Instruction, Feedback and Biometrics: the User Interface for Fingerprint Authentication Systems

Chris Riley[1], Graham Johnson, Heather McCracken, and Ahmed Al-Saffar

Advanced Technology & Research
NCR Labs
Dundee
United Kingdom
[1]cr230046@ncr.com

Abstract. Biometric authentication is the process of establishing an individual's identity through measurable characteristics of their behaviour, anatomy or physiology. Biometric technologies, such as fingerprint systems, are increasingly being used in a diverse range of contexts from immigration control, to banking and personal computing. As is often the case with emerging technologies, the usability aspects of system design have received less attention than technical aspects. Fingerprint systems pose a number of challenges for users and past research has identified issues with correct finger placement, system feedback and instruction. This paper describes the development of an interface for fingerprint systems using an iterative, participative design approach. During this process, several different methods for the presentation of instruction and feedback were identified. The different types of instruction and feedback were tested in a study involving 82 participants. The results showed that feedback had a statistically significant effect on overall system performance, but instruction did not. The design recommendations emerging from this study, and the use of participatory design in this context, are discussed.

Key Words: Biometrics, Fingerprint, Instruction, Feedback

1 Introduction

As information and communication technologies (ICT) become ever more pervasive in modern life, the security of these systems has become an increasingly important issue. Authenticating legitimate users of computing systems is a necessary process with a number of unique challenges. User authentication falls into three different categories; knowledge-based authentication, token-based authentication and biometrics [1]. Knowledge-based authentication, such as passwords and personal identification numbers (PINs) rely on non-obvious information to confirm the legitimacy of an individual. Token-based authentication relies on the presence of a physical object to authenticate users. In contrast, biometric authentication technologies measure physical, behavioural or anatomical characteristics of the user to verify identity. The attraction of using biometrics is that the characteristics used to

authenticate people cannot be lost, forgotten or readily stolen [2]. Biometrics have the potential to confirm the presence of the actual user, rather than just their password or identity token and are therefore seen as more secure than other forms of authentication.

Biometric authentication technology is beginning to mature and the technology is finding application in both commercial and public sector environments. The International Biometrics Group predicts that the biometrics market will see steady growth and will double in size over the next 5 years [3]. There are a number of trends that underscore this increasing uptake of biometrics. Firstly, there is an international trend towards secure user identification. There are now several large-scale, public facing implementations of biometric systems, including the US-VISIT scheme and the proposed identity card scheme in the United Kingdom. Secondly, the increase of computer security incidents and the need to safeguard information will contribute to an increased usage of biometric technology [4, 5]. Finally, biometric technology is often described as a positive development for the public at large [6]. According to some authors, the benefits of biometrics will eventually lead to the technology being used in almost every application that requires personal authentication [7].

1.1 Usability of Biometric Authentication Systems

Biometrics may be described as the future of user authentication, but there are a number of issues associated with the use of biometrics. The process of biometric authentication involves two stages; an enrolment or registration stage and an authentication stage. During enrolment a biometric sample is associated with an individuals' identity. Identification or verification is the process of matching a second biometric sample with the enrolment sample to verify an individual's identity [8]. The process of automated identity verification through biometrics is often not transparent to users though and most people have little or no familiarity with the technology. Obtaining a high quality enrolment sample is key to ensuring overall system performance, as a poor quality enrolment has a detrimental effect on all subsequent authentications. However, enrolment is the first time most people will have ever used a biometric system, so ensuring quality enrolment is a challenge for all biometric systems. Furthermore, like many other user authentication systems there is a negative relationship between the security and usability of biometric systems [9]. If an implementation of biometric technology is to be successful, both the performance and usability of the system must be carefully considered.

Other usability issues have been identified with specific biometric technologies. Most of the user-centric research on biometrics to date has centered on fingerprint systems, as these systems are the most commonly used biometric [3]. A number of usability issues have been identified with fingerprint systems. For instance past research [10] has found that that finger placement issues arose as users had difficulty placing their finger in a consistent manner. Difficulties in placing the correct part of the finger on the sensing surface, and applying the correct amount of pressure, were also described as problems with fingerprint systems. A lack of system feedback and a lack of instruction were further issues identified when different fingerprint systems were evaluated [10, 11]. They argued that the design of the systems needed to be

improved to facilitate image acquisition. Usability problems with biometric systems have significant ramifications, as people are unlikely to tolerate being mistakenly denied access to their place of work, computer or funds.

