Usability and Biometric Verification at the ATM Interface

Lynne Coventry, Antonella De Angeli and Graham Johnson
Advanced Technology and Research
NCR Financial Solutions Division
3 Fulton Road, Dundee, DD2 4SW
lynne.coventry, antonella.de_angeli, graham.johnson@scotland.ncr.com

ABSTRACT
This paper describes some of the consumer-driven usability research conducted by NCR Self Service Strategic Solutions in the development of an understanding of usability and user acceptance of leading-edge biometrics verification techniques. We discuss biometric techniques in general and focus upon the usability phases and issues, associated with iris verification technology at the Automated Teller Machine (ATM) user interface. The paper concludes with a review of some of the major research issues encountered, and an outline of future work in the area.

Keywords
biometrics technology, iris verification, ATMs, usability techniques.

INTRODUCTION

Traditionally, access to secure areas or sensitive information has been controlled by possession of a particular artifact (such as a card or key) and/or knowledge of a specific piece of information such as a Personal Identification Number (PIN) or a password. Today, many people have PINs and passwords for a multitude of devices, from the car radio and mobile phone, to the computer, web-based services and their bank information.

Herein lies a major difficulty involving the trade-off between usability, memorability and security [1, 2, 22]. Methods for increasing security, such as regularly changing PINs and passwords, increasing their length, ensuring they do not form words and ensuring all are different, makes them more difficult to remember and, therefore, error-prone. Alternatives to the traditional Personal Identification Number (PIN) have also been investigated for instance using pictures instead of numbers [7,10].

CHI 2003, April 5–10, 2003, Ft. Lauderdale, Florida, USA.

Of course, traditional methods rely upon the assumption that the artifact (such as key or card) will be in the possession of the rightful owner and that the information to activate it will be kept secret. Unfortunately, neither of these assumptions can be wholly relied upon.

Gong and colleagues [12] noted that if people are permitted to choose their own passwords they tend to select ones which are easily guessed. People tend to choose ones that are related to their everyday life [1]. They choose passwords which are easy to remember, and, typically, easily predicted, or they change all PINs to be the same. Also, people are often lax about the security of this information and may deliberately share the information, say with a spouse or family member, or write the PIN down and even keep it with the card itself.

Biometric techniques [3] may ease many of these problems: they can confirm that a person is actually present (rather than their token or passwords) without requiring the user to remember anything.

Pioneering work on biometrics technology date back to the late '60s [3] when researchers started looking at voice patterns, fingerprints, and hand geometry as a means for establishing unique individual identity. By the early 1990s, the biometrics industry was established and the first systems went live in controlled environments.

So far, however, the growth of biometrics technologies has been driven by a mainly system-centred approach, dealing with the problems of unique digital identifier extraction, template handling and recognition algorithms. With a very few exceptions [8,9], the HCI community has not been too involved in design or evaluation of biometrics. However, the CHI 2002 conference hosted its very first discussion on biometrics and started a debate on the relevance of this technology to HCI and especially on the role that we can play in designing "an infrastructure for this changed world that minimizes the changes required of us" [18].

As part of a multidisciplinary Advanced Technology and Research Team at NCR, the HCI group has been involved for a number of years in tracking and evaluating biometric technologies. The aim is to ensure that while this

technology is developing we understand both the system and the user issues associated with it. The aim of this paper is to provide a summary of the user-centred aspect of the research we have carried out over the last five years to understand attitudes towards, and behaviour with, biometrics verification at the Automated Teller Machine (ATM) interface. Following a brief introduction to biometrics technology, we present some of our research on biometrics, concentrating predominantly on iris-verification, noting methods and principal findings. We then briefly conclude with an outline of future research.

BIOMETRICS TECHNOLOGY

The term biometrics refers to any and all of a variety of identification techniques, which are based on some physical, or behavioural characteristics of the individual, contrasted with those of the wider population. Unique digital identifiers are created from the measurement of the characteristic.

