About user acceptance in hand, face and signature biometric systems

Aythami Morales, Miguel A. Ferrer, Carlos M. Travieso, Jesús B. Alonso

Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones (IDeTIC)
Universidad de Las Palmas de Gran Canaria
Campus de Tafira, 35017, Las Palmas, Spain
phone: +34928451269, fax: +34928452861, email: mferrer@dsc.ulpgc.es
web: www.gpds.ulpgc.es

Abstract. In this article we present several studies about user acceptance when using a hand based biometric system. A survey has been conducted to two groups of biometric systems users. The first group consist of 100 users using a multibiometric scheme during four month in an access control scenario. The biometric scheme include contact-less hand and face as physical biometrics and on-line signature as behavioural biometry The second group include 100 users using a contact-less hand based biometric system also during four month and in the same access control scenario. The second experiment started one year later that the first one and approximately the 30% of the user participate in both experiments. After both experiments, several questions about the acceptance of the different biometrics used were asked to the users in an anonymous way. From the answer we conclude that that the hand biometry is more acceptable than the others when the users have used all of them.

Keywords: Biometrics, user acceptance, hand, face and online signature based identification system.

1 Introduction

Biometrics plays an increasingly important part in authentication and identification systems. The processes of biometric recognition allow the identification of individual based on the physical or behavioral characteristics.

Usually, the different biometric technologies are evaluated by means of the next quality measures:

- **Universality:** each person should have the characteristic**.**
- **Uniqueness**: is how well the biometric separates individuals from another.

- **Permanence:** measures how well a biometric resists aging and other variance over time.
- **Collectability:** ease of acquisition for measurement.
- **Performance**: accuracy, speed, and robustness of technology used.
- **Circumvention**: ease of use of a substitute
- **Acceptability**: degree of approval of a technology.

Universality, uniqueness, permanence, collectability and performance have been the most studied topics in the last 10 years usually in terms of FAR, FRR, EER, DET curves, etc. Instead, a few researches have been focus on user acceptance.

Acceptance of any new technology has been recognized as a main factor affecting its successful implementation. What causes people to accept or reject a new technology? One of the most determinant factors is the perceived ease of use. Refers to the degree to which a person believes that using a particular system would be free of effort. The Technology Acceptance Model [2] is a well-known general model for assessing such success. The model suggests that when users are presented with a new technology, the perceived usefulness and perceived ease-of-use are factors that influence their decision about how and when they will use it.

In [3] was presented a perceived acceptability study of biometric systems. The 76 users respond to different questions about acceptability and sensitivity of privacy details. The results are divided into behavioral (signature, voice, keystroke and pointing) and physiological (fingerprint, hand geometry and retina) biometrics. In general, the behavioral based systems shows better results than physiological and 76 respondents indicated that all biometric systems were perceived as less acceptable than the traditional password approach. Is important to emphasize that this was a study of perceived acceptability. The users were not questioned about if they had been use a biometric system.

Another interesting factor related with acceptability is the “habituation”, defined as continued use of a biometric device. In [4] was establishes a model of the processes of habituation and provides score data from hand geometry to show how this concept works with actual data. Habituation can be defined as the process in which a user of a biometric system adapts his or her techniques to achieve a proper match of his or her biometric template. How does feedback and habituation affect to image quality? In [5] researches try to respond this question. Centered in fingerprint biometry they found that habituation with no feedback at all was not shown to affect the quality of prints. But, feedback and acclimatization did translate into improvement of quality.

Obviously, performance is strong related with user acceptance. If a biometric system has a bad performance (high EER) the user won’t be confident on it and it will be rejected instead of accepted. Besides, user acceptance also depends on subjective assessment of speed and ease of the person-scheme interaction, i.e. if the users are willing to perform the actions required to them to be verified. Aspects as detailed user guidance are also important to be considered because occasional users tend to forget details of operation, such as which finger they should be presenting.

Take into account that when the system requires more cooperation of the user it will be less accepted by the user but less cooperation use to convey longer image processing increasing the answer time which also decrease the user acceptance. A tradeoff between both terms is required.

Other non technological operations that some users could not be willing to perform are those based on privacy, hygiene concerns or religious reasons.

In this article, we focus the attention on acceptability when using a multibiometric device in realistic condition in an access control scenario.

Therefore, the next section will describe the two scenarios considered, Section III will present the questions asked to the user about the acceptance of the different biometrics, following in section IV with a statistic analysis and discussion of the user answers. Conclusions will finish the paper.

2 Scenario Description

We have done two experiments. The first one use hand and face as physical biometrics and on line signature as behavioral biometric, figure 1. 100 users were enrolled and attendee to the experiment once per week during 4 month.

