Finger Vein Authentication: White Paper

Abstract

Finger vein authentication is a new biometric method utilizing the vein patterns inside one's fingers for personal identity verification. Vein patterns are different for each finger and for each person; and as they are hidden underneath the skin's surface, forgery is extremely difficult. These unique aspects of finger vein pattern recognition set it apart from previous forms of biometrics and have led to its adoption by the major Japanese financial institutions as their newest security technology. This white paper discusses the origins, features, technology, applications and future development of finger vein authentication.

1. History: R&D to Commercialization

Originally, the motivation to develop finger vein pattern recognition technology was born of Hitachi's advanced research to measure brain-function activity in the field of medical science. In that research, near-infrared light was used to observe the increase in blood flow and was found to be applicable to recognition of the finger vein pattern. As finger vein patterns differ for each finger and for each person, Hitachi thus discovered that finger vein pattern recognition is a viable biometric personal authentication technology for the commercial market.

In the first phase (1997-2000), Hitachi developed its original light transmission technology for finger vein biometric authentication. As opposed to light reflection, whereby a captured image is taken from light reflected off the surface of the skin, light transmission captures a vein pattern image from light that passes through the surface of the skin (see Section 4 for details). In the second phase (2000-2003), the technology was adapted into product form, and the first physical access control system was developed and released in 2002. In 2002 research began on the logical access systems, with commercialization in Japan beginning in 2004. Hitachi developed ATM applications in 2004 and commercialized them in 2005. Finger vein authentication technology has thrived in the Japanese financial sector, with major banks in Japan employing it for ATM end-user verification.

2. Summary of Authentication Process

The basic principle on which the finger vein authentication system is based is shown in Fig. 2. 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 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 are then authenticated by means of a pattern-matching technique. Devices were developed by Hitachi to perform the detection process described above.

3. Features and Comparison

Finger vein authentication technology has several important features that set it apart from other forms of biometrics as a highly secure and convenient means of personal authentication.

(1) Resistant to criminal tampering: Because veins are hidden inside the body, there is little risk of forgery or theft.

(2) High accuracy: The authentication accuracy is less than 0.01% for the FRR (False Rejection Rate), less than 0.0001% for the FAR (False Acceptance Rate), and 0% for the FTE (Failure To Enroll).

(3) Unique and constant: Finger vein patterns are different even among identical twins and remain constant through the adult years.

(4) Contactless: The use of near-infrared light allows for non-invasive, contactless imaging that ensures both convenience and cleanliness for the user experience.

(5) Ease of feature extraction: Finger vein patterns are relatively stable and clearly captured, enabling the use of low-resolution cameras to take vein images for small-size, simple data image processing.

(6) Fast authentication speed: One-to-one authentication takes less than one second. Moreover, the authentication device can be compact due to the small size of fingers.

Finger vein authentication thus offers several key advantages compared to other forms of biometrics. These comparative advantages are collectively shown in Table 1.

Table 1 Comparison of Major Biometrics Methods

BIOMETRICS	SECURITY		CONVENIENCE				
	Anti-Forgery	Accuracy	Speed	Enrollment Rates	Resistance	Cost	Size
Fingerprint	×	○	○	×	×	◎	◎
Iris	○	◎	○	○	×	×	×
Face	○	×	○	○	◎	×	×
Voice	○	×	○	○	◎	○	○
Vein Pattern	◎	◎	◎	○	○	○	○

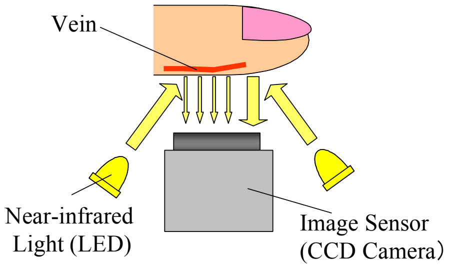


Fig. 1 Light Reflection Method

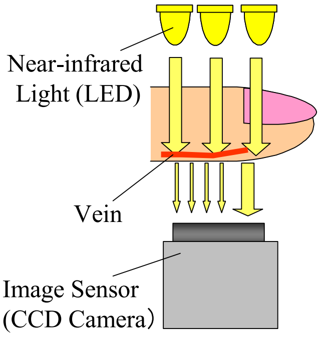
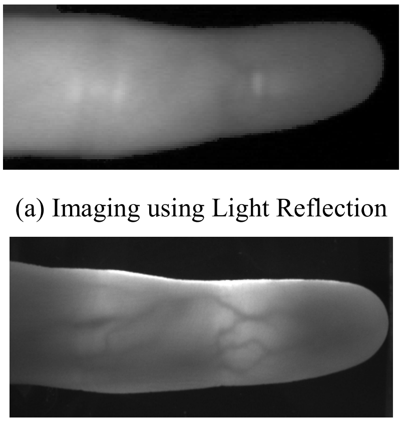