Physiological biometrics techniques include those based on the verification of fingerprint, hand and/or finger geometry, eye (retina or iris), face, wrist (vein), and so forth. Behavioural techniques include those based on voice, signature, typing behaviour, and pointing. New voice biometrics would place it in the physiological rather than behavioural category. All biometrics approaches follow a similar operation: a digital template is created during an enrolment process, then the template is stored in a database. On attempted verification, the relevant template is extracted and compared with the data input, say in the form of a fingerprint, or an acquired iris image, for positive identification.

At the ATM, verification (i.e. answering the question "are you who you say you are?)" rather than identification (i.e. answering the question "who are you?") has been adopted. There are many reasons from business, technical and consumer perspectives behind this decision. Verification requires a one-on-one match of a template to an acquired image rather than an attempt to match and search against a database of all customers. This means that the ATM user would still require their access token (card). This would either provide a unique identifier to access the template to verify the user against or in the case of smart cards may store the template on the card reducing some of the database storage issues, both privacy and security based, which surround biometrics.

The performance of biometrics is measured using statistical techniques to predict their technical accuracy. Two measures, false accept rate (FAR) – the likelihood that the wrong person is accepted and false reject rate (FRR) – the likelihood that a legitimate person is rejected form the basis for comparisons. The problem is that these measures are interconnected, as one increases, the other decreases. A second problem is that the method by which the base data are collected can seriously impact the performance achieved. Performance estimates in sales literature are often far more impressive than actual performance [17]. Systems tested in laboratory conditions with a small, homogenous set of "good", trained, young, cooperative users may generate completely different results than testing in a live environment with a diverse, inexperienced and perhaps non-cooperative user population as experienced at ATMs. 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 [6]. One of the big issues with the ATM is that ultimately it has to deal with the entire banking population of the world.

Other factors to consider are template size, speed of enrolment and recognition or verification. It is also necessary to consider failure to enroll and failure to acquire. Failure to enroll refers to those people who either do not possess the biometric or can not use the system (outliers). In the case of fingerprints this is thought to be as much as 10% of the population and with iris 0.005%. Failure to acquire is where the interaction between the user and the system breaks down and the system does not succeed in acquiring an adequate image to validate respectively.

Clarke [4] presents the desirable characteristics of a human identifier; an ideal biometrics characteristic would be - universal, unique and exclusive, permanent through life, indispensable, collectable, digitally storable, precise, easy to record, efficient to record, and acceptable to contemporary social standards. It seems that not all these objectives can be fully achieved by any current method.

Iris Verification

With iris verification, for application at ATMs, a wide-angle camera finds the head of the person to be identified. A zoom lens then targets in on the user's iris and takes a digital photo. A template of concentric lines is laid on the iris image (see Figure 1) and a number of specific points are recorded and the information converted into a digital template. This can then be compared with others for verification and identification purposes.

The general interest in iris verification applied to public technology is centred upon its accuracy or reliability, which is much greater than say fingerprints [15,16], and the fact that the biometric itself can be acquired without the individual having to come into physical contact with the 'end-point'. The next section of this paper reviews our work in the pursuit of an understanding of financial consumers with regard to biometrics in general, and iris verification in particular.

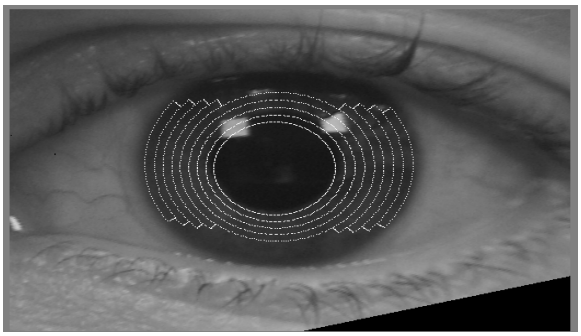

Figure 1. Iris image

BIOMETRIC RESEARCH AT NCR

At NCR, investigations into the use of biometrics to verify and/or identify bank customers have been undertaken since the 1990's and continue to be the focus of research. These investigations have used a variety of methods and looked at a number of technologies, with the aim of gradually acquiring a sound understanding of the issues from the consumers' perspective within a self-service environment.

