Door-access-control System Based on Finger-vein Authentication

OVERVIEW: Door-access control is a physical security system that assures the security of a room or building by means of limiting the access to that room or building to specific people and by keeping records of such accesses. It utilizes an individual-authentication method in order to limit access to specific people. The most widespread authentication method for such systems is based on smart cards. Such a system limits room access to only those people who hold an allocated smart card. However, in the case of smart-card systems, on top of the difficulty in preventing another person from attaining and using a legitimate person's card, there is the inconvenience of processing lost cards. In the meantime, accompanying the continuing development of fingerprints as the main biometrics method for individual authentication, the practical application of door-access-control systems utilizing biometric data has begun. Biometrics authentication uses information specific to a person's body in order to assure a high level of security that makes it difficult for a stranger to impersonate that person. Although there are several types of biometrics authentication methods, the one — called finger-vein authentication — presented here is the most suitable method for controlling door access by a large number of people. This paper describes the features of the developed finger-vein-authentication method and presents two applications of this authentication method to door-access control.

INTRODUCTION

BIOMETRICS methods used for personal authentication utilize such features as the face, the voice, the hand shape, the fingerprints, and the iris. Each method has particular characteristics and can be categorized in terms of usability and security as shown in Fig. 1.

The main parameters for assessing usability can be summed up as follows:
(1) simplicity for the user
(2) feeling of resistance
(3) speed of authentication
(4) level of false-rejection rate

And the main parameters for assessing security can be summed up as follows:
(1) difficulty of acquiring biological data
(2) difficulty of forgery
(3) level of false-acceptance rate

Voice authentication is easy to use: if you are asked, "Who are you?," and you answer, "It's me," the door opens and lets you in. There is not a more convenient system than that. However, vocal data can easily be stolen by means of audio technology and forgeries can be made. Face authentication faces a similar problem. That is, it is not impossible for a stranger to pass off their face as another's by means of donning disguises

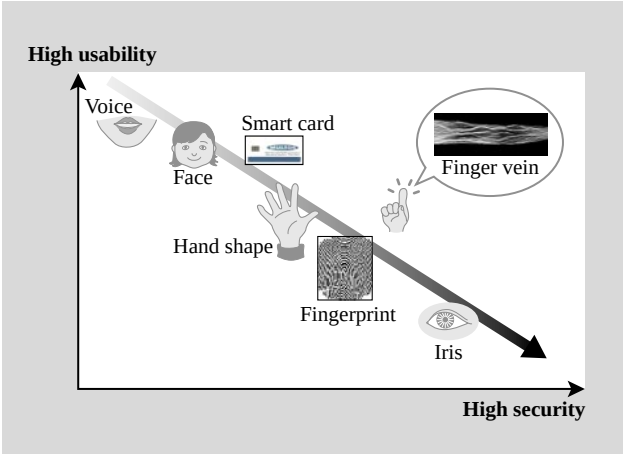

Fig. 1—Comparison of Various Biometrics Methods. Each biometric method can be categorized in terms of usability and security.

Fig. 2—Fingerprint Sensor.
Fingerprint sensor can be used to replace a password for a personal computer.

or holding up a legitimate person's photo. Face and voice authentications are thus only effective methods in an environment in which an attendant or guard is present to ensure that fraud is impossible.

Fingerprint authentication is a reliable method widely acknowledged across society. When a person places their finger on a special semiconductor pad (i.e. a fingerprint sensor), their fingerprint is extracted and its image is analyzed. The analysis result is then checked against that person's previously registered fingerprint for authentication. Being easy to operate by means of a compact device (see Fig. 2), this method is widely used as a replacement for PC passwords.

Although fingerprint authentication is useful for individual applications like PC access, applying it to door-access control faces several problems from the viewpoint of usability. For example, pressing the whole fingerprint up against a sensor gives an uncomfortable feeling, and the sensor gets dirty, thus decreasing the authentication success ratio. In addition, fingerprint systems have a negative image associated with crime.

Iris authentication uses image processing to authenticate an image of the iris taken by a camera. Though this method is said to provide high security, it is inconvenient from the viewpoint that aligning the eye with the camera takes time.

