Networked biometrics systems — requirements based on iris recognition

M M Gifford, D J McCartney and C H Seal

Future user verification and validation for networked access to computer applications, trust services and e-commerce could rely upon biometrics-based user authentication. This paper discusses requirements for networked biometrics access, based on experience with iris recognition systems. Also described is the development of a prototype WindowsNT log-on system using iris recognition.

1. Introduction

Biometrics systems assert the identity of an individual based on characteristic features or behaviours of that person, for example their facial appearance, hand geometry, fingerprints, voice patterns. The work described here has predominantly concentrated on iris recognition. The iris tissue of either eye contains a richly detailed pattern that is unique. Although the colour of the iris may alter through life, the actual iris pattern remains largely unchanged (and is in fact mainly determined by random growth processes before birth). Iris recognition is acknowledged as a leading biometrics technology [1, 2] offering unparalleled accuracy and robustness in correctly identifying individuals from large databases.

Biometrics systems have had a somewhat chequered past with many technological innovations, but relatively little commercial success. A number of factors that appear to have contributed towards this may include:

- exaggerated claims or hype of early systems,
- inadequately developed, expensive or unfriendly user interfaces,
- a lack of social acceptance (for instance, fingerprints are associated with criminal records).

However, a number of recent important developments suggest that biometrics may soon experience more widespread applications. These include:

- greater use of and more extensive computer networks — where users are now required to remember and maintain ever more PINs and passwords, biometrics offers an increasingly attractive solution, a 'key' that the user cannot lose or forget,
- emerging e-commerce — Internet shopping and trust-service offerings require secure user verification procedures that prevent fraud and are sufficiently robust to stand up in a court of law,
- low-cost biometrics-capture terminals — the next couple of years will see new, low-cost, biometrics-capture devices become available as personal computer (PC) add-ons, while cheap, powerful, embedded processors make it possible to integrate such devices further and include them in other systems (e.g. payphones, mobile-phones),
- advances in the science of computer vision have resulted in faster and improved textural analysis tools and, consequently, better defined biometrics 'templates'.

In this paper, experience in the use of iris recognition and in developing PC-based log-in processes is used to illustrate the requirements for secure biometrics-based access protocols.

2. Existing biometrics solutions

Currently there are a plethora of biometrics systems vendors — particularly with fingerprint systems — offering bespoke solutions using proprietary technology. The reports of laboratory or 'real-world' trials have tended to be limited and unsatisfactory. A cross-comparison of biometrics systems is difficult, particularly as most have not demonstrated any rigorous statistical foundation for their claims. In this regard, iris recognition has performed well, with published detailed mathematical analyses of the system being available [3]. The authors have subsequently corroborated these claims for iris recognition [4] (see the Appendix).

Most biometrics systems have been designed initially for application in the access control market. There are two main stages in their operation — enrolment and recognition. In the enrolment stage a master 'template' is created for the user, based on the analyses of a sequence of biometric data captures. The template may represent an average of the capture sequences or it may represent the single data capture that appears to be most representative of the user. In the case of iris recognition, a number of images are taken (usually between 3 and 10). The images are independently processed and an enrolment template (iriscode) is formed, based on the best image. When users wish to gain access, they present themselves for validation. The newly generated biometric data is compared with the enrolment template. If an authorised match is found, access is permitted.

2.1 *Verification versus identification*

There are two possible methods of operation for recognising users, depending upon whether users are required to state who they are. If the user has to declare their identity — for instance by typing in a username or by presenting a smart card — then, in principle, it is only necessary to do a one-to-one comparison. Such applications are known as **verification** systems. If the user's identity is not known, then it becomes necessary to search the whole database for the matching template, i.e. an **identification** system. Iris recognition is particularly suited to these applications as it can rapidly search large databases (hundreds of thousands of eyes/sec on a Pentium PC). Depending upon the application, the latter can have important advantages, in that the user need not carry or remember anything. This is especially true for high-throughput access-barrier systems where the act of typing or producing cards can impose considerable delays.

When comparing false accept numbers, an important difference emerges between identification and verification systems. With identification, a comparison is made with every entry in the database, while with verification only one comparison is made. This means that with identification, the odds of a false match grow with the database size. However, with iris recognition, the initial false accept odds are so good that even with everyone in the world enrolled in one database, the odds of getting a false match are less than is achievable in available commercial fingerprint verification systems.

