Technology and Future Prospects for Finger Vein Authentication Using Visible-light Cameras

With electronic transactions and mobile payments using mobile devices having entered widespread use in recent years, markets for these services are expanding rapidly. Unfortunately, this is also accompanied by increasing losses from fraudulent use, creating a need for some way of ensuring the security of mobile devices. While biometric authentication based on user characteristics such as faces or fingerprints is being tried, the difficulties with using such techniques on mobile devices include poor identification accuracy and the need for special sensors. Hitachi, meanwhile, has developed a technique for highly accurate finger vein authentication using the visible-light cameras typically built into mobile devices. Using this technique together with encryption techniques that Hitachi has built up in previous work will make it possible to deploy identity verification solutions in a wide range of fields such as banking and retail.

Naoto Miura, Ph.D.
Keiichiro Nakazaki
Masakazu Fujio, Ph.D.
Kenta Takahashi, Ph.D.

1. Introduction

Mobile devices such as smartphones and tablets have become commonplace around the world and are widely used for purposes such as online shopping payments and Internet banking transactions. The number of mobile payment users who utilize their devices as a form of electronic money is also rapidly increasing. The total value of the market for mobile payments in the USA, which totaled 112 billion dollars in 2016, is expected to triple by 2021[(1)].

Unfortunately, incidents of loss due to identity theft are on the rise, with total FY2015 losses in Japan due to unauthorized use of Internet banking totaling 1.26 billion yen for individuals alone, for example[(2)]. This makes ensuring the security of mobile devices a crucial challenge, creating the need for a way of determining personal identity to verify that the person using a device is in fact its owner.

Personal identification numbers and passwords have been widely used in the past for verifying identity on mobile devices. The problems with these methods, however, include the inconvenience of having to enter them and the risk of their being stolen or forgotten. While this has led to the use in recent years of identity verification methods based on biological characteristics such as faces or fingerprints, the challenge with biometric identification techniques developed for use on mobile devices is that they have been unsuited for widespread use in diverse situations, suffering from poor identification accuracy and the need for special sensors.

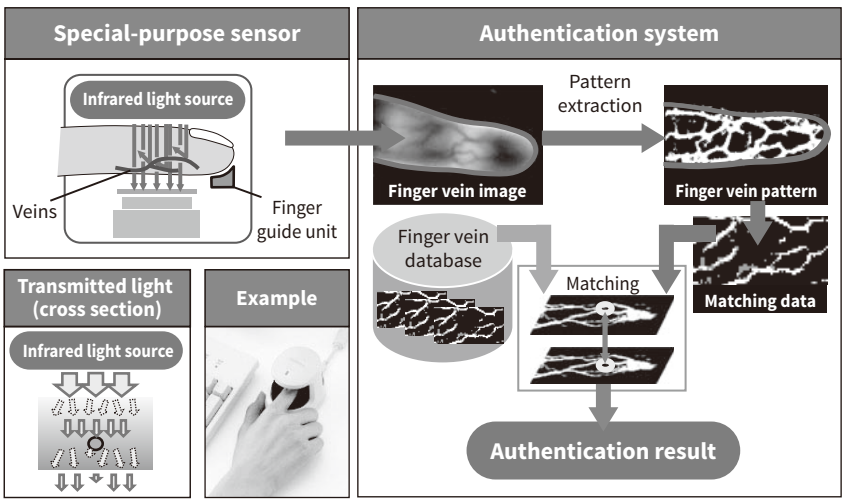


Figure 1 — Overview of Finger Vein Authentication Technology

Finger vein authentication is a method for verifying personal identity based on the unique patterns of veins in each person's fingers. Because the veins run through the interior of the finger, the patterns are extracted by shining infrared light through the fingers and using a special-purpose sensor to capture their image. This use of transmitted light provides a high level of authentication accuracy because it can image the veins inside fingers.

In response, Hitachi has developed a highly accurate finger vein authentication technology that uses the visible-light camera typically built into mobile devices. Whereas past finger vein authentication has used a special-purpose infrared sensor to capture finger vein images, this new technology can perform biometric identification using finger vein images taken with a general-purpose camera.

This article describes the technology used to perform finger vein authentication using a visible-light camera, and its potential for use in identity verification solutions.

