The Intelligent Fingerprint Authentication System "SecureFinger"

By Seiichi HIRATSUKA* and Yukio HOSHINO†

ABSTRACT Highly accurate AFIS(Automated Fingerprint Identification System) of NEC was developed in 1982 and many systems have been installed for law enforcement offices in the world. The fingerprint feature extraction and comparison algorithm used in the AFIS were modified and adjusted so as to permit authentication of individual identity. Three kinds of peripheral units, mobile PC-embedded-model, SDK (Software Development Kit) were developed. As the hardware module in the unit and model employs an MPU (Microprocessor Unit) for authentication (image capturing, feature extraction and comparison), each unit and model is an intelligent type which has all functions in one hardware module for fingerprint authentication. This fingerprint authentication system is called "SecureFinger."

KEYWORDS **Biometrics, Fingerprint, Authentication, Identification, Verification, Network security, Access control, Minutia**

1. INTRODUCTION

In the past several years, the drastic development of networks such as the Internet has enabled various virtual societies to be configured on networks. Thus, it is becoming indispensable to have a mechanism of "authentication" (identification and/or verification) to provide users with a confirmation method in order to prove one's identity over the network. Since the traditional method of using a combination of identification number and password easily allows impersonation by someone else, and IC cards are sometimes dropped or stolen, authentications by using biometrics such as fingerprints authentication technology are attracting much attention as a tool for higher security or better usability (Fig. 1). Among various types of biometrics, fingerprint authentication is a leading technology for practical use for several reasons; e.g., requirement of only a small area for image capturing allows the device to be compact, the technology is much more mature compared to other biometrics technologies, etc.

In the history of fingerprint application, many fingerprint scientists have studied minutia (the ending point or bifurcation of ridgeline which composes a fingerprint.)

William Hershel (1833-1917), Henry Faulds (1843-1930) suspected that fingerprints do not change in an individual's lifetime, and that no two fingerprints are exactly the same. Francis Galton (1822-1911) proved that the probability of one fingerprint being equal to another individual's fingerprint is 1 in 64 billion as the result of research on minutia[1]. Accordingly the fingerprint system has been used as the best tool for law enforcement investigations on the basis of these research results.

Minutia information (minutia position and direction) was already utilized by J. H. Wegstien in research on automatic fingerprint identification algorithm[2]. But this was not enough for identifying of strongly distorted and low-quality fingerprint images such as fingerprints detected from the scene of a crime.

Research activity for fingerprint identification algorithm by NEC started in 1971. As research effort a decade later, NEC developed the "Minutia and

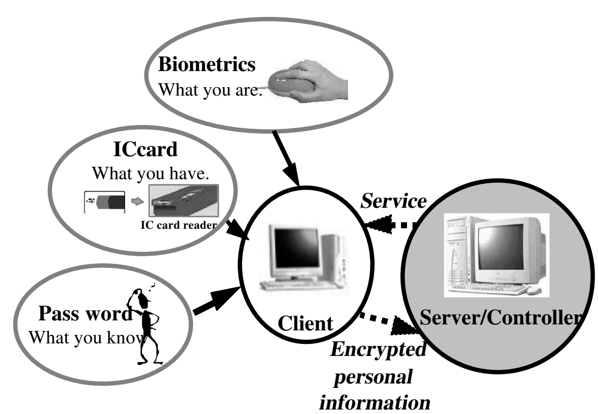


Fig. 1 Biometrics for higher security and better usability.

*Personal ID Systems Sales Division
†NEC Soft, Ltd.

relation method" realizing highly accurate identification[3]. As the highly accurate algorithm was recognized, the technology was first put into a practical system for the National Police Agency of Japan in 1982[4-6]. Since then a large number of contracts for the law enforcement systems were obtained in Japan and abroad. It was reported that NEC has 69% of the total market share in the base of the number of registered fingerprints in the world[7].

2. FINGERPRINT IDENTIFICATION ALGORITHM

The most important idea of the "Minutia and relation method" is "Relation," which means ridge count between minutiae as shown in Fig. 2. The detail algorithm of feature extraction and comparison are described in reference[3]. The minutia and the relation are extracted from the fingerprint image, and comparison of these data with registered data is performed as shown in Fig. 3. This identification method identifies any distorted image.

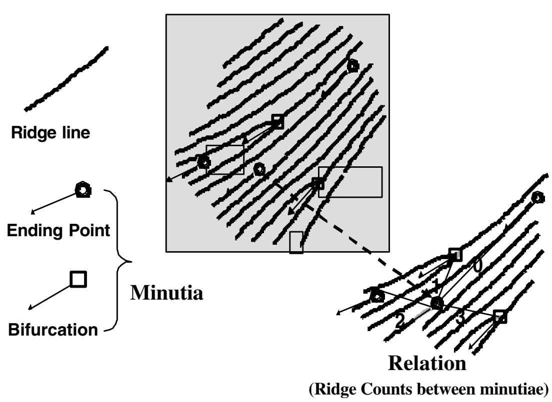


Fig. 2 Ridge line, minutia and relation.