1.2 The Biometric Interface

The interface plays an integral role in the usability, or otherwise, of any interactive system and biometrics are no different. Recent examples include the importance of interface design for web tasks [12] and the effect of interface design on peoples' ability to use encryption tools [13]. The design of the interface for fingerprint systems has received an increased amount of attention over the previous few years. Broadly speaking, this research has assessed the instruction and feedback provided to people as they use biometric systems. These issues will be discussed in turn.

Previous research conducted within the financial industry has found that different types of instruction have a significant impact on the overall performance of fingerprint systems. In our experience, verbal instruction from an experienced operator helps people give the highest quality enrolment and is superior to other forms of instruction. Other research has investigated modes of instruction, comparing the effectiveness of face-to-face, video and graphical instructions on the use of a fingerprint system [14]. It was found that pictorial instruction performed significantly worse than either face-to-face or video instruction. Graphical and pictorial instruction for biometric systems has started to be investigated by others [15, 16], however it is unclear how these approaches were evaluated. The small number of studies published to date suggest that face-to-face instruction best facilitates the enrolment process. Verbal instruction is often not a practical approach however, as many biometric systems are used in unattended environments such as automatic teller machines (ATMs) and access to secure physical locations [7]. There is a need to understand how to effectively deliver instruction for biometric systems without face-to-face communication. The information that should be contained in instructions for fingerprint systems is also not well understood.

The feedback a system provides is a second essential aspect of biometric authentication. In addition to providing information about when to place and remove the finger from the sensor, feedback about finger placement is necessary to facilitate the image acquisition process. The position of the finger on the sensor, pressure, finger movement and skin wettedness all affect the image acquisition process, but it is difficult to relay all of this information without overloading users. Feedback in the form of a biometric sample quality measure has been investigated and the effect of image acquisition assessed [17]. The effect of this 'quality gauge' feedback over several weeks and it was found that peoples' performance with the fingerprint sensor improved overtime. This is not an optimal approach to presenting feedback however, as no specific information about finger placement is provided. It was argued that people are not readily able to view an image of their fingerprint on screen and assess whether it is a high or a low quality image [17]. A well designed fingerprint system should provide feedback that is immediately understandable the first time it is used, though it remains unclear which type of feedback is most helpful for users.

We set out to design a graphical user interface for a fingerprint system that would include instructional and feedback aspects that would allow people to use the system effectively without assistance. A participatory design process was used to develop this interface. The development and testing of this interface are described below.

2 System Development

A graphical user interface was developed to support a commercially available, capacitance fingerprint sensor. An image of the sensor can be seen in figure 1 below. An iterative participative approach was taken when developing the user interface and both experienced and novice users where brought into the design process. Firstly, a review of existing instruction and graphical interfaces for biometric systems was carried out and six people were invited to use the fingerprint sensor with a legacy interface. Participants were then asked to volunteer ideas or ways to improve the instruction, interface or overall design of the system. A number of these interface design ideas were then explored using low fidelity paper prototypes. These low fidelity prototypes were then evaluated with a further six people, including 2 individuals from the first group of participants. Numerous issues with the interface were discovered during this design and evaluation process, such as a lack of understanding about the difference between enrolment and verification and the need for graphical instruction. A combination of the designs that were viewed most favourably by participants, and the approaches the designers believed to be most appropriate, were then developed in functional prototypes. Images of the low and high fidelity designs can be seen below in Figure 1.

