Biometric Personal Identification Technology and Its Applications

By Kaoru UCHIDA*

ABSTRACT This paper surveys the state of the art in biometrics: the technology of automatically identifying individuals using their physiological or behavioral characteristics. In response to the security need to authenticate users in networked interactions, biometric technology has advanced significantly over the last few years, and a wide range of applications, based on a variety of biometric approaches, are to be found both in the literature and in the market today. Here, I describe general principles and some of the key concepts involved in biometric-based identification, and explain different biometric technologies. As an actual example of mature biometrics, I present in detail how fingerprint-based systems work. I also discuss Fingerprint User Interface, a novel application of fingerprint identification technology used to enhance man-machine interface. With it, a user can assign commands, data objects, or personalized status to individual fingers to facilitate human-machine interactions.

KEYWORDS **Biometrics, Fingerprint, User interface, Networked services**

1. INTRODUCTION

With advances in information technology, more and more people have come to use computer systems and networked services to exchange things of value without actually seeing the persons with whom they are dealing. To protect users in these interactions, much effort has been made in the research and development of such security techniques as the use of cryptography and firewalls. Such measures only ensure security on the paths between terminals, however, and demand is increasing for improved "user authentication" to help establish the identity of an actual user and to bar access to a terminal by anyone unauthorized.

Conventionally, such authentication has been conducted on the basis of either:

1) "what only that person possesses," such as a key or a magnetic card, or
2) "what only that person knows," such as a PIN (Personal Identification Number) or password.

This means, however, that loss of a card or forgetting a password will result in access being denied to genuine users, and that imposters might gain access either by stealing or forging cards or by guessing or fraudulently obtaining passwords.

Personal identification using biometrics, i.e. on the basis of a person's personal physiological or behavioral characteristics, has come to attract increased attention as a possible solution to these problems, one that might offer reliable systems at reasonable costs[1,2]. While such technology has traditionally been available only on such expensive, high-end systems as those used in law enforcement and other areas of government, personal-level applications have also now become practical thanks to advancements in pattern recognition technology. Biometrics is, in fact, one of the most promising "real" applications of pattern recognition; it has great potential to meet increasing demands for security, most particularly in helping to maintain the integrity of information systems and networked services.

This paper surveys the state of the art in biometrics technology, which has advanced significantly over the last few years. I first describe general principles and key concepts with respect to biometric-based identification, and then outline some of the key features and differences among the wide variety of biometric technologies to be found in the literature and on the market today. As an actual example of mature biometrics, I also present how reliable fingerprint identification systems are built and how they work. Finally, I discuss Fingerprint User Interface, a novel application of fingerprint identification to the facilitation of human-machine interactions.

2. BIOMETRIC TECHNOLOGY: OVERVIEW

With the wide variety of biometric technologies currently available (or soon to be available), it may

*Multimedia Research Laboratories

NEC Research and Development v. 43(1) Jan., 2002

seem difficult to determine just what particular one might best suited for a given security purpose, and no single biometric approach is expected to perfectly meet the needs of all applications in the field. As an initial guideline, we should at least first consider the degree to which measured features are characterized by:

- Universality: What percentage of persons can be expected to have the feature in a measurable form?
- Uniqueness: To what extent can the feature be expected to be distinguishable for any two people?
- Permanence: To what extent can the feature be expected not to vary over time?

Simply stated, a biometrics-based user authentication* system

1) first acquires, using an "input sensor," the biometric data that the user who seeks a service presents,
2) extracts features from the acquired data,
3) compares the extracted features with those of stored data obtained from authorized users in advance, and
4) then decides whether the two sufficiently match.

In this regard, when considering the feasibility of actually implementing a biometric-based authentication system, the criteria to be considered might also include:

- Acceptability: How willing will people be to be measured by the system?
- Collectability: How easy is it to measure the relevant feature(s) quantitatively? How much might obtained values be influenced by changes in the measurement environment (e.g., lighting, etc.)? How costly will the data acquisition be?
- Performance: How much reliability and accuracy of identification can be expected of a system, and what will be the cost of achieving such reliability and accuracy?