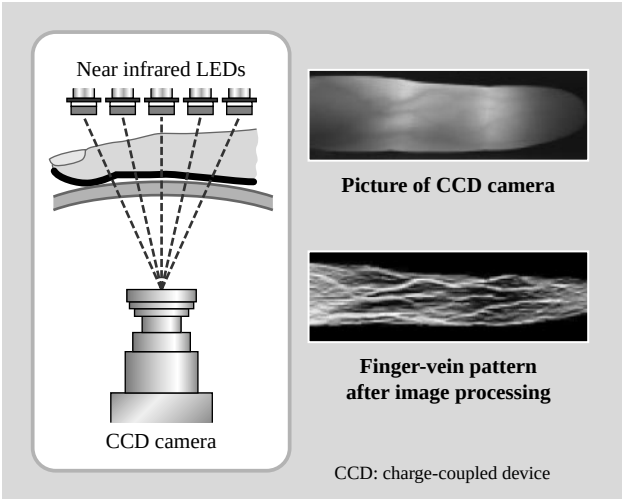

Fig. 3—Theory of Finger-vein Authentication.
Near-infrared rays form a vein pattern on a CCD camera.

Fig. 4—Finger-vein Scanner.
The finger-vein scanner detects the finger-vein pattern and sends it to the controller.

The newly developed method presented in this paper — called finger-vein authentication — utilizes the vein pattern inside a person's finger for authenticating that person. Since the above-mentioned methods achieve authentication by utilizing information from the "external" body (i.e. face, fingerprints, iris, etc.), it is not difficult for another person to acquire that information. On the other hand, information from the "internal" body, such as the vein pattern inside a finger, cannot be acquired so easily. Likewise, internal-body information cannot be forged easily.

FINGER-VEIN AUTHENTICATION

The basic principle on which the finger-vein-authentication system is based is shown in Fig. 3. Near-infrared rays generated from a bank of LEDs (light emitting diodes) penetrate the finger and are absorbed by the hemoglobin in the blood. The areas in which the rays are absorbed (i.e. veins) thus appear as dark areas in an image taken by a CCD camera located on the opposite side of the finger. Image processing can then construct a finger-vein pattern from the camera image. This pattern is then compressed and digitized so that it can be registered as a template of a person's biometric authentication data.

The finger-vein pattern and the template can be authenticated by means of a pattern-matching technique. The device developed to perform the above-described detection process (finger-vein pattern scanner) is shown in Fig. 4.

The part of the finger-vein scanner on the right

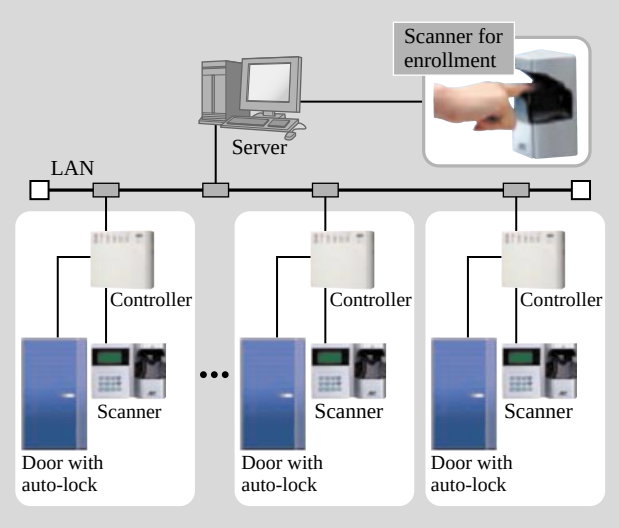

Fig. 5—Configuration of Door-access System.
All personal data required for opening doors are downloaded to the specified controller by the server.

contains the LEDs (mounted above) and the CCD camera (mounted below). The authentication system is configured so that a person just stands in front of the door of the room they want to enter, inserts a finger into the scanner located by the door, and thereby pushes a switch set at the back of the scanner with their fingertip. On doing so, an image of the finger-vein pattern is captured and authenticated. This configuration is easy to use from an ergonomic viewpoint since door-access control is performed while the person is standing.

