Finger Vein Authentication Technology and its Future

Junichi Hashimoto
Information & Telecommunication Systems Group, Hitachi, Ltd.
Kawasaki, Kanagawa, Japan

Abstract

In this paper, finger vein authentication, a new biometric method utilizing the vein patterns inside one's fingers for personal identification, is introduced. 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 paper discusses the technology and applications of finger vein authentication, as well as the importance of semiconductor devices in its future development.

1. Introduction

With our progress toward a globalized, ubiquitous information society, the average person's life has at the same time become threatened by heinous occurrences that can originate anywhere in the world. Horrors can spread throughout the globe in an instant, heightening and intensifying risk. As a result, there has developed a sudden and intense need for personal authentication systems that can prevent spoofing and other criminal impersonation in such areas as financial (cash or credit card) withdrawals, passport and driver's license identification, entry into important facilities, apartment complexes or offices, access to IT equipment, and a broad range of other applications. As such, biometrics systems, which are highly accurate and use a part of one's body, have become the ideal answer to these heightened security needs and are already being adopted worldwide. According to forecasts by the International Biometrics Group (IBG), the world biometrics market is expected to reach US$5.7 billion by 2010 (Fig.1). Among biometrics, fingerprint and iris were first to be applied, but recently finger vein authentication has been a focus of popular attention and has already been adopted by Japan's major financial institutions. In the following, we will discuss the unique aspects and practical applications of finger vein authentication technology, as well as the importance of semiconductor technologies in these developments.

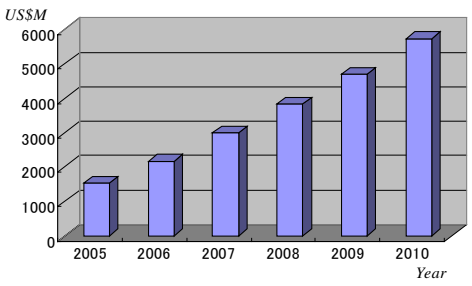


Fig.1 World Biometric Market Size (Source: IBG)

2. Comparing with Other Biometrics Methods

Finger vein authentication is a biometrics technology based on the criss-crossing vein patterns underneath the skin's surface that are unique to each finger and each person. The three main advantages of finger vein authentication are the following:

(1) As veins are hidden inside the body, there is little risk of forgery or theft, and the surface conditions of the hands have no effect on authentication.
(2) The use of infrared light allows for non-invasive, contactless imaging that ensures both convenience and cleanliness for the user experience.
(3) Vein patterns are stable and clearly defined, allowing the use of low-resolution cameras to capture vein images for small-size, simple data image processing.

Finger vein authentication thus offers considerably more advantages compared to other forms of biometrics. These comparative advantages are collectively shown in Table 1. For example, fingerprinting is known for being widely applicable due to the small size of its devices, 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 due to the fact that certain people's fingerprints are worn away or sweaty and 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 done and accuracy rates for these are limited. Meanwhile, finger vein pattern recognition offers high accuracy personal authentication that is at the same time difficult to forge, non-invasive, and easy to use, offering a balance of advantages that makes it superior as a form of biometric identification. Moreover, finger vein patterns are different even among identical twins and remain constant through the adult years.

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	◎	◎	◎	○	○	○	○

: good, : normal, : insufficient

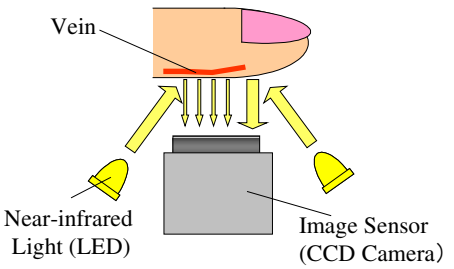


Fig.2 Light Reflection Method

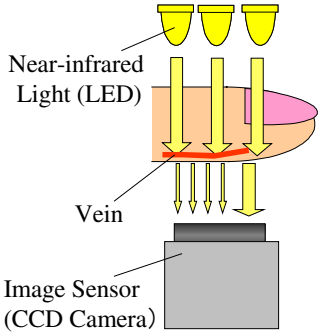
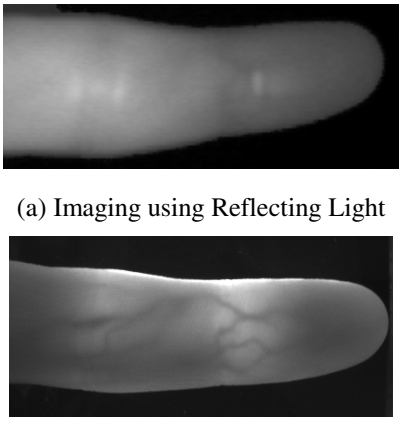


Fig.3 Light Transmission Method



(a) Imaging using Reflecting Light

(b) Imaging using Transmitting Light

Fig.4 Comparison of Lighting Methods

3. Finger Vein Patten Imaging

As mentioned, vein patterns cannot be observed using normal, visible rays of light since they are beneath the skin's surface. However, vein patterns can be viewed through an image sensor which is sensitive to near-infrared light (wavelengths between 700 and 1000 nanometers), because near-infrared light passes through human body tissues and are 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 near-infrared image. (Arteries usually do not appear in the image because they are deep inside the finger and cannot be detected by the image sensor, since finger tissue scatters the light in the deep part of the finger).