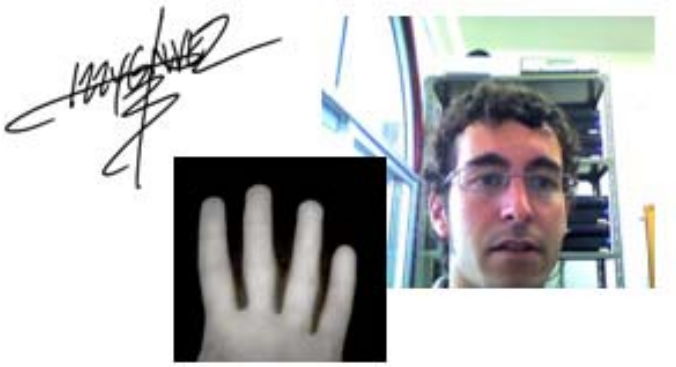

Figure 1 – Signature, face and hand images used for recognition

In the experiment, the users were asked to introduce a personal identification number (PIN) and his/her identity was verified asking for two out of the three biometric randomly selected. The system "open" the door if both biometrics agree giving a positive verification of the user identity. In our experiments, the EER performance was 2%.

The face based biometric technology is an example of contact-less system with a low user interaction. The user collaboration is basically to put the face in front of an acquisition device. We use a simple example of face biometric system composed by a webcam and pc. For hand based biometric, we proposed a contact-less hand base biometric device [5] in order to improve the acceptability of the user: A hand shape was shown in the PC screen and the user is required to adjust his/her right hand to the mask. The hand mask in the screen is as wide as possible in order to make the adjustment procedure as easy as possible. When the overlap between the user hand

and the mask exceed the 75% the hand is parameterized. The hand images were acquired with a webcam in the infrared band.

The on line signature was acquired showing a box in the PC screen and asking the user to sign on the PC screen inside the box. This biometric requires contact with the pen and the screen.

The tablet PC was built in a device that includes the webcam and IR illumination for the hand based biometric, the power supply and the relay system to open the door. The device can be seen in figure 2.

The enrolment was performed with the assistance of a supervisor who explained how to use the system. The next time the acquisitions were done without supervision. The users attendee to the experiment once per week during four months.

The second experiment was done with just one biometric: contact-less hand based biometric. The position of the hand during the acquisition was changed, from the vertical position of the first experiment to a horizontal plane in the second. The place of the experiment was the same than the first experiment. It started one year later than the first one. A 30% of the user participated in both experiments. The device used in this case can be seen in figure 2. Searching an improvement in user usability, the acquisition algorithms were adapted to use a more generic mask. In this case, the EER obtained was a 2.2%.

Figure 2 – On the left device used in the second experiment; on the right device used in the first experiment.

3 Surveys

The last day of each experiment, the user were required to ask for several questions about the acceptance of the device. The questions are divided in two groups, the first one compare the different biometric systems. The questions try to measure the user perception of the different technologies: signature, face and contactless hand. The second group of questions compares the 2 experiments and the user perception about the biometric identification systems. The questions in the first experiment about the user systems perception were:

- Is comfortable the system? Where 5 correspond fully comfortable system – 4 very comfortable – 3 comfortable – 2 poor comfortable – 1 non comfortable and 0 very non comfortable.
- The time necessary to realize the authentication is… Where 5 correspond too much – 4 excessive – 3 normal – 2 good – 1 low and 0 very low.
- Do you feel the system attack your privacy? Where 5 correspond with a strong perception of privacy attack – 4 strong privacy attack – 3 normal privacy attack – 2 poor privacy attack – 1 low privacy attack and 0 a very low perception of privacy attack.

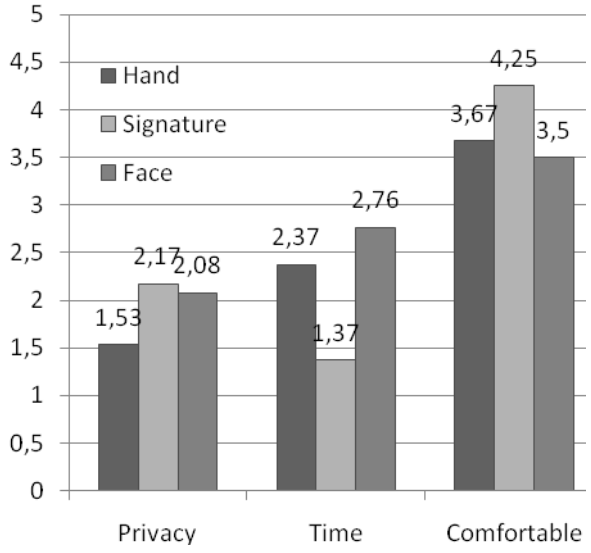

Figure 3 – Systems user perception in first experiment

For the second experiment the questions about the user system perception were:

- Is comfortable the system? Where 5 correspond fully comfortable system – 4 very comfortable – 3 comfortable – 2 poor comfortable – 1 non comfortable and 0 very non comfortable.