The authentication algorithm is burnt into a microcomputer housed in a controller separated from the scanner.

The main features of the finger-vein-authentication scanner are summarized as follows:

(1) Internal biometric information makes forgery difficult.

(2) The scanner is a non-contact type and different from existing systems, i.e., the images are taken using LEDs (light emitting diodes) and a CCD. And there is a switch set at the back of the scanner that is pushed with the fingertips; thus, there is no need to touch the censor surface directly and it is hygienic.

(3) Microcomputerized authentication device ensures fast image scanning and short authentication time, so high-speed authentication allows door-opening commands to be issued promptly.

(4) Advanced authentication algorithm assures high level of security.

DOOR-ACCESS SYSTEM

An example adaptation of the finger-vein-authentication system, namely, door-access control, is shown in Fig. 5. A controller is located at each door and houses a microcomputer system — which recalls and individuals' biometric information stored in a database and executes the authentication algorithm — as well as a control device connected to an automatic door lock and a LAN. A finger-vein scanner is fixed to the wall next to the door of each room, and the finger-vein-pattern image data is sent to the controller via a USB (universal serial bus) connection. Ordinarily, as shown in the set up in Fig. 5, a scanner is located next to each door (with one controller) in order to control room access. However, the system can be set up not only for controlling room access but also for controlling room leaving by placing another scanner inside each room. In that case, the controller for each door controls the two scanners.

Each controller supports a LAN connection. That is, the authentication status and open/closed information for each door are relayed in real-time to a server. And since the controller can store data on a maximum of 1,000 access events, even if the server or LAN connection is down, door-access control can still be continued to operate. Furthermore, a finger-vein scanner for enrolling individuals' biometric information, which is downloaded to each controller, can be connected directly to the server.

Implementation Example 1

Fig. 6 shows an example of the door-access-control system implemented at a major software house. To ensure rigorous control of the security of each client's data, each door of the software-design room is fitted with a full-time automatic lock. As shown in the figure, to enter the room, a person must put his/her finger in the scanner to receive the authentication that automatically unlocks the door. The access of the authenticated person is then reported to the server, and a record of his/her door access is made. As a result of introducing this system, security of the software house's business has been dramatically improved. Moreover, as can be clearly seen in the photograph, the compact design of the scanner is neat and simple.

Implementation Example 2

Another example of an implementation of the door-access-control system is in a 37-floor office building in Singapore. The building accommodates several

Fig. 6—Door-access Control for Computer Software House. Personal authentication is required to enter the design room.

Fig. 7—Finger-vein-authentication System for Office Building. About 1,500 persons are enrolled in this system.

different companies, and the system controls security by using smart cards formatted differently for each company.

For providing security for the whole building, three guards are permanently deployed in the elevator hall on the ground floor to confirm the identities of the people entering the building. To improve the security of the whole building, and reduce the burden on the security guards at the same time, a "finger-vein-authentication gate" was installed in the elevator hall. Though this gate system performs authentication by means of smart cards, it eliminates the burden of having to carry two cards (one for access to a person's company and one for building access) and provides a high level of security by biometric authentication. A total of six gates were installed and control the coming and going of about 1,500 people occupying the building.

An authentication scanner is mounted at the entrance of each gate, and a person inputs his personal identification number into the numeric keypad on the left of the finger scanner. His finger-vein information is then authenticated by the controller incorporated in the gate. On authentication of that person, the gate opens and the server is informed of the access via the LAN connection. In that way, the server can keep a full-time record of that person's comings and goings. Fig. 7 shows a scene of the finger-vein-authentication gates in operation.

Fig. 8 shows a finger-vein scanner on an entrance gate.

Fig. 8—Gate Equipped with Finger-vein Scanner. The entrance gate is fitted with an authentication scanner.

CONCLUSIONS

A door-access-control system that utilizes finger-vein patterns was developed. This is a biometric authentication technology for controlling door access in a convenient way by applying the high level of security provided by finger-vein patterns. Biometrics has started to be applied for civilian-identification purposes like passport inspection. We consider that finger-vein patterns can take a leading role in such applications; accordingly, we will strive to push forward commercialization and development of this product to make finger-vein-pattern authentication more convenient.