Biometric verification at a self service interface

Lynne Coventry
Antonella De Angeli
Graham Johnson

Biometric Verification at a Self Service Interface

Lynne Coventry, Antonella De Angeli and Graham Johnson

NCR- FSD Advanced Technology and Research,
Discovery Centre, 3 Fulton Road,
Dundee, UK, DD2 4SW

The term biometrics refers to a variety of identification techniques, based on a physical, or behavioural user characteristic. Traditionally, access to ATMs, has been controlled by possession of an artefact (card) and knowledge of a Personal Identification Number (PIN). Biometric verification is a potential alternative. At NCR, investigations into biometrics have been undertaken over a number of years. These investigations have used a variety of methods to gradually acquire a sound understanding of consumers' issues. Our research has revealed a number of non-trivial issues with the introduction of this type of technology to the general public. We will present some of our findings and general understanding of the public's attitudes towards and behaviour with, biometrics verification in general and specifically fingerprint at the ATM.

Introduction

Biometrics can be defined as the use of anatomical, physiological or behaviour characteristics to recognise or verify the claimed identity of a person. It requires the collection, processing and storage of details of person's physical characteristics. Biometric technologies are used to confirm that the person is present rather than their token (e.g. bankcard) or identifier (e.g. PIN). A name, password, card, PIN, or key does not confirm the presence of the legitimate person. They rely on the assumption that the card is always with the owner and owners do not reveal their PIN/password to others, however loss and sharing of cards are big security weaknesses in a system.

The appeal of biometrics is a technology, which can not be easily stolen, lost or transferred. Our usability research, based on consumers and their behaviour and attitudes has been instrumental in directing developments of these technologies and their use in self-service settings. It is too easy to forget that advanced technologies per se will not succeed without easy adoption by the intended users. Biometric technologies are a good example of advanced technology that impresses many, without understanding the impact users may have on successful implementation.

Biometric Techniques

Physiological biometrics includes those based on verification of fingerprints, hand and/or finger geometry, eye (retina or iris), face, wrist (vein). Behavioural techniques include those based on voice, signature and typing behaviour. The performance of these systems varies greatly.

Performance metrics

The performance of a biometric system must be excellent if users are to trust and accept it. Performance metrics should indicate how well a system performs but it is difficult to get reliable data on particular systems and more independent testing is required. Performance is measured in terms of false accept rates (FAR) – the likelihood that an illegitimate person will be able to access the system, and false reject rates (FRR) – the likelihood that a legitimate person will be denied access. The problem is the interconnection between these two measures, as one improves the other worsens.

Two other measures are important, failure to enrol (FTR) and failure to acquire an image (FTA). These effectively identify those people who will not be able to use the system (outliers) and those who may have difficulty using the system. It is also necessary to consider the effect of ageing on the chosen technique – facial and fingerprint templates would need updated.

The method by which these figures are gathered can seriously impact the performance achieved. Performance estimates are often far more impressive than actual performance (Phillips et al 2000). Systems tested in laboratory conditions with a small homogenous set of "good", trained, young, co-operative users may generate completely different results than testing in a live environment with inexperienced and less co-operative users.

Biometrics and the ATM

On the surface there appears to be many valid reasons to replace PIN at the ATM: the PIN does not prove the identification of the cardholder; PINs can be forgotten leading to user frustration; using the wrong combination of card and PIN may result in retention on cards; people write PINs and disclose to others increasing the risk of fraud (Hone et al 1998); and PINs can be stolen by observations.

Clarke (1994) presents the desirable characteristics of an ideal biometric. The characteristics are that it be universal, unique and exclusive, permanent through life, indispensable, digitally storable, precise, easy and efficient to record and acceptable to contemporary social standards. It seems that not all these objectives can be met by any current method. Many systems do not live up to expectations because they prove unable to cope with the enormous variations among large populations or fail to take into account the needs of people. (Davies 1994)

One of the big issues with the ATM environment is the potential size of the user base – even a small financial institution could have millions of customers. Ultimately the system would have to deal with the entire banking population of the world. This affects a number of factors associated with biometrics including use of verification rather than recognition, enrolment, template storage and handling of outliers.

Verification

Given the potential size of user base, the processing time alone required to identify a person would make it impossible to use in a real time application. Thus the use of verification – one to one match with template for claimed identity is used. The does not preclude back office identification testing for fraudulent identity.

The users must collaborate with the system to produce a biometric for instance placing a finger on the device or looking at a camera.

Enrolment

Any one wishing to use a biometric system must be enrolled. This is a key opportunity for learning as well as providing the biometric images from which a template is produced. A good enrolment template is key to efficient and accurate verification. This is also the point where the user can be trained how to use the system and any misconceptions resolved.

Template storage

This has size, bandwidth, privacy and security issues to balance. If fingerprint is adopted, this could be done locally on a smart card with the user carrying the template on their card, even processing their fingerprint on the card to enable use of the card. Thus eliminating the complications of remote storage and processing.