Accuracy of identification is usually expressed in terms of the following two criteria:

1) FAR (False Acceptance Rate): the rate at which a system falsely accepts unauthorized users, and
2) FRR (False Rejection Rate): the rate at which a system erroneously rejects the request of an authorized user.

In actual implementation, adjustment of these two rates inevitably involves a trade-off: the lower the FAR, the higher the FRR is likely to be (and vice-versa), and in practical terms, a high FAR is likely to result in insufficient security, while a high FRR is likely to result in significant user dissatisfaction.

3. VARIOUS BIOMETRICS TECHNOLOGIES

Below is a brief introduction to some of the biometric approaches that are either currently in actual use or have recently been proposed for use (not introduced in this section is fingerprint technology, which is described in detail in Section 4).

(1) Iris

The visual texture of the iris, the circular membrane surrounding the pupil on the surface of the eyeball, is known to be unique for each person and invariant throughout life (Fig. 1). Less user cooperation is needed to capture an iris image than to take a fingerprint (i.e., the process is less "intrusive"); the fact that it requires no physical contact with a sensor gives it a high "acceptability" rating. While the error rate in iris identification is extremely low and operations are fast, the requirements for a highly precise, zooming camera and the maintenance of stable lighting conditions make such systems expensive. For that reason, they have tended to be limited mainly to institutional use, in such physical access control applications as, for example, gate control.

Fig. 1 Iris image.

*Strictly speaking, a distinction might be made here between "authentication" and "identification." That is, in "authentication," or "verification," a person gives a user name, presents biometric data, and is then either granted or denied access on the basis of "one-to-one" matching of those two elements. In "identification," on the other hand, a person presents biometric data alone, which is then compared to a set of previously established biometric identities. This is usually referred to as "one-to-many" matching.

(2) Retina

The uniqueness of the retinal vascular pattern, observable on the inside back of the eyeball, has long been known, and this pattern is also stable throughout life. The algorithm required for retinal identification can also be simpler than that for use with irises, in which allowance must be made for the shape changes that result from pupil dilation/contraction. While the reliability of retinal identification is very high, a user has to bring an eye to the sensor device, and a low-level light will be emitted into the eye. This severely lowers general acceptability. Costs for such systems are high, as well, and their use has generally been limited to high-end security applications.

(3) Hand Geometry

Here, a hand scanner captures the overall bone structure of the hand, either in two dimensions (silhouette), or three. Parameters include finger length, width, thickness, curvature and relative location of distinctive features. Although the identification accuracy is not as high as in other systems, it enjoys extremely high "acceptability" and has become popular as an easy-to-use means of physical access control.

(4) Face

Facial features, the most common means by which humans visually identify one another, have high biometric acceptability because they can be captured non-intrusively. Current systems are generally based on one of the following approaches: 1) the transform approach, in which the face image is represented by a set of orthonormal basis vectors, e.g., the "eigenface" approach, 2) the attribute-based approach, in which such facial attributes (landmarks) as the nose and eyes are extracted from the face image and the invariance of the geometric relationships among these attributes is then used for identification, and 3) the 3-dimensional approach, in which a special camera system is used to acquire a 3-dimensinal face structure, including nose height and cheek shape. This permits matching with 2-dimensional face shots taken from different angels. Recent research has made it possible to cope with the effects of changing facial expressions and variations in lighting and angle of view, and there are now various commercial systems in actual use.

(5) Voice

Voice capture is non-intrusive and voiceprints are an acceptable biometric in almost all applications. A further advantage is that identification can be carried out remotely (e.g., by a telephone, etc.). Figure 2 is an example of a voice signal wave. One serious disadvantage here is the fact that verification reliability can be degraded by particular characteristics of a microphone, communication channel, and/or digitizer, as well as by the influence on the voice of a person's current physical condition, stress-level, and/or emotional state. Measures also have to be taken to prevent the use of a recorded voice.

