Compact Fingerprint Verification Device: FingerToken

Hiroki Suto†, Satoshi Shigematsu, Takahiro Hatano, Chikara Yamaguchi, Yukio Okazaki, and Katsuyuki Machida

Abstract

As more and more information services become available over networks, personal identification is becoming more important than ever. This has raised interest in fingerprint verification as a more convenient and robust method of allowing access to protected data than using passwords. FingerToken is a compact personal fingerprint verification device that gives legitimate users easy yet secure access to a full range of services anytime and anywhere.

1. Importance of personal authentication and emergence of biometric authentication technologies

For secure and hassle-free access to information services provided over the Internet, local area networks, and other networks, personal authentication proving that you are a valid user is just as important as encryption and PKI (public key infrastructure) technology to safeguard the communication itself. Passwords have been extensively used for authentication, but they are inherently vulnerable. This is because people tend to use personal information about themselves so that they can remember their passwords. However, birthdays, telephone numbers, and family names are readily available and in many cases can even be guessed.

This vulnerability of passwords has fueled a growing interest in biometrics-based identification methods that cannot be lost or forgotten and make it virtually impossible for others to pose as legitimate users. The main types use fingerprint, hand geometry, face, iris, signature, and voice recognition. **Table 1** compares them in terms of authentication accuracy, cost, and user acceptability (i.e., methods producing the least feeling of unease or resistance on the part of users). The fingerprint-based approach clearly represents the best balance between authentication accuracy and cost and is the most practical biometric for implementing a personal authentication system [1]-

† NTT Microsystem Integration Laboratories
Atsugi-shi, 243-0198 Japan
E-mail: suto@aecl.ntt.co.jp

Table 1. Comparison of biometrics technologies.

	Authentication error		Cost	Ease of use	Acceptability
	FRR*1 (%)	FAR*2 (%)			
Fingerprint	approx 0.1	approx 0.1	Low	High	User resistance to registering
Hand geometry	approx 0.15	approx 0.15	Medium	High	Easy
Face	approx 1	approx 1	Medium	Medium	Easy
Iris	approx 0.1	approx 0.001	High	Medium	Takes time and effort to register
Signature	approx 3	approx 3	Low	High	Easy
Voice print	approx 1	approx 1	Medium	High	Easy

*1 FRR: false rejection rate
*2 FAR: false acceptance rate

[3].

Table 2 lists some of the main areas in which fingerprint-based authentication is being either used or contemplated. A number of stationary fingerprint authentication systems have been described [2], but we expect fingerprint-based systems to be used in many more application areas as authentication is extended to mobile environments. However, before a fingerprint authentication system can be implemented for mobile environments that provide secure access only to legitimate users anytime and anywhere, a number of drawbacks that are characteristic of existing fingerprint authentication system must be resolved. Many existing systems:

1. Can be used only on particular systems that have special proprietary authentication software and/or drivers installed.
2. Are fairly large and require cables, making them unsuitable to carry around.
3. Worry users because fingerprint data is managed on the system side.

In the remainder of this article we present an overview of FingerToken, a mobile authentication device that addresses the above issues and can replace the use of passwords in home and small office environments.

Table 2. Current and future applications of fingerprint authentication.

General	Entry/exit control, vehicle keys, medical uses
Electronic equipment	PC login, database access management
E-commerce	ATMs, vending machines, debit cards, credit cards, digital cash, financial settlement
Government	Health insurance cards, passports, drivers' licenses, various IDs, and licensing documents

2. What is FingerToken?

FingerToken is essentially a personal password storage tool with all the capabilities required for fingerprint authentication—scanning fingerprints, storing fingerprint reference data, and matching the verification data against the reference—built right into the device. **Figure 1** highlights the features of FingerToken.

FingerToken is recognized as a standard keyboard when it is plugged into a USB (universal serial bus) port on a personal computer (PC). The user touches the fingerprint sensor, and FingerToken checks to see if the fingerprint matches fingerprint reference data stored in the device. If it does, the password associated with the fingerprint is sent to the PC just as if it were entered from the keyboard.

FingerToken consists of a capacitance type CMOS (complementary metal oxide semiconductor) fingerprint sensor, a non-volatile memory to store fingerprints and passwords, and a CPU (central processing unit) to perform the authentication processing. Similar in size and weight to popular keyring USB flash memory drives, FingerToken is small and light enough to be carried around, so it is a convenient and secure authentication device that can be used in any environment.

Figure 2 shows the steps involved in using FingerToken. First, a fingerprint is scanned and registered in FingerToken, and a password associated with the fingerprint is set in the system. Once a fingerprint template has been stored in the system, FingerToken is

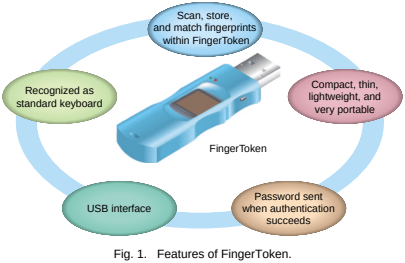

Fig. 1. Features of FingerToken.