Fig. 2 Light Transmission Method



(a) Imaging using Light Reflection

(b) Imaging using Light Transmission

Fig. 3 Comparison of Lighting Methods

◎: good, ○: normal, ×: insufficient

For example, fingerprinting is known for being widely applicable due to the small size of its readers, yet because the fingerprint is a trait found on the exterior of the body, it is not only easily stolen but also has issues with low user enrollment rates, as worn away or sweaty fingerprints cannot be registered. Iris recognition is known for low error rates of authentication, but some users feel psychological resistance to the direct application of light into their eyes. Moreover, as precise positioning of the eyes is required for accurate iris authentication, it becomes necessary either to adopt high-cost position adjustment mechanisms or to place the burden of proficiency onto the user. As for face and voice recognition, they are the means by which humans recognize one another in everyday social interaction and are thus the most natural forms of personal identification; yet impersonation is easily performed, and accuracy rates for these are limited.

4. Finger Vein Pattern Imaging

Vein patterns, invisible to the naked eye, can be viewed through an image sensor sensitive to near-infrared light (wavelengths between 700 and 1000 nanometers). Near-infrared light passes through the tissues of the human body and is blocked by pigments such as hemoglobin or melanin. As hemoglobin exists densely in blood vessels, near-infrared light shining through causes the veins to appear as dark shadow lines in the captured image.

There are two methods used for capturing vein pattern images: “light refection” (Fig. 1) and “light transmission” (Fig. 2). In the case of “light reflection,” the light source and the image sensor are placed on the same side of the finger, and the image sensor captures the reflected light from the surface of the finger. In the case of “light transmission,” the finger is placed between the image sensor and the light source, and the near-infrared light passes through the finger where it is captured by the image sensor.

In the case of the light reflection method, the vein pattern image is formed by minute differences in the intensity of the reflected light. Since the veins absorb the light, the image shows feeble light from the veins and bright light from the other parts of the blood vessels. (Fig.3 (a) depicts an image taken by the reflection method.) The light reflection method offers some advantages for the design of the device. The light source and the image sensor can be packed together so that the device can be more compact. The surface of the device looks open for the user, and there is no obstacle between the user and the device. Today, there are some biometrics systems using vein patterns in the palm or the back of the hand, all of which employ the light reflection method. However, the strong reflection from the skin’s surface and the shallow penetration of light under the skin causes the image contrast to be weak. In addition, the roughness and furrows on the skin’s surface are part of the captured image and interfere with detection of vein patterns. By contrast, the light transmission method delivers a high-contrast vein pattern image, because light is introduced from the opposite side of the finger, and there is no effect of reflection. (Fig.3 (b) shows an image taken by the light transmission method.) In this method, since the light must pass through the human body, only certain body parts with the appropriate thickness or volume can be used for this type of authentication. The finger, however, is suitable.

Although this method delivers high accuracy of authentication, the finger has to be placed between the light source and the image sensor, causing the device to be relatively large and sometimes causing discomfort to the user.

As such, Hitachi has developed a new method called 'side lighting' which combines advantages from both of the conventional methods. In this new method, light sources are placed on both sides of the finger as shown in Fig. 4. Near-infrared light shines through the sides of the finger and scatters inside the finger, then passing through the other side of the finger and detected by the image sensor to capture the vein pattern image. This new method enables high-contrast imaging as well as easy placement of the finger on an open, ceiling-less device.

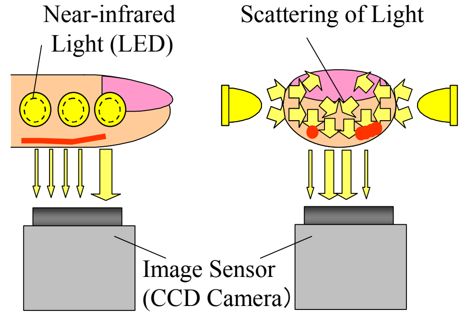
As discussed above, the near-infrared light source and the image sensor are essential technologies for finger vein pattern imaging. In particular, the performance of the image sensor has a strong effect on authentication accuracy. As shown in Fig. 3, finger vein pattern images are relatively coarse and large compared with fingerprint or iris images, thus requiring only QVGA resolution; however, for this the image sensor has to be highly sensitive and low-noise in the wavelength range of the near-infrared light source. In addition, due to variations in finger size, the brightness of the light source must adapt accordingly and the image sensor must be as responsive to changes in brightness as that of a video image sensor so as to ensure the most accurate image. As applications expand to include outdoor use, the ability of the device to function in a broader range of environments with varying brightness, temperature and humidity will soon become an important issue.

