Recent Activities Concerning Fingerprint Identification Devices

Yoshimitsu Arai†

Abstract

This article provides an update on NTT's efforts to develop a portable fingerprint identification device and describes recent commercialization activities.

1. Background

In Japan, several well-publicized leaks of customer information from companies and the passing of the Personal Information Protection Act by the Diet (May 2003) have recently made information management more important than ever before and attracted attention to the use of fingerprints as a means of user identification in place of passwords. Passwords can often be guessed by other people because users tend to choose characters that are meaningful to them and easy to remember. Instead, biometrics is considered a promising approach to identifying users from biological information about fingerprints, irises, veins, voiceprints, retinas, palms, and faces, which cannot be forgotten and is difficult to forge. While various biometric identification methods are being evaluated comparatively [1], the most promising one is fingerprint identification because of its good balance between accuracy and cost for easy introduction. NTT developed FingerToken as a compact device aimed at general users. It stores hard-to-break passwords in tamper-resistant memory accessed via a fingerprint identification method [2].

One practical application of fingerprint recognition is a stationary fingerprint identification device for checking people entering and leaving a room for security purposes [3]. To increase the security of personal objects, there has also been some consideration of extending fingerprint identification to portable devices, such as laptop computers and credit cards so that they can be used only by users who registered their fingerprints. This article describes NTT's latest fingerprint technology and efforts to commercialize it.

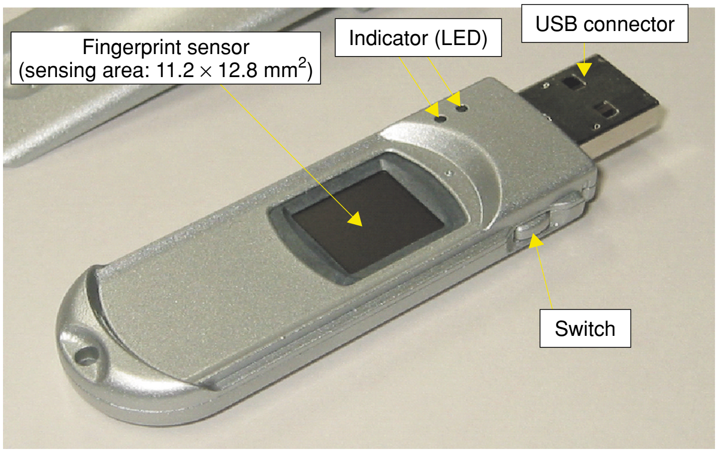
2. FingerQuick

NTT Group has developed and commercialized a fingerprint identification token called FingerQuick* (**Fig. 1**) [4]. Like FingerToken, it can read fingerprints, register and store fingerprint data, and compare fingerprints. It inherits all of the key features of FingerToken, but it is aimed more at the corporate market with large systems run by administrators. Compared with other products of this kind, FingerQuick is better suited to the mobile environment because it has a unique capacitance-type fingerprint sensor that is highly resistant to static electricity and contamination. It is also small and light due to high-density packaging. It measures 23 × 85 × 11 mm^3, including the cap, and weighs 15 g. Since it uses the USB interface, FingerQuick does not need any dedicated authentication and driver software or cables, so it is highly versatile and portable. The integrated fingerprint comparing function means that fingerprint data does not have to leave the FingerQuick unit, which ensures data confidentiality and increases user acceptance of the device.

The procedures for using FingerQuick are shown in **Fig. 2**. Two modes are supported. As shown on the left, if the administrator performs both configuration and fingerprint registration, he first configures Fin-