This section outlines some of the research undertaken, in particular, addressing iris verification at the ATM user interface. Different devices have progressed to different stages of evaluation depending on the maturity of the technology. Iris verification is one of the few we have taken to a full field trial. We have adopted a pluralistic approach to fully understand the issues from a user's perspective, including:

- **focus groups and surveys** to understand user understanding of and attitude towards either biometrics in general or one specific biometric device,
- **dynamic anthropometry study** to understand the physical constraints within which a device must operate,
- **functional prototype testing** to understand the base performance level of different technologies with untrained users
- **laboratory-based usability evaluations** to investigate usability issues with devices and iteratively design towards a self-service solution
- **field trials** with a real system, and customers accessing their own bank accounts to measure real consumer acceptance.

Focus Groups

Over the last few years, a number of focus groups have been held, frequently in association with different financial institutions and in different locations around the world. The aim of these is to continually gauge the consumer attitudes towards biometrics technology in general.

There are many issues which influence consumers and their perceptions of public technology. It is important to separate general attitudes from actual behaviour. What consumers think and what they really do does not necessarily follow an obvious relationship. This is particularly true when dealing with the diversity of the general public, and with technology, services or concepts that have rarely been encountered before.

The focus groups have 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. In general, people believe facial recognition could work, as they believe that is the way humans identify each other, and that fingerprint technology must work, after all, they are used as evidence in law enforcement. The major findings of the series of focus groups are summarised below.

a) There is little perceived need for the addition of biometrics at the standard ATM. Years of experience with PIN have led consumers to believe that it is sufficiently secure. Consumers rarely report forgetting their PIN, unless prompted. They do report the potential for others to acquire their PIN, but they also can misuse this by giving their cards and PINs to friends and family on occasions.

b) Consumers have difficulty believing that such 'futuristic' technology can work well. In the case of iris verification technology, consumers assume there are difficulties with the process of image capture and the uniqueness of the iris. They also worry that the technique could fail to recognise them leaving them unable to access their money at a critical time.

c) People also believe some biometrics will be easy to defraud e.g. voice with a recording or facial with a photograph or by false fingers. While measures can be put in place to ensure that this is not the case, a recent study [19] tested a number of released products and found that they could be easily defrauded.

d) There is a general concern about the potential for the misuse of personal, biometrics data collected, which is seen as having the potential to violate their privacy and civil liberties. This issue is reviewed extensively by [21].

e) Consumers also express some concerns about potential health risks associated with the technology. For instance, misunderstandings of iris verification can lead the consumer to believe the technology involved may lead to eye damage.

On occasion focus groups were held before and after the participants used the actual system. The pre-use focus groups with iris verification highlighted several general, negative attitudes from potential users. However, we found that attitudes altered positively provided that the consumer had a successful experience with the technology. It may be that fears could be alleviated by a careful marketing campaign, or through utilising the enrolment process as an educational opportunity, or simply through exposure to, and experience with, the technology.

Focus groups were held prior to a field trial of iris verification. These specifically addressed key acceptance issues. Participants were asked how they would convince others to use the system. They were also asked to comment on a first draft of a marketing leaflet which explained how the system worked. Comments made within these groups suggested that the marketing information should stress how simple the process is, and use the analogy of a photograph. Any mention of security or military was seen as having negative connotations within this context. Participants believed the value to the consumer, of speed and convenience, should be emphasised.

Dynamic anthropometry study

Alongside understanding consumer attitudes, it is also necessary to understand the physical characteristics of potential users that will impact the design of a self-service technology. One design must attempt to fit all consumers. The iris image must be acquired in a non-obtrusive manner. This means that the user can not be expected to be standing with the eye in a predefined position. Thus, the ATM-iris unit must cope with a naturally wide range of consumers' eye positions in front of the ATM.

In contrast to the qualitative nature of focus groups, an in-depth investigation of the dynamic anthropometry of consumers and their eye positions when using ATMs was carried out [13]. The aim of this study was to produce three-dimensional co-ordinates of consumers' eye positions at three key stages, during an everyday ATM transaction. Those points were card entry, PIN entry and general screen use. A series of LED markers in combination with CODA (gait) motion analysis system were used to determine these 3-D co-ordinates. A sample of over 100 participants from the ages of 13 to 79 years took part in the study, including some wheelchair-bound users. The measurements were taken on two different ATM machines, upon which the angle of the screen was varied.

