part of the installation packet is the software, mainly the VisionAccess Enrollment Application (for the operation and setup of the first part of the system) and Vision 3DI (for the operation and setup of the second part of the system).

This system is resistant to the change in the flesh-colour, beard and accessories (earring, etc.). Unfortunately, the system is not able to recognize the face covered by glassess or other things (like scarf, etc.).

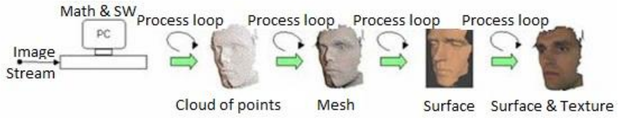

Fig. 2. The process of making the model of the face

The VisionAccess works on the 3D comparison of the face's model principle. The 3D EnrolCam is a specialized camera system placed on the tripod. This device serves to import the new referential templates of users to the system. The device is equipped with the IR camera as liveness detection. 40,000 identification points are used for the face scanning and the main focus is on the forehead, area around the eyes and the dorsum of the nose.

Fig. 3. Enrollment station (left), and FaceReader (right)

The second part is the 3D FaceReader Optical Unit (FRO), which is scanning the face and serves to the identification (1:N, one to many) or to the verification (1:1). The unit is connected via the patchboard called the Easy Install Box to the FaceReader Controller (FRC). The FRC is an industrial computer supplying the recognition of faces and their consequent comparison with the templates in the database. The information interchange runs through the ethernet network. The FRO can be also connected to the card reader for the higher security level. The FaceReader can work as a network or stand-alone application.

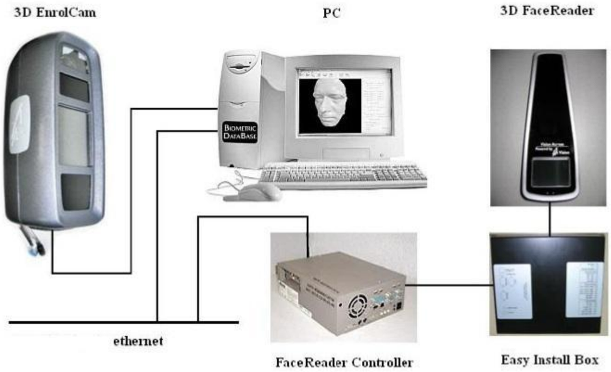

Fig. 4. Simplified diagram of the system

3. EVALUATING THE SYSTEM

3.1 Controlled characteristics

FAR (False Acceptance Rate, Error type II or False Match Rate (FMR)) - the probability that the unauthorized user is accepted by the system; the unauthorized user is wrongly recognized as one of the authorized users. The FAR is very significant error in terms of the security.

$$FAR = \frac{\text{No. of incorrect acceptance}}{\text{No. of all authentization attempts}} \tag{1}$$

FRR (False Rejection Rate, Error type I or False Non-Match Rate (FNMR)) - the probability that the access of the authorized user is denied by the system; the authorized user is not recognized by the system. The FRR is inacceptable in terms of the user perspective.

$$FRR = \frac{\text{No. of incorrect rejections}}{\text{No. of all authentization attempts}} \tag{2}$$

3.2 Measurement procedure

The measurements were done for 10 persons. Each person has its own biometric template in the A4 Vision. Than, 200 attempt to access the system were done for each one. The threshold was set to 80 % to obtain high security level. The most important thing is the distance from the FRO (80 cm). The identification takes only few seconds as specified by the manufacturer. The system notifies errors only when the conditions are not kept. The results are listed in the table below.

A4 Vision				
User No.	Attempts	False identification	FRR [%]	FAR [%]
1	200	3	1.5	0
2	200	6	3	0
3	200	2	1	0
4	200	4	2	0
5	200	0	0	0
6	200	2	1	0
7	200	3	1.5	0
8	200	7	3.5	0
9	200	2	2	0
10	200	8	4	0.5
Total	**2000**	**37**	**1.85**	**0.05**

Tab. 1. Results of measuring the FRR and the FAR

4. DISCUSSION

As can be seen in the Tab. 1, the highest number of the false identification (8) occurs only in one case. Although this user had problems under an indefinable causes, the overall FRR for the system is 1.85 %. It can be said that this percentage is highly satisfactory due to the common conditions during the testing. The data in Tab. 1 also shows unexceptionable value of FRR (0) and FAR (0) in the case of User No. 5.

During the testing, the User No. 10 was swapped for another one in one case. Unfortunately, these two users have nothing in common, so the replacement was done by the matter of change or software error. The total FAR amount is after this cimrcumstance 0.05 %, which moves the system to the cathegory with the medium level of reliability. The total FRR unlike that falls into the category with low level of reliability, as the total value is 1.85 %. This could be caused by the fact that the the maximal horizontal head rotation is of c. 8.5° and the distance between the face and the EnrolCam is c. ± 10 cm, and the user broke these limits. The application is considering its security level (tested at the 80 % threshold) a good application, which can sometimes cause the inconveniency to its owners with the minimal possibility that the unauthorized person is accepted.

5. CONCLUSION

The face recognition system AccessVision 4 is the notional top between these systems. However, the face recognition is more exacting in the template importing. If the 3D face appearance scanning is unsuccessful, the problems with recognizing occur, as it is shown in Tab. 1.

Nowadays, the main disadvantage of the face recognition systems is the functionality. While using the tokens, PINs or smart cards, the 100 % success is secured. Unfortunately, the face verification does not reach such results as our research shows. There is always some error rate (the FRR and FAR). As the biometric systems dedicated to the face are still under the large-scale research, it can be said that this area experiences a great improvement and this method will be more exact and rapid in the future.

6. ACKNOWLEDGEMENTS

This paper is supported by the Internal Grant Agency at TBU in Zlín (project No. IGA/43/FAI/10/D), and by the European Regional Development Fund (project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089). We also want to thank Mr. Lukáš Svozil and Mr. Petr Hrazdira for their help with the research.

7. REFERENCES

Cipolla, R et al. (2010) *Computer Vision: Detection, recognition and reconstruction*. Berlin Heidelberg: Springer-Verlag, 2010, ISBN 978-3-642-12847-9

Jain, A et al. (2004) *An Introduction to Biometric Recognition.* IEEE Transactions on Circuits and Systems for Video Technology, 2004, vol. 14, no. 1

Mou, D. (2010) *Machine based intelligent face recognition*. Berlin Heidelberg: Springer-Verlag, 2010, ISBN 978-3-642-00750-7

Norman, T. (2007) *Integrated security systems design: Concepts, design, and implementation.* Oxford: Elsevier Inc., 2007, ISBN 978-0-7506-7909-1

Rak, R. et al. (2008). *Biometry and identity of the person in forensic and commercial application*, Prague, Grada Publishing, 2008, ISBN 978-80-247-2365-5

TistarellI, M.; Bigun, J. (2003) *Advanced studies in biometrics*. Summer School in Biometrics. Alghero, Italy, June 2003, Revised selected lectures and papers. Berlin Heildelberg: Springer-Verlag, 2005, ISBN 3-540-26204-0

Wayman, J., et al. (2005) *Biometric Systems: Technology, design and performance evaluation*. London: Springer-Verlag, 2005, ISBN 1-85233-596-3