(6) Signature

In contrast to static signature verification, in which only the geometric features of a signature are used, dynamic signature verification additionally employs such features as the acceleration, velocity, and trajectory profiles of pen movement, as sensed by a special pen-tablet device. This makes dynamic signature verification much more reliable, and although its identification accuracy is still not especially high and the potential for forging has not as yet been totally eliminated, dynamic signature identification is easy-to-use, offers high acceptability, and can be economically implemented on pen-type terminals, such as PDAs (Personal Digital Assistants).

(7) Other Biometrics

Examples of other biometrics that appear in the literature include:

- Vein patterns: The reading of the vein pattern on the back of a hand by means of an infrared light and using its tree structure for verification.
- Keystroke dynamics: The use of the patterns created by such features as the rhythm and strength of typing and the inter-key delay times of computer keyboard users.
- Ear shape: Use of the distinctiveness of the ear shape and of the structure of the cartilaginous tissue of the pinna.

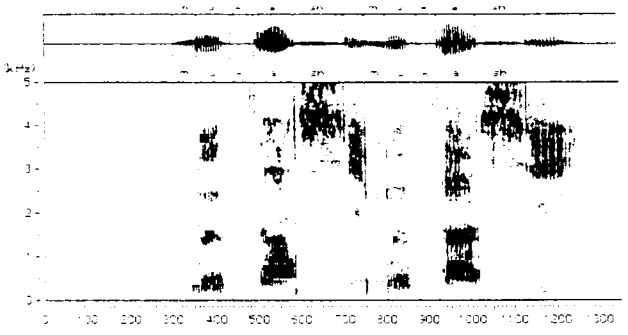

Fig. 2 Voice pattern (spectrogram).

- Gait: The way one walks can be sufficiently characteristic to allow identity authentication.
- Odor: An odor verifier employing an electronic nose can be to identify a user's body odor.

4. FINGERPRINT-BASED PERSONAL IDENTIFICATION TECHNOLOGY

4.1 History and Current Technology

Fingerprints are the most widely used biometric and have the longest history in real-world law enforcement applications. Research into automated fingerprint identification began in the 1960s, and the resulting AFISs (Automated Fingerprint Identification Systems) are 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 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 the following two advantages:

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

4.2 Fingerprint Sensors

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. Optical sensors have long been used as a common 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 sensor) (Fig. 3). The strength of reflectance at any given point on a ridge will vary, depending on its distance off the prism surface. The ridge pattern is then obtained in the form of a gray-level image.

Non-optical, solid-state sensors have also recently appeared on the market. 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 capacitance, temperature, or pressure. Such one-chip sensors offer low-cost implementation of small-area, thin devices.

4.3 Identification Algorithms

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 a registered 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 also less robust against image distortions, which, because the finger is elastic, not rigid, are unavoidable and which represent the biggest hurdle to the successful application of 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. This approach is more robust against fingerprint distortions.

NEC has developed a highly reliable identification algorithm, "Minutia-relation-based Matching," which uses, in addition to distances between minutiae, the number of ridges that cross line segments running between minutiae. Figure 5 shows how this algorithm works[3]. NEC's AFIS, which is equipped with this algorithm, has demonstrated high accuracy and has been used in law enforcement by the National Police

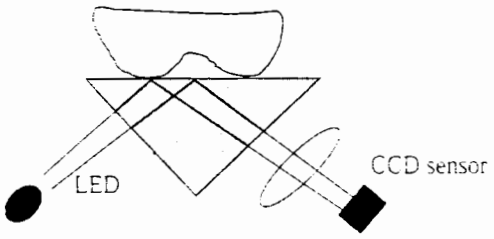

Fig. 3 Optical fingerprint sensor using a prism.

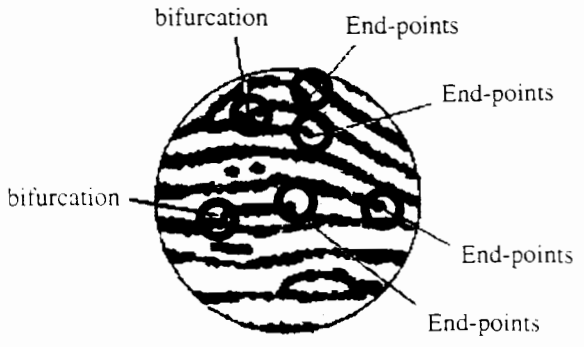

Fig. 4 Ridge structure and minutiae (circled).