2.2 *Networking biometrics*

Current commercial biometrics systems have, on the whole, a limited networking capability. There are hopes that this will change with the recent formation of consortia to look at this issue [5, 6] and with the introduction of some simple small-scale network solutions [7, 8].

Many small-system solutions do not scale well. For example, the current commercially available iris recognition system requires the entire iriscode masterfile to be stored in the local memory of every terminal. Regular synchronisation is required to ensure that any new enrolees are distributed to remote copies of the masterfile. This soon becomes unmanageable as a networked solution grows in size. The only advantage in storing templates locally is that access is less susceptible to network failures as authorisation can also occur locally.

The application of biometrics could, however, go well beyond small office solutions. Large-scale computer access methods are needed for corporate log-on, social security, health records, ticketless travel, service billing and customer records, banking, e-commerce, mobile telephone authentication, etc. Identification systems are likely to have some key advantages for these systems. For example, in current systems for large organisations it is not possible to use real names as usernames as there is too much commonality (e.g. there would be more than one John Smith). In these situations, customers currently need to remember a non-obvious username as well as a PIN or password.

Networked biometrics-based access systems should consider the following attributes:

- authorisation to occur across a network to centralised access server(s) — this enables a scalable and secure platform to be built in which template masterfiles are managed effectively,
- a robust biometric capable of use with systems handling large user populations — in the authors' opinion, iris recognition is the only form of biometrics that currently meets this criterion,
- greater assurance of the system end-to-end security — authorisation across open networks (e.g. the Internet) requires the use of advanced cryptographic tools to avoid interception and replay attacks, for example, if the user has unsupervised access to the client biometrics-capture device, anti-tamper methods need to ensure that the captured data is genuine,
- limited access in case of network failure — the need for such access will depend upon the application, for example, for building access, one might cache the most recent visitors and permanently store templates for the building supervisor(s), or for financial transactions, one might set a small payment limit for which authorisation is taken on trust (the biometric template can in any event be traced at a later date).

Currently there is a difficulty in constructing such a network service offering with available technology. For a real commercial service it would be preferable if the complete system could be built using 'off-the-shelf' components from a range of suppliers. Compatibility and scalability issues need to be addressed if such a viable commercial networked application of iris recognition is to be implemented.

3. Demonstration prototypes using iris recognition technology

Three demonstration applications, using IriScan proprietary software for the recognition process and tested with a range of optical image capture units, have been developed at BT Laboratories (BTL):

- a smart card demonstration,
- a networked demonstration,
- a WindowsNT log-on application.

3.1 Smart card demonstration

This system is a verification application, which integrates iris recognition with smart card technology. The demonstration allows iris verification without the need for an on-line network connection. The operational procedure is as follows:

- a smart card is inserted into the reader,
- the user presents an eye to the optical unit,
- recognition iriscode is generated,
- recognition iriscode is compared with the enrolment template held on the smart card,
- the cardholder is accepted or rejected.

This system was implemented on a laptop computer using a PCMCIA frame grabber to convert the video from an optical unit. Overall the system worked well, but performance was limited by the low bandwidth of the PCMCIA interface — this allowed the system to analyse about 1 frame every 3 seconds. A modern laptop with a USB port would operate considerably more quickly and eliminate the need for a frame grabber.

3.2 Networked PC demonstration

The first BTL networked demonstration system was built using an Oracle^{TM} database running on a WindowsNT server and used a number of remote devices to capture and encode the image of an eye (Fig 1).

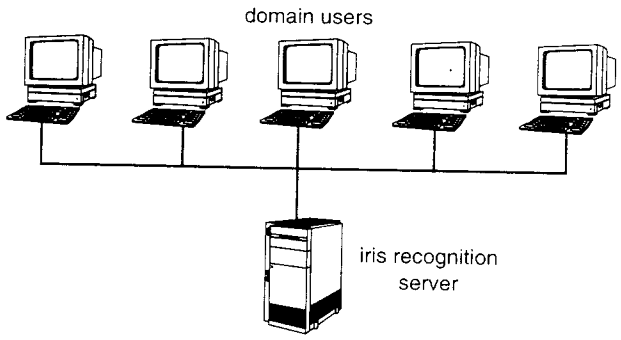

Fig 1 A typical networked iris-recognition log-on system.

