FACE RECOGNITION SYSTEMS - RELIABILITY AND CREDIBILITY

SULOVSKA, K.

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. The face recognition technology has emerged as an attractive solution to address many contemporary needs for identification and verification of identity claims. Face recognition systems are based on the anthropological minutiae on the face. One of the easiest methods used during the 1960s is the graphical method based on descriptive geometry principles made by the Soviets. This chapter may be divided into two main parts – measuring faces by the A4Vision biometric system and measuring faces by the analytical-statistical method. The chapter introduces reliability of the A4Vision system tested in laboratory conditions and shows the bases of this system – the analytical-statistical method applied to measurement of changes in the face of ten different women, and ten emotional changes of one woman, which were measured to obtain better understanding of programming requirements for better reliability of those systems.*

Key words: *biometric systems, face recognition, anthropometrical points, photoanthropometry*

Authors´ data: MSc. et MSc. **Sulovska**, K[aterina], Tomas Bata University in Zlín, Faculty of Applied Informatics, nám. T. G. Masaryka 5555, 760 01 Zlín, the Czech Republic, sulovska@fai.utb.cz

This Publication has to be referred as: Sulovska, K[aterina] (2012). Face Recognition Systems - Reliability and Credibility, Chapter 06 in DAAAM International Scientific Book 2012, pp. 065-074, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-86-5, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2012.06

1. Introduction

Identification of a person by his/her externals is a necessary tool in the criminalistics and in other security applications important not only for investigation tasks and a searching for missing or suspected, but also for a direct identification. Biometric systems combine many disciplines and by their depth and complexity is often well beyond starting with computer vision and its algorithms (Cipolla et al., 2010; Mou 2010), anatomy, design, programming etc.

It can be said that the modern bases of biometric systems were laid by Frenchman Alphonse Bertillon in the 19th century. His anthropological method (founded on the anthropology) can be divided into two groups: an anthropometrical and a somatoscopical one. The anthropometry evaluates the characteristics by the objective tools, and is expressed by length measures, circumferences, arches, axes, weight, etc. The somatoscopy studies the evolution, size or absence of certain characteristic by an observation. These two approaches are complementary, or one may predominate where necessary (Rak et al., 2008). The description of the person is mainly limited to the somatoscopy, while the identification system by A. Bertillon was based mostly on the anthropometry.