Agency of Japan since 1982. It is also used worldwide and has come to have the largest registry database of any AFIS.

When identification is to be made from a huge registry database, as it is in AFISs, a technology called "automated fingerprint classification" is additionally employed to help reduce the number of fingerprints that are candidates for matching[4].

5. FINGERPRINT-BASED AUTHENTICATION SYSTEMS AND APPLICATIONS

5.1 Stand-Alone System

In a fingerprint-based system, an authorized user enrolls his fingerprint in advance, and the fingerprint feature data (also referred to as its "template") is stored. When a user requests a service from the system, he is required to present his fingerprint, and if its features sufficiently resemble the template, he is granted that service.

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.

5.2 Network-Based Identification

Fingerprint identification can also be used with networked services, for log-ins to remote computers, access to remote database servers, and membership-based Web services, including electronic commerce, etc.

In network-based services that use fingerprint user authentication, an authorized user's fingerprint template is typically stored either (1) in the server (as in Fig. 6), or (2) in such a user possession as an IC card (as in Fig. 7).

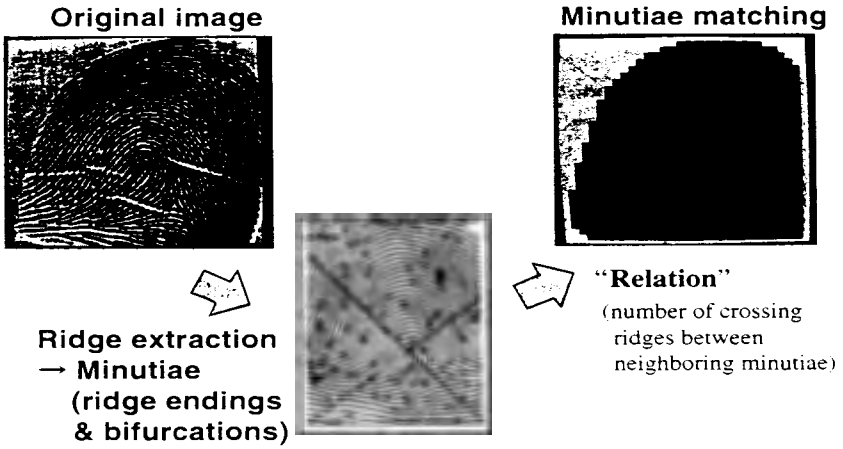

Fig. 5 NEC's minutia-based matching.

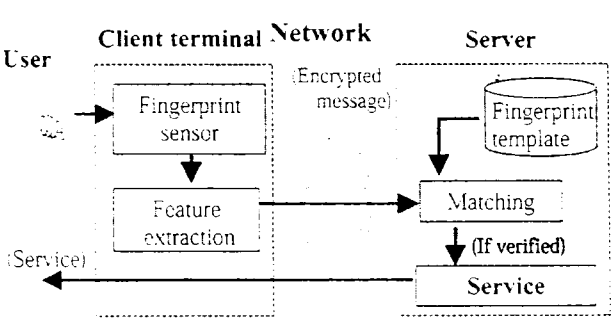

Fig. 6 Server-based authentication.

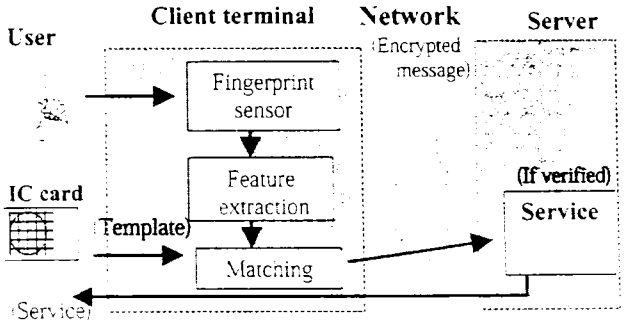

Fig. 7 Authentication using an IC card.