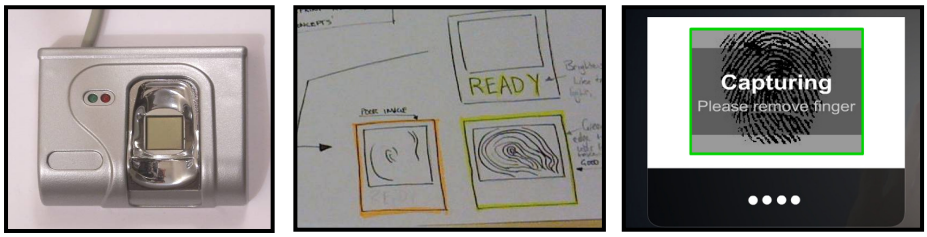

Fig. 1. The fingerprint sensor used in this evaluation (left). Low and high fidelity design prototypes

During the design process, two different types of instructional lead-through were developed into fully functional prototypes. Both instructional approaches were designed to assist people with correct finger placement when using the fingerprint sensor. The first focused on which part of the finger should be placed on the sensor, as placing the tip of the finger on the sensor is a common behaviour that leads to poor quality images. The second method focused on using tactile features of the sensor as a finger placement guide. The fingerprint system used had a defined ridge at the lower edge of the sensing surface, designed to sit under the crease of the distal interphalangeal joint, when a finger is placed on the sensor. The tactile instruction

emphasised this ridge and encouraged people to use it to assist finger alignment. A decision was made to make the lead-through animated, as the work of Theofanos et. al. [14] suggests that static pictorial instruction is less effective than video instruction. Each instructional video was 20 seconds in duration. Still images from both types of instructional lead-through can be seen below in figure 2 below.

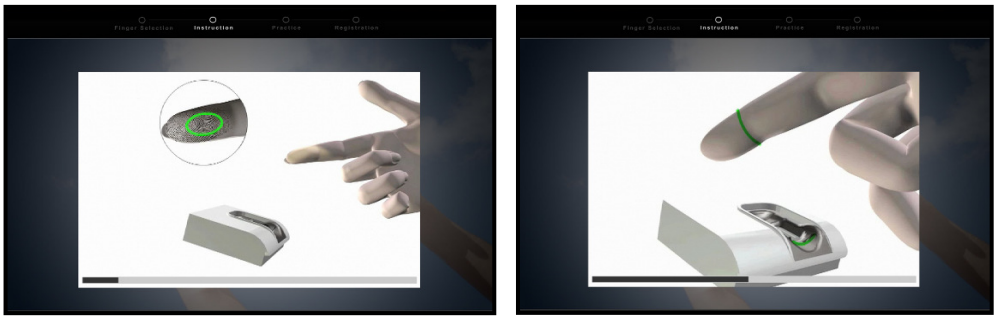

Fig. 2. Images of the lead-through focusing on finger placement (left) and tactile cues (right)

Two different approaches to the presentation of feedback were also identified during the development process. Displaying an image of the user's fingerprint on-screen emerged as one way to assist users during image acquisition. A graphical representation of the quality of the fingerprint image also received positive feedback from people involved in the design process. The image quality feedback used here was similar to the quality feedback used by Theofanos et. al. [17]. A third feedback approach was also developed into a functional prototype, a combination of pictorial and quality feedback. Here, a pictorial image of the users fingerprint is displayed on screen along with an associated measure of quality for that image. These three types of feedback can be seen in figure 3 below, and will be referred to as *pictorial, quality* and *combined* feedback for clarity. All feedback was displayed during image acquisition in near real time. The quality feedback was based an algorithm specific measure of the quality of a fingerprint image.

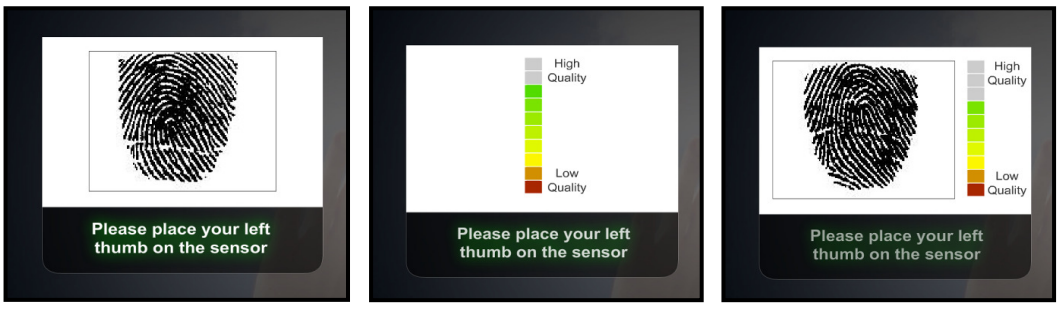

Fig. 3. Images of different feedback approaches: *Pictorial* image of users fingerprint (left), image *quality* (centre) and *combined* pictorial plus quality (right).