The recorded eye positions demonstrated that for non-wheel chair users, the majority of eye positions fall within a relatively small envelope, roughly 300mm across the face of the interface, 300mm vertical and 400mm away from the front of the machine.

This study provided real dimensions upon which to base the requirements for the ATM-iris unit, so that it is able to easily locate user's iris, where that user is drawn from the general population, without requiring any self-positioning when using the ATM.

Functional prototype testing

The functional prototype evaluations formed the basis of understanding how well the technology works without trained users. One of the first iris verification technologies, with the potential to be utilised within a self-service environment underwent usability and feasibility testing. This trial was carried out with approximately 300 participants.

As a first test of the prototype, the evaluation was mainly focused on the actual performance of the technology, specifically, its accuracy and reliability. The technology was not fully integrated into a self-service environment, and required that the participants remember what to do when asked to return to the system after a week. This caused some problems with mistiming and misdirected gaze. Participants also noted that the system was slower than expected, and 31% reported experiencing problems using the system as they kept looking at the associated computer screen, rather than the verification unit. This meant that iris images were not easily captured. Perhaps, not surprisingly, iris verification was not considered that acceptable to the majority of participants.

General biometric prototype testing

Similar studies have been carried out with facial recognition and fingerprint technologies. These technologies have been released and were tested with their standard interface. Two fingerprint and two facial recognition systems were tested with 200 participants at the National Physical Laboratory for us, following their standard biometric evaluation procedure [14]. This extended trial took place over 3 months with participants using the biometrics on a weekly basis. This period gave some understanding of how people's appearance changed over time and if they would remember how to use the system without continual daily use.

The results found significant performance differences between systems on the significant measures of Failure To Enroll (FTE), Failure To Acquire (FTA), False Accept Rate (FAR) and False Reject Rate (FRR), as well as user preferences. One of the key factors thought to affect FTE and FTA was whether or not the system provided feedback to the user about the nature of the image they had captured of the user's biometric. It is essential this feedback takes a form the user could understand, for

instance an image of the face or the fingerprint. The facial system in particular did not cope well with changes in participants' appearance over time.

Although people at first thought they would prefer facial verification to fingerprint, they found the system difficult to use with 10% of attempts failing to be recognised (FRR). The system could not tell them why the failures had occurred. Conversely people, did not initially prefer fingerprint but after finding it the easiest to use, changed their preference after use.

Another technology we have tested is that of finger swipe. In this case the user moves their finger over a sensor and a thermal scan of the fingerprint is taken (Figure 2). The system was tested with 82 members of the general public in Edinburgh In this study participants were asked to enroll and were then asked to use the system 6 times for verification purposes. With the finger swipe technology we found that 17% of participants failed to get more than half of their attempts to access the system verified. More details of this study are provided in [5].

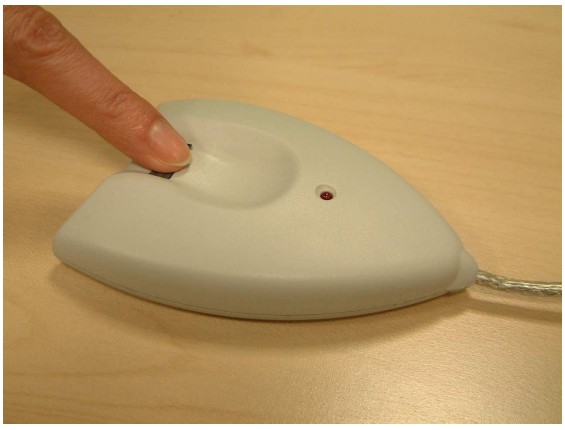

Figure 2. Finger swipe

In all cases we have found usability issues with biometrics technologies. This means that they can not be simply incorporated into a self-service machine and used by a wide selection of the general public. However, successful use of the system increased acceptance, with the majority of participants stating that they believed it would be more secure than a PIN.

