Finger Vein Authentication Technique – A Fast and Highly Secure Approach for Customer Authentication

Executive Summary

With an ever-increasing number of enterprise data security breaches, the pressure on corporations to implement methods of password management, identity management, data and network security, and two-factor authentication has never been stronger.

The sharing or theft of user passwords still remains the most frequent way that corporate data is compromised[1].

Developed by Hitachi, finger vein authentication verifies a person's identity based on the lattice work of minute blood vessels under the skin. In Japan, thousands of cash machines are operated by finger vein technology. Hitachi announced that it will introduce 20,000 finger vein authentication systems at shops and kiosks, which will use the devices to protect the privacy of customer information by requiring store workers to authenticate themselves before accessing the customer database.

This white paper explains finger vein authentication technology and discusses different aspects of customer security associated with it.

Finger Vein Authentication

The principle behind the finger vein authentication technique is as follows:

The pattern of blood vessels is captured by transmitting near-infrared light at different angles through the finger, usually the middle finger. This can be done in a small instrument attached to a wall or as part of an ATM machine. The light is partially absorbed by hemoglobin in the veins and the pattern is captured by a camera as a unique 3-D finger vein profile. This is turned into a simple digital code which is then matched with a pre-registered profile to verify an individual's identity. Even twins are said to have different finger vein patterns! Because the veins are inside the body, invisible to the eye, it is extremely difficult to forge and impossible to manipulate, Hitachi claims.

The gruesome possibility that criminals may hack off a finger has already been discounted by Hitachi's scientists. Authentication cannot be forged with a severed finger, as the blood would flow out of a disconnected finger, making authentication impossible. Hitachi says finger vein authentication is less expensive than iris scanning or face/voice recognition and that the false rejection rate is much lower than with

Anatomy of Finger Vein Imaging

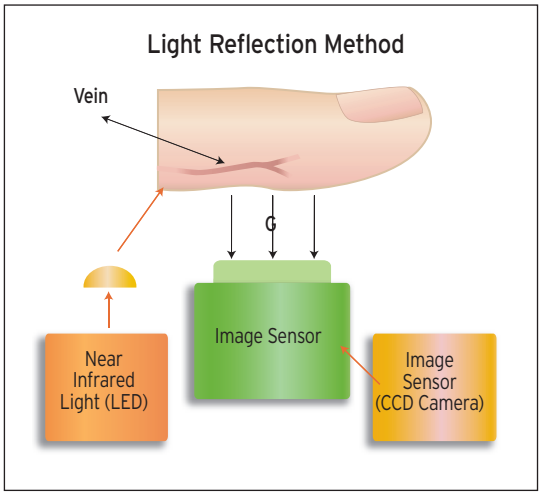

Figure 1

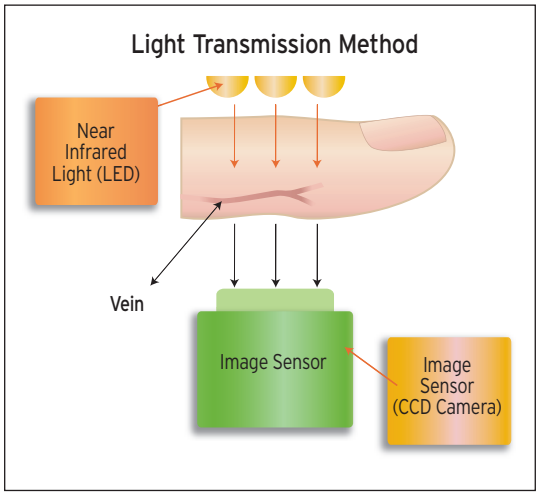

Figure 2

fingerprinting. And people don't have to remember a pin number. Hitachi's system is being used in Japan to verify user identities for ATMs, door access systems and computer log-in systems.

Summary of Authentication Process

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.

Features

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.

- **Resistant to criminal tampering:** Because veins are hidden inside the body, there is little risk of forgery or theft.
- **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).
- **Unique and constant:** Finger vein patterns are different even among identical twins and remain constant through the adult years.
- **Contactless:** The use of near-infrared light allows for non-invasive, contactless imaging that ensures both convenience and cleanliness for the user experience.
- **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.
- **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 the fingers.