Handling outliers

Extreme examples are those people who do not have the required characteristic, for instance no eyes or no fingers. However some people may be unable to use the system through illness, e.g. tremors, glaucoma, traumas e.g. cut to the fingers, broken hand. The ageing process can also cause problems and with some biometrics the template would require updating. Outliers must be accommodated without causing discrimination.

Understanding the consumer

To fully understand the role of the consumer in the performance and acceptance of biometrics, we have utilised a number of research methods through different stages of development of new biometric technologies. The most extensive research has been carried out on iris verification. This is reported in Coventry and Johnson (1999) and Coventry *et al* (2003) Our methods include focus groups to identify consumers' understanding, misconceptions, and barriers to acceptance of biometric techniques. This technique elicits attitudes, which may or may not correlate with actual behaviour. Specific studies help to understand how well a specific technology works with the general, untrained public and if it can be adapted to a self service environment. An iterative design and evaluation process is followed to build a self-service application and field trials are used to fully test performance and acceptance. We have found that experience with the actual technology can change people's attitudes in both positive and negative directions.

The remainder of this paper will present results about biometrics in general with focus on recent fingerprint studies.

Consumer attitudes to biometrics

Our research has shown that there is a general lack of public understanding of how a biometric or even a PIN works. This is often expressed in terms of a level of suspicion or distrust. Some key findings are that:

- There is little perceived need for the addition of biometrics.
- Consumers have difficulty believing some "futuristic" technologies can work well.
- There is a general concern about the potential misuse use of personal data and is seen as potentially violating privacy and civil liberties. These views vary between countries and cultures and are extensively reviewed in Woodward (1997).
- There are concerns about hygiene with touching such devices and health risks for more advanced technologies such as iris or retina. Fear of criminals killing to steal

their eye or finger. This view is not helped by films such as Mission Impossible (Davies, 1997)!

With reference to fingerprint our focus group studies have found different attitudes to those reported elsewhere. We found that people believed fingerprints would work because it was extensively used in criminology. They did not believe that its association with crime deemed it socially unacceptable. However, a UK based survey of 500 people found that it was deemed to be most reliable biometric but least socially acceptable when compared to signature, facial and PIN.

A user study of finger print technology

We are currently involved with the development of a new fingerprint technology that requires the user to move their finger across a thermal sensor rather than placing their finger on a optical or capacitive sensor. This swiping action ensures no fingerprint is left behind and the technology removes some of the problems with other fingerprint technology dealing with fine, aged or damaged skin.

This study looked at the base usability of the sensor and assessed the amount of support a user would require in order to provide an adequate image. The trial was conducted over 2 days in Edinburgh. Participants were required to enrol and authenticate using the system. A total of 82 people participated in the evaluation. The evaluation included a representative sample range of height, sex, and age. People were spread across three different enrolment conditions:

- Level 0: No *instruction and limited feedback*. Participants were instructed to "swipe their finger" and told whether it was a good/bad swipe. Unsuccessful participants progressed to the next level after 8 attempts.
- Level 1: Instruction *and limited feedback*. Participants were given clear instructions on how to swipe their finger and told whether it was a good/bad swipe. Unsuccessful participants then progressed to the next level after 8 attempts.
- Level 2: Full *instruction and feedback*. Participants were given clear instructions on how to swipe their finger and they were shown their fingerprint image on a laptop. Additionally they were told whether the image was good or bad. Unsuccessful participants were required to repeat the enrolment in the same condition.

Each participant chose which finger to enrol and then used that finger for the duration of the trial. Each participant had to achieve a minimum of four good fingerprint images in order to pass the enrolment procedure. The interviewers subjectively assessed the quality of the fingerprint image and allocated it as "pass" or "fail". Once the interviewer has submitted three good images, the fourth one was automatically compared to the other three and if it matched the participant had successfully completed the enrolment procedure.

During the authentication trial, all participants were given the same instruction. A total of six authentications were required from each participant. At the end participants were asked to complete a questionnaire.

Results

The average age of participant was 34.6 years (SD 14.44), with a range of ages from 16 to 73 years, almost equal numbers of men and women (N = 82, 42 men and 40 women). The majority of participants (78%) used their right index finger to swipe with. 20% used their right middle finger and 2 participants used their left middle finger. Seven

participants (8.5%) failed to enrol. The next analyses are conducted on the sample that succeeded to enrol (N=75).

Figure 1 reports the percentage of participants who successfully enrolled after 1, 2 or 3 enrolment sessions as a function of experimental conditions. The effect of feedback is evident: there is a consistent increase in the number of participants enrolling first time as the initial level of instruction and feedback increases. In Level 0, when no instruction and limited feedback was provided, only 40% of participants succeeded to enrol at the first attempt. In Level 1, when participants were provided with clear instruction on how to swipe their feedback, this percentage raised to 64%. In Level 2, when participants were given instruction and visual feedback, the majority of the sample (80%) enrolled at the first attempt. However, it is also evident that some people had problems with the systems, and needed more practice with the system, independent of the amount of instruction or feedback received.