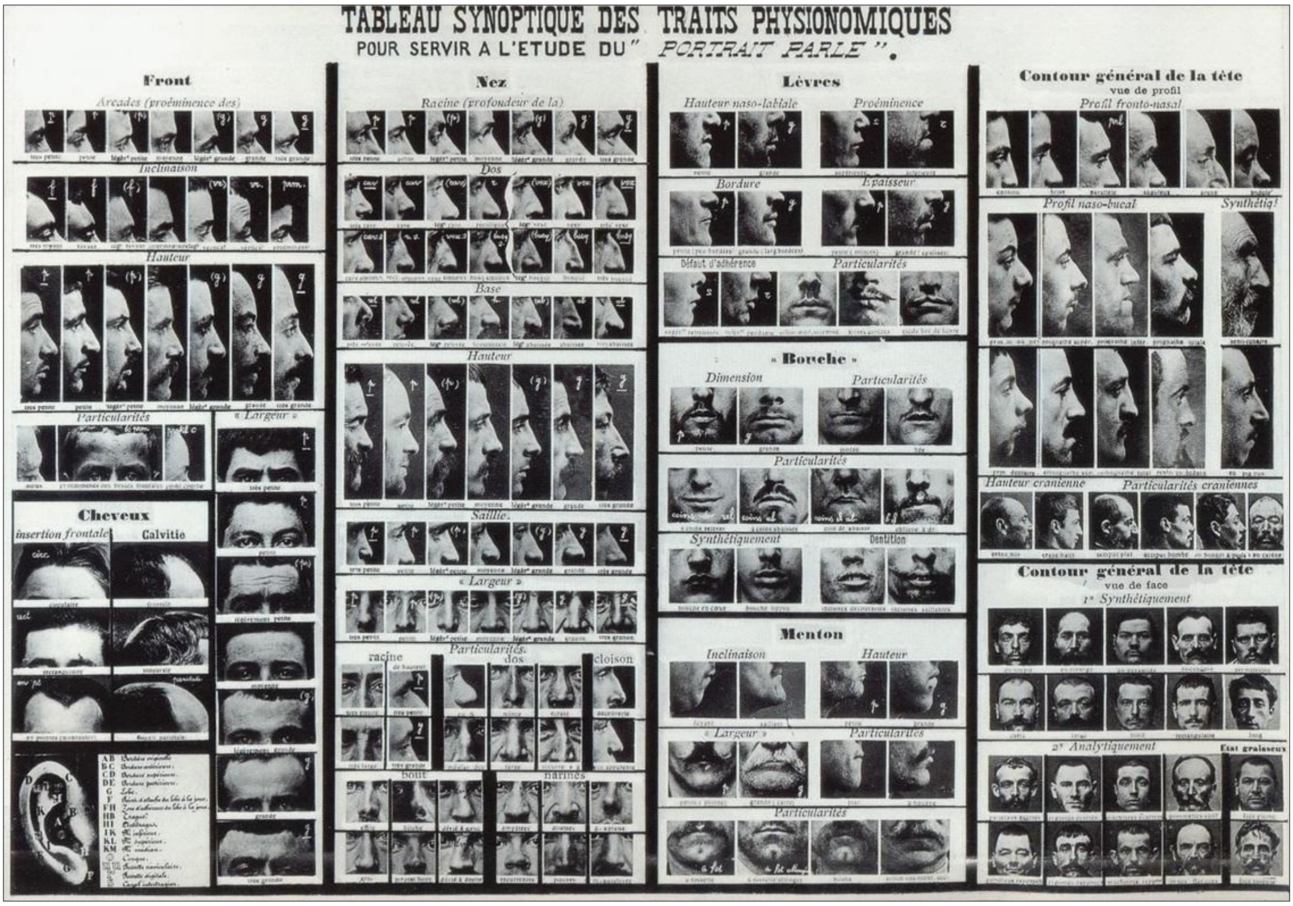

Fig. 1. Anthropometry features by Bertillon [http://nuriavv.blogspot.cz]

Security issues in companies and a public sector is often inflected topic. This is due to a fact that a risk of not only terrorist attacks rises every day and we want to protect our assets. The face recognition system is one of the options that can help us protect selected area. However, the selection of the best biometric system from many is not easy. We must always take into account the place of deployment, the number of users, and working conditions of the system. It is also necessary to consider the system data reported by the device manufacturer. These systems mostly cannot work with 98 % accuracy under common conditions as specified by the manufacturer. For that reason, each device should be tested to obtain real data. This chapter deals with the analogous testing procedure on the selected face recognition system 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, software, and algorithms, which will give us the idea of advancement in the face recognition field.

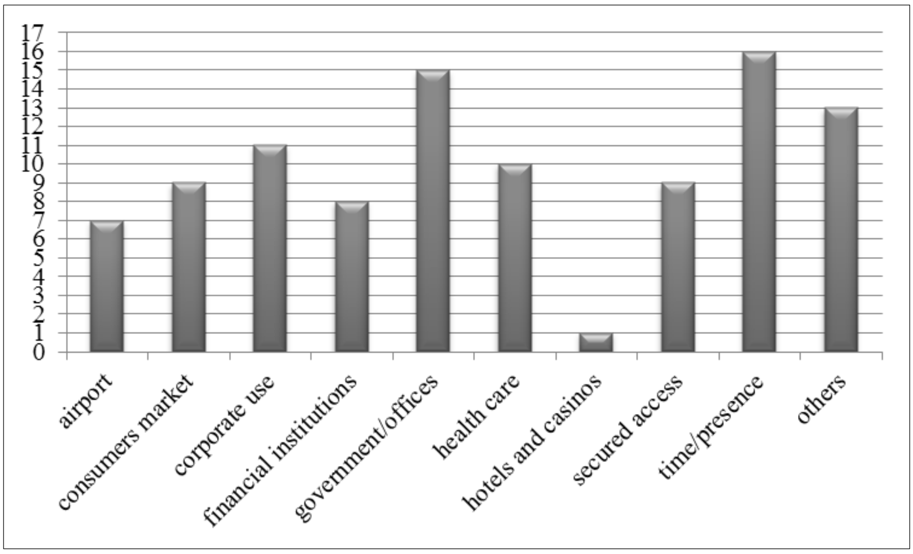

Fig. 2. Percentage of biometric systems in different market segments in 2008 [IBG]

As the identification is, in our case (commercial application), done by software, a utilization of the somatoscopy as the only one tool may be misleading and sometimes insufficient. Therefore, this chapter also deals mainly with the anthropometry to test the chosen system (A4Vision) and to evaluate statistically differences in single images of faces and their emotional changes, and use this knowledge as a background for a further research in statistical evaluation of aging faces. Consequently, a better view on how the software works should be obtained and reviewed.