With server storage, fingerprint information obtained from the finger presented at the client terminal is sent via the network to the server for verification against the user's enrolled template. Here, bandwidth considerations make it more sensible to perform feature extraction at the client terminal and send only that extracted data to the server rather than sending full fingerprint image data. With regard to security, the server-storage approach would appear to be reasonable for intranet-based closed systems, but for open-network-based services, users might be likely to feel uneasy about the management and handling of their biometric data at the server and in the open network.

With IC card or other personal-possession storage, verification is conducted at the client terminal. That is, the user presents, for example, both an IC card containing his feature data and his actual finger for verification. When he has been verified at the client terminal as being the proper possessor of that card, the client terminal will send to the server whatever information is required for access authorization (e.g., a simple "verified" message, a secret passcode stored in the card, etc.). This design is especially well-suited, then, to open-networked-based systems, for users can feel safe in knowing that their personal biometric data cannot be accessed from anywhere outside their control.

5.3 Real Examples of Fingerprint-Based Systems

NEC's SecureFinger series (Fig. 8) uses identification software based on the previously mentioned minutia-relation-based algorithm. It provides reliable identification, and not only has its accuracy been proven in AFIS applications, it can be employed in a small, inexpensive micro-computer-based system. Its thin, small-area apparatus is made possible by use of a capacitance-based (as opposed to optical) one-chip sensor. 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.

In addition to identification within the unit, the system can easily be extended to server-based identification by means of the SDK (Software Development Kit) provided for network system integration.

6. A NOVEL APPLICATION OF BIOMETRICS: FINGERPRINT USER INTERFACE

6.1 Concept: Exploiting the Potential of Biometrics

In order for biometrics to be more widely utilized, the technology will have to be willingly accepted not only by those who might be compelled to use it to prove their identities but also by a more general public that are likely to consider, in addition to a system's functionality and performance, its social acceptability, user-friendliness, and general familiarity to them. With this in mind, I have proposed "Fingerprint User Interface" (FpUI), which is based on the fact that fingerprints are different not only person to person but from finger to finger as well[5,6].

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.

Let us consider the situation in which the Fingerprint User Interface is applied to a single-sensor human-machine system. A table is first prepared, describing the relationship between a fingerprint and an FpUI action. This table specifies what action is to

(a) Serial interface type. (b) PCMCIA interface type. (c) Stand-alone module.

Fig. 8 Fingerprint identification unit: SecureFinger.

be taken by the system when a person X presents his N-th finger to a given sensor.

Figure 9 illustrates how FpUI works. When a user touches the sensor with a certain finger, the sensor obtains an image of the fingerprint. Note that the automated image capture mechanism employed must be good enough to obtain a usable image when the user puts his finger on the sensor in a natural manner. 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. Below are some examples of applications that might be expected to expand the use of biometrics technology.

6.2 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. It also facilitates the use of those "blind operations" which may be needed, for example, when a car-driver operates a stereo or when a user needs to operate appliances in the dark.

6.3 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 used, a user might choose among multiple sets of working environments. In addition to static setups, the dynamic status of a pending session can be saved and later restored merely by presenting a fingertip, so that users could continue their work more easily.

Metaphorically, this FpUI represents "saving" a state in each finger, and its significance increases dramatically when used on a small terminal, as opposed to on a computer with a large keyboard. It is also particularly well-suited to digital appliances designed for use by children or elderly people not familiar with conventional user interfaces. For example, when a group of children share a computer game or an electronic picture book at home or at school, each user might make a finger "remember" how far he/she had played or read, and could resume later with just a touch of that finger. Such "fingertip bookmarking" is a good example of the potential user-friendliness of FpUI for non-experts.

It would be particularly useful for users to be able to resume their work at the touch of a fingertip and at any terminal whatever among multiple client terminals connected in a network, and such a networked-FpUI can be implemented simply by customizing the client where the input was made on the basis of the results of fingerprint identification carried out on the server. Figure 10 shows how networked-based FpUI works.