3 System Evaluation

The functional prototypes underwent a further evaluation to determine which type of lead-through and which type of feedback are the most appropriate for commercial applications of fingerprint technology. A no instruction condition was also tested to understand how helpful the instructional graphics actually were. The different instruction and feedback approaches were counterbalanced to produce nine different evaluation interfaces. The structure of the evaluation and the number of participants who used each interface can be seen in table 1 below. Each participant used only a single instruction/ feedback combination in an independent groups design. A repeated measures design was not used as assessing the impact of instruction would be problematic if learning affects were present. The functional prototypes were tested with a group of people who had not been involved in the design process.

Table 1. Number of participants who used each type of instruction and feedback. In total 9 different prototype interfaces were tested.

	Pictorial Feedback	**Quality Feedback**	**Combined Feedback**	**Total**
Finger Placement	9	9	9	**27**
Tactile Instruction	9	9	9	**27**
No Instruction	9	9	9	**27**
Total	**27**	**27**	**27**	**82**

During the evaluation participants were asked to follow the instructions on screen, enrol and subsequently verify their identity using the fingerprint system. Four images were captured by the system during the enrolment process. Participants were then asked to use the system five times to verify their identity. A number of dependent measures were recorded during system use including image acquisition time, a measure of image quality and a matching score. The fingerprint system was tested with the default image acquisition and matching settings. During system usage the experimenter provided no assistance and only stepped in if the participant became stuck or experienced significant difficulty. After using the fingerprint system, participants completed a questionnaire designed to collect subjective information about their experience using the system. Finally, a brief semi-structured interview concluded the evaluation.

4 Results

A total of 82 people took part in this evaluation, with 27 people experiencing each of the instruction and feedback approaches. Participants ranged in age from 18 to 62 years with a mean age of 26.1 years. 51 of the participants were female and 30 were

male, with gender information not recorded for one participant. All participants were recruited from a local university and were a mixture of students and staff. Participation in this study was voluntary, though people were rewarded for taking part.

4.1 Instruction

The different types of instruction did not have a significant effect on the overall performance of the fingerprint system. One way ANOVA tests revealed that there was no significant effect of instruction on any of the enrolment or verification metrics recorded by the system. Table 2 summarizes the performance of the three different types of instruction.

	Mean enrolment quality	Mean enrolment time	No. of failures to enrol	Mean verification quality	Mean verification time	Mean matching score	No. of false rejection
Finger placement	248.0 (18.9)	24.0 (19.5)	0	247.6 (18.6)	4.1 (3.2)	457.3 (229.0)	7
Tactile Instruction	247.4 (13.7)	21.9 (17.8)	1	245.7 (21.8)	5.2 (3.1)	423.4 (162.2)	7
No Instruction	237.8 (40.2)	36.7 (44.2)	2	247.1 (23.7)	5.0 (4.9)	472.9 (229.5)	7

Table 2. Summary of performance metrics across the different instruction conditions. Measures of time are given in seconds. Standard deviations in parenthesis.

4.2 Feedback

The different methods of feedback affected the overall performance of the fingerprint system. There was a significant difference in average image quality during enrolment across the three feedback conditions. Assumptions of parametric testing were not met, so non-parametric tests were used. A Kruskal-Wallis test revealed that there was a significant effect of feedback ($H(2) = 8.45$, $p < .05$) on image quality. Bonferroni corrected post hoc testing revealed that there was a difference between the *pictorial* and *quality* feedback approaches ($U = 242$, $p < .0167$), but no other differences. Figure 4 below shows the differences in quality scores for the three types of feedback. It should also be noted that all three failures to enrol occurred where participants did not have pictorial feedback, though this data is not suitable for hypothesis testing.