This work, with the early, functional prototypes, even those released as products, identified the requirement for further iterations to improve speed, provide meaningful feedback to the users to assist them in adapting their behaviour, and to enhance the system's ability to consistently acquire a high quality biometric image within a self service environment. Administering pre and post use questionnaires has shown us that successful and unsuccessful experiences can change user opinion about these technologies. This leaves us with the dilemma of deciding when a technology is mature enough to test with the general public.

Laboratory based usability evaluation

Following prototype testing, the iris verification unit underwent several changes and was incorporated into a self-service ATM with appropriate graphical lead-through for users. During the prototype development it was crucial to, firstly, ensure that usability was maximised and, secondly, to ensure that the acceptance of the technology would be influenced by actual usage of the system in a positive direction.

Recruited from our own organisation, 42 people who were not involved with the biometrics self-service projects, were asked to take part in the lab-based usability trial. The height of participants varied form 4 foot 10 inches to 6 foot 2 inches. The majority of participants were young (under 40) males (69%), of whom 14 % wore contact lenses, and 17% wore spectacles.

To understand the general acceptance issues, qualitative data were captured via questionnaires at three points in the study: Firstly, before participants had any experience with the system, then after they had taken part in the enrolment procedure and lastly after they had used the prototype iris-ATM system. Usage of the system by individual participants averaged 6 times during a three-day period.

The results showed that, even with internal, largely technically-aware staff, before enrolling over a third had concerns about using the system were it implemented in their own bank. These concerns were in the areas of reliability, health issues and misuse of data. Around a third, at pre-trial stage, also said their concerns were so great that they would not feel very confident using the system.

After enrolment with the iris verification system, 26% said that enrolment had caused a positive change in their opinion of the system. Further, *after* use of the system to carry out normal transactions such as withdrawing cash, 31% quoted a positive change in attitude. Only a small number still had some concerns, and these were primarily about potential misuse of personal data. Following full use of the prototype system, 96% of the participants said they would now be confident using the system in future.

From the usability perspective, performance data were collected by using the system to log the 'verify time' and videotaping the prototype usage. The verification time (i.e. how long it takes for a user to be 'recognised' by the system) achieved by users varied greatly from a min of 2.2 seconds to a max of 33.5 seconds. Only 2 users could

not achieve at least one verification time of less than 4 seconds, a time comparable to PIN entry. The mean verification time was 4.6 seconds.

In further reviewing the behavioural evidence (the videotape records) many of the usability issues were attributable to the user looking away when the verification process started. However, the issue of misdirected gaze was still not fully resolved. This was due to the distance between the ATM screen and the separate prototype unit. Occasionally, the user would look down at the screen to see what was happening and would then not have the iris in view of the system for verification. Two immediate recommendations were made for the prototype development, either increase the visibility of the cueing on the prototype unit (similar to a photo-booth's red light flashing) and/or incorporate an audio cue to signal that the 'picture' has been taken. Ultimately, it would be preferable if the user did not have to look away from the screen when the iris image was being captured.

The in-house work ensured that the potential usability issues with the system were understood, and could be acted on. It also provided concrete evidence that the experience with the system was sufficient to positively influence participants' attitude. However, this in-house evaluation did not fully answer the fundamental question of whether consumer attitudes would be translated into actual behaviour in the field: Would people use the system in real life, with their own money?

Field Trial

After the in-house, laboratory-based work, it was important to investigate whether or not the system would be usable and acceptable in a real environment with consumers using the system to access their own money. A 6-month field trial was established with a major UK financial institution.

The trial was located in Swindon, the site chosen as there was a small branch accessible to both the general public and a large population of the institution's staff, who were also customers. A refined prototype IRIS ATM replaced the existing ATM (Figure 3) and the three teller (counter) stations were also equipped with iris verification units, to replace traditional signature methods.

Figure 3. IRIS ATM (iris unit about the screen)

A basic marketing campaign was developed to inform customers of the trial and invite then to 'convert' to iris verification in place of PIN. No monetary incentives were provided. During the trial over 1,000 people enrolled in the system of which 39% of these were general public.

Two types of data were collected. Attitudinal data were collected via telephone surveys, carried out by an independent market research bureau. Performance data were collected via system logging of the performance details for each and every transaction.