5. Finger Vein Authentication Process

Fig. 5 shows a block diagram of the complete finger vein authentication system. The system consists of an authentication unit and other related devices in addition to the near-infrared light source and the image sensor. The authentication unit includes a CPU core for all sorts of signal processing, video I/O for capturing data from the image sensor, LED power controller, and I/O controller. The authentication outcome flows through the I/O controller. Security applications such as door locking are activated by the signal from the controller. The system executes four tasks:

(1) Capturing of finger vein pattern image,
(2) Normalization of the image,
(3) Feature pattern extraction from the image, and
(4) Pattern matching followed by judgment of outcome.

In Task (1), the system takes an image of the finger vein pattern through the image sensor and transfers the image data to the memory of the CPU. At this point, the CPU adjusts the brightness of the light source through the LED power controller to eliminate error caused by individual variations or environmental fluctuations.



(a) Side View (b) Front View

Task (2) normalizes the finger vein image to accommodate geometric changes in the positioning or angle of the finger used for authentication. In practical terms, the outline of the finger in the image is detected and then the entire image is rotated so that the slope of the outline remains constant.

In Task (3), the distinctive feature patterns are extracted from the image. This process is essential for reliable authentication so as to control the variation of image data caused by body metabolism or changes in imaging conditions. In particular, uneven brightness due to individual variations in finger size or lighting conditions often appears in the vein pattern image, so the system must extract only the vein patterns from such an otherwise unstable image. (Fig. 6 shows variations in brightness across a single vein in a vein pattern image, where veins clearly appear as dark lines. The shape of the variation forms a 'valley'.)

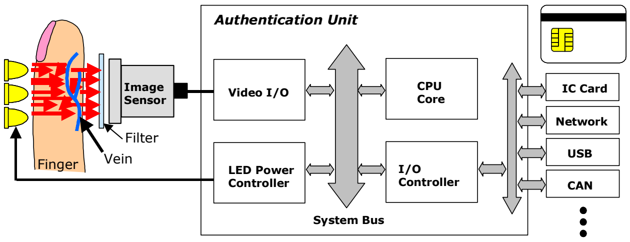
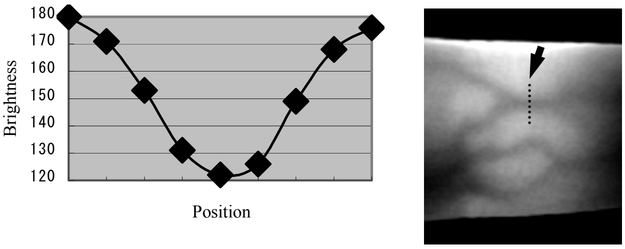


Fig. 5 Block Diagram of Finger Vein Authentication

Task (4) calculates the correlation between the extracted feature pattern and the registered pattern in a database – the "matching" process. If the correlation value is higher than a pre-defined threshold value, the vein pattern is authenticated.

The vein pattern image and the extracted feature pattern represent ultimate personal information. Therefore, strict administration of that information is required when it is stored or transferred. In addition to encryption of the data, tamper resistance is necessary for the device against unauthorized access to the system. A smart card, which



(a) Cross-sectional Profile (b) Location of Profile

Fig. 6 Cross-sectional Profile of Finger Vein Image

includes high–level tamper resistance, has already been introduced to store the feature pattern. The internal program execution function of the smart card has been used to execute all or a part of the pattern matching process so that no personal information leaks out from the card. The authentication accuracy of the system is less than 0.01% for FRR (False Rejection Rate), and less than 0.0001% for FAR (False Acceptance Rate). These accuracy figures are superior to those of other methods based on fingerprint or iris recognition.