2. Methods

2.1 The A4 VisionAccess System

For the purposes of this research, the face recognition system A4 VisionAccess by the Canadian company Bioscrypt, Inc. was chosen. This biometric system was introduced in 2007, consisting of two main parts: the Enrolment 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 Enrolment Application (for the operation and setup of the first part of the system) and the Vision 3DI (for the operation and setup of the second part of the system).

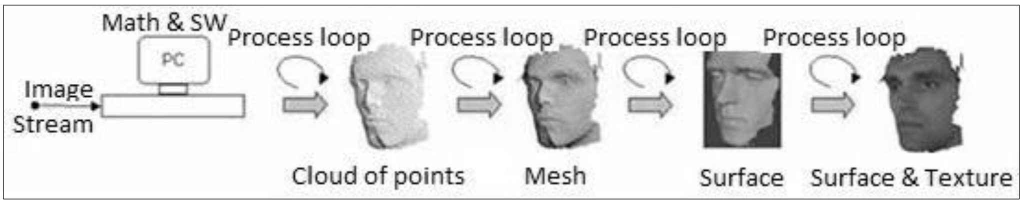

Fig. 3. The process of making the face model [Mou, 2010]

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

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

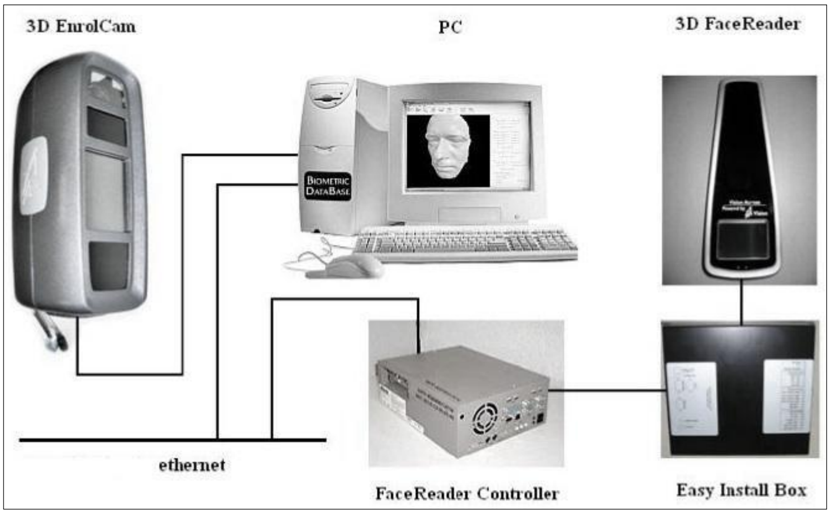

Fig. 4. Simplified diagram of the system

The second part is the 3D FaceReader Optical Unit (FRO), which scans the face and serves to the identification (1:N, one to many) or to the verification (1:1). The unit is connected via the patch board 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.

2.2 Controlled Characteristics

To evaluate the biometric system, several characteristics can be used (Jain et al., 2004; Wayman, 2005; Tistarelli & Bigun, 2003). Those characteristics can give us a sophisticated insight into selected system and its functionality. For the purposes of our research, only two of these characteristics were chosen as the system was placed indoors and the required threshold was 80 %.

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 unacceptable in terms of the user perspective.

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

2.3 Software for Anthropometrical Measurements

The basic measurements were done by the help of the Adobe Photoshop CS 5 ver. 10.0 (64 bit version), where the images obtained from the University of Stirling (UK) could be easily measured manually in pixels or centimetres. The manual measurement was chosen to avoid errors made by the software and to compare coefficients calculated in previous research (Rak et al., 2008) and in this research. As the whole process of data acquisition is very demanding, ten faces were chosen to simplify the procedure.

The data were collected, calculated and evaluated in the MS Excel 2010. The in-depth control of data was done by the STATISTICA ver. 7.0.