6.4 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 allows a user to browse Web sites merely by changing fingers. Creating documents can also be facilitated by allocating frequently used text segments (such as the user's signature or greetings) to fingers, so as to be able to insert them instantly. By using a "memorize then retrieve"

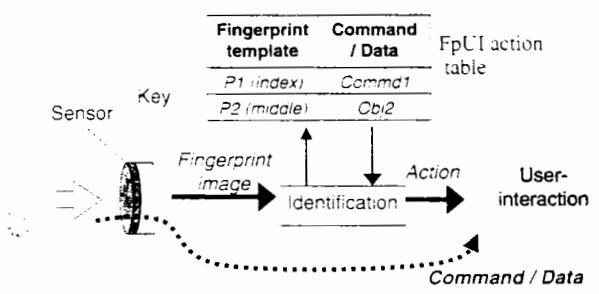

Fig. 9 Fingerprint user interface.

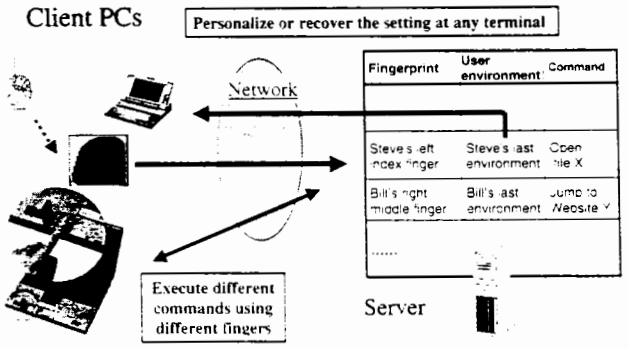

Fig. 10 Network-based FpUI.

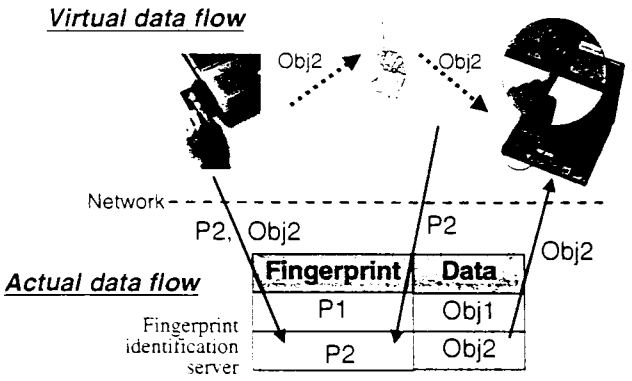

Fig. 11 Implementation of fingertip memo.

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. For example, suppose we were consulting a network information terminal (kiosk) located in a train station or at a convenience store. We could easily "save" onto a fingertip whatever useful piece of information we might find there about "good restaurants" or "films currently being shown" and then "carry" that information home on a finger, to be "retrieved" later at any other terminal connected to the same network. Figure 11 shows how this would appear to a user and how it might actually be implemented.

7. CONCLUSION

As a kind of introductory survey, I have presented here general principles and key concepts related to biometrics, have briefly discussed different biometric approaches, 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 proposed and discussed the enhanced user interface "FpUI," which takes advantage of fingerprint identification technology to broaden the scope of its potential real-world application.

FpUI is expected to be of increasing significance in the future, when ever greater numbers of computer non-experts come to use, on a daily basis, digital appliances and intelligent mobile terminals for such Internet services as net-banking and electronic commerce. I hope this paper might help augment the general user's understanding of biometrics, particularly with respect to its utility, acceptability, and familiarity, and 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] K. Asai, Y. Kato, et al., "Automatic Fingerprint Identification," Proceedings of the Society of Photo-Optical Instrumentation Engineers, **182**, pp.49-56, 1979.
[4] 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, August 1998.
[5] 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.
[6] 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 November 9, 2001

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

Kaoru UCHIDA received his B.E. degree in Mathematical Engineering and Information Physics from the University of Tokyo, Tokyo, Japan, in 1984 and his M.S. degree in Computer Science from Stanford University, California, U.S.A., in 1991. He is currently a Principal Researcher at the Multimedia 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.