There was also a significant difference in the average matching scores across the feedback conditions as revealed by a one way independent ANOVA ($F(2,77) = 4.97$, $p < .01$). The matching score is a statistics reflecting the similarity of verification images to the enrolment template and is used to determine the match/ no match result. Bonferroni corrected post hoc testing revealed that the *pictorial* feedback preformed significantly better than the *quality* feedback approach ($t(48) = 2.73$, $p < .0167$). There were no other differences in matching score between the different types of feedback. The mean matching scores are illustrated in figure 4 below. Table 3 below summarizes the performance statistics across the three types of feedback. Interaction

effects between instruction and feedback were also tested in a two way ANOVA, for all dependant variables, but none were found to be significant.

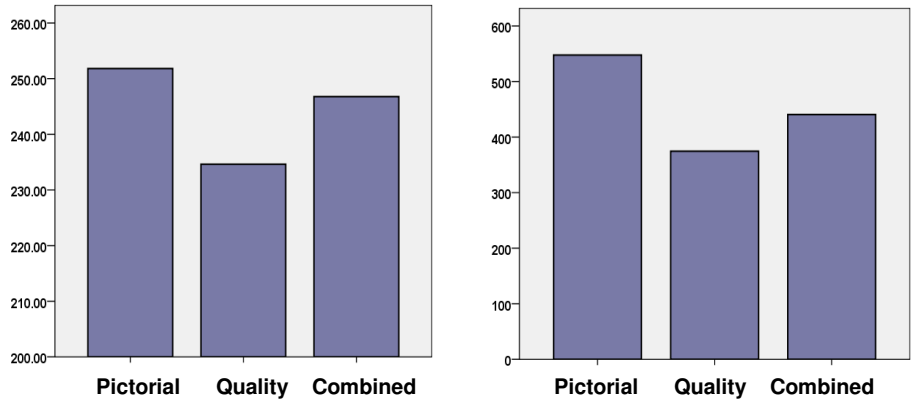

Fig. 4. Graphs of average image quality during enrolment (left) and average verification score (right) across the different feedback conditions.

Table 3. Summary of performance metrics across the different feedback conditions. Measures of time are given in seconds. Standard deviations in parenthesis.

	Mean Enrolment Quality	Mean Enrolment time	No. of failures to enrol	Mean verification quality	Mean verification time	Mean matching score	No. of false rejection
Pictorial Feedback	**251.8 (9.8)**	25.8 (28.1)	0	249.1 (19.2)	4.9 (3.6)	**547.5 (216.5)**	3
Quality Feedback	**234.6 (37.1)**	25.9 (24.0)	3	245.9 (16.6)	4.3 (3.1)	**374.5 (184.2)**	13
Combined Feedback	**246.7 (24.3)**	31.3 (38.0)	0	245.2 (26.5)	5.1 (5.6)	**440.5 (191.8)**	3

4.3 User Perception of the System

After using the fingerprint system participants completed a short questionnaire. Questions about the ease of use, speed, security, acceptability, aesthetics, privacy impact and clarity of feedback and instructions were included. A number of questions about participants' wiliness to use biometric systems in the future were also included. Figure 5 below shows participants' average ratings of system ease of use, privacy impact of biometrics and willingness to use biometrics across all feedback and instruction conditions. Overall, participants had a positive perception of the fingerprint system and the mean scores for all questions were towards the positive end of the scale. Kruskal-Wallis tests revealed that participants' perception of the fingerprint system was not affected by the different interface designs. There were no

differences in participants' answers for any question, across the three types of instruction. There were also no significantly differences in participants' opinion towards the system across the different types of feedback.

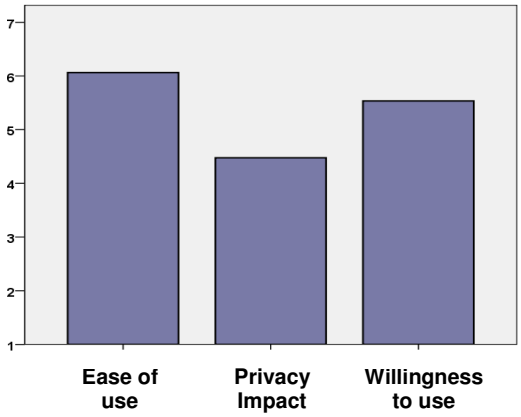

Fig. 5. Participants' mean ratings of system ease of use, privacy impact and willingness to use biometrics across all participants. Questions used a rating scale where 1 was negative and 7 was positive.