The fingerprint feature extraction and comparison algorithm used in the AFIS(Automated Fingerprint Identification System) were modified and adjusted in order to be suitable for authentication.

In the case of AFIS, inked fingerprint or photographed fingerprint is scanned. But in the case of authentication system, because the surface of a live finger is scanned directly, human-machine interface for capturing fingerprint and processing are different from AFIS.

In the case of AFIS, the fingerprint specialist must confirm the output candidate list from the AFIS. Because there is no such kind of specialist, image quality control and final decision must be done by the system automatically in the case of an authentication system.

3. AUTHENTICATION SYSTEM "SecureFinger"

"SecureFinger" products consist of units, mobile PC-embedded-model, and SDK (Software Development Kit).

3.1 Peripheral Units, Mobile PC-Embedded-Model

An authentication hardware module is included in the unit and the model. It has an MPU (Microprocessor Unit), and has the following advantages.

(1) Multiple Secure Modes

1) Mode 1

It captures fingerprint image, extracts minutia and relation information, and compares the extracted features with prior registered fingerprint features as shown in Fig. 4. When the verification (one to one comparison), or the identification (one to many

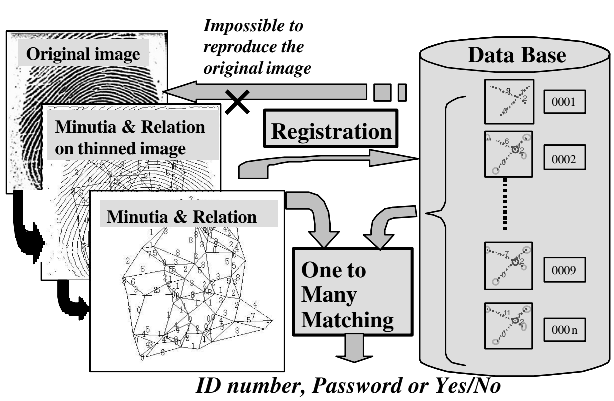


Fig. 3 Feature extraction and matching.

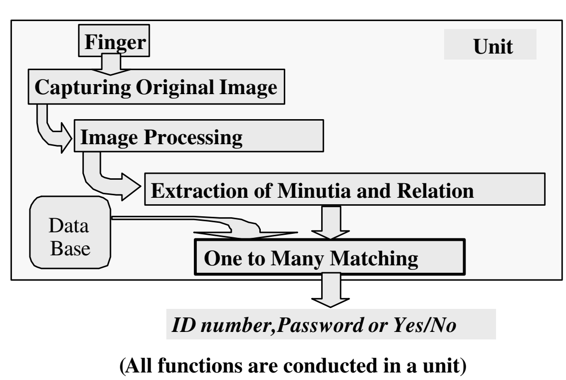


Fig. 4 Intelligent type.

comparison) is utilized, fingerprint authentication can be realized within the unit without sending a fingerprint image or feature (characteristic data) to the network.

2) Mode 2

It captures fingerprint image, extracts minutia and relation information, and encrypts the information within the unit. Encryption function is necessary in order to send minutia data to the client personal computer securely. Decryption of encrypted feature and matching it with registered features are performed in the PC or a server machine.

(2) Intelligent Type

The unit does not release the fingerprint image data to the network for fingerprint authentication. This module is called the "Intelligent Type." It is not a "Non-Intelligent Type." (In the case of "Non-Intelligent Type," the unit has no feature extraction capability. It sends the scanned fingerprint image to the PC. The PC conducts feature extraction and matching of the extracted feature with the registered fingerprint feature as shown in Fig. 5.)

(3) Multiple Scanner Type

There are "optical type" and "semiconductor type" sensors. Whereas the "optical type" can be characterized as having a wider capturing area, the "semiconductor type" can be characterized for its small and slim shape. There is one "optical unit" and there are two "semiconductor type" units.

Fingerprint scanning resolution is 500dpi. In the case of scanning area, the semiconductor type is 15 × 15mm, and the optical type is 19.2 × 19.2mm.

(4) Fingerprint Registration in Module

Registered fingerprint feature is about 400 ~ 500 bytes per fingerprint. The maximum number of registered fingerprints in a module is 200 fingerprints. There is no limitation within PC or server. It depends on memory size.

(5) Powerful Basic Utility

If a PC with the unit or a mobile PC embedded model has basic utility functions,

1) "BIOS LOCK (pre-boot security check) (only with NEC PC)"
2) "OS logon"
3) "Unlocking of screen saver"
4) "Replacing Password"

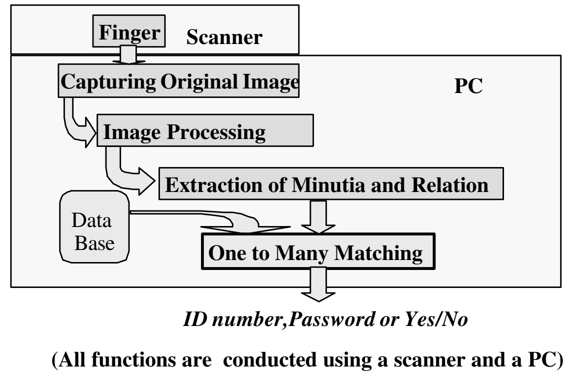


Fig. 5 Non-intelligent type.

