Special Issue on Networks: UDC 343.982.323 : 612.842.1

"Irispass" Identification System

Kyosuke HOSHINO*, Takeshi OKAMOTO**

Abstract

As networks become progressively more open, the number of terminals to be connected and services to be provided are increasing. Interest in security is also becoming more critical every day. This paper describes the importance of a personal authentication technology as a "key" in the security field, from entering and departure gate management to electronic settlement, and also describes a case where a personal authentication system (Irispass), using the iris of the human eye, in development by Oki, was used at the Nagano Winter Olympics.

1. Introduction

Networks represented by the Internet saw dramatic growth, with services on networks improving and electronic settlements are becoming more practical through successful validation experiments. The number of terminals connected to networks, such as portable terminals, including telephones, and remote supervisory and management systems, is constantly increasing, and information exchange and the sale of products are becoming possible anytime and anywhere. Initially only the advantages were emphasized for using networks, but now the potential risks are becoming clear. In order to secure safety on networks under such conditions, advanced security systems using personal authentication technology is demanded.

2. Security on networks

In the case of information transfers via networks, the following illegal actions may cause problems.

- Falsification of information
- Illegal operation by impersonators
- Wiretapping and leaking of information on networks
- Illegally obtaining data
- Information transmission based on illegal actions
- Using encryption for illegal purposes

The concealment and integrity of data were improved by the advancement of encryption technology. However, if encryption technology is used for illegal purposes, various crimes may be committed with skill and in secret. For example, the settlement of illegal transactions and tax evasion, and the laundering of funds may spread internationally[1]. Authentication of an individual by encryption technology is based on the assumption that "cipher key owner = the authorized individual". This means that when encryption technology is made available on a terminal and is used, only that terminal is authenticated. If an illegal individual obtains the cipher key of an owner, that individual can impersonate the cipher key owner. So a personal authentication technology to check who is actually connected to a network is required to prevent impersonation.

3. Personal authentication

The following are the methods to recognize an individual connecting to a network.

- By a personal possession: a personal possession which only the individual has is used
- By knowledge: Knowledge or something in memory which only the individual can know is used
- By biometrics: the use of a physical feature or characteristic unique to the user is used

Table 1 shows the parameters of personal authentication.

Parameters	Examples
Personal possessions	Key, magnetic card, IC card, identification card
Personal knowledge	Password, identification number
Biometrics	Iris, fingerprint, retina, face, voice, handwriting, palm shape

Table 1: Parameters of personal authentication

When these personal authentication methods are repeatedly used in daily life, an appropriate method should be selected according to the evaluations shown in Table 2. Table 3 shows the general evaluation results[1]. In terms of safety, personal authentication by a personal possession and knowledge involves risk, but if biometrics is used, a high degree of safety can be assured. Table 4 shows the features of personal authentication technologies using various biometrics[4]. If these biometrics based personal authentication technologies are evaluated according to the evaluation items in Table 2, it becomes clear that the personal identification technology which uses the human iris is effective in terms of safety, user comfort, social acceptance and level of security.

Evaluation item	Content
Security level and cost	Balance of scale for assets to be protected and cost
Safety	Collating accuracy, avoidance of theft and forgery
User comfort	Processing speed, ease of operation
Social acceptance	General acceptance with society, protection of privacy

Table 2: Evaluation examples for personal authentication

* Multimedia Development Division, HI Development Center, System Business Group
** First Development Division, Local Information System Development, Public Business Group

Parameter	Personal possessions		Personal knowledge		Biometrics	
Item	Evaluation	Comment	Evaluation	Comment	Evaluation	Comment
Security level and cost	○	Cost of IC cards will eventually decrease	◎		△	Security level is high Expensive at the moment
Safety	×	Forgery, loss, theft possible	×	Loss is possible May be known by personal information	◎	High accuracy Forgery is difficult
User comfort	○		○		△	Personal knowledge is unnecessary Collating may take time Many not portable at the moment
Social acceptance	○	Already common	○	Already common	○	Some have a negative impression about fingerprint collating

Table 3: Evaluation result of personal authentication parameters

4. Effectiveness of Irispass*1

The iris is the pigmented part of the human eye surrounding the pupil, and is comprised of muscular tissue which adjusts the diameter of the pupil. The radial muscles of the iris are unique to an individual. Personal authentication by an iris is implemented by taking a picture of an iris with an CCD camera, encoding the features of the obtained image, and collating this data with data which has been registered[2,3]. The iris of the human eyeball can easily be checked externally. The features of iris based personal authentication are as follows.