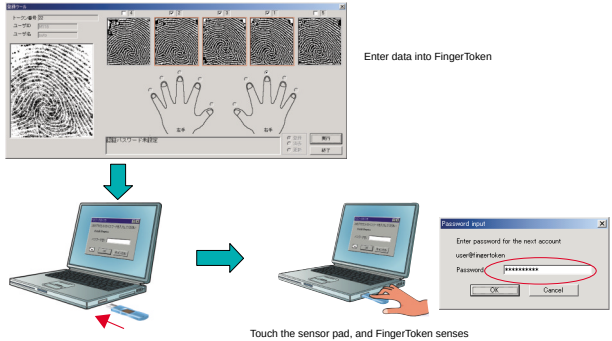

Fig. 2. Using FingerToken.

ready to use to provide secure access to web sites, critical applications, and other resources that require authentication. When a user wants to start up a password-protected application and a dialog box appears asking for a password, the user plugs FingerToken into a USB port, presses the tip of the registered finger on the sensing pad (which is always on and ready to scan). The system attempts to match the sensed print against the fingerprint template stored in the system. If the user checks out, FingerToken sends the corresponding password to the PC, and the application can be accessed and started. FingerToken is powered via the USB port. Once the password has been sent to the PC, FingerToken goes into sleep mode. Since it draws very little power, it can be left in the USB port. The main specifications of the FingerToken system are listed in **Table 3**.

Table 3. FingerToken specifications.

Functions	▪ Sense fingerprint ▪ Store fingerprint template (max. ten fingers) ▪ Match fingerprint ▪ Send password (max. 63 characters per finger) ▪ Generate one-time password
Fingerprint sensor	Capacitance-type CMOS fingerprint sensor
External interface	USB 1.1 (bus-powered)
Mobile environment	Windows98SE, ME, 2000, XP
Recognition time	Less than 2 s per finger
Size	22 mm × 75 mm × 10 mm
Weight	17 g

3. Advantages of FingerToken

3.1 Easy to use in password-protected applications

There is no need to install any special software or drivers on the computer, so fingerprint authentication can be easily used in any application requiring password access. The fact that fingerprint authentication can be simply introduced without modifying the password-protected application means that there is no need to construct any kind of new system. In addition to reusable passwords, FingerToken also has the built-in ability to generate one-time passwords[*1] where a fingerprint is represented as a personal identification number for systems requiring more robust security.

3.2 Strong passwords

Everyone knows that security is enhanced by using strong passwords made up of long random strings

*1 One-time password: a password that can only be used once, so even if it is stolen after being used, it will not allow unauthorized access.

containing both letters and numbers, but in fact most users choose either easy-to-remember passwords or complicated passwords that they write down somewhere, which compromises the security. Since FingerToken assigns a strong password to each valid fingerprint stored on the system and then forwards the password to the PC when it reads the correct fingerprint, it solves the inherent flaws of conventional password authentication: the need to memorize or jot down passwords.

FingerToken also supports multiple fingerprint templates for different fingers on the same hand, with different passwords associated with each finger. This way, different passwords can be set up for different applications and a different finger is presented for authentication of each application.

3.3 Secure storage of fingerprint data

Fingerprint templates are securely stored in FingerToken and managed by the user, so even users who are concerned about their personal information and privacy can use the system with confidence. The scanning, matching, and storing of fingerprint data is done entirely within the device, and the fingerprint data never leaves the device, so FingerToken provides excellent fingerprint confidentiality (i.e., the fingerprint data cannot be seen or extracted by anyone other than the individual who provided the fingerprint).

3.4 Tamper-proof

FingerToken is designed to withstand attacks (unauthorized accesses, attempts to alter or tamper with the data, etc.) on the fingerprint data, passwords, and other personal information it contains, and both hardware and software have been implemented in such a way as to be tamper-proof*2. Since the personal information stored in FingerToken is protected by fingerprint authentication, only the recognized user can access and use the data. This also raises user confidence in FingerToken.

3.5 Customizable authentication tailored to individual users

The fingerprint-matching rate may be affected by variations in different users' skin and fingertips if the user has extremely dry, sweaty, or rough skin. FingerToken is intended for individual users, so the device's fingerprint scanning and matching conditions can be adjusted and optimized for different users' skin conditions to improve the matching rate.

4. Application examples and future enhancements

Personal authentication systems for accessing information systems and services must provide

*2 Tamper-proof means it is exceedingly difficult to gain access to or tamper with data stored in the device by breaking into it. Attempts to gain unauthorized access are also tracked.