2. Finger Vein Authentication Technology

2. 1
Current Technology Using Special-purpose Sensor

Figure 1 shows an overview of the current finger vein authentication technology, which uses a special-purpose sensor. The user places their finger on a finger guide unit where it is exposed to light from an infrared light source. The infrared light that passes through the finger is captured by an infrared camera, providing a transparent image of the finger. As the veins under the skin of the fingertip are opaque to infrared light, they appear as a pattern of dark lines in this image. Compared to using reflected light, the benefits of acquiring images using transmitted light are that it can show veins that are located deeper into the finger, and with greater contrast.

The image acquired using transmitted light is passed to a processing system that compensates for variations in how the finger is presented to the scanner by identifying the finger silhouette and correcting the image (by rotation or enlargement). Next, a feature extraction algorithm[3] is used to reliably separate the pattern of finger veins from other image elements. Finally, the extracted pattern is compared with data in a database of finger vein patterns and the identity of the user is verified if a match is found. This identification is then used in applications such as personal computer (PC) login or payment processing.

2. 2
Finger Vein Authentication Using Visible-light Camera

The technology shown in **Figure 1** is used in a wide variety of situations, including desktop applications such as PC login or attendance management, and embedded system applications such as bank automated teller machines (ATMs) or access control systems. Unfortunately, the size and cost of the hardware makes the technology impractical for mobile devices. Accordingly, Hitachi has developed a finger vein authentication technology that uses the visible-light cameras typically built into mobile devices. This section describes the technology itself as well as the technical challenges that had to be overcome during its development.

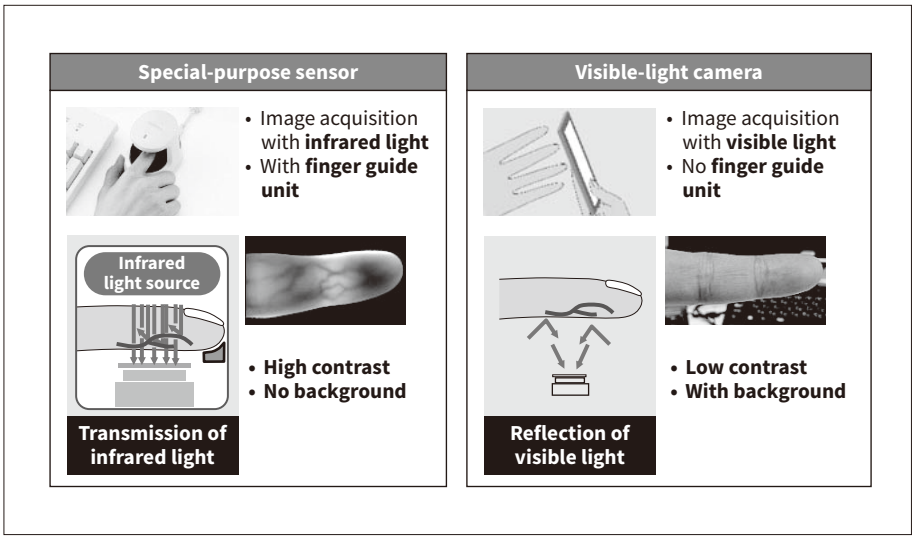


Figure 2 — Differences between Imaging by Special-purpose Sensor and Visible-light Camera

The use of infrared light by the special-purpose sensor means it can capture images of veins deep inside the finger while also using a purpose-designed finger guide unit to hold the finger in place. A general-purpose visible-light camera, in contrast, needs to extract the vein patterns from a visible-light image using reflected rather than transmitted light. Finger identification is also made more difficult by the presence of extraneous background details and by there being nothing to constrain how the fingers are oriented relative to the camera. This means that using visible-light cameras requires more sophisticated authentication techniques than in the past.

2. 2. 1 Technical Challenges

Figure 2 shows the differences between finger vein imaging using a special-purpose sensor and using a visible-light camera. As noted above, use of a special-purpose sensor achieves high identification accuracy not only by capturing high-contrast finger vein images from infrared light transmitted through the finger, but also by taking advantage of the way the finger is inserted into the scanner and fixed into position, which minimizes both the variation in finger orientation and the level of extraneous light from the surroundings.

In contrast, when a smartphone or other general-purpose camera is used to obtain finger vein images, it is unable to capture infrared light and instead takes a color image of the finger using ambient light. Furthermore, the lack of a finger support means that the image must be taken of the finger held over the camera, creating uncertainty about finger location and allowing extraneous light from sources other than the finger to be included in the image. In other words, authentication must be performed under conditions likely to be detrimental to identification accuracy compared to the previous method.