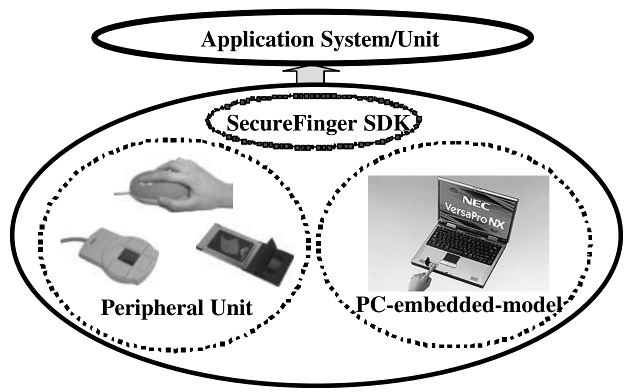


Fig. 6 "SecureFinger" products.

are provided.

3.2 SDK (Software Development Kit)

The "SecureFinger" SDK was developed for implementation of the "SecureFinger" for any kind of user's application system (Fig. 6).

4. APPLICATION SYSTEM

The module can be embedded in various types of specific application equipment such as IC card reader, POS, ATM, door control panel, time & attendance unit, etc. NEC has developed the "FingerThrough" for door control system and "FingerRecorder" for a time & attendance system.

5. CONCLUSION

Both NEC's "optical type" and "semiconductor type" sensors have a resolution of 500dpi. Other vendors, sensors are generally less than 400dpi. NEC's sensor is superior to almost all of other vendors' sensors. This, together with the superiority in image processing technology, allows the system to maintain a high rate of registration. However, if in the future the scope of fingerprint authentication application spreads widely in the consumer market, various aspects will have to be taken into consideration. For example, the system may be used to capture children's fingerprints. In order to meet this purpose, it may require development of a sensor that can support capturing of children's thin ridgelines. Also, development of sensors that can cope with a wider scope of application may be considered necessary.

ACKNOWLEDGMENTS

The authors would like to express their thanks Mr. Sanshirou KUSUNOSE, Senior Manager of NEC Solutions, 1st Solutions Sales Operation Unit, Personal ID Systems Sales Department and Ms. Rei SUWATA of Assistant Manager of NEC Solutions, 1st Solutions Sales Operation Unit, Personal ID Systems Sales Department for their valuable advice in preparing this document.

REFERENCES

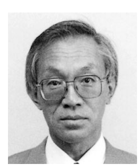
[1] E. Keogh, "An Overview of the Science of Fingerprints," Anil Aggrawal's Internet Journal of Forensic Medicine and Toxicology, 2001, **2**, 1, January - June 2001; http://anil299.tripod.com/vol_002_no_001/papers/paper005.html; Published January 8, 2001.
[2] J. H. Wegstein, "An Automatic Fingerprint Identification System," NBS Special Publication 500-89, Feb. 1982.
[3] K. Asai, Y. Kato, et al., "Automatic Fingerprint Identification," Proc. Society of Photo-Optical Instrumentation Engineers, **182**, pp.49-56, 1979.
[4] Kazuo Kiji, Yukio Hoshino and Koh Asai, "Automated Fingerprint Identification System," NEC Res. & Develop., 96, pp.143-146, March 1990.
[5] Masatada Seto and Yukio Hoshino, "Computer Technologies for Fingerprint Identification," Institute of Image Electronics Engineers of Japan, **15**, 3, pp.184-191, 1986.
[6] Misao Kawashima and Yukio Hoshino, "Automatic Reading and Matching Method for Fingerprint Identification," International Fingerprint Conference, London, 27-30 Nov. 1984,(in Japanese).
[7] J. L. Peterson, "The Status of AFIS systems worldwide" Issues of Organization, Performance and Impact, Presented at the International Symposium on Fingerprint Detection and Identification, Ne'urim, Israel, June 1995.

Received October 22, 2001

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

Seiichi HIRATSUKA received his bachelor's degree in electrical engineering from the faculty of engineering, Hiroshima University in 1971. He joined NEC Corporation in 1971 and is now a system manager of NEC Solutions, 1st Solutions Sales Operation Unit, Personal ID Systems Sales Division. He has been engaged in the research and development of fingerprint identification systems, palmprint identification systems and fingerprint authentication systems since then.

Mr. Hiratsuka is a member of the Japan Division of the International Association of Investigation.



Yukio HOSHINO received his bachelor's degree in mathematics from Hokkaido University in 1961. He joined NEC Corporation in 1961 and is now a corporate chief engineer of NEC Soft, Ltd. He was engaged in the research and development of optical character reader and fingerprint identification system at the NEC central research laboratory from the same year. He was transferred to NEC Soft, Ltd. through NEC Security Systems, Ltd. and the government systems division of NEC. He has been engaged in the development of fingerprint identification/authentication systems since 1982.

Mr. Hoshino won the Japan Society for the Promotion of Machine Industry prize in 1978. He is a member of the Japan Division of the International Association of Investigation.

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