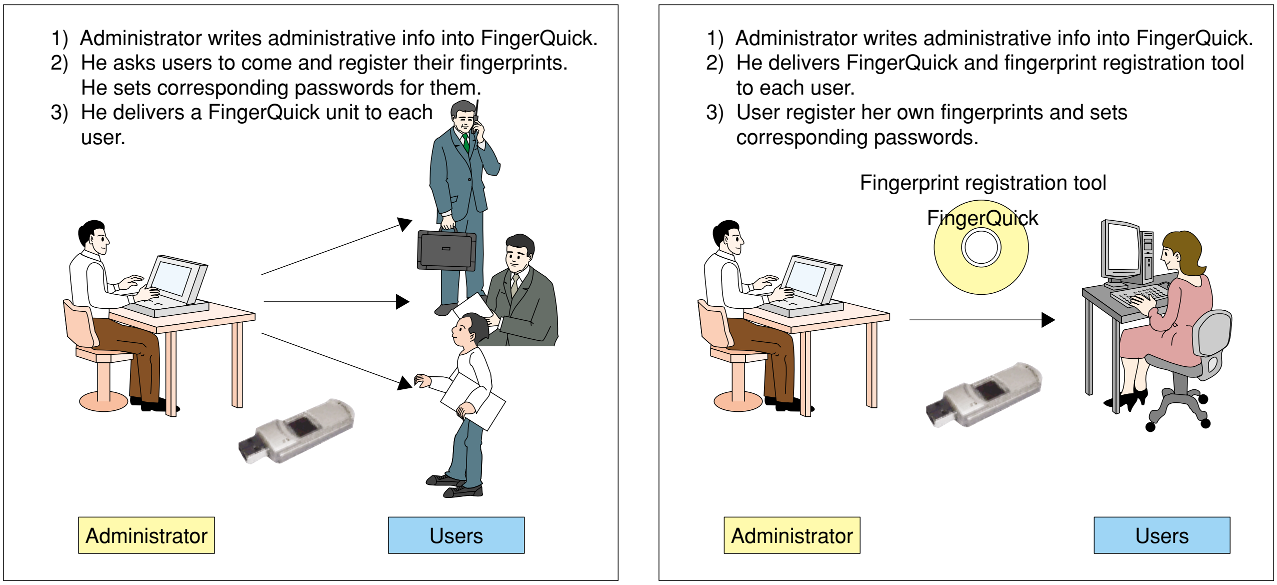
† NTT Department III
Chiyoda-ku, Tokyo, 100-8116 Japan
E-mail: y.arai@hco.ntt.co.jp

* FingerQuick is a registered trademark of NTT Electronics Corporation.



Dimensions: 23 mm × 85 mm × 11 mm (cap included)

Fig. 1. Appearance of FingerQuick.


1) Administrator writes administrative info into FingerQuick.
2) He asks users to come and register their fingerprints. He sets corresponding passwords for them.
3) He delivers a FingerQuick unit to each user.

Configured and registered by administrator.

1) Administrator writes administrative info into FingerQuick.
2) He delivers FingerQuick and fingerprint registration tool to each user.
3) User register her own fingerprints and sets corresponding passwords.

Configured by administrator and registered by user.

Fig. 2. Procedures for using FingerQuick.

gerQuick by writing administrative information, such as an individual's ID and then asks users to register their fingerprints and sets passwords for them. Configured FingerQuick devices are then delivered to corresponding individuals. Only the administrator can set and change passwords, so this mode is suitable for applications where centralized management is desirable. As shown on the right, it is also possible for the administrator to set administrative information alone and deliver the FingerQuick together with a fingerprint registration tool so that users can register their own fingerprint data into the FingerQuick devices and set passwords by themselves. In this case, the convenient registration tool allows users to have free access to the register and change their fingerprint data and passwords. However, the tool can only be activated by an authenticated user to prevent other people from accessing such data and passwords.

Configured FingerQuick devices can be used for user identification required to perform personal computer (PC) login and use some application programs. For example, when the operating system login screen appears when a PC is started up, you can insert FingerQuick into the PC's USB port. FingerQuick initially enters waiting mode. When a finger is placed on the fingerprint sensor, the fingerprint sensing and comparison functions begin. When the user has been authenticated, FingerQuick sends a password corresponding to the fingerprint to the PC via the USB interface. Then the FingerQuick device turns itself off.

3. Applications and promotional efforts

Company employees often need to take customer information off the company premises or access their company network from outside. Currently, passwords are the most popular means of identification. However, there is the danger that someone might observe the password being entered. FingerQuick eliminates such anxiety altogether. Even if the user writes a note saying “right thumb for login, left thumb for network access”, this information is useless to a thief. Thus, FingerQuick provides greater security both inside and outside the company. FingerQuick can also be combined with file encryption software on the market and provide strong security for single sign-on to multiple systems without reducing user convenience.

We expect FingerQuick to be used first at security-conscious corporations. There have recently been growing demands from companies that possess huge amounts of customer information and want to manage it with great social responsibility. Our press release about FingerQuick in June 2004 was covered by most major newspapers and other media. We received a significant response with as many as 100 inquiries immediately after the announcement. Since then, we have been receiving a growing number of inquiries from local governments and industries that handle a large amount of customer and private information. These are beginning to create some business for us.