Finger Vein Pattern Imaging

There are two methods used for capturing vein pattern images: "light refection" (see Figure 1) and "light transmission" (see Figure 2). In the case of "light reflection," the light source and

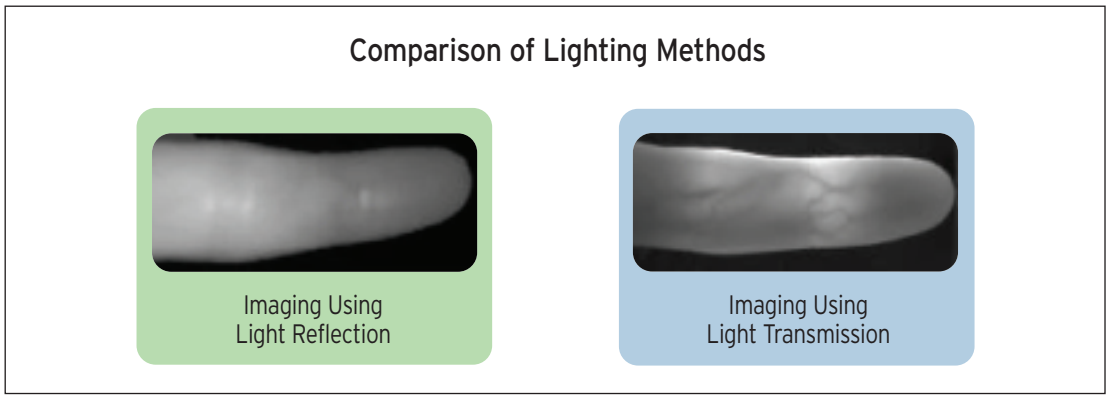

Figure 3

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.

Figure 3 (above) shows the imaging comparison between light reflection and light transmission methods.

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 Figure 4 (below). 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.