A total of 411 participants were interviewed during two waves of market research. The first wave occurred just after enrolment, and the second wave took place three months later. This market research showed that 70% of enrolees used the system at least once. Some 44% of those interviewed after enrolment said they were comfortable using the system. After extended usage, the second wave of interviews revealed that this had increased to 94% of users.

Over 90% of the interviewees were satisfied with the iris verification and would elect iris over PIN or signature. These consumers regarded the system as more secure, more reliable and faster. Of those who did not continue to use the system, the main reason given was that they had not been at the branch. Following use of the system, no one expressed any major negative attitude towards the concept.

ISSUES & FUTURE WORK

It is clear from our experiences with the on-going development of the iris verification prototypes, that there exists a gulf between those general pre-usage attitudes, and subjective opinion following iris-ATM use. Our ability to predict consumer acceptance of new technologies and services requires that we acknowledge some of the inherent limitations of focus groups and surveys. Whether these are developed with scenarios, or involve grounded discussion, our experiences demonstrate clearly that there is no substitute for 'hands-on' experience with functional prototypes that adhere to the contextual attributes of the task to ensure that predicted behaviour will be converted into real behaviour. The earlier we engage consumers with prototypes of the intended system, the better. In a recent American survey [20] 78% of respondents said that it would be acceptable to them to have biometric access to ATMs. This suggests a shift in pre-use expectance levels than we found in our work in 1998 and 1999. However this acceptance is based on little or no real experience of biometrics. More research is required to enable the design of usable biometrics to ensure that the experience with the system is satisfactory.

Some of the main issues emerging from our research with the iris verification technology are specific to this type of non-contact approach (e.g. 'natural' user positioning), whilst others relate to more general concerns (e.g. potential use of personal data). Future development of the iris technology for ATMs will take full account of the range of consumer issues highlighted. The development of this biometrics approach for ATM consumers, whether via an iris or an alternative, will now be well informed as a result of these studies.

Every biometric device has its own set of usability issues and more work is required to ensure to understand the nature of permanent and transient exclusions to any biometric technology as well as how to maximise the usability of a biometric to enable it to be utilised within public technology. Biometric technologies do not resolve the usability/security trade off. Biometric devices have to establish fault tolerance limits. Setting these narrowly maximises security but means the ease of use could decline. Further research is required to understand the relationship between security and issues such as false rejects and failure to acquire.

It should be noted that our progress with definition and resolution of some of the usability aspects of the proposed system has been the result of a pluralist approach as far as methods are concerned. The value of qualitative techniques in identifying potential barriers, and the use of sophisticated technology determining user positions and envelopes, shows that a deliberately wide variety of usability methods need to be incorporated in the pursuit of ease-of-use of biometrics and understanding of issues with new technology in general.

Implementation issues

This paper has not addressed many of the implementation issues which surround biometrics. These issues include establishing an effective enrolment process which educates the user and prevents identity fraud, dealing with those people who can not use the chosen biometric either temporarily (failure to acquire) or permanently (failure to enroll) and how to deal with false rejects. Effective processes must be established to deal with these situations.

CONCLUSIONS

This paper has provided an overview of the user-centred work focussed upon the provision of biometrics verification at the ATM user interface. Having adopted a variety of qualitative and quantitative methods, with laboratory- and field-based studies, our research has revealed a number of non-trivial issues with the introduction of this type of technology to the general public. Moreover, as a result of our interventions we have made progress in significantly improving, from a user's perspective, the implementation of this technology.

While technology continues to evolve and improve, more work is required to address the usability issues which will be key to successful implementation of biometrics within a general public application such as banking.

Finally, our understanding of user issues with respect to public technology, and specifically the ATM, is enhanced, as is our understanding of the relevance and application of usability techniques at different stages of the design and development lifecycle.

ACKNOWLEDGEMENTS

We would like to thank our Advanced Solution Concepts and Advanced Technology colleagues for their support and encouragement of this work. Also National Physical Laboratory, University of Loughborough and HFE Solutions Ltd for their contributions to the research.