A product might comprise an eye image acquisition device, a frame grabber, and software delivered over the network or on CD-ROM. The product could be offered as part of a recognition service in conjunction with a network-based iris-recognition server. This would allow BT to offer a remote iris-recognition service that could enable transactions, or services.

The current prototype transports images between the clients and server. Conventional cryptographic methods can be used to secure the communications channel by which the images are transported. Replay attacks can be detected by looking for the use of the same image twice [9]. However, in general it is felt that image-based solutions (as opposed to template-based solutions) are less desirable as the underlying image(s) of an eye may be known to fraudsters and because greater demands are placed on bandwidth and central processing power.

3.3 WindowsNT log-on demonstration

The demonstration WindowsNT log-on system has been implemented at the client workstation as shown in Fig 2. The system captures an image of an eye from which the iriscode is generated. The iriscodes of known users are searched and the user is logged on if a match is found and the user is authorised to access the computer.

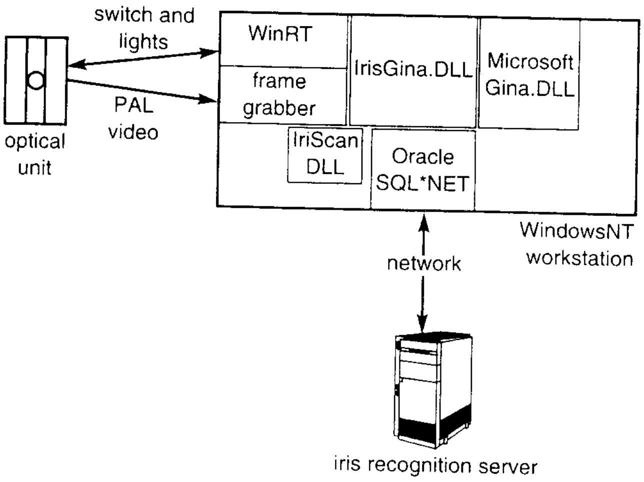

Fig 2 Structure of iris-recognition log-on demonstration.

A new log-on Gina.dll was written (IrisGina.dll) which controls the log-on process and connects to the Oracle database at the server. This DLL accesses IriScan software components to peform the iris recognition functionality and frame grabber software to grab images. The WinRT software reads the output from the 'start' switch and drives the user-feedback lamps to tell users whether they have been identified or not. In the demonstration log-on system, the remote clients collect all the iriscodes from the database and keep a local copy. This configuration was adopted because the current software components from IriScan do not allow the separation of the iriscode generation and search algorithms. In a production system it is envisaged that the search and matching operations would be carried out at the server.

The server (Fig 3) monitors requests and sends the iriscodes and user profile information to log-on clients as needed. A separate enrolment program was written that allowed the enrolment of an eye and insertion of the user profile information into the database.

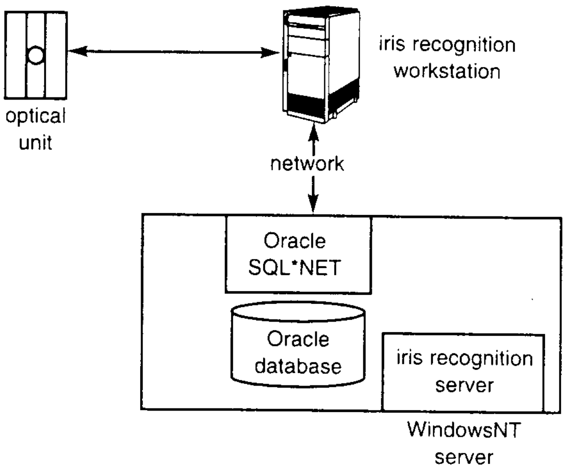

Fig 3 Structure of iris-recognition demonstration server.

The WindowsNT demonstration was rapidly prototyped to demonstrate its potential. A small number of users were enrolled and their access to the internal local network controlled via the iris-recognition log-on process; operation was rapid (less than 3 seconds for the complete process).

For the prototype demonstration system, the iriscodes are stored in the database. Upon start-up of each client, every iriscode is fetched from the database along with a unique eye identifier. The iriscodes are appended into an array in memory and this array is handed to the IriScan recognition functions. The IriScan functions then return an offset for a recognised eye. This offset is used to fetch the user profile information about the owner of the eye from the database.

4. Key design issues for future networked biometric access

The role of networking biometric access systems goes beyond simple messaging protocols between clients and server(s). Total system security and future proofing need to be considered.