2.4 Images

The nowadays methodology using calculation of distances is the method based on geometrical shapes and an identification of anthropometric points, which has only the bases of the analytical-statistical method in common. The resolution of processed image for the use in police-court (forensic) applications is set to be standardly 500 dpi (e.g. used by FBI also for fingerprint recognition (Rak et al., 2008)). Generally, the higher the resolution of the processed image, the more precise the identification process is (Siegel et al., 2000).

The proportions of images were 720 × 576 pixels (≈ 25.4 cm × 20.32 cm), the resolution was 72 dpi. The project was at first done for 12 selected anthropometrical points for better comparison with fully computerized method, though 17 and finally 28 points were chosen for further data analyses. For this 12 points, the distance between each pair of points, respectively the lengths of chosen abscissae were measured three times. As the pupils or eyebrows were not visible in some cases, or the boundaries were not sharp enough, their length were not derived. For the selected two sets of images, the angles between chosen anthropometric points were measured to see the changes against the direct look/various emotions of the model(s). The distances were measured in pixels, angles were read in degrees. The images were divided into two groups - first set contains various faces, second set contains same faces with different emotions.

As in all analyses, the points used for indices must be clearly visible and defined, if they are not on standard sites (e.g. 28 chosen points).

Fig. 5. Chosen face points (left to right 12, 17, 28 points)

2.5 Comparing Two Faces

For the experimental comparison of the face the expert uses a referential album of model photographs of one person. As our project was focused on manual measurement of the face, our referential album contains, in comparison to 700 images from the research made in (Rak et al., 2008), reduced number of images. To get the relative coefficient K_F, following three simple equations are available:

$$K_n = \frac{l_1}{l_2} \tag{3}$$

$$K_{ij} = \frac{K_{F1}}{K_{F2}} \tag{4}$$

$$\lambda = \frac{K_n}{K_{ij}} \tag{5}$$

where:

l₁ - distance between anthropometrical points *i* and *j* in the first image,

$\boldsymbol{l_2}$ - distance between anthropometrical points *i* and *j* in the second image,
$\boldsymbol{K_{F1}}$ - change coefficient of abscissa between point *I* and *j* for the first image set from the table,
$\boldsymbol{K_{F2}}$ - coefficient for the second image,
$\boldsymbol{\lambda}$ - relative value.

The method can be utilized for the images with a format at least 18 x 24 cm. The face with the same space orientation as the examined image is searched in the referential album. The λ_{ij} is calculated for each abscissa. Based on the experience, if the difference of minimal and maximal λ_{ij} value is lower than 0.2, then the tested face is identified as identical (to that in database). (Rak et al., 2008)

3. Result and Discussion

3.1 Measurement Procedure via A4 VisionAccess

The measurements were done for 10 persons. Each person has its own biometric template in the A4 Vision. Then, 200 attempts 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 in our case). The identification takes only few seconds as specified by the manufacturer. The system notifies errors only when the conditions are not kept (e.g. swings, emotional changes, and distances below 70 cm and above 90 cm). 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**

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

As can be seen in the Table 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 common conditions during testing. The data in Table 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 circumstance 0.05 %, which moves the system to the category 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 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.

According to the General Accounting Office USA (2004), the amount of FRR is from 0.3 % to 5 %, and the FAR differs from 3.3 % to 70 %. The former (2010) research at TBU showed the FRR and the FAR equal 1 %, so the system was qualified as that with high security level. This result is however not as significant as this one as a smaller number of participants were used.

3.2 Anthropometrical Analysis

Computationally demanding calculations of different and same faces for comparison purposes shows very analogous results to those obtained by the fully computerized method. It can be said the coefficients' results are close according to results (s. Table 2). The main disadvantage of this method is the time - a set of 10 faces is measured for at least 3 hours in contrast to c. 0.2 - 10 s to whole process by the automated biometric system.