Accordingly, the three technical challenges that needed to be overcome to make finger vein authentication possible using a visible-light camera were the ability to identify the finger vein patterns reliably without using infrared light, to do so regardless of how the finger is oriented over the camera, and to improve the level of authentication accuracy to enable use in diverse applications.

2. 2. 2 Proposed Techniques

Figure 3 shows an overview of finger vein authentication technology using a visible-light camera. The user starts by holding multiple fingers over a camera that captures a color image. The background is eliminated and the finger silhouettes identified to determine the locations of the fingers in the image. This is then used as a basis for deciding whether the image is adequate for the purpose. If so, the image is split into a separate image for each finger by using the finger silhouettes to adjust the orientation of each finger image. The finger vein patterns for each finger are obtained and the final authentication result is determined by checking the patterns for multiple fingers.

The three elemental techniques proposed for this purpose are as follows (see **Figure 3**).

(1) Eliminate background and correct finger positions based on color and shape

(2) Extract finger vein patterns from color information

(3) Verify authentication result based on multiple fingers

In relation to the technical challenges described above, technique (1) makes it possible to perform authentication regardless of how the fingers are oriented over the camera, technique (2) obtains finger vein patterns without using infrared light, and technique (3) improves authentication accuracy.

(1) Eliminate background and correct finger positions based on color and shape

Given that all sorts of different objects could appear in the background of finger images, two important

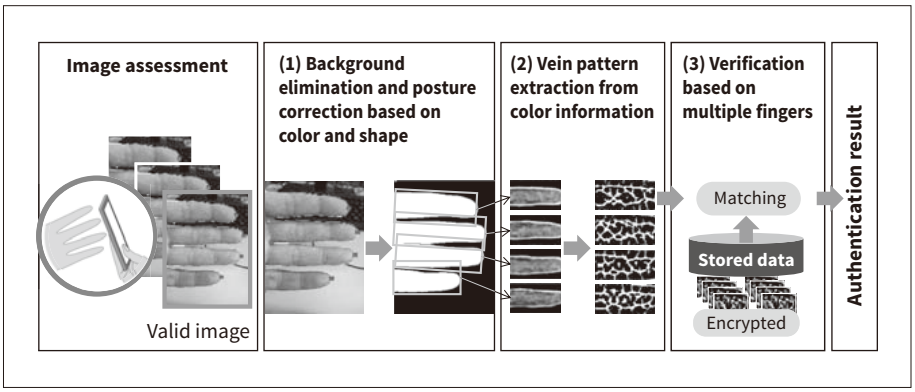


Figure 3 — Overview of Finger Vein Authentication Technology Using Visible-light Cameras

Hitachi's technology for performing finger vein authentication using a visible-light camera is made easier to use by providing a guide function to instruct the user how to place their hand over the camera and by incorporating a technique for correcting finger orientation in the acquired image. Similarly, a high level of authentication accuracy is achieved by using a new image recognition technique that can reliably extract the finger vein patterns from multiple fingers in a visible-light image.

functions required for accurate authentication are a way to eliminate background elements to prevent them from interfering with the accurate detection of fingers, and a way to standardize finger position to ensure that the finger images all have the same size and orientation.

The method developed for separating the fingers from the image background does so based on features that have the color and shape of fingers, using machine learning and statistical techniques. The method for standardizing finger position then uses the finger-only images so obtained, resizing and rotating them so that they all have the same size and orientation.

(2) Extract finger vein patterns from color information

As the color finger images include a lot more than just veins, it is important for accurate authentication that the vein patterns can be obtained accurately without being influenced by this other image content.

The pattern extraction technique devised to achieve this works by highlighting colors that are characteristic of veins, taking advantage of the fact that veins show up slightly bluer than average under near-white ambient light similar to that from fluorescent lighting. The finger vein pattern (information that represents only the pattern of the veins) is then extracted from this highlighted image.

This makes it possible to obtain the finger vein patterns using a visible-light camera, without the need for a special-purpose sensor.

(3) Verify authentication result based on multiple fingers

Because the technique captures an image of multiple fingers at the same time, authentication accuracy can be improved by using multiple fingers, without any added inconvenience for the user.

As up to four fingers can be identified from the image of a hand held over the camera, all of the finger vein patterns extracted from the image can be checked against the stored data. In this case, the two patterns that have the highest degree of match with the stored data are used as the basis for authentication. In other words, if two or more of the four fingers match the stored patterns, the identification is verified.