4.1 End-to-end security

Secure networked authorisation requires that each stage in the authorisation process be protected. This is particularly true for unsupervised validation scenarios.

- Communications security

  There will be a requirement to transmit users' biometric templates over open or hostile networks. Cryptographic tools are believed to offer a good solution to this problem and digital signatures could be used to show that transmitted templates have not been subjected to any interference.

- Biometrics tamper-proofing

  The biometrics-capture devices need to be capable of ensuring that they are inspecting genuine user features (as opposed to a photograph or recording) and that the output signal cannot be substituted. This will help prevent replay attacks from lifted fingerprints or by video-signal substitution, for instance by connecting a video recorder to the frame-grabber. This is an important aspect and must be considered at the design stage as it implies that the server and client need to operate various challenge/response methods to authenticate the data captured.

  In a networked configuration the client could be remotely instructed or controlled by the server to vary template-capture conditions, to issue a response to a challenge, or to define the encoding or transmission algorithm to be used. These features could allow more flexibility in operational use, and provide added security and privacy for the individual.

- Tight integration with computer operating system

  While a number of prototype networked computer log-on applications have been built using iris recognition, these systems are not robust enough to prevent attacks from hackers, etc. If a network-based service is to be developed, the biometrics log-on application needs to be tightly integrated with the computer operating system. With the WindowsNT log-on, this is partially achieved by the rewriting of the Gina.dll. However, a conventional password file still exists, access to which would circumvent any additional security. The possibility of hackers creating 'workarounds' needs to be forestalled.

4.2 *Customer-tailored solutions*

Customers like to understand the security of systems they use, and naturally request that they can reconfigure the system to establish their own security cordon. Bespoke and black-box systems are disliked as they run the risk that backdoor routes exist in the system left by system integration or manufacturing personnel.

Customers may wish to define their own cryptography algorithms, their own variant of the biometric template algorithm, their own template comparison logic, etc. Therefore, while the choice of biometrics technology used is supplier-dependent, it is considered desirable to allow system managers to set their own private configuration fields to prevent attack from others with supposed inside knowledge. Building these options into future systems requires flexibility at the design stage and should be addressed by manufacturers. After all, it is the customer and not the manufacturer who will end up taking the risk.

4.3 *Data protection*

There has been some concern from those working in the privacy arena that biometrics will disadvantage those who cannot or will not use the developed systems [10]. The primary concern is about the use of a single source of biometrics for a range of applications. The danger is that the biometric template could be used as a discriminatory key, disadvantaging those with particular 'problems' identified in associated data fields. One example of this would be in the use of the same template by health and insurance agencies. Unscrupulous organisations could select preferred clients if access could be obtained to relevant information in the other authority's databases. While this would be illegal under most data protection laws, the crime would be difficult to detect.

One solution with iris recognition is to use different versions of the iriscode template-generating algorithm per organisation. Different authorities (e.g. healthcare, banking, immigration) would then run incompatible versions of the system so that the templates generated would not be cross-readable. This would add privacy and give a greater degree of protection to the individual and reduce the risk from any security breaches.

Another way of protecting individual privacy is to arrange to have only a partial disclosure of the user template from the client to the server. The elements disclosed in any one transaction will be negotiated between client and server. This makes an intercepted template not reusable and can create a multiplicity of secure passwords for an individual [9].

4.4 *Future proofing*

Under server control, new encoding or transmission algorithms could be incorporated after system launch, thereby future proofing system design. Procedures to manage such enhancements need to be considered at the design stage to make sure that hardware does not go 'out of date'. Transmitted user templates could also usefully include a description of the version numbers for hardware and firmware, allowing the server to adapt its response accordingly.

5. Future iris recognition systems

Ideally the recognition process would be split between the client and server. The image would be captured at the workstation and an iriscode generated locally. This iriscode would then be transferred over the network to the server where it is compared with the iriscodes in the database. If the comparison of iriscodes is moved to the server, rapid data transfer and fast search procedures will be required for good user perception. There are a number of ways to implement the search algorithm at the server:

- the search could be carried out within memory on the server but outside the database — this would require fetching the iriscodes from the database at start-up and the maintenance of the iriscode list in memory as enrolments and deletions take place,
- the database could be modified to handle the search directly from the database tables, which would require modifications to the database itself but may be memory and processing efficient, as the search would be within the database management system — the handling of enrolments and deletions (additions and removals from the database) requires careful consideration,
- the search could be carried out in a bespoke hardware system, which would carry out many millions of searches a second — the iriscodes would have to be loaded into the system from the database, and again new enrolments and deletions would have to be managed.