- Stability: Since an iris exists in the human eyeball, scratches and abrasions rarely occur
- Complexity: Forgery is very difficult
- Visibility: Authentication is possible from a distant location without contacting the individual

According to the parameters of personal authentication described in Section 3, the effective of Irispass as a personal authentication means is shown next.

1. Security level and cost

   It is generally believed that the security level to assure safety increases as the scale of the assets to protect increases. So in order to increase the security level, some parameters of personal authentication are combined, as shown in Table 5[4]. Irispass can satisfy the conditions of security level III.

	Parameter	Features	Problem
Fingerprint	Line pattern of fingerprints	Unique to individual Unchangeable during lifetime	Stabilizing input quality Handling of skin problems which mask fingerprints Poor social acceptance due to negative image
Retina	Capillary pattern of retina	Unique to individual Unchangeable during lifetime Artificial change impossible	Close checking necessary Resistance to irradiation of infrared rays
Palm Shape	Length of finger	Long history	Stabilizing input quality Hygiene
Facial features	Shape and position of eyes, mouth & nose	Authentication possible without contact Little psychological resistance	Changes considerably over time Influence by glasses, beard, mustache, hair style Restrictions by illumination, background, and angle of photographing
Voice	Voice spectrum (envelope, pitch)	Authentication possible by telephone Authentication possible without contact	Changes considerably over time Influence of colds, etc.
Handwriting	Writing sequence, writing speed, writing pressure	Little psychological resistance	Changes considerably over time Handwriting forgery possible
Iris	Iris pattern	Unique to individual Unchangeable during lifetime Authentication possible without contact	Environmental light conditions

Table 4: Features of biometrics based personal authentication technologies

2. Safety

   A personal possession for authentication may be lost, stolen or be subject to forgery. In the case of knowledge and memory based authentication, such as a password, priority tends to be given to something which is easy to remember, therefore personal information, such as a birthday or telephone number, is often used, which can be used by another individual. Whereas biometrics based personal authentication has a low potential for loss, theft and forgery, and is high in accuracy. In the case of Irispass, FAR (False Accept Rate), which is the recognition error rate, is 1/100,000 or less, and forgery is very difficult. As a result, safety can be assured.

3. User comfort

   Personal authentication by Irispass is hygienic because there is no contact, requires no special operation, and takes a short collation time, several seconds. As a result users experience comfort.

4. Social acceptance

   Personal authentication by personal possessions and knowledge is already quite common to us. And personal

*1 Irispass is a registered trademark of Oki Electric Industry Co. Ltd.
*2 TCP/IP is a protocol developed by the Department of Defense, USA.

authentication using a fingerprint tends to leave us with a negative feeling, since fingerprinting is used in criminal investigations. A feature of Irispass is that an individual is authenticated in a process barely noticeable. Although this is convenient it may intrude on one's privacy. To solve this problem, in actual operation, an authentication approval step by the user is added.

In this way, personal authentication by Irispass has an advantage over other methods.

5. Iris gate system at Nagano Winter Olympics

This section introduces the gate management system using Irispass, which was used at the Nagano Winter Olympics.

This system was developed for the gate system at gun storage for the biathlon event, which required an extremely high level of security, at the Nagano Winter Olympics. This is security level III in the categories of Table 5. As for the combination of parameters, memory (password) + iris pass were used at Nagano, since personal possession used for authentication may be lost, which was seen previously at the Lillehammer and Albertville Olympics.

5.1 System configuration

Fig. 1 shows the hardware configuration of this system. This system is comprised of management center equipment, iris registration equipment, and an iris collating terminal (iris collating gate).

The management center equipment, which supervises the operation status of the system, supervises/controls the iris collating terminal, sets/displays the operation information of this system, and outputs lists.

The iris registration equipment, which registers personal information (name, country, etc.) passwords and iris codes to a database, detects irises which are registered, generates an iris code, and transfers an iris image and iris code to the centralized supervisory equipment.

Level	Key	Cost	Asset scale	Application example
1	Personal possessions (keys, magnetic cards)	¥50K	$¥10^5$	Gate control
2	Personal possessions (keys, magnetic cards) + memory (password)	¥80K	$¥10^8$	Automatic teller machine (ATM)
3	Personal possessions (keys, magnetic cards) + biometrics (Iris pass)	¥650K	$¥10^{11}$	Vault, military related

Table 5: Example of combination of parameters vs. security level

The iris collating terminal accepts a password (input on a ten-key pad) of a visitor, collates the iris code of the visitor with the iris code registered to a database, and controls the electric lock of a gate.

The management center equipment, iris registration equipment and iris collating terminal are inter-connected via a router backbone network based on TCP/IP[*2] protocol.