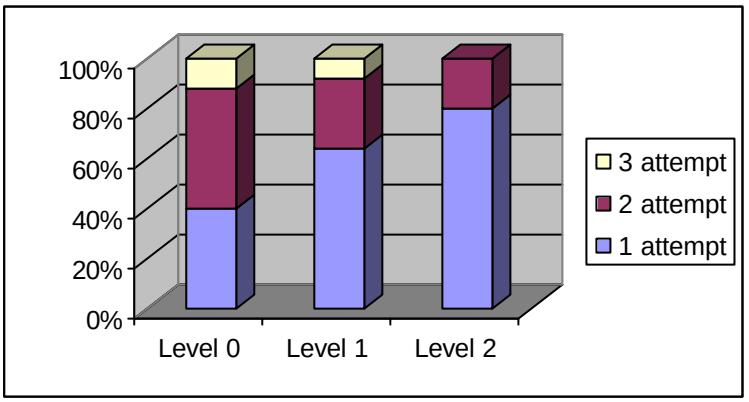

Figure 1: Percentage of successful enrolments

After enrolment people were required to authenticate 6 times. This part of the experiment highlighted new problems with the system. Less than half of the sample (47%) achieved 6/6 successful verifications. Some 28% could be verified 5 out of 6 times and 8% 4 times. The remaining 17% were successful only 3 times or less out of 6 (with 1 participant never being successful).

Because of its severely skewed distribution, the number of successful verifications were analysed by the Kruskal-Wallis H tests, the non-parametric analogue of one-way analysis of variance. Two analyses were conducted to test the effect of feedback received and number of enrolment sessions on the likelihood of successful verifications. Number of enrolment sessions was considered as an indicator of individual difficulties in using the system.

To test the effect of feedback, the final level of enrolment was entered as grouping variable. Results demonstrated that the likelihood of successful verification is not affected by type of instruction and feedback received ($\chi^2_{(1)}$=.16 p = ns).

To test the effect of number of enrolment sessions, two groups of people were compared: those who succeeded at the first attempt and those requiring 2 or more. This analysis showed a significant effect ($\chi^2_{(1)}$= 8.46, p = < .01). Independent of the level of enrolment, people who completed their enrolment after one attempt were much more likely to authenticate that people who needed 2 or more different enrolment sessions. The first group succeed on average 5.2 times, the second group 4.2. This finding confirm

the hypothesis that some people had individual problem with the system which could not be solved by instruction, training or feedback.

In the questionnaire people reported believing the fingerprint system would be more secure than PIN.

Discussion

Although biometric technologies are still improving, there are inherent performance limitations, which remain and are extremely difficult to work around, except perhaps by combining multiple technologies. These limitations are unique to each kind of biometric technology. We found that some participants simply could not use the system and we were unable to identify the reasons for the failure. This situation would be unacceptable at an ATM if it prevented people from accessing their money.

Our evaluations with the diverse and untrained general public push technology to its limits and see past the hype. Work is still required to ensure biometric technologies are universally usable but resistance to this approach is reducing. Our pluralistic approach has ensured both a broad and deep understanding of the issues to be resolved and understanding the impact of the users on the success of new technologies.

References

Clark, R. 1994, Human Identification in information systems: Management challenges and public policy issues, *Information Technology and People*, 7,4,6-37.

Coventry, L. and Johnson, G.I. 1999. More than Meets the eye! Usability and Iris Verification at the ATM Interface. In S. Brewster et al (eds) *Proceedings of the IFIP TC 13 International Conference on Human Compute r Interaction – Interact 99*, Vol 2 (IOS Press/IFIP)

Coventry, L., Johnson, G.I. and De Angeli, A. 2003. Usability and Biometrics at the ATM. *Proceedings of the ACM Human Factors in Computer Systems- CHI'03* (ACM Press)

Davies, A. 1997, The Body as password, *Wired*, July.

Davies, S.G. 1994, How biometric technology will fuse flesh and machine, *Information Technology and People*, 7,4.

Deane, F., Barrelle, K., Henderson, R. and Mahar, D. 1995, Perceived acceptability of biometric security systems. *Computers and Security*, 14, 225-231.

Deane, F.P., Henderson, R.D., Mahar, D.P. and Saliba, A.J. 1995. Theoretical examination of the effects of anxiety and electronic performance monitoring on biometric security systems, *Interacting with Computers*, **7**, 395-411.

De Angeli, A., Coutts, M., Coventry L., Johnson, G.I., Cameron D., and Fischer M. 2002. VIP: a visual approach to user authentication. *Proceedings of the Working Conference on Advanced Visual Interfaces AVI 2002*, 316-323 (ACM Press)

Hone, K.S., Graham, R., Maguire, M.C., Baber, C, and Johnson G.I. 1998. Speech technology for automatic teller machines: an investigation of user attitude and performance, *Ergonomics*, **41**, 7, 962-981.

Phillips, P.J., Martin, A., Wilson, C.L. and Przybocki, M. 2000. An introduction to evaluating biometric systems. *Computer*, February, 56-62.

Woodward, J.D. 1997. Biometrics: Privacy's Foe or Privacy's Friend? *Proceedings of IEEE*, **85**, 9, 1480-1492.