Finger Vein Authentication Process

Figure 5 (next page) 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

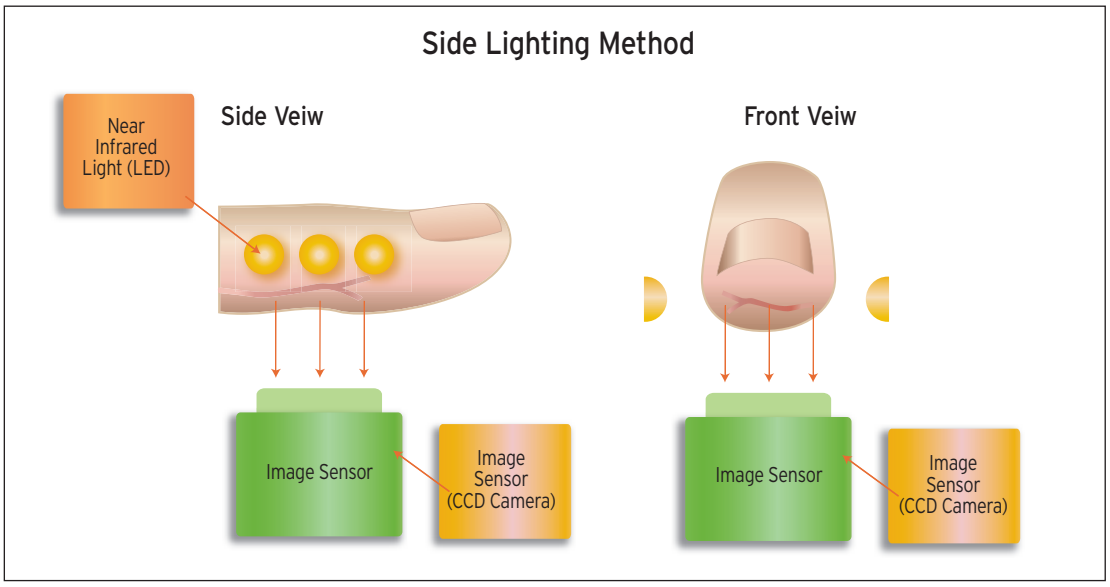

Figure 4

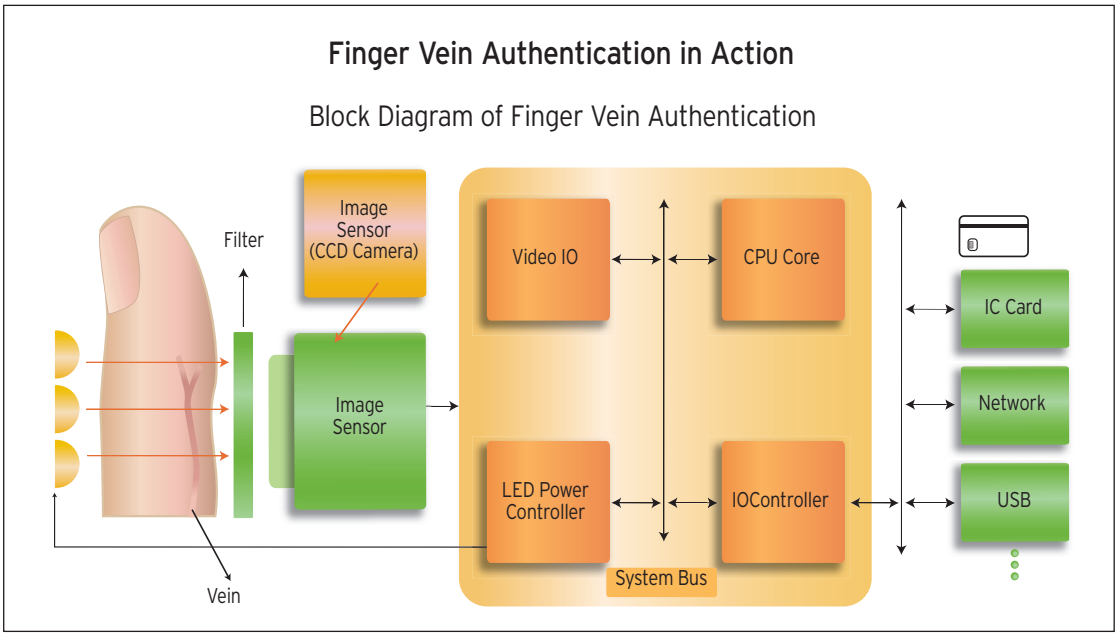

Figure 5

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

(4) Pattern matching followed by judgment of outcome

Conclusion

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. In Japan, finger vein products have enjoyed great success in the financial sector[2]. 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.

Beyond embedded applications for portable IT devices such as cellular phones, finger vein authentication will in the future likely 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.

The expansion of finger vein authentication applications is the miniaturization of this technology. 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.

Using the highly secure authentication principle of finger vein authentication, corporate and banking Institutions can ensure customer identity and data security and minimize data security breaches and cyber crimes taking place at enterprises worldwide.

Footnotes

[1] Hitachi Omron – Finger Vein Authentication Technology
The biometric method known as "Finger Vein Authentication" (introduced widely by Japanese banks few years ago), is claimed to be the fastest and most secure biometric method.

[2] 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.

About the Author

Dhananjay Sakhalkar is a consultant within the Cognizant Business Consulting, Wholesale Banking group. His areas of expertise include Payments & Cash Management, Financial Messaging, and Business Lending. Dhananjay has more than 12 years of experience in the areas of business consulting, application development, requirements gathering, project management, and is a PMP certified professional. He can be reached at Dhananjay.sakhalkar@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services. Cognizant's single-minded passion is to dedicate our global technology and innovation know-how, our industry expertise and worldwide resources to working together with clients to make their businesses stronger. With over 50 global delivery centers and more than 68,000 employees as of September 30, 2009, we combine a unique onsite/offshore delivery model infused by a distinct culture of customer satisfaction. A member of the NASDAQ-100 Index and S&P 500 Index, Cognizant is a Forbes Global 2000 company and a member of the Fortune 1000 and is ranked among the top information technology companies in BusinessWeek's Hot Growth and Top 50 Performers listings.

Start Today

For more information on how to drive your business results with Cognizant, contact us at inquiry@cognizant.com or visit our website at www.cognizant.com.

Cognizant
Passion for building stronger businesses

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
Haymarket House
28-29 Haymarket
London SW1Y 4SP UK
Phone: +44 (0) 20 7321 4888
Fax: +44 (0) 20 7321 4890
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com