Performing authentication this way means that, even if one of the fingers is covered by a bandage, for example, and so cannot be used, identification is still possible using the remaining fingers. Authentication is thereby enhanced by taking advantage of the redundancy provided by being able to capture images of multiple fingers at the same time.

Accuracy testing conducted using approximately 100 people found that it was adequate for practical use, with a false negative rate of about 0.1% given a one-in-one-million chance of a false positive. Hitachi intends to conduct further testing of the system under a variety of conditions to improve accuracy in practical use.

3. Secure Biometric Authentication over Open Networks

Enabling finger vein authentication using a visible-light camera makes the method suitable for use on a variety of devices, including smartphones and tablets, or web cameras. Once a user has recorded their finger vein data and personal information, from a location such as their home, for example, it then becomes possible to provide them with a universal personal identity verification service that can be used in a variety of authentication applications. However, such open use

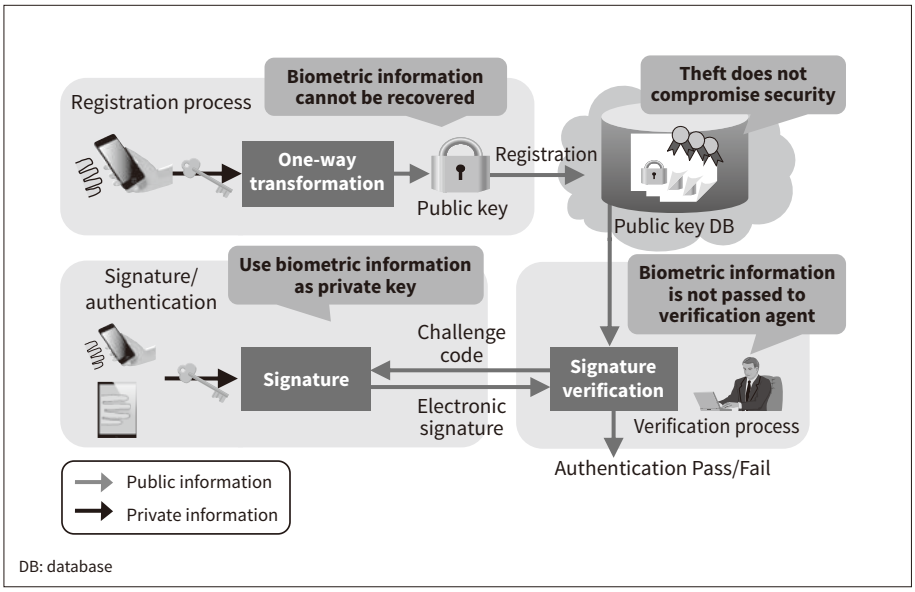


Figure 4 — PBI

A public biometric infrastructure (PBI) is a means of generating electronic signatures or performing online authentication that is guaranteed to be cryptographically secure and that works by generating a digital public key from variable analog biometric information such as finger veins or fingerprint patterns. This provides an open and secure mechanism for authentication on the Internet that can be implemented without divulging the biometric information being used, and without the need for a password, smartcard, or other security token.

of authentication templates creates the potential for data leaks of biometric information or other confidential data, resulting in identity theft or other losses.

This section describes the technique used to ensure the security of authentication templates, and also how it can be used in tandem with the Fast Identity Online (FIDO*) standard for online authentication that is being endorsed by an increasing number of companies.

3. 1
PBI

A public biometric infrastructure (PBI) is a means of verifying personal identity using biometric electronic signatures that works by converting the finger vein patterns, fingerprints, or other biometric information used for authentication into public keys in such a way that the original data cannot be recovered (see **Figure 4**). The electronic signature is based on a public key infrastructure (PKI) and provides a way of verifying the connection between the public key and the person who holds it. Whereas conventional encryption requires the authentication server to hold the encryption key, PKI verifies personal identity by using a signature that is produced using the private key held by the client and verified using the corresponding public key.

In a PBI, because the biometric information is used in place of the private key and is used as a key that is only available at the time of authentication, no private key needs to be stored, and therefore the risk of its being divulged can be reduced to an absolute minimum[4]. Using this template protection technique means that the biometric information used on various different devices can be deployed securely over open networks and utilized on different authentication services. In the following sections, the term "open template" is used to indicate authentication templates that can be used in this way on open networks.