6. Conclusions

Network biometrics messaging protocols need to be designed with versatility, flexibility, total security and service management in mind. Designers need to consider the following features:

- incorporating cryptographic security for secure end-to-end communications,
- tightly integrating the biometrics log-on procedure to the computer operating system to reduce the risk of computer hacking or of bypassing system security.

- judicious use of biometrics signatures so that a cracked intercepted message does not invalidate the system operation,
- provision of circumstantial information from the capture devices, e.g. time-stamping, equipment version numbers, algorithm version numbers, caller line identity (CLI) — this allows the server(s) to correctly respond to network requests and eases the introduction of future improvements,
- arbitration between the server and client on biometrics-capture conditions — there may be a number of image features that can be tested for in the biometric template which depend on capture conditions, and can be used as a test that the user is really present when the record is taken,
- future-proofed solutions that are tailored to the customer need.

Iris recognition offers great potential for networked applications. The base technology has been tested in the laboratory, in closed user groups and in real-world trials [11], and has been seen to perform rapidly, accurately and robustly to identify individuals correctly.

Recent technological developments, including handheld optical units developed at BTL (see Figs 4 and 5) and elsewhere [12, 13], indicate that hardware will soon become available at low cost for computer log-on and other network-based applications. This paper has described a number of prototype system demonstrators and outlined a range of issues for consideration before the technology is deployed widely.

Acknowledgements

The authors acknowledge the work of G Tomlin and I Reid, and the support of M Mooney, M Arnavutian and P Gill at BT in support of this project. Thanks also go to IriScan Inc for the provision of test equipment throughout the work programme.

Appendix

BT results with iris recognition

BT has tested iris recognition technology in a number of trials. The base technology was evaluated in a laboratory assessment exercise in 1996. Results have been reported elsewhere [4]. In addition, a networked system was installed and used to control access to an internal door within a BT operational building for testing in 1997. All co-operative users within the building were enrolled and the more than 150 regular building occupants used the iris recognition system as an alternative to a 'swipe card' reader to get access to the first floor. In total, 474 eyes were enrolled and there were more than 20 000 recognitions in the 6-week trial period. The overall system response time in this configuration was less than 3 sec. User reaction was positive.

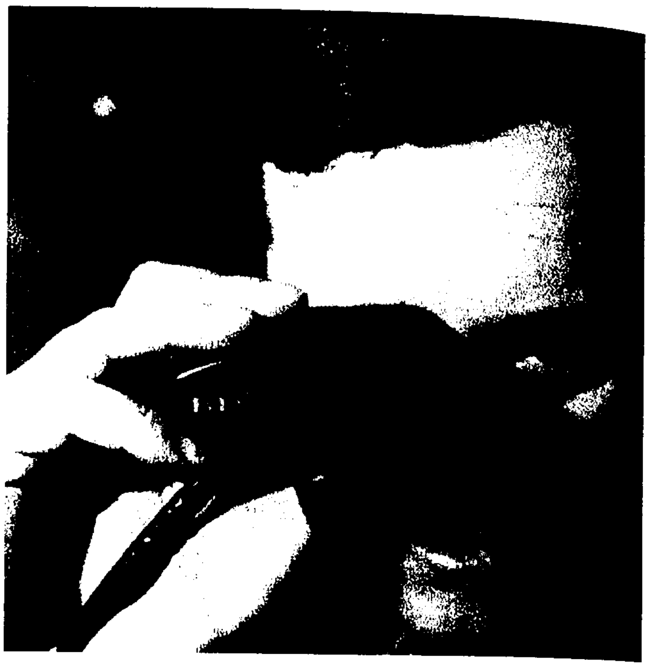

Fig 4 BTL 'look-through' handheld optical unit.