4.4 Demographic Effects

Tests were performed to identify any demographic effects present in the results. There were no significant effects of age, gender, height, handedness or previous experience with biometrics on system performance. Age and gender were also compared with results from all questionnaire responses. In all 20 tests were carried out and one relationship was statistically significant. One test would be expected to return a significant result at the .05 level (type I error) over this number of tests however, so this no effects are reported.

5 Discussion

5.1 Effect of Instruction

The instruction used to support use of the fingerprint system did not have an effect on overall system performance in this study. It was though that there would be considerable differences in the way the system was used with different levels of instruction. Based on the work of Coventry [2] and Sasse [18] this would have seemed to be a reasonable prediction to make. There were no differences between the

two types of graphical lead-through and no difference between the presence and absence of instruction seen in any of the dependant measures recorded. This result would seem to be at odds with the previous work by Theofanos et. al. [14] who found clear differences between instruction models. This study compared the semantic content of instructions rather than the way the instructions were delivered, so the results are not directly comparable. However, the lack of difference between the presence and absence of instruction suggests that the instruction had very little effect.

One possible explanation of the lack of effect of instruction, is that participants did not understand the graphical instructions. After using the fingerprint system participants were asked about the clarity of instruction and feedback. Almost all participants described the instruction as clear or easy to understand. Some participants demonstrated they understood the instruction and comments such as the following were not uncommon:

"It was telling me to line my finger up with that ridge so I did that…" A second explanation that is more consistent with participants' comments, is that people expected the system to be easy to use and so were less inclined to attend to the instructions. For instance, one participant tried to swipe their finger across the sensor despite the animated lead-through showing a finger being placed on the sensor. It is not unusual for people to ignore instructions, and Sasse [19] has described situations where users have ignored instructions for other authentication and security systems. Comments from participants such as:

"The video at the start was too long" were also common. Overall, the transaction was comparatively simple; participants had to enrol and validate with only one finger, so the level of instruction may have exceeded the complexity of the task. If the different instructions had been tested in a more challenging environment, differences between instruction types may have emerged. This study however, where most participants did not experience significant problems using the system, was not sensitive enough to detect any difference between the presence and absence of instruction.

5.2 Effect of Feedback

The different types of feedback presented to users during the image acquisition had a clearer effect on the performance of the fingerprint system. Feedback had a significant effect on the quality of images captured during enrolment and the overall verification performance was also different. Feedback based on the *quality* of the fingerprint image resulted in a lower average matching score than *pictorial* feedback of the users own fingerprint. Lower matching scores mean that users are more likely to be falsely denied access to the system. All cases of participants failing to enrol with the system also occurred when people had no pictorial feedback. From these results it seems reasonable to conclude that the *pictorial* feedback is preferable to feedback relating to the *quality* of the biometric sample.

Feedback about the quality of a submitted image has been shown to improve users' interaction with fingerprint systems in the past [17]. This study did not test *quality* feedback against no feedback at all, but it did show that *pictorial* feedback is more helpful to users than information about *quality* only. An assertion that underpinned

Theofanos et. al. [17] study was that normal users were not good at visually interpreting an image of their fingerprint onscreen and adjusting their behaviour. Participants in this study described the *pictorial* feedback positively and it appeared that people were able to interpret the *pictorial* feedback and adjust their behaviour accordingly during image acquisition. Inconsistent finger placement between enrolment and verification is one of the main reasons for false rejection, and *pictorial* feedback seemed to make people more aware of this issue.

The fingerprint technology used in this study and the Theofanos et. al. [17] study was not the same. The sensor used here was a small, direct contact, silicon sensor with a sensing area of 14mm x 14mm. A larger, optical sensor was used in past research [17], which could capture images from multiple fingers at a time. Though *Pictorial* feedback proved to be useful in this evaluation, it is likely that larger fingerprint sensors are more tolerant of inconsistent finger placement and *pictorial* feedback may not be as useful in this situation. Although participants' comments suggest *pictorial* feedback was also useful when determining how pressure affected the image quality, so *pictorial* feedback may still be useful for larger optical fingerprint systems.