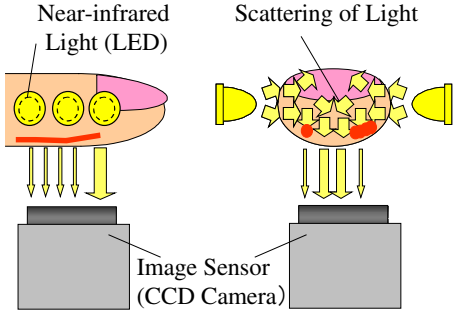
There are two methods used for to capture vein pattern images: "light refection" (Fig. 2) and "light transmission" (Fig. 3). In the case of "light reflection," the light source and the image sensor are placed on the same side of the finger, and the reflected light from the surface of finger is captured by the image sensor. 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.

With 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.4 (a) shows 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 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, this method requires a high-level image processing technique, because the contrast between the vein part and the other parts is usually subtle(the strong reflection from the skin's surface and the shallow penetration of light under the skin makes the contrast very small). In addition, the roughness and furrows on the skin's surface are obstructive to the detection of vein patterns.

On the other hand, 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.4 (b) shows the image taken by the light transmission method.) In this method, since the light must pass through the human body, the body parts with the appropriate thickness or volume to be used for this type of authentication is limited. The finger, however, meets the requirements. 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 users discomfort.

As such, we have 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.5. 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 gives high contrast of the image as well as easy placement of finger with the open structure of upper side of the 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. 4, finger vein pattern images are relatively thick and large compared with fingerprint or iris images, thus requiring only QVGA resolution. However, the image



(a) Side View (b) Front View

Fig.5 Side Lighting Method

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 increase, it will become necessary for the device to be used outdoors. As such, 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.

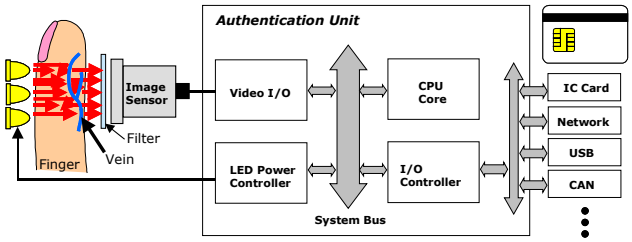


Fig.6 Block Diagram of Finger Vein Authentication

4. System Architecture for Finger Vein Authentication

Fig. 6 shows a block diagram of our total 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 is outputted through the I/O controller. Security applications such as door locking is 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 appropriately controls the brightness of the light source through the LED power controller to eliminate error caused by individual variations or environmental fluctuations.

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 is to be constant.

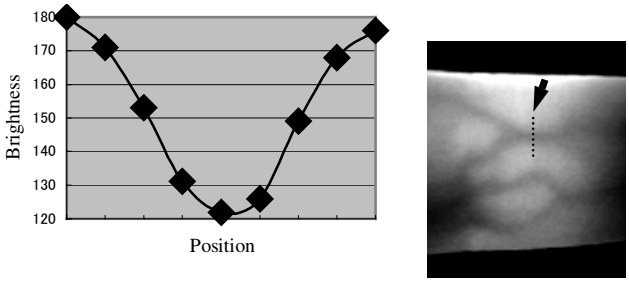
In Task (3), the distinctive feature patterns are extracted from the image [1][2]. This process is essential for reliable authentication while controlling the variation of image data caused by body metabolism or changes in imaging conditions. In particular, unevenness of brightness due to individual 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.

To extract line-shaped subjects like vein patterns, several image processing methods have been proposed thus far. For example, image filtering technique such as matched filter and morphological image analysis, or image tracking technique based on connectivity of edges. Both the matched filter and the morphological method simply emphasize the entire image using globally uniform parameters. Therefore, if unevenness of brightness appears locally in the image, the emphasized image also reflects on the local unevenness and makes the extracted lines to be disconnected. In addition, speckle noise may be unnecessarily emphasized since line connectivity is not considered in these methods. The image tracking method has capability of extracting the line-shaped features smoothly utilizing connectivity of edges. However, this method requires a large amount of computation for edge extraction and judgments of connectivity between edges.