- Do you consider the system a hygienic solution? Where 5 correspond a fully hygienic perception – 4 good hygienic perception – 3 medium hygienic perception – 2 poor hygienic perception – 1 low hygienic perception an 0 very low hygienic perception
- Do you feel the system attack your privacy? Where 5 correspond with a strong perception of privacy attack – 4 strong privacy attack – 3 normal privacy attack – 2 poor privacy attack – 1 low privacy attack and 0 a very low perception of privacy attack.

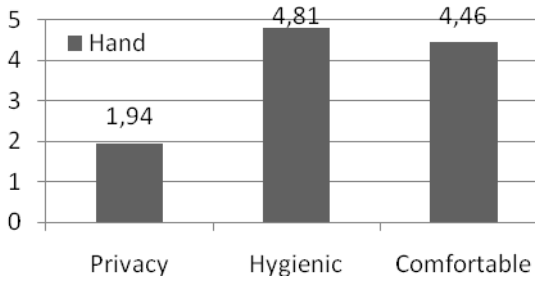

Figure 4 – System user perception in second experiment

Questioned about which of these technologies: contact-less hand, fingerprint, face, signature, speech and iris is the most privacy invasive the users respond that face is the most invasive followed in order by fingerprint, iris, speech, contact-less hand and signature.

In Fig 6 we show the question comparison between both experiments. In the first experiment, each person used the 3 biometric systems, one contact based system and 2 contact-less system. For the second experiment the user only used the contact-less hand biometric system. The questions were:

- Do you prefer contactless systems against contact system? Yes/No response.
- Do you prefer biometric identification against classic identification methods (passwords, ID cards)? Yes/No response.
- Would you be willing to use the contactless hand biometric system daily? Yes/No response.

The figure 5 shows the “Yes” response percentage:

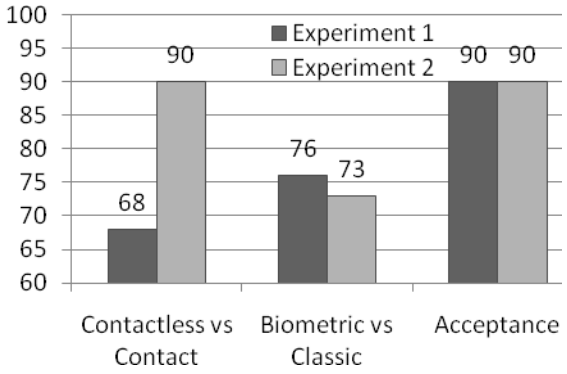

Figure 5 - Comparison between both experiments

4 Conclusions

In general, all system obtains good users response. Comparing the user acceptance of the different biometrics, it looks like the hand is better accepted than face and signature. The hand obtains the best response in privacy term. The signature shows the best response in comfortable term. We think it response is due to the user habituation to this kind of system. The use of signature as identity verifier is common in credit cards payments, the people are habituated to these methods. For new technologies, the habituation is an important factor in user acceptance.

If the user has used just one, it looks like more invasive to his/her privacy than the other no used. The user experience with the system is an important factor to take account in these evaluation questionnaires. Three of each four users prefer the biometric identification against the classic identification methods and nine of each ten users are willing to use the contactless hand biometric system daily.

The use of generic mask improves the user comfortable in the contactless hand. To add a multimodal scheme based on hand geometry and palm texture could solve the performance problems.

Acknowledgments. This work has been produced with the support by the Spanish government in the project. TEC2009-14123-C04.

References

1. Davis, F., Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3): Pages(s). 319-340, 1989.
2. Frank Deane, Kate Barrelle, Ron Henderson and Doug Mahar, “Perceived acceptability of biometric security systems”. Computers & Security. Volume 14, Issue 3, Pages 225-231, 1995.

3. Kukula, E.P.; Elliott, S.J.; Gresock, B.P.; Dunning, N.W; “Defining Habituation using Hand Geometry” on
IEEE Workshop on Automatic Identification Advanced Technologies, Page(s):242 – 246. 7-8 June 2007.
4. Theofanos, M.; Stanton, B.; Micheals, R.; Orandi, S.; “Biometric Systematic Uncertainty and the User” on
First IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS.
Page(s):1 – 6, 27-29 Sept. 2007.
5. Morales, A.; Ferrer, M.A.; Alonso, J.B.; Travieso, C.M.; “Comparing infrared and visible illumination for contactless hand based biometric scheme” on
Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference, Page(s):191 – 197, 2008.