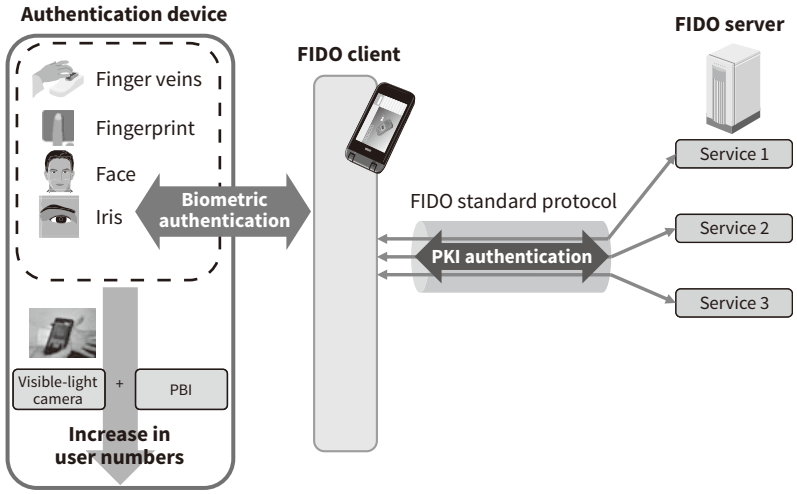
3. 2
Increasing User Numbers by Integrating PBI-FIDO

FIDO is a technical specification for simple and secure online user authentication that does not rely on passwords. The FIDO Alliance industry consortium has a membership of more than 250 companies, including Google LLC, Microsoft Corporation, Intel Corporation, and NTT DOCOMO, Inc., all of which are board members. It is anticipated that numerous services will be deployed in the future that comply with the FIDO standard.

FIDO authentication enhances security and interoperability by separating network authentication and the use of a security device to authenticate the user of a personal device. As network authentication uses a PKI, it is also capable of being integrated with a PBI (PBI-FIDO integration).

The major benefit provided by integrating PBI-FIDO with finger vein authentication using a

* FIDO is a trademark or registered trademark of Fido Alliance, Inc.



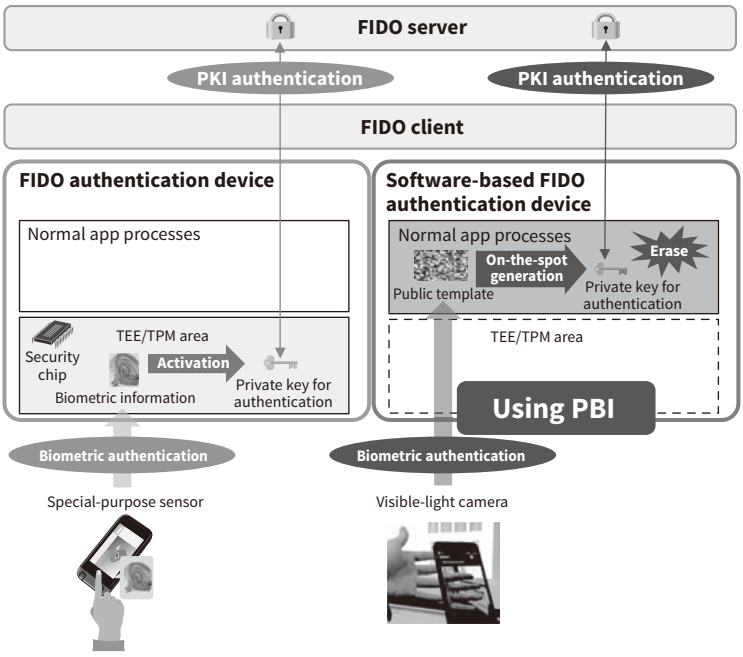
FIDO: Fast Identity Online

Figure 5 — Increase Service User Numbers by Integrating PBI-FIDO with Finger Vein Authentication Using Visible-light Cameras

Online authentication can be performed using a public key infrastructure (PKI) even on devices that lack a biometric authentication sensor. As adoption of FIDO authentication is expected to increase in the future, using the technology in combination with FIDO should help attract users to a variety of services.

visible-light camera is that devices that lack a special-purpose sensor for biometric authentication can still be used as FIDO devices (see **Figure 5**).