Figure 7 shows variations in brightness across a single vein in a vein pattern image. It shows clearly that the veins appear as dark lines which were less bright than that of the surrounding area. The shape of the variation forms a 'valley'. Though the depth of the valley may vary from place to place caused by the unevenness of brightness, the valley-formed variation itself is common with the vein parts in the image. Accordingly, detecting such characteristic variation of brightness in the entire image, a robust feature extraction against the unevenness of brightness can be achieved. Since this method does not include time-consuming filtering, such as noise reduction or connection of separated lines, a high-speed authentication can be realized on a standard CPU architecture.

In Task (4), a correlation between the extracted feature pattern and the registered pattern in a database is calculated. If the correlation value is higher than a pre-defined threshold value, the input vein pattern is authenticated. The vein pattern image and the extracted feature pattern are ultimate personal information. Therefore, strict administration of that information is required when they are 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 has high–level tamper resistance, has already introduced to store the feature pattern. The internal program execution function of the smart card has already been utilized to execute all or a part of the pattern matching process so that no personal information is leaked out from the card.

The authentication accuracy of the system is less than



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

Fig.7 Cross-sectional Profile of Finger Vein Image

0.01% in FRR (False Rejection Rate), and less than 0.00002% in FAR (False Acceptance Rate). This level is much more superior to those of other methods based on fingerprint or iris.

5. Future Plans and the Importance of VLSI Devices

Currently, the applications of finger vein authentication are steadily increasing. As shown in Fig. 8, while at first applications included only door access control, they soon expanded to include personal computer login and has even begun to be adopted by financial institutions for banking applications such as personal identification at automatic teller machines (ATMs). 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 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 future without keys that nevertheless allows one to protect personal property with the utmost security.

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 prevention against data tampering, semiconductor technologies will be of great importance in the future of finger vein authentication technology.

6. Conclusion

In this paper we have discussed the unique characteristics of finger vein authentication technology as well as its future development. As society becomes more information-oriented and more globalized, the importance of security technologies in a variety of sectors will continue to grow steadily. The advantages of finger vein authentication in accuracy and ease of use depends considerably on microcomputers, image sensors and other such semiconductor devices, and thus there is great hope placed in the advancement of semiconductor technologies.

References

[1] N.Miura, et al., “Automatic Feature Extraction from Non-Uniform Finger Vein Image and its Application to Personal Identification,” IAPR MVA 2002 7-4 p. 252-256 (2002)

[2] N.Miura, et al., “Extraction of Finger Vein Patterns Using Maximum Curvature Points in Image Profiles,” IAPR MVA 2005 8-30 p. 347-350 (2005)

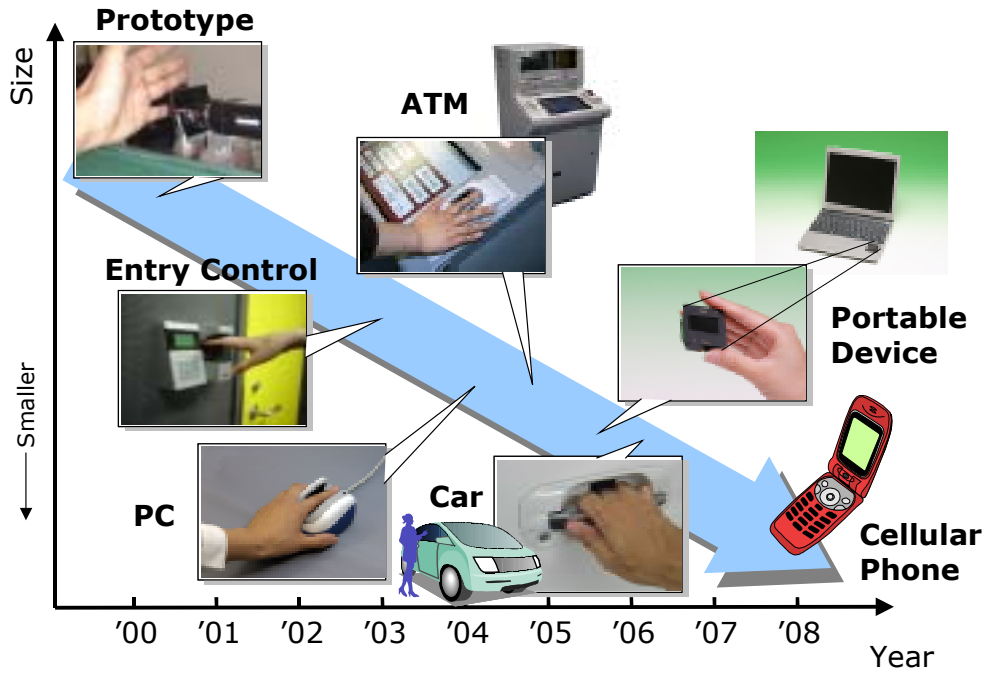


Fig.8 Applications of finger vein authentication and future developments