At the start of this study it was hypothesised that combining *pictorial* and *quality* style feedback would be the easiest for people to interpret, and would consequently lead to better performance. This was not the case however, as there was no statistically significant difference between *pictorial* feedback and the *combined* feedback approach. Across most measures, there was a trend of *pictorial* feedback performing better than the *combined* feedback. A possible explanation for this result is that the *combined* feedback approach was too busy or complicated for people to usefully interpret. Having both an image of the fingerprint and a measure of quality on screen, each updating several times a second, could have been too much for people to attend to. Displaying two types of feedback may have caused participants to divide their attention between the two information sources, with a corresponding deterioration in performance. If this was the case a different design, with the two information sources more closely integrated may not have suffered the same drop in performance. Alternatively, the *combined* feedback could have been too information rich for people to use. Our aim of making the fingerprint system as usable and accessible as possible may have resulted in an overcomplicated interface, relative to the task. The image acquisition process is short, typically lasting only a few seconds, so any feedback presented to people must be simple and easy to understand.

5.3 User Perception of Biometrics

In general the people who took part in this study had a positive opinion towards the fingerprint system. People rated the system as easy to use and described themselves as willing to use biometrics again in the future, however some people in this study were concerned about the privacy impact of biometrics. This question about privacy received the lowest rating overall and the mean score was just above the scale midpoint. This result is consistent with previous research which has identified privacy concerns about biometric technology [20, 21]. It is worth noting that peoples' opinion of the fingerprint system were not affected by the interface they used; neither

instruction nor feedback had an effect on participants' ratings of biometrics. This suggests that it is difficult to influence peoples' opinion towards biometrics by altering the design of the interface.

5.4 Participative Design Process

A participative design approach was taken when developing this interface. People were brought into the design process at several stages and a number of different lead-though and feedback approaches were discussed. In general, it proved difficult for people to articulate and describe the problems they encountered when using the fingerprint system, or to provide suggestions for improvement. Most of the people we talked to thought that fingerprint systems would be easy to use and this perception persisted throughout discussions of system design. This interface was essentially designed to support a single behaviour – placing one's finger on a fingerprint sensor. This would seem to be a simple task and the difference in the biomechanical movement between good and poor finger placement is very small. In our experience, it was difficult to engage people in discussion about this particular issue. People were happy to volunteer their thoughts and feelings about the applications for, and suitability of biometric systems, but it proved difficult to engage people when discussing this narrow aspect of interface design. The participative design process yielded richer information for wider issues such as the acceptability of biometrics, rather than issues like instruction and interface design.

6 Conclusions

Designing usable biometric systems is a challenging task. Ensuring that people can use systems effectively on first use remains an issue for biometric authentication systems. The results of this evaluation show that the design of the interface is essential element of usable fingerprint systems and the way feedback is presented effects overall system performance. Based on the results of this study we make the following design recommendations for fingerprint systems:

- Displaying pictorial feedback is beneficial for people using a small fingerprint sensor.
- Provide a graduated level of assistance to users. Instruction proved unnecessary for most people, but is helpful for those who do experience difficulties. Provide more instruction and guidance if people struggle during the image acquisition process.
- Keep the information on screen to a minimum. For most, the interaction with a fingerprint sensor is very brief, so people do not have time to process large amounts of information.
- Ensuring a high quality enrolment is an essential aspect of biometric authentication system design.

The challenges inherent in implementing biometric technology are one reason why biometric systems have not received wider uptake despite their reputed advantages. Designing a biometric system that can be used by the general public, without

providing assistance, would have a significant benefit and would increase the number of applications and contexts were biometrics could usefully be used.

A usable interface for biometric systems is only part of the issue however. Many people are genuinely concerned about data security and the use of biometric systems, and these concerns must be addressed if any implementation of biometrics is to be successful. These issues are much broader than the user interface, and further research should address how to effectively convey information about data storage, data access rights and security policies to the people who will use biometrics. Making biometric systems usable is an essential element of system design. However, biometrics must also be acceptable for the people who use them and this issue has not received the attention it deserves.