Figure 6 shows how PBI-FIDO integration works in practice. In a conventional FIDO device, the security device and private key are incorporated into a protected area at the time of manufacture. When using a mobile device with a visible-light camera, in contrast, a PBI can be used to implement FIDO as software (see the right side of **Figure 6**). This means it has the potential both to increase the number of finger vein authentication service users by serving as a gateway to FIDO services, and to make online services more attractive. Moreover, if the public templates are made compatible across both general-purpose cameras and special-purpose sensors, the technique also has the potential to attract more users to services that already use finger vein authentication, such as banking transactions or building access control.



TEE: trusted execution environment TPM: trusted platform module

Figure 6 — Implementation of Software-based FIDO Using PBI

The on-the-spot generation of private keys and the use of a PKI for online authentication on smartphones, tablets, or other devices that lack a special-purpose sensor are made possible by combining finger vein authentication using a visible-light camera with a PBI.

4. Future Prospects

This section uses practical examples to show what form personal identity verification solutions that combine template protection with finger vein authentication using a visible-light camera might take in the future.

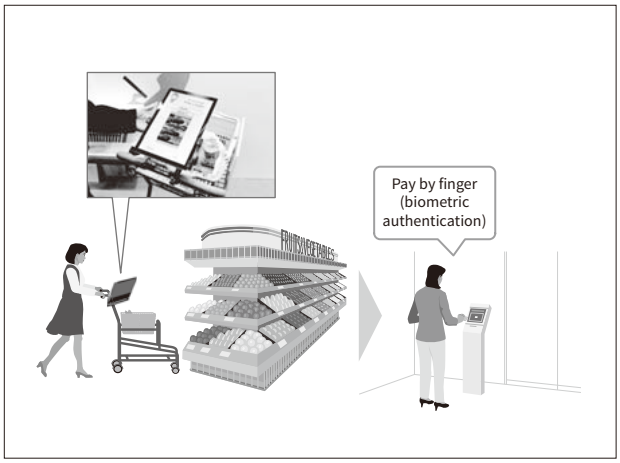
4. 1
Self-checkout at Retail Stores

The authentication technique described in this article could be used to provide a self-checkout service at supermarkets, convenience stores, or other retailers (see **Figure 7**).

In this example, the shopping carts provided for customer use are equipped with tablet devices. The customer first scans their fingers over the tablet to verify their identity and then checks that their name and payment method are correct before proceeding. The customer then uses the tablet camera to scan product barcodes as they place them in the cart.

When finished, they push the cart to the exit where the checkout process is initiated. The weight of the cart is checked against the items scanned to ensure that they match and then the customer scans their fingers over the tablet again to reconfirm their identity. If this authentication is successful, the payment is made using the pre-defined method and the customer can leave with their purchases.

Figure 7 — Self-checkout Using Tablet-based Authentication
Self-checkout without the need for cash or a card can be implemented by storing the public template for finger vein authentication using a visible-light camera on a tablet device attached to a shopping cart.



This reduces the time that customers spend waiting in the checkout line and has the added convenience that they can pay "empty-handed" even if they do not have their wallet with them. Benefits for the store, meanwhile, include being able to present customers with recommendations based on their previous purchase history and automatically calculating optimal stock-ordering quantities. It also helps recruit new service users because the initial biometric information can be acquired using a user's own smartphone, meaning that registration can be performed at any time or place.

In this way, the use in self-checkout of a finger vein authentication solution that uses visible-light cameras could help add value throughout the retail sector.

4. 2
One-stop Biometric Authentication for Hotels

Finger vein authentication using a visible-light camera is suitable for deployment anywhere a camera can be installed. Possible examples include room rentals and other accommodation check-in, serving as keys to executive lounges, or for engaging with an interactive robot. This includes centralized one-stop biometric authentication that is utilized by a variety of different services and works by having users create a public template on a smartphone or other device and then distributing the template to other devices.

One example of how this might be used in the future is the hotel hospitality service shown in **Figure 8**. When guests use their smartphones to make a reservation, their public template is passed to the hotel. The guests' templates are then passed to the authentication devices, which might include concierge robots, their room door knobs, and lounge payment terminals.

On arriving at the hotel, the guests are greeted by a robot and can check-in simply by allowing the robot's camera to scan their fingers. While being shown to their room, the guests are provided with information about hotel services tailored to their preferences. Using cameras fitted into door knobs, guests can also gain access to facilities such as their rooms or hotel lounges simply by having their fingers scanned. Similarly, they can also gain simple and trouble-free admittance to nearby theatres, stadiums, or other facilities through integration with the associated ticketing services.