REFERENCES

1. Adams, A. and Chang, S.Y. An investigation of keypad interface security. *Information & Management,* 24, 53-59, 1993.
2. Adams, A. and Sasse, M.A. Users are not the enemy. *Communications of the ACM,* 42, 41-46, 1999.
3. Ashbourn, J. *Biometrics. Advanced Identity Verification*. Springer Verlag, London, 2000.

4. Clarke, R. Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information technology and People*, 74, 6-37, 1994.
5. Coventry, L., De Angeli, A., and Johnson, G. Biometric verification at a self service interface. *Proceedings of the British Ergonomic Society Conference* (Edinburgh April 2003), Contemporary Ergonomics (to be published).
6. Davies, S.G. How biometrics will fuse flesh and machine, *Information Technology and People*, 7,4, 1994.
7. De Angeli, A., Coutts, M. Coventry, L., Johnson, G.I, Cameron D., and Fischer M. VIP: a visual approach to user authentication. *Proceedings of the Working Conference on Advanced Visual Interfaces AVI 2002*, ACM Press, pp. 316-323, 2002.
8. Deane, F.P., Barelle K., Henderson R.D. and Mahar D.P., Employee acceptance of computerised biometrics security systems, *Computers and Security*, 14, 225-231, 1995.
9. Deane, F.P., Henderson R.D., Mahar D.P. and Saliba A.J. Theoretical examination of the effects of anxiety and electronic performance monitoring on biometric security systems, *Interacting with Computers*, **7**, 395-411, 1995
10. Dhamija, R. & Perrig, A. Déjà vu: A User Study Using Images for Authentication. In *Proceedings of 9th USENIX Security Symposium*, August 2000.
11. Feustal, T.C. and Velius, G.A. Speaker identity verification over telephone lines: Where we are and where we are going. *Proceedings of the 1989 International Carahan conference on security technology,* (3-5 Oct), 181-182, 1989.
12. Gong, L., Lomas, M.A., Needham, R.M. and Saltzer, J.H. Protecting poorly chosen secrets from guessing attacks. *IEEE J. on Selected Areas in Communications*, 11(5), 648 – 656, 1993.
13. Hide, S. Haslegrave, C.M. Hopkinson, N., Robertson D. and Johnson G.I. Tracking eye positions during the use of an Automatic Teller Machine (ATM), *Proceedings of CAES '99*, May: Barcelona, Spain. 1999.
14. Mansfield, A.J. & Wayman, J.L. Best Practices in Testing and Reporting Performance of Biometric Devices. NPL Report CMSC 14/02 August 2002.
15. Mansfield, A.J., Kelly, G., Chandler, P. and Kane, J. Biometric product testing final report. www.cesg.gov.uk/technology/biometrics, March 2001.
16. Negin, M., Chmielewski, T.A., Salganicoff, M., Camus, T.A., Cahn von Seelen, M.M., Venetianer, P.L. and Zhang, G.G. An iris biometric system for public and personal use. *Computer*, 33,2, 70-75, 2000.
17. Phillips, P.J., Martin, A., Wilson, C.L. and Prozybocki, M. An introduction to evaluating biometric systems, *Computer,* 33,2, 56-62, 2000.
18. Scholtz, J. and Johnson, J. Interacting with identification technology: Can it make us more secure? *CHI2002 Extended Abstracts*, ACM Press, 2002.
19. Thalheim, L., Krissler, J. and Ziegler, P.M. Bodycheck: Biometric access protection devices and their programs put to the test. *C'T*, 11, May 22, 2002 (www.heise.de/ct/english/02/11/114/)
20. Westin, A. Biometrics in the mainstream: What does the U.S. public think. *Privacy and American Business Newsletter*, 9,8, December 2002.
21. Woodward. J.D. Biometrics: Privacy's Foe or Privacy's Friend? *Proceedings of IEEE*, 85, 9, pp 1480-1492, 1997.
22. Yan, J., Blackwell, A., Anderson, R. and Grant, A. The memorability and security of passwords – Some empirical results. *Technical Report No. 500 2001,* Computer Laboratory University of Cambridge, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf, 2001.

.