5.2 Operation format

According to operator instructions, a user who accesses gun storage is registered by iris registration equipment in advance. An average registration time is about three minutes, and when registration finishes the user can access gun storage. To access gun storage, the user stands in front of an Irispass based collating terminal (Photo 1) which is positioned in front of the gun storage gate. Here the user inputs their password via a ten-key pad. With this input Irispass starts collating, finishing user authentication in about two seconds. As soon as the user is authenticated, the electric lock of the gate opens to allow the user to enter storage.

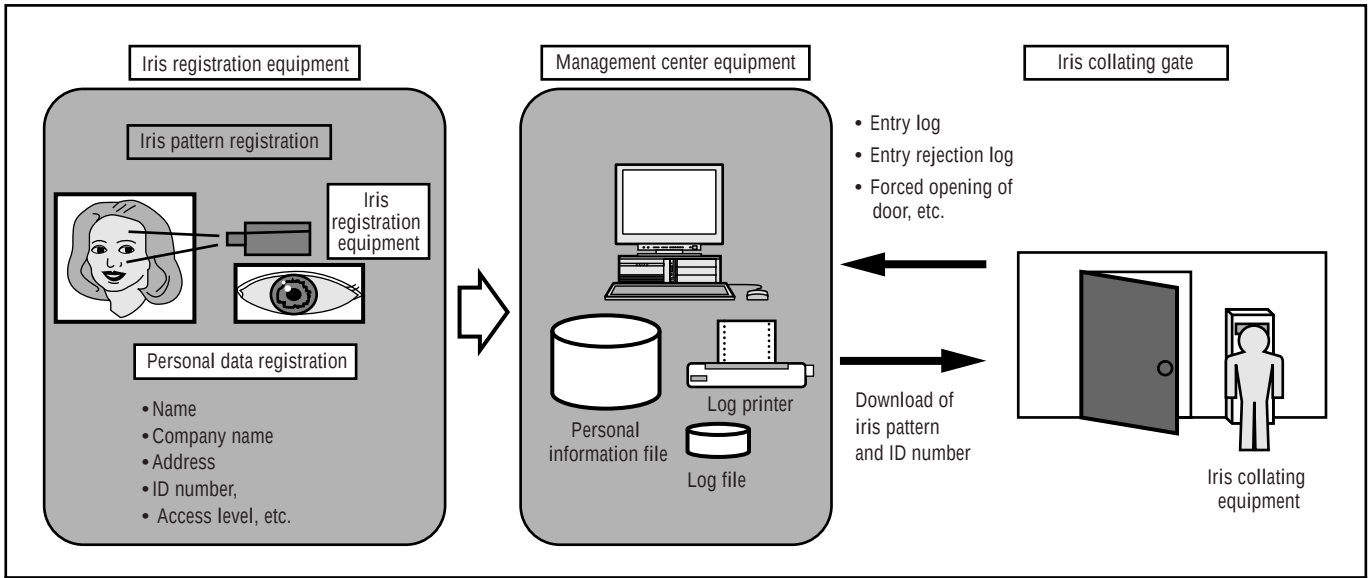

Figure 1: Configuration of Irispass identification system used at Nagano Winter Olympics

5.3 Result

At the Nagano Winter Olympics, a total of 141 players and officials registered for the Irispass system, and there were 2,676 accesses during the 28 day Olympics. During this operation period, the gate system using Irispass was favorably received by both players and officials. The major reasons for this included a short authentication time, user comfort without requiring personal possessions for authentication, and ease of use, requiring only looking into the system from 50 cm away after inputting a password.

6. Conclusion

This paper described the importance of personal authentication on networks and the effectiveness of a biometrics based personal authentication, and introduced the gate system using Irispass, used at the Nagano Winter Olympics. Demands for biometrics based personal authentication technologies will progressively increase in the future. There are high expectations with particular application to the network security field. To meet these demands, we will continuously advance research and development for Irispass, aiming at faster speeds, smaller size and lower cost, and will expand the application fields of Irispass utilizing non-contact authentication and high authentication accuracy.

Photo 1: Iris collator used at Nagano Winter Olympics

7. References

1. Tsujii: Report on information security investigation and research, Security Investigation and Research Committee of Social Safety Research Institute, http://www.npa.go.jp/seiankis/
2. J.G. Daugman : Two-dimensional spectral analysis of cortical receptive field profiles, Vision Res. Vol. 20, (1980): 847 ~ 856.
3. Matsumoto, Tanimoto, Wada: Iris personal identification system, *Oki Kenkyu Kaihatsu*, 175, 64, 3, (1997): 107 ~ 110.
4. Komatsu; Information communication and security ~ authentication technology, Japan Data Communication Association, Japan Data Communication, No. 97, (Sept. 1979): 19 ~ 39.