To expand the field of business applications, we must develop more competitive fingerprint identification devices. We led the world in developing a single-chip fingerprint identification LSI (large-scale integrated circuit), which integrates all processing abilities from fingerprint sensing through identification within one chip [5]. **Figure 3** shows this LSI and some application examples. This LSI is extremely small, measuring 11 × 15 × 1.4 mm^3. It protects fingerprint data completely because it does not allow the data to go outside the chip: it only outputs the result of the identification process. It can also achieve fingerprint identification when mounted on a unit without a processor. In addition, its power consumption is low enough to allow it to run on button batteries. To publicize these features, we exhibited some applications of this LSI at various places, including CEATEC (Combined Exhibition of Advanced Technologies) JAPAN in October 2004. Due to its advantages of ultrasmall size, no need for a processor, and low power consumption, we expect this single-chip fingerprint identification LSI to find many applications, including being built into electrical and electronic appliances. Using this and other NTT technol-

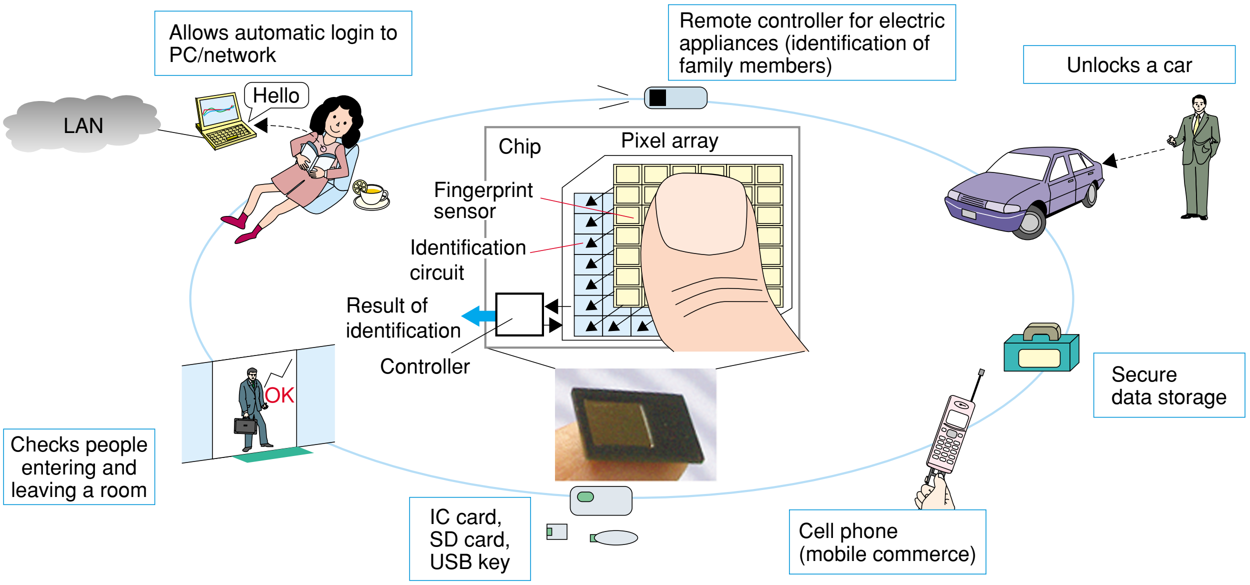

Allows automatic login to PC/network
Hello
LAN
Remote controller for electric appliances (identification of family members)
Unlocks a car
Chip
Pixel array
Fingerprint sensor
Identification circuit
Result of identification
Controller
OK
Checks people entering and leaving a room
Secure data storage
IC card, SD card, USB key
Cell phone (mobile commerce)

Fig. 3. Single-chip fingerprint identification LSI and its application examples.

ogy, we intend to increase the business opportunities for fingerprint identification in close cooperation with companies inside and outside the NTT Group.

References

[1] H. Suto, S. Shigematsu, T. Hatano, C. Yamaguchi, Y. Okazaki, and K. Machida, "Compact Fingerprint Verification Device: FingerToken," NTT Technical Review, Vol. 2, No. 2, pp. 65-69, 2004.

[2] Y. Okazaki and H. Kyuragi, "Trends in User Identification by Using Fingerprints," NTT R&D Vol. 51, No. 3, pp. 189-193, 2002 (in Japanese).

[3] http://www.sw.nec.co.jp/pid/product/sk800-10.html (in Japanese).

[4] http://www.nel.co.jp/product/security/fq_series.html (in Japanese).

[5] S. Shigematsu, K. Fujii, H. Morimura, T. Hatano, M. Nakanishi, T. Adachi, N. Ikeda, T. Shimamura, K. Machida, Y. Okazaki, and H. Kyuragi, "A 500-dpi 224 × 256-pixel single-chip fingerprint identification LSI with pixel-parallel image enhancement and rotation schemes," ISSCC Dig. Of Tech. Papers, pp. 354-473, Feb. 2002.

Yoshimitsu Arai

Producer, Innovative Devices Team, NTT Department III (R&D Strategy Department).

He received the B.E. and M.E. degrees in electrical engineering from Gunma University, Kiryu, Gunma in 1982 and 1984, respectively. Since joining NTT Electrical Communications Laboratories in 1984, he has been engaged in research on packaging technology for electrical and optical components of communications systems. From 2001 to 2003, he managed R&D of high-speed optical interconnections and media converters for access networks. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan.