Detection and Recognition Technologies

Fingerprint Identification

By Kaoru UCHIDA*

ABSTRACT Biometrics technology, which uses physical or behavioral characteristics to identify users, has come to attract increased attention as a means of reliable personal authentication that helps establish the identity of an actual user. Among various modalities of biometrics, fingerprints are known to have the longest history of actual use in law enforcement applications with proven performance. This paper surveys the state of the art in fingerprint identification technology. The current trend of fingerprint sensing and identification algorithms are presented first in detail in order to show how fingerprint-based systems work and then some topics with regard to fingerprint identification are discussed. These include actual examples of fingerprint-based personal identification systems, large-scale fingerprint identification systems (AFIS), international activities on standardization and performance evaluation, and a "Fingerprint User Interface" (FpUI), which is a new type of application of this technology used to enhance human-machine interactions.

KEYWORDS **Biometrics, Fingerprint, Security, Identification**

1. INTRODUCTION

In order to protect users of computer systems and to secure network-based transactions, demand is increasing for improved user authentication procedures to establish the identity of an actual user and to bar access to a terminal to anyone who is unauthorized. Personal identification using biometrics, i.e., a person's physical or behavioral characteristics, has come to attract increased attention as a possible solution to this issue and one that might offer reliable systems at a reasonable cost[1,2]. While traditionally this technology has been available only with such expensive, high-end systems as those used in law enforcement and other government applications, today many personal-level applications have also become possible thanks to the advancements in pattern recognition technology.

When compared with the conventional authentication methods that are based on "what only the person possesses" or "what only the person knows," biometrics authentication offers two distinctive advantages:

- Enhanced convenience: By merely presenting his biometric features, a user can easily prove himself or herself. There are no troubles such that authorized users are denied access because of loss of a card or forgetting a password.
- Augmented security: The reliable rejection of impostors, who might attempt to gain access either by stealing or forging cards or by guessing or fraudulently obtaining passwords, becomes possible.

Among various modalities in biometrics, such as fingerprints, face, iris, etc., fingerprints are the most widely used and have the longest history in real-world law enforcement applications[3-5]. Research into automated fingerprint identification began in the 1960's, and the resulting AFISs (Automated Fingerprint Identification Systems) have been used worldwide with established dependability. Millions of identifications over a century of actual forensic history have clearly shown that fingerprints are unique and permanent and thus that fingerprint identification is extremely reliable. Recent technical advances have made identification (i.e., one-to-many matching) systems low enough in cost for civilian applications.

Fingerprints have, among many, the following two advantages when compared with other modalities:

1) Stable, reliable and highly accurate identification software is currently available even for use on personal computers.
2) Fingerprint sensors can be made small and thin enough to be implemented easily on small computers and even on pocket-sized terminals.

*Media and Information Research Laboratories

A fingerprint-based personal authentication system operates in two distinct modes: enrollment and authentication (identification), as is shown in **Fig. 1**. During enrollment, a fingerprint image is acquired from a finger presented by an authorized user using a "fingerprint sensor," and relevant features are extracted by the features extractor. The set of extracted features, also referred to as a "template" is stored in a database, along with the user's information necessary for granting service, and some form of ID assigned for the user.

When the user seeks for a service, i.e. in authentication mode, the user inputs his assigned ID and presents his fingerprint to the sensor. The system captures the image, extracts (input) features from it, and attempts to match the input features to the template features corresponding to the subject's ID in the system database. If the calculated similarity score between the input and the template is larger than the predetermined threshold, the system determines that the subject is who he claims to be and offer the service; otherwise would reject the claim.

In identification mode, on the other hand, the user who seeks for a service presents his fingerprint only without his ID, and the system may either be able to determine the identity of the subject or decide the person is not enrolled in the database.

In this paper, having first described the general process of fingerprint-based identification, I will now present the current trend of fingerprint sensing and identification technologies in more detail, in order to show how actual fingerprint-based systems work. I will then illustrate some actual systems with a fingerprint identification capability that are in use; "SecureFinger," some actual examples of fingerprint-based personal identification systems and large-scale fingerprint identification systems (AFIS). I will also discuss some new issues with regard to this technology, international activities on standardization and performance evaluation methods. Fingerprint User Interface (FpUI), a new type of application of this technology used to enhance human-machine interactions, will also be considered.

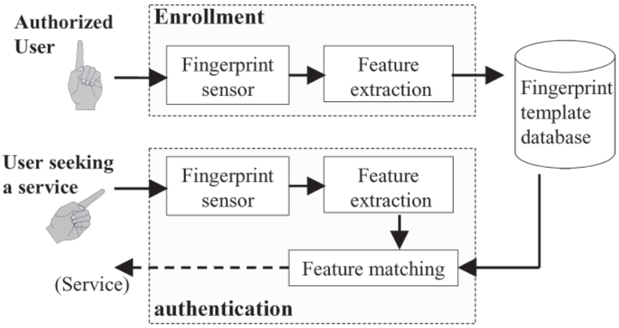


Fig. 1 Fingerprint-based personal authentication.

2. FINGERPRINT SENSING TECHNOLOGY

A fingerprint is a pattern of fine ridges and valleys (spaces between ridges) on the surface of a finger, and a fingerprint sensor makes a digitized image of it. The sensing resolution is 500ppi (pixel per inch; also known as 500dpi, i.e., dots per inch) in most cases, which is equivalent to 20 pixels in 1 millimeter. The obtained image size is typically in the range of between 300×300 and 512×512 pixels, which makes the area covering the fingerprint between 15 to 25 millimeters square.

2.1 Conventional Prism-Type Optical Sensor

Optical sensors using a prism have long been used as a common (and formerly the only) capture device. In them, the light from an LED illuminates a finger placed on a prism, and its reflected image is captured by a small, optical sensing device (e.g., a CCD or CMOS imager chip), as in **Fig. 2**. This device operates basically on the principle of frustrated total internal reflection (FTIR). The strength of reflectance at any given point on a finger will vary, depending on its distance off the prism surface. The ridge pattern is then obtained in the form of a gray-level image. Although this type of sensor can provide good sensitivity even for dry or overly sweaty fingers, the unit tends to be expensive and bulky due to the various kinds of components used.

2.2 Solid-State Sensor

Non-optical, solid-state sensors have also appeared on the market in recent years. In this case, the ridge patterns of a finger placed directly on a silicon chip (sufficiently coated, of course, to protect its surface) are sensed on the basis of differences in either

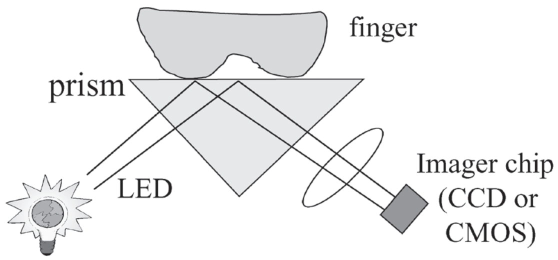


Fig. 2 Optical fingerprint sensor using a prism.

capacitance, temperature, or pressure. Such one-chip sensors offer a low-cost implementation for small-area, thin devices.

Although these sensors can be small, thin, and comparatively cheap, they tend to be fragile against ESD (Electrostatic discharge) and have insufficient sensitivity especially for dry or overly sweaty fingers.

2.3 New Optical Sensor Using In-Finger Light Dispersion

NEC has developed a new type of optical sensor based on in-finger light dispersion[6], which can make use of the advantages of both the above types. In this sensing mechanism, as a finger is placed directly on the sensor, it is illuminated by ambient light, and the optical imager chip senses the strength of the dispersed light that reaches through the finger. The light emanating from the valley part of the finger is dispersed in the air and becomes weak, leaving the corresponding pixels darker. A proprietary, special surface glass over the imager chip ensures good imaging and protection. **Figure 3** illustrates the mechanism of the method.

As this method is based on direct-touch sensing, it can increase the imaging resolution by merely using higher resolution imager chips; the present implementation has 800 and 1,200 ppi resolution. This sensor solution offers the following advantages:

- Attains good sensitivity even for dry and sweaty fingers
- It can be used under strong background light illumination (such as direct sunlight)
- Resistant against mechanical impact and ESD
- Small and thin implementation is possible
- Sufficiently high resolution sensing is possible, which can deal with fingerprints with high ridge pitch. This type is common among some females and children.

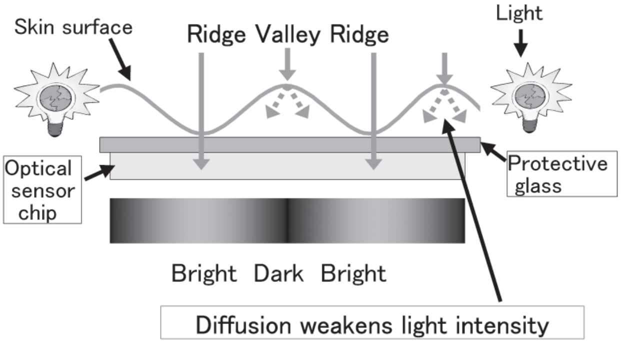


Fig. 3 Optical sensor using in-finger light dispersion.

3. FINGERPRINT IDENTIFICATION ALGORITHMS

3.1 Correlation and Feature-Based Approaches

There are two major approaches to fingerprint identification: image correlation and structural feature matching.

The image correlation approach is based on global pattern matching between an enrolled fingerprint and the given fingerprint to be matched. After two images are aligned, they are checked for correspondence. In general, this kind of matching requires less computation but is less robust against image distortions, which are unavoidable in fingerprint matching because fingers are elastic and not rigid, and which represent the biggest hurdle to the successful application of a simple pattern matching approach.

In structural feature matching, on the other hand, ridge endings and bifurcations (collectively called "minutia"; see **Fig. 4**) in the ridge patterns are located, and their positional relationships are noted. In the matching phase, the minutia sets extracted from the input image and in a template data in the database are aligned in location as in **Fig. 5**, and the difference in minutia correspondence is accumulated to evaluate the (dis)similarity of the two images. This approach is more robust against fingerprint distortions.

3.2 "Minutia-Relation Matching" Based on Ridge Counting

To attain more highly accurate feature-based fingerprint identification, NEC has developed an algorithm called "Minutia-relation-based Matching,"

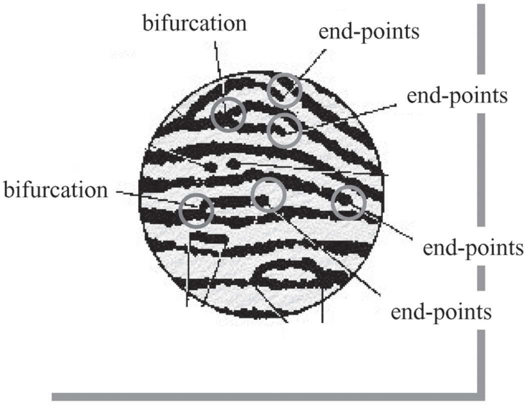


Fig. 4 Ridge structure and minutiae (circled).

which uses, in addition to distances between minutiae, ridge counts, i.e., the number of ridges that cross line segments running between minutiae[7-9]. **Figure 6** illustrates an example of ridge counts, where, although the distance between M_1 and M_2 is the same in both patterns, we can distinguish the two by using the ridge counts.

In the enrollment phase, the "relation," that is, relational map of the ridge counts, is computed from the enrollment finger and the template is constructed as in **Fig. 7**. Then when identification is necessary, the relation is extracted from the user's presented finger, and it is compared to the templates in the database, as in **Fig. 8**.

When identification is to be made from a database containing a large number of entries, as in AFISs, a technology called "automated fingerprint preselection (or classification)" is additionally employed to help reduce the number of candidates for fingerprint matching[10].

3.3 Fingerprint Authentication Based on Individual FMR

In fingerprint (or, biometrics, in general) authentication, as we have seen, the system calculates a similarity score between an input and the template and accepts or rejects the claimant based on whether the score is larger than the predetermined threshold. In conventional approaches, the algorithm for calculating a score and the threshold are determined through experiments using a large number of test samples, based on the assumption that the system meets the security requirements if the observed FMR (False Match Rate), which is the probability of imposter fingers accepted*, is below the target value. For example, if the FMR reported from the test is one in 10,000, we would assume that the system attains the imposter error rate of 1/10,000.

But this figure only assures that the "average" FMR is at a certain level, and it is likely that, for half of all the actual fingers, its "individual" FMR is greater than the average FMR. This means that for some users, the risk of imposter acceptance is to some extent, or by far in some worst cases, larger than the security requirement [12]. This means that the concept of individual FMR is important as a performance measure of biometric systems for security applications, and that ideal secure algorithms should assure sufficiently small individual FMR for a larger proportion of users, instead of merely attaining average FMR at a certain level.

NEC has developed a fingerprint matching algorithm which can meet this important requirement for biometric use in security applications[13,14]. This algorithm, based on accidental coincidence probability of fingerprint features, first hypothesizes that two fingerprints, the input and the template, are from different fingers. It then calculates the accidental probability that an occurrence of greater coincidence of features (such as the position of minutiae) is more probable in any two fingers than in the actual observed results. It then decides that two are actually from the same finger only if this calculated accidental coincidence probability is sufficiently small. This algorithm, which directly evaluates the possibility of two different fingers being accidentally coincident, can assure lower individual FMR for a greater proportion of users and thus can prove effective in highly sensitive secure applications.

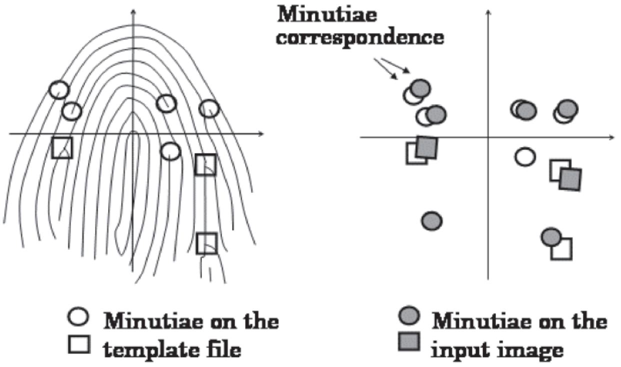

Minutiae correspondence
○ □ Minutiae on the template file
● ■ Minutiae on the input image

Fig. 5 Minutiae correspondence computation.

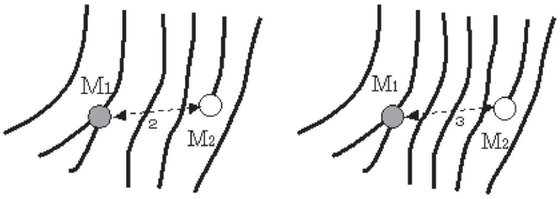


Fig. 6 Ridge count between minutiae.

*FMR is defined as "proportion of zero-effort impostor attempt sample features falsely declared to match the compared non-self" in the Final Committee Draft 19795-1, Biometric Performance Testing and Reporting - Part 1: Principles and Framework[11], prepared by Working Group 5 (Biometric Testing and Reporting), ISO/IEC JTC1, Subcommittee SC 37, Biometrics.

4. EXAMPLES OF ACTUAL APPLICATIONS

4.1 “SecureFinger” - Fingerprint Authentication System

NEC’s SecureFinger series (**Fig. 9**) are personal authentication systems for information security purposes. These systems use identification software based on the previously mentioned minutia-relation-based algorithm[15] and achieve highly reliable authentication and identification on small, inexpensive micro-computer-based systems. SecureFinger uses an in-finger light dispersion optical sensor, which captures good images even when the fingers are dry or sweaty. Mutual authentication and data stream encryption protocols for ensuring user data privacy are implemented in the communication between the SecureFinger unit and the PC to which it is connected.

Such a basic authentication system coupled with a computer can verify a user so as to allow OS log-ins, screen-saver unlocks, and file encryption/decryption. To protect data in case a computer is stolen, a pre-boot lock function, which requires fingerprint verification upon system boot-up, can be integrated with the PC’s BIOS (Basic Input Output System) mechanism to offer added security.

SecureFinger can also be used with networked services, for log-ins to remote computers and for access

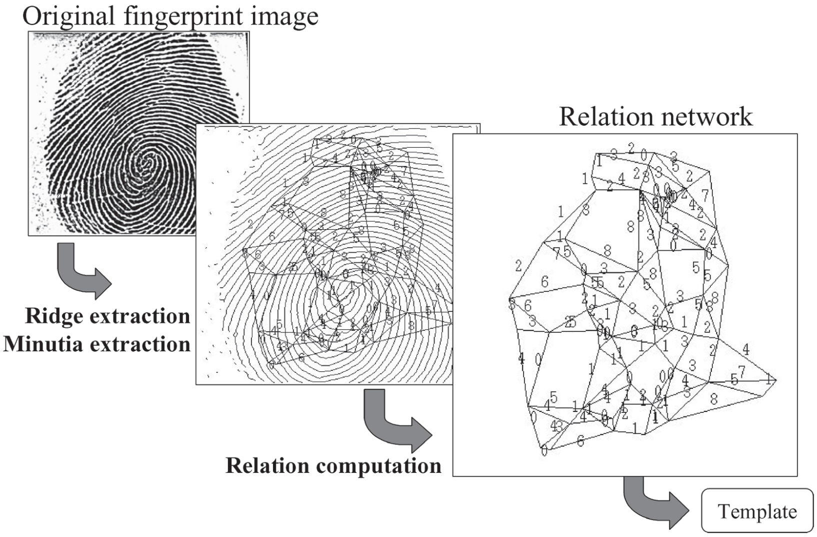


Fig. 7 Ridge extraction, minutiae location and “Relation” computation.

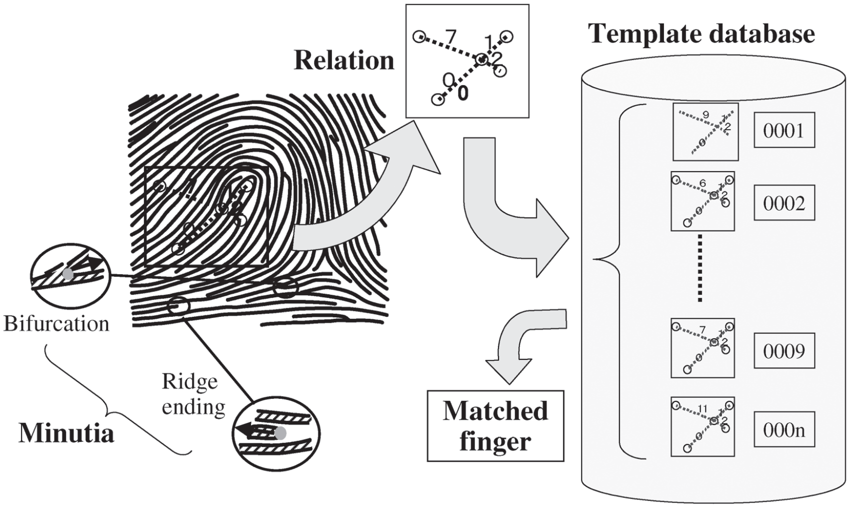
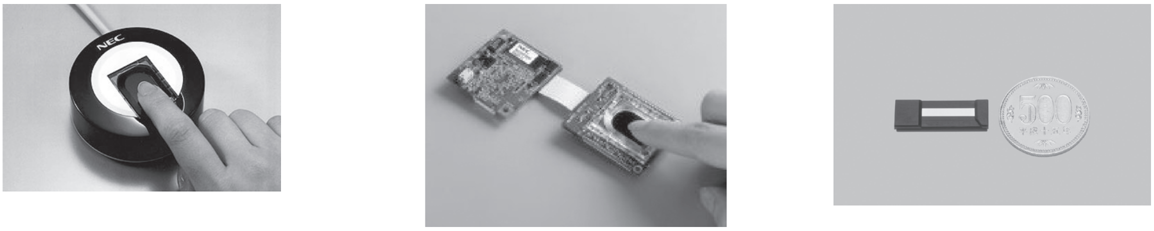


Fig. 8 Search in a template database.



(a) Optical type using in-finger dispersion.

(b) Stand-alone module.

(c) Line-type sensor.

【For more details, please see http://www.sw.nec.co.jp/pid】

Fig. 9 Fingerprint identification unit: SecureFinger.

to remote database servers and membership-based Web services, including electronic commerce, etc. The system can easily be extended to server-based identification by means of the SDK (Software Development Kit) provided for network system integration.

NEC has also developed a line-type fingerprint sensor based on in-finger light dispersion. Because line-type sensors are much smaller and less expensive than area-type sensors, they can now be applied to smaller information technology appliances, such as PDAs (Personal Digital Assistants) and USB memory units.

4.2. Large-Scale AFIS

The core technology used in SecureFinger originates from the long history of NEC's research and development in large-scale systems for law enforcement applications. NEC started its research activity into automated fingerprint identification in 1971, and developed a highly reliable AFIS (Automated Fingerprint Identification System) after decade-long efforts that began operation at the National Police Agency of Japan in 1982[16]. Since then, a large number of AFISs have been developed for various law enforcement applications both in Japan and abroad. It has been reported that NEC's systems hold a 69% share of the fingerprint record in databases for law enforcement purposes worldwide[17].

4.3. Palmprint Identification

NEC has also developed a palmprint identification system. While palmprint identification is effective in cases where no latent fingerprints but only a latent palmprint is left at the crime scene, some major technological difficulties had delayed the implementation of highly reliable automated palmprint identification. One difficulty is that, when compared with fingerprint identification, ridge lines are less apparent due to crease lines that often conceal the ridges, and another is that the image alignment is more difficult because there are fewer singularities (such as core points) and the processing area is much larger. NEC has successfully overcome these technical difficulties[18,19] and has applied some large-sized automated palmprint identification systems to real operations*.

5. INTERNATIONAL STANDARDIZATION ACTIVITIES AND TECHNOLOGY EVALUATION EFFORTS

International standardization efforts in biometrics have been very active recently, especially since Subcommittee SC 37, which focuses on biometric technology, was founded in ISO/IEC JTC1 (International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1) in 2002[20]. At SC37, standardizations of interchange data formats, API and performance testing methods are discussed.

Another topic of international cooperation is technology evaluation efforts, or authentication accuracy competition, to compare performance among various systems. In 2003, a first large-scale project of this kind, "Fingerprint Vendor Technology Evaluation" (FpVTE) was conducted by NIST (National Institute

*The California Department of Justice (DOJ), which is one of NEC's major clients in the U.S., was honored in December 2004, with the "2004 Best of California" award by the Center for Digital Government, for its California Automated Palm Print System (CAPPS), the first statewide automated palmprint database in the U.S.

of Standards and Technology) to evaluate the accuracy of fingerprint matching, identification and verification systems[21]. The tests, in which 18 vendors, including the four major AFIS vendors, participated, were to evaluate error rates at various fingerprint image databases, from one million comparisons (Small Scale Test = SST) to one billion comparisons (Large Scale Test = LST). In these tests, NEC produced the most accurate results and extremely low error rates over a variety of image types, by achieving, for example, the best score at 42 out of 44 test partitions in an LST that contained a large number of low quality, or difficult, fingerprint images[22].

6. NEW APPLICATION OF BIOMETRICS: FINGERPRINT UI

In conventional applications, as we have seen, fingerprints have only been used as a means of personal verification, based on the fact that they are invariant with time and unique among people, and system designers have only exploited this single aspect of their huge potential. Focusing on the fact that a person's fingerprints are different from finger to finger as well, I have previously proposed "Fingerprint User Interface" (FpUI)[23,24].

When we interact with computer systems by, for example, hitting keys, all that the system knows is which key has been hit and when. If, however, keys were equipped with fingerprint sensors and software were utilized that could distinguish differences among fingerprints, a system might additionally be able to take actions determined by both whose and which finger activated a given sensor. This is the concept behind the use of FpUI to enhance human-machine interactions.

Figure 10 illustrates one typical example of how FpUI works. When a user touches the sensor with a certain finger, the sensor obtains an image of the fingerprint. Fingerprint identification is then executed on the acquired image; a matching fingerprint is located in the prepared table, and the action associated with that match is carried out in response.

While the FpUI concept itself is quite simple, it might be applied very effectively in a number of ways, especially when utilized in systems and appliances designed for general use. I will briefly outline some examples of applications that might be expected to expand the use of biometrics technology.

(1) Fingertip Commands

Different commands can be assigned to different fingers. While the conventional "hitting the key" action only provides a direct execution trigger, this user interface enables execution of specific actions tied to specific fingers. Using such "fingertip commands," an interface designer can reduce the number of required keys and avoid the use of mode keys (such as ctrl and alt keys), which often confuse computer novices. **Figure 11** illustrates the comparison of fingertip commands with a conventional user interface.

(2) Fingertip Saver

At the time of log-in, a fingerprint can be used not only for user verification but also for system customization (e.g. desktop design, shortcuts, etc.) based on that individual user's preferences. By the choice of finger employed, a user might choose among multiple sets of working environments. In addition to static setups, the dynamic status of a pending session might be saved and later restored merely by presenting a fingertip, so that users could continue their work more easily.

(3) Fingertip Memo

The concept of "state memorization" represents the idea of a user interface utilizing fingers as virtual "data storage" for various data objects. For example, keeping a URL in each finger allow a user to browse Web sites merely by changing fingers. By using a "memorize then retrieve" sequence dynamically, a user could copy-and-paste via multiple fingertip copy buffers (clipboards).

This application could also be used over a network, with one object that has been virtually copied to a finger on one PC being pasted on another by the touch of that finger. This naturally represents a metaphor of "saving and carrying a data object" in his finger. **Figure 12** shows an actual implementation of the fingertip memo. This also shows virtual data flow, i.e. how the action of data copy appears to a (novice) user.

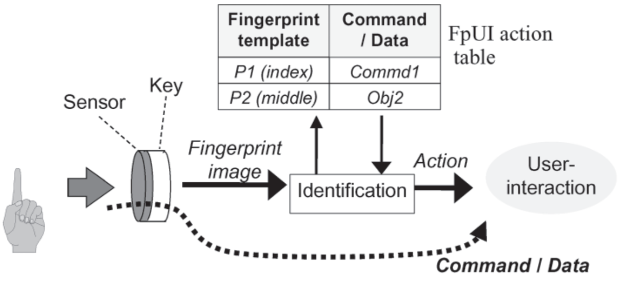


Fig. 10 Fingerprint user interface.

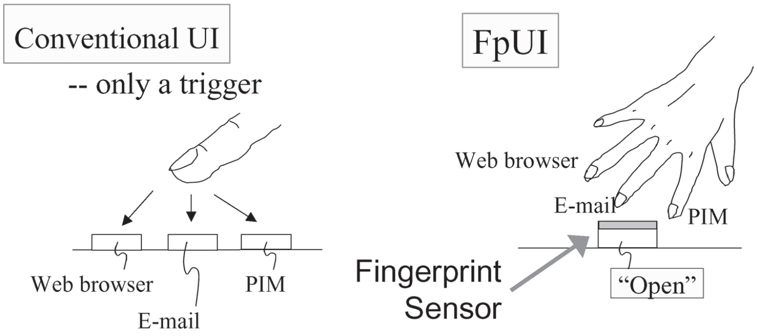


Fig. 11 Fingertip commands.

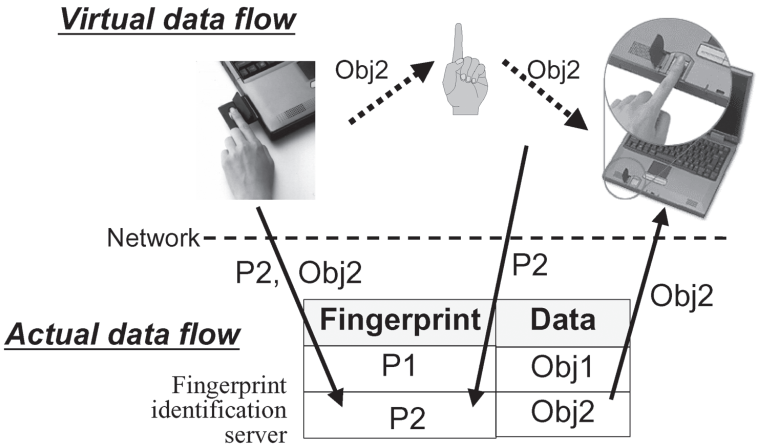


Fig. 12 Implementation of "Fingertip memo."

7. CONCLUSION

I have surveyed key technologies about fingerprint identification and have described in detail the working of fingerprint-based systems, the most widely-employed of all systems based on biometrics technology. I have also illustrated some actual systems based on these technologies in use, and presented some new activities that are taking place internationally. I have also briefly discussed the enhanced user interface "FpUI," which takes advantage of fingerprint identification technology to broaden the scope of its potential real-world application.

I hope this paper might help augment the general user's understanding of biometrics and fingerprint technology, particularly with respect to its utility, acceptability, and familiarity and moreover, to lead as well to a heightened awareness of the important role that biometrics can be expected to play in enhancing the overall security of systems.

REFERENCES

[1] Special Issue on Automated Biometrics, Proceedings of the IEEE, **85**, Sept. 1997.

[2] Anil Jain, (ed), "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

[3] L. O'Gorman, "Fingerprint Verification," in Biometrics: Personal Identification in Networked Society, pp.43-64, Kluwer Academic Publishers, 1999.

[4] D. Maltoni, et al., "Handbook of Fingerprint Recognition," Springer, 2003.

[5] N. Ratha, et al., "Automatic Fingerprint Recognition Systems," Springer, 2003.

[6] T. Higuchi, "Fingerprint authentication system / New fingerprint sensor," *NEC Tech. J.* , **55**, 3, pp.19-22, Mar. 2002 (in Japanese).

[7] K. Asai, Y. Kato, et al., "Automatic Fingerprint Identification," Proceedings of the Society of Photo-Optical Instrumentation Engineers, **182**, pp.49-56, 1979.

[8] K. Asai, Y. Hoshino and K. Kiji, "Automatic fingerprint identification by minutia-network feature - Feature extraction process," *Transactions of IEICE D-II*, **J72-D-II**, 5, pp.724-732, May 1989 (in Japanese).

[9] K. Asai, Y. Hoshino and K. Kiji, "Automatic fingerprint identification by minutia-network feature - Matching process," *Transactions of IEICE D-II*, **J72-D-II**, 5, pp.733-740, May 1989 (in Japanese).

[10] K. Uchida, et al, "Fingerprint card classification with statistical feature integration," Proceedings of the 14th International Conference on Pattern Recognition, Brisbane, Australia, pp.1833-1839, Aug. 1998.

[11] Text of Final Committee Draft 19795-1, Biometric Performance Testing and Reporting - Part 1: Principles and Framework, ISO/IEC JTC1/SC37 N908, 2005.

[12] A. Monden, L. Huang and S. Yoshimoto, "A Performance Evaluation Assuring the Security Strength of Individual Fingerprints," Proc. of the 2005 Symposium on Cryptography and Information Security, pp.541-546, 2005 (in Japanese).

[13] A. Monden and S. Yoshimoto, "Fingerprint Identification for Security Applications," *NEC Res. & Develop.* , **44**, 4, pp.328-332, Oct. 2003.

[14] L. Huang, A. Monden and S. Yoshimoto, "Fingerprint Identification Based on False Acceptance Probability," Proc. of the 2004 Symposium on Cryptography and Information Security, pp.579-584, 2004 (in Japanese).

[15] S. Hiratsuka and Y. Hoshino, "The Intelligent Fingerprint Authentication System 'SecureFinger'," *NEC Res. & Develop.* , **43**, 1, pp.11-14, Jan. 2002.

[16] K. Kiji, Y. Hoshino and K. Asai, "Automated Fingerprint Identification (AFIS)," *NEC Res. & Develop.* , 96, pp.143-146, Mar. 1990.

[17] J. L. Peterson, "The Status of AFIS systems worldwide - Issues of Organization, Performance and Impact," International Symposium on Fingerprint Detection and Identification, Ne'urim, Israel, June, 1995.

[18] J. Funada, et al, "Feature Extraction Method for Palmprint Considering Elimination of Creases," Proceedings of the 14th International Conference on Pattern Recognition, Brisbane, Australia, pp.1849-1854, Aug. 1998.

[19] A. Monden, et al, Correct Position Search for Palmprint Using Neighbor Minutiae, Technical Report of IEICE, PRMU97-40, pp.23-29, 1997 (in Japanese).

[20] http://www.jtc1.org/sc37

[21] http://fpvte.nist.gov

[22] C. L. Wilson et al., "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report," NISTIR 7123, NIST, 2004.

[23] K. Uchida, "Fingerprint-based User-friendly Interface and Pocket-PID for Mobile Authentication," Proceedings of the 15th International Conference on Pattern Recognition, Barcelona, Spain, **4**, pp.205-209, Sept. 2000.

[24] K. Uchida, "Fingerprint identification for enhanced user interface and for secure Internet services," IEICE (The Institute of Electronics, Information and Communication Engineers) Transactions on Information and Systems, **E84-D**, 7, pp.806-811, July 2001.

Received January 14, 2005

* * * * * * * * * * * * * * *

Kaoru UCHIDA received his B.E. degree in Mathematical Engineering and Information Physics from The University of Tokyo, Japan, in 1984, his M.Sc degree in Computer Science from Stanford University, U.S.A., in 1991, and his Ph.D. degree in Information Sciences from Tohoku University, Japan, in 2003. He is currently a Principal Researcher at the Media and Information Research Laboratories, NEC Corporation. His research interests include pattern recognition and computer vision; in particular, they include algorithms, systems, and the application of biometrics to personal identification.

Dr. Uchida is the secretary of Working Group 5 for biometric performance testing and reporting, Japanese National Body, for ISO/IEC JTC1/SC37, Biometrics Subcommittee, and a member of the Institute of Electronics, Information and Communication Engineers.

* * * * * * * * * * * * * * *