Abscissae connecting points	**Images**										
	41	**42**	**43**	**$_{1}1$**	**$_{1}2$**	**$_{1}3$**	**$_{1}4$**	**$_{2}1$**	**$_{2}2$**	**$_{2}3$**	**$_{2}4$**
2-5	0.963	0.969	0.973	0.964	1.143	1.024	0.900	0.963	1.027	0.967	1.045
2-10	1.021	1.179	1.314	1.072	1.105	**1.332**	**0.749**	0.979	1.042	0.958	1.113
3-7	0.545	0.628	0.736	1.004	1.038	0.942	1.094	1.024	0.954	0.946	1.032
3-8	0.878	0.887	0.900	0.988	1.141	0.845	**1.288**	1.035	0.923	0.938	1.077
3-5	0.850	0.900	0.957	0.917	1.063	1.006	1.038	0.960	0.923	0.938	1.077
3-12	1.441	1.330	1.501	0.857	**1.072**	0.989	1.021	0.854	**1.115**	0.911	1.037

Tab. 2. Examples of relative coefficients (notes: images 41 – 43 = computerized values of one face; images $_{1}1$ - $_{1}4$ = manually measured values of different faces; images $_{2}1$ – $_{2}4$ = manually measured values of same faces with different expressions; bold = position with λ_{ij} lower than 0.2 - only for manually measured values)

Unfortunately, the values of points 3-7 embody ship rise of nearly 0.4 points, which represent the highest growth in values obtained manually. The slight increase of values can be also observed for the values 3-8 and 3-5 in the exemplary table. The most significant decrease of values appears in the points 3-12. These values are higher for more than 0.2 ratio points. These differences between measured and computerized method may be caused by several reasons (Sulovská, 2012):

- images' resolution is different, according to the results of λ_{ij} values the resolution of our images is higher, which means better conditions for measurements,
- or the fully computerized method was not too accurate – the edges of points could be in shadow,
- or the data cannot be directly compared as the faces are various,
- or the human error may occur despite all the precautions.

Apart from the different values of relative coefficients that can be a bit misleading, the λ_{ij} values show exactly the similarity of faces. The faces from the second set (emotions) have the λ_{ij}, according to expectation, lower than 0.2. The mean value is 0.06, and the value is slightly above the 0.2 only a few times in the whole set. This can be taken as a result of the expression on the face, which could change (deform) the normal proportion of the face. In practical terms, changes like this will occur and brings the requirement for the utilization of additional methods for the face recognition. When exploring the λ_{ij} for various faces (first set), the mean value is 0.12, but the value above 0.2 limit emerges multiple times. This clearly shows the difference of each face, which is the intention of the recognition. The data agreement in the first set - different faces - is 83.00 %. These results, as may be obvious from the previous results, also show high percentage of diversity between various faces as expected. The data agreement for various emotions of one face is 88.37 %, which means high resemblance of data calculated only statistically.

While using more data (proposed 28 points), the accuracy is higher in case of various emotions, respectively lower in case of various faces, which increases the probability of correct recognition or identification of individual. However, decrease in number of points to 12 basic ones will decrease the probability of correct recognition and increase the percentage of errors during recognition.

4. Conclusion

Nowadays, the main disadvantage of the face recognition systems is already the functionality. Unfortunately, the face verification does not reach such results as our research shows in every case. There is always some error rates (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.

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 shows our research. The systems' accuracy and reliability can be heightened by a proper installation of the whole system in the space, respectively the enrolment camera.

The bases of the face identification/verification were proved by testing the manually measured data of selected faces. Based on that information it can be said that the face biometrics may be very reliable according to the behaviour of the data. The level of reliability depends mainly on used technology - hardware and software (algorithms, programming language, working conditions). The future work will lie in functionality of appliances at aging (and variant face changes), swings, distances and light conditions. Some of these requirements may be already applied in the forensic and military field, where the technology is in advance and highly secured.

5. Acknowledgements

This paper is supported by the Internal Grant Agency at TBU in Zlín (project No. IGA/FAI/2012/016). The author would like to thank the project “Psychological Image Collection”- at University of Stirling accessible at pics.stir.ac.uk for the variable datasets of faces, and to Mr. Lukáš Svozil and Mr. Petr Hrazdira for their help with the research.

6. 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

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

Siegel J. A. et al. (2000) “Encyclopedia of Forensic Sciences”, Four-Volume Set, pgs. 773 – 815, Elsevier, 2000, ISBN: 978-0-12-227215-8

Sulovská, K. (2012) Comparing manually measured anthropometrical points of human faces with fully computerized ones. In XX. IMEKO World Congress, Metrology for Green Growth, 9. - 14. September 2012, Busan, Republic of Korea

Sulovska, K., Kovac, P., (2011). Research on face recognition systems in term of their reliability and credibility, Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, ISSN 1726-9679, ISBN 978-3-901509-83-4, Editor B[ranko] Katalinic, Published by DAAAM International, Vienna, Austria 2011