6. Applications and Future Plans

Since the first sale in 2003, finger vein products have been successfully adopted by major corporations in the fields of financial, physical and logical security in Japan and other parts of Asia (see Fig. 7). In Japan, finger vein products have enjoyed great success in the financial sector, where 70% of major financial institutions have adopted finger vein technology as a biometrics solution that ensures privacy by storing templates securely on a smart card rather than in a database. Physical security systems (standalone or connected by server and used with a smartcard, PIN code or by itself) have also sold widely in Asia, and particularly in Singapore, where well-known buildings such as IBM Singapore, Mizuho Bank, the Caltex Tower, and the Hitachi Tower have adopted finger vein technology for biometric entry access. Logical security products in the form of a USB-connected mouse-sized device have sold widely in Japan and throughout Asia to major companies like Aeon Credit Service as well as various government agencies and information management companies.

In the future, besides embedded applications for portable IT devices such as cellular phones, finger vein authentication will take full advantage of its unique use of the finger to expand into applications such as opening automobile doors with a simple grip of the handle, for which the necessary grip-type authentication technology is already in development. Grip-type technology embeds personal authentication in the natural motion of opening a door, ensuring the highest security without forcing the user to learn complicated new procedures. This technology will be applicable to home, office or car doors and will usher in a secure future without keys.

Supporting this expansion of finger vein authentication applications is the miniaturization of this technology. The very first prototype was as large as over one liter in volume, while the newest embedded module in mobile PCs has shrunk to 19 cc. Miniaturization enables finger vein authentication technology to be embedded in a greater variety of devices and is thus the driving force behind the expansion of finger vein authentication applications.

One of the principal mechanisms behind miniaturization of finger vein authentication technology is the miniaturization of the image sensor. With the popularization of camera phones, small yet highly sensitive image sensors have become widely accessible. Moreover, the performance capabilities of the latest one-chip microcomputers have become advanced enough to easily execute complicated image processing tasks such as feature pattern extraction without the inclusion of specialized circuits. Hereafter, for even smaller and even higher security, for encryption of data transmission and data memory, for strengthening resistance to data tampering, semiconductor technologies will be of great importance in the future of finger vein authentication technology.

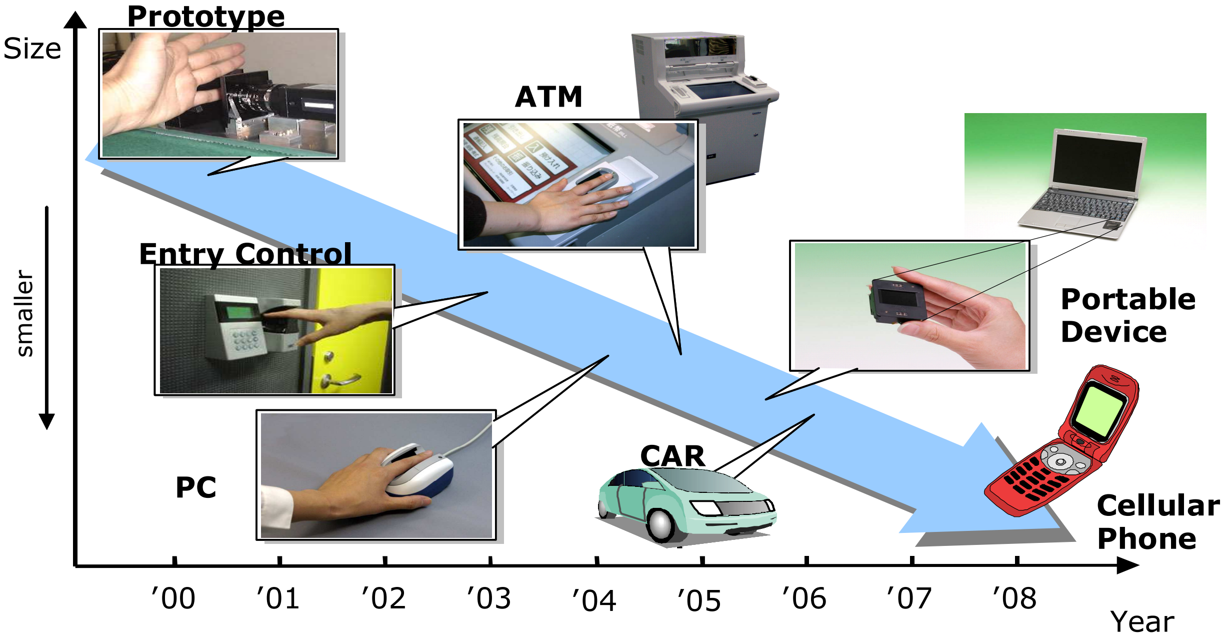


Fig.7 Applications of finger vein authentication and future developments