Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

RESEARCH ON BIOMETRICAL SYSTEMS: AN OVERVIEW

SULOVSKA, K[aterina] & ADAMEK, M[ilan]

Abstract: *The most commonly used biometrical systems nowadays are fingerprint and face recognition systems. As the technics develops, so do tresspassers. In our research, we test the endurance, reliability, credibility and integrity of those systems by the use of modern utilities and materials for defeating satefy devices. This paper mainly deals with the contemporary results of research currently progressing in the world as our own research is still in progress.*
Key words: *biometrics, face recognition, iris recognition, fingerprint recognition*

1. INTRODUCTION

The need of assets protection increases every day. To protect them, several methods and procedures can be used. One way is to use the standard methods as possesion of a thing like an identification token or a smart/electronic card or knowledge of PINs or passwords. The main disadvantage of these is that they can be stolen or the person can be forced to leak the essential information. This is why biometrical systems experience unusual upswing in use. The biggest convenience of biometrical systems is the permanent holding of biometric character by its living carrier and minimal opportunity for stealing it by a trespasser. Although biometrical systems bring high safety level and serve as precautions while accessing protected areas, almost any can be passed by the tresspasser with different knowledge and equipment.

The main aim of our research is to test the readily available biometrical systems with an emphasis on face and fingerprint recognition systems, which are nowadays frequently used. Most of the systems manufactured at the present time still do not have the liveness detection so that they can be overcome under certain circumstances. The purpose of all testing procedures of biometrical systems and generating new algorithms for pattern recognition with effective, rapid and reliable functioning is to reduce the vulnerability and improve the security level.

2. FACE RECOGNITION

Identification of a person based on their face is a method with lower identfication exactness and it is the most complicated area of automated image recognition. The method enables scanning at larger distances. This is why the research laboratories and teams are urged to improve this technology to the maximum. Since 1960, many algorithms and methods for computer recognition were done in order to recognize the face correctly. Dividing these to categories depend on various classification criteria (for example: form of processed image, spectrum, way of scanning, time view-point, algorithms, etc.).

The use of artificial neural network brings more reliability to face recognition systems as artefacts like sun glusses can be eliminated and the person can be still identified.

In the next part of our research, the vulnerability of the face recognition system will be tested in a variety of ways and improvement coming out of this research will be done. This improvement should be based on human sensorium for recognition of objects.

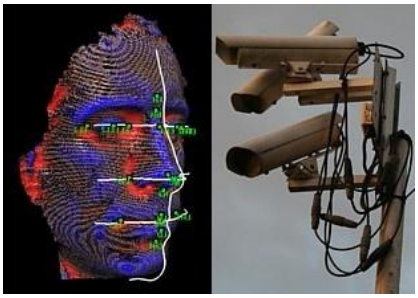

Fig. 1. NEC's biometric face recognition system in Hong Kong

3. IRIS RECOGNITION

Iris recognition is one of the emerging technologies, which has the most useful modalities for biometrical identification. It is one of the most accurate methods as it is said that the patterns in iris do not change during the time and are very variable between individuals (even each of irises differs).

Recognition systems use variety of algorithms and attitudes to iris recognition. Over the last two years, a great amount of novel approaches were made including the use of different types of algorithms using Haar, db4, db8, Gabor and other wavelet techniques for feature extraction. But the research goes further, when an idea of color iris recognition appeared (Ghouti, Al-Qunaieer, 2009). Proposals of algorithms were done and the methodoly is further deepening for obtaining a better level of accuracy while recognizing and matching color irises, which could bring improvement in performance of iris recognition systems.

Those newly-made approaches give us an opportunity for further measurements of iris pattern's inalterability and improvement of existing algorithms. Very appealing would be a study of whether the iris pattern is changing during the time, for example because of the medication or drug dependence as mentioned by Pierscionek, Crawford and Scotney (2008), which could contribute to higher vulnerability of wide-spread iris recognition systems. This will be a part of our next research if a suitable collection of samples for study is obtained.

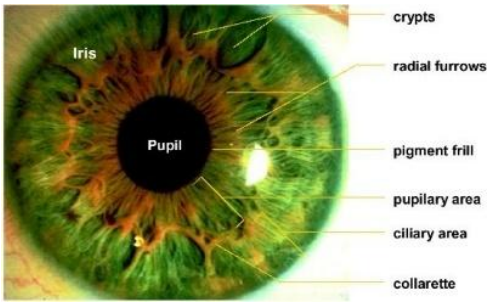

Fig. 2. Structure of iris

4. FINGERPRINT RECOGNITION

The fingerprint recognition is one of the most used ones. Human fingers have a unique desing of skin corrugations (minutiaes) that forms different types of patterns. These patterns are on fingers, palms, feet and toes. While for forensic use all these body parts can be used, for commercial devices only patterns on fingers are used. In contrast to other biometrical systems, fingerprint recognition is one of the least disturbing identification methods. This could be caused by awareness of its use since ancient times.

Although the fingerprint readers are wide-spread, there are still some security issues that should be solved. New solutions are being made. The main problem is that the system can be, in some cases, easily attacked. This can be solved by newly-made algorithms with the influence of cryptology for attacks on software basis (e.g. old data replication, modification of data extractor, vector characteristics counterfeit, modification of comparison subsystem, comparison results cange, blocking of communication with database, modification of pattern in database). Another issue is hardware attacks. Modern devices include liveness detection (based on recognition of physiological activities serving as signs of life) to prevent usage of counterfeit fingerprints or fingerprints from dead body fingers (separated or unsevered ones).