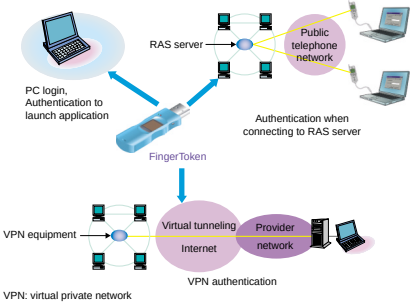

Fig. 3. Examples of FingerToken applications.

robust security but must also be convenient to use. Conventional authentication technologies have had trouble satisfying both objectives at the same time, but using FingerToken for authentication permits the development and deployment of information systems that are both secure and user friendly.

As illustrated in **Fig. 3**, FingerToken could provide authentication to launch various applications on a PC, to issue a one-time password to gain access to a RAS (remote access service) server, or to authorize communication over a virtual private network (VPN) that requires high security.

We expect to see a rapid growth in demand for convenient reliable personal authentication systems combining fingerprint-based authentication with one-time passwords for accessing services via the Internet and corporate intranets. We plan to further refine and promote FingerToken as a widely available authentication solution for accessing ubiquitous services.

References

[1] A. Jain, R. Bolle, and S. Pankanti (editors), "Biometrics, Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

[2] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," IEEE Computer, Vol. 33, No. 2, pp. 56-63, 2000.

[3] A. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance," IEICE Trans. Inf. & Syst., Vol. E84-D, No. 7, pp. 788-799, 2001.

Hiroki Suto
Senior Research Engineer, First Promotion Project, NTT Microsystem Integration Laboratories.
He received the B.E. and M.E. degrees in applied physics from the University of Tokyo, Tokyo in 1983 and 1985, respectively. He joined NTT Atsugi Electrical Communications Laboratories, Kanagawa, Japan in 1985. Since then, he has been engaged in R&D on GaAs and Si integrated circuit design for high-speed applications. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan (IEICE) and IEEE.

Satoshi Shigematsu
Senior Research Engineer, First Promotion Project, NTT Microsystem Integration Laboratories.
He received the B.S. and M.E. degrees in system engineering from Tokyo Denki University, Tokyo in 1990 and 1992, respectively. Since joining NTT in 1992, he has been engaged in R&D of low-voltage, low-power CMOS circuits. His research interests include biometrics sensor technology and low-power and high-speed circuit design techniques. He is currently researching parallel processing circuits for a CMOS fingerprint identifier and developing a single-chip fingerprint identification LSI and user authentication system. He is a member of IEEE, IEICE and the Information Processing Society of Japan.

Takahiro Hatano
Senior Research Engineer, First Promotion Project, NTT Microsystem Integration Laboratories.
He received the B.S. and M.S. degrees in electronics, Information and communication engineering from Waseda University, Tokyo in 1990 and 1992, respectively. In 1992, he joined NTT LSI Laboratories, Tokyo, Japan. He is currently engaged in R&D of fingerprint recognition algorithms and systems. He is a member of IEICE.

Chikara Yamaguchi
Senior Research Engineer, First Promotion Project, NTT Microsystem Integration Laboratories.
He received the B.S. degree in electronics from the University of Yamanashi, Kofu in 1978. In 1978, he joined the Electrical Communication Laboratories, Nippon Telegraph and Telephone Public Corporation (now NTT), Tokyo, Japan, where he was engaged in research on highly reliable LSIs. In 1983, he moved to Atsugi Electrical Communications Laboratories, Kanagawa, Japan, where he engaged in R&D of high-speed Si bipolar devices and process integration, radio data transmission systems, and fingerprint authentication systems. He is a member of IEICE.

Yukio Okazaki
Senior Research Engineer, Supervisor, NTT Microsystem Integration Laboratories.
He received the B.S. and M.S. degrees in physics from Tohoku University, Sendai, Miyagi in 1983 and 1986, respectively. He joined NTT Atsugi Electrical Communications Laboratories, Kanagawa, Japan, in 1986, where he worked on scaled-down CMOS devices and process integration. From 1999 to 2001, he researched fingerprint authentication systems. Since 2001, he has managed R&D of fingerprint sensor LSIs and authentication systems. He is a member of the Japan Society of Applied Physics (JSAP) and IEICE.

Katsuyuki Machida
Senior Research Engineer, Supervisor, NTT Microsystem Integration Laboratories.
He received the B.E., M.E., and Dr. Eng. degrees in electronics engineering from Kyushu Institute of Technology, Kitakyushu, Fukuoka in 1979, 1981, and 1995, respectively. In 1981, he joined the Musashino Electrical Communication Laboratory, Nippon Telegraph and Telephone Public Corporation (now NTT), Musashino, Tokyo, Japan. Since then, he has researched ECR plasma CVD and developed LSI process and manufacturing technologies. He is currently engaged in R&D of the material and manufacturing technologies for MEMS. He is a member of JSAP, IEICE, and IEEE.