Acknowledgements. We would like to thank Jamie Shek for his invaluable help during the design stages of this project. We would also like to thank Andrea Szymkowiak and Jim Bown from the University of Abertay Dundee for their support of this research. Finally, we are indebted to the Scottish Executive and Technology Strategy Board U.K. for their sponsorship of this project through the Knowledge Transfer Partnership scheme.

References

1. Renaud, K.: Evaluating Authentication Mechanisms. In L. F. Cranor & S. Garfinkel Security and Usability: O'Reilly (2005)
2. Coventry, L.: Usable Biometrics. In L. F. Cranor & S. Garfinkel, Security and Usability: O'Reilly (2005)
3. International Biometrics Group (IBG): Biometrics Market and Industry Report 2009-2014. (2009) from http://www.biometricgroup.com/reports/public/market_report.html
4. Chandra, A., & Calderon, T.: Challenges and Constraints to the Diffusion of Biometrics in Information Systems. Communications of the ACM. December 2005/Vol. 48, No. 12, 48(12), 101-106 (2005)
5. Maple, C., & Norrington, P.: The Usability and Practicality of Biometric Authentication in the Workplace. Paper presented at the First International Conference on Availability, Reliability and Security. IEEE Computer Society. (2006)
6. Celent.: Biometric Technologies: Are We There Yet? Celent Communications, Boston. (2006)
7. Jain, A., Hong, L., & Pankanti, S.: Biometric Identification. Communications of the ACM, 43(2), 91-98 (2000)
8. Ashbourn, J.: Biometrics: Advanced Identity Management: Springer. (2000)
9. Patrick, A.: Usability and acceptability of biometric security systems. Paper presented at the NATO Workshop on Enhancing Information Systems Security Through Biometrics, Ottawa, Canada. (2004).
10. Coventry, L., DeAngeli, A., & Johnson, G. I.: Biometric Verification at a Self Service Interface. In Contemporary Ergonomics 2003. Rutledge, U.K. 247-252 (2003b)
11. Coventry, L., Angeli, A. D., & Johnson, G. I.: Honest It's Me! Self Service Verification. In the Proceedings of the CHI Conference on Human Factors in Computing Systems, Workshop on Human-Computer Interaction and Security Systems. Fort Lauderdale, Florida (2003a)

12. Miller, R. C., Chou, V. H., Bernstein, M., Little, G., Kleek, M. V., Karger, D., et al.: Inky: A Sloppy Command Line for the Web with Rich Visual Feedback. Paper presented at the Symposium on User Interface Software and Technology, Monterey (2000)
13. Garfinkel, S. L., & Miller, R. C.: Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. Paper presented at the Symposium on Usable privacy and security (SOUPS), Pittsburgh (2005)
14. Theofanos, M., Stanton, B., Orandi, S., Micheals, R., & Zhang, N.-F.: Ten-Print Fingerprint Capture: Effect of Instructional Modes on User Performance. Paper presented at the Human Factors and Ergonomics Society 51st Annual Meeting (2007)
15. Hoffman, P.: Visualizing the Use of Biometric Systems: Tackling Symbolism, Context and Interpretation Paper presented at the International Workshop on Usability and Biometrics, Washington (2008)
16. Ormiston, G.: Addressing the Worldwide Biometric Enrolment Challenge: Guidance Without Words. Paper presented at the International Workshop on Usability and Biometrics, Washington (2008)
17. Theofanos, M., Micheals, R., Scholtz, J., Morse, E., & May, P.: Does Habituation Affect Fingerprint Quality? Paper presented at the CHI Conference of Human Factors in Computing Systems, Montréal., Canada (2006)
18. Sasse, A.: Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems. IEEE Security & Privacy, 78-81 (2007)
19. Sasse, A.: Usability and trust in information systems. Cyber Trust & Crime Prevention Project. University College London, London (2004)
20. BioSec.: Report on results of first phase usability testing and guidelines for developers. BioSec Consortium (2004)
21. Toledano, D. T., Pozo, R. F., Trapote, A. H., & Gomez, L. H.: Usability evaluation of multi-modal biometric verification systems. Interacting with Computers, 18 1101-1122 (2006)