We are mainly focusing on FAR (false accept/match rate) and FRR (false rejection rate) using genuine and counterfeit fingerprints in our research. As our research is still in progress, we do not have sufficient results, yet. Our partial results show suitability of adhezive from fusion gun as a mould for counterfeit fingerprint. Unfortunately, first tests with silicone fingerprints were not successful (Kováč, Sulovská, 2009), as the silicone deformed a little bit during gouging out of the mould, probably due to a higher amount of glue contained. This silicone cast test will be repeated with other types of silicone. We would also like to make tests with resins (epoxy, etc.) and other suitable materials. A possibility of using the PMMA as mould and cast will be also tried and tested during the first part of our grant project.

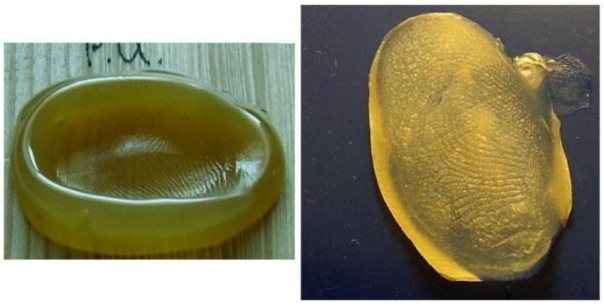

Fig. 3. Mould for plastic casting (left) and gelatine cast (right)

5. CONCLUSION

Biometrical systems are world-wide spread due to the growth in (financial) frauds, forays, rioting, terrorism, computer and information criminality or only for heightening the security level or as preventive means. As many researchers have noticed, there is an emphasis on personal identification and verification. This could be done by the most reliable biometrical systems accessible on the world market - fingerprint recognition, iris and retina recognition and vein recognition.

However, individuals who cannot be identified/verified or even enrolled to the system via their iris or fingerprints characteristics do exist. To enhance utilization of biometrical systems, it appears useful to use a multi-biometric system (Besbes et. al, 2008; Mishra and Pathak, 2009) in order to prevent incommodity during identification. These systems are now being proposed to ensure their effective operation. A multi-biometrical system is also multiple evidence of the same identity using a combination of biometric modalities. This can be compared to systems in highly secured areas where biometric characteristic and the possession of a password/PIN or a token/card are both required for successful access to the area. There is a number of combinations of recognition methods such as iris&face, iris&fingerprint, iris&ear, iris&vein recognitions and many others.

This paper mainly focused on a brief overview of three recognition systems that are included in our grant project at TBU or are intended to be done as consequential research. Each paragraph desribes our aim to be done during our future research activities. As the fingerprint recognition testing is in progress, a short comment on our current results was made with successive procedure for the future. Hovewer, the main issue arisen during our research is the lack of financial resources in relation to purchasing suitable equipment.

6. ACKNOWLEDGEMENTS

This paper is supported by the Internal Grant Agency at TBU in Zlin, project No. IGA/43/FAI/10/D (Research on biometrical systems in term of their endurance, reliability, credibility and integrity).

7. REFERENCES

Besbes, F.; Trichili, H.; Solaiman, B. (). Multimodal Biometric System Based on Fingerprint Identification and Iris Recognition. *3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008*, pp. 1-5, ISBN 978-1-4244-1751-3, Damascus, April 2008

Ghouti, L.,; Al-Qunaieer, F.S. (2009). Color Iris Recognition Using Quaternion Phase Correlation. *Symposium on Bio-inspired Learning and Intelligent Systems for Security, 2009,* pp. 20-25, ISBN 978-0-7695-3754-2, Edinburgh, August 2009

Kováč, P.; Sulovská, K. (2009). Biometrical systems and their usage in IT and data protection. *XII. Ročník mezinárodní konference Internet, bezpečnost a konkurenceschopnost organizací: Řízení procesů a využití moderních terminálových technologií*, Jašek, R. (Ed.), s. 232 - 240, ISBN 978-83-61645-16-0, Kraków – Zlín: EAS, Tomas Bata University, Zlin, 2009

Mishra, R.; Pathak, V. (2009). Human recognition using fusion of IRIS and Ear data. *Proceeding of International Conference on Methods and Models in Computer Science, 2009,* pp. 1-5, ISBN 978-1-4244-5051-0, Delhi, December 2009

Pierscionek, B.; Crawford, S.; Scotney, B. (2008). Iris Recognition and Ocular Biometrics - The Salient Features, *International Machine Vision and Image Processing Conference, 2008*, pp. 170-175, ISBN 978-0-7695-3332-2, Portrush, September 2008

Phillips, P.J.; Scruggs, W.T., O'Toole, A.J; Flynn, P.J.; Bowzer, K.W.; Schott, C.L.; Sharpe, M. (2010). FRVT 2006 and ICE 2006 Large-Scale Experimental Results. *IEEE Transaction on Pattern Analysis and Machine Intelligence 2010*, pp. 831-846, Issue 5, Volume 32, May 2010, ISSN 0162-8828

*** (2007 http://pinktentacle.com/2007/07/necs-drive-thru-face-recognition-system/ - NEC's drive-thru face recognition system, *Accessed on: 2010-09-08*

*** (2005) http://pagesperso-orange.fr/fingerchip/biometrics/types/iris/iris_structure2.jpg, *Accessed on: 2010-09-08*