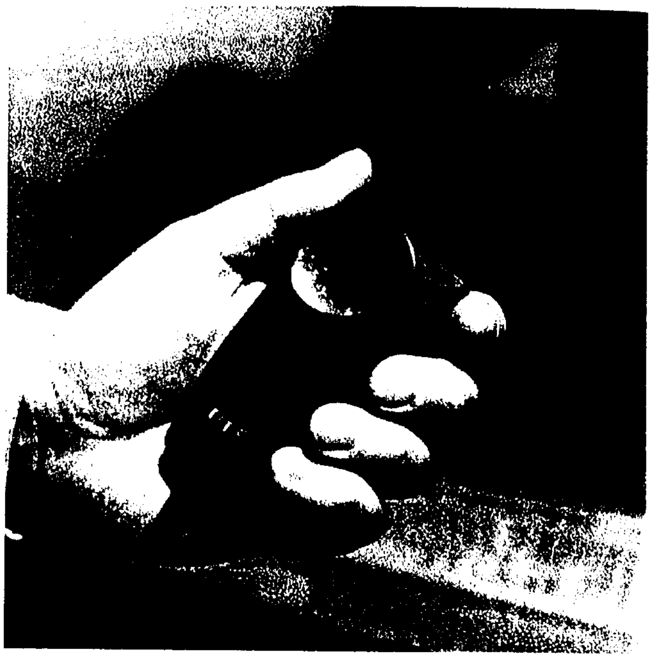

Fig 5 BTL 'mirror style' handheld optical unit.

A successful outcome of this trial has resulted in the technology being adopted to provide secure access to a 'server farm' within a BT operational building. The latest system uses a commercial IriScan networked system with seven remote terminals controlling door access. In this installation, the enrolment, system management and control functions are managed from a WindowsNT server located within the secure area.

In all, during the course of this work more than 1500 eyes have been enrolled by the BTL team, giving confidence in the capabilities of the technology [14].

References

1 Bouchier F, Ahrens J S and Wells G: 'Laboratory evaluation of the IriScan prototype biometric identifier', Sandia National Laboratories, SAND96-1033 (April 1996).

2 http://www.nationwide.co.uk/whatsnew/Iris0212.htm

3 Daugman J: 'High confidence visual recognition of persons by a test of statistical independence', IEEE Trans Pattern Analysis and Machine Intelligence, 15, No 11, pp 1148 — 1161 (1993).

4 Seal C H, Gifford M M, McCartney D J: 'Iris recognition for user validation', British Telecommunications Eng J, 16, No 2 (July 1997).

5 BioAPI — http://www.bioapi.org/

6 HA-API — http://www.biometrics.org/html/standards.html

7 Compaq — http://www.compaq.co.uk/finger/

8 IriScan — http://www.iriscan.com/

9 BT published patent applications: WO97/46978 (11 December 1997), WO97/46979 (11 December 1997), WO97/46980 (11 December 1997), WO98/32093 (23 July 1998), WO98/39740 (9 September 1998).

10 Davies S G: 'Touching Big Brother — how biometric technology will fuse flesh and machine', Information Technology & People, 7, No 4 (1994).

11 Sensar — http://www.sensar.com/

12 'OKI Handheld', Nikkei Weekly, 36, No 1846 (13 October 1998).

13 LG — http://www.lg.co.kr/e_lg/about/news/newsflash/9810/981016.html

14 Innovate — http://innovate.bt.com/showcase/iris_scanning/index.htm

Maurice Gifford received a BSc honours degree in Electronic Physics from the University of London ih 1983. He joined BT Laboratories (BTL) in October 1989 initially working on the development of an ISDN switch. Following this work he was involved in the development of a number of network management tools including exchange log analysis, network traffic management system and a C7 signalling monitoring system. He was team leader for the BTL Iris Recognition project for three years. Prior to joining BT, he was involved in computer systems design for Ferranti Computer Systems.

David McCartney is a research group leader at BT Laboratories. His team explore the telecommunications opportunities for new technologies and produce prototype solutions for a range of business sectors. Recently, he has had a keen interest in biometric applications. He is now exploring new intelligent networking applications and business opportunities. He is a Fellow of the Institute of Physics and has BSc and PhD degrees in Physics from the Queens University in Belfast.

After graduating from the University of Reading with an MSc in Optics in 1990, Chris Seal worked as a contractor to BT developing 3-D displays before spending 3 years with SIRA Technology Centre, working on virtual reality systems. He joined BT full-time in 1995.

During the last four years, he has been involved in researching on-line virtual worlds, and security systems, in particular iris recognition. This work has involved a number of user trials, technology evaluations, systems integration and intellectual property innovations.

He is now working within communication technology business analysis looking at novel next-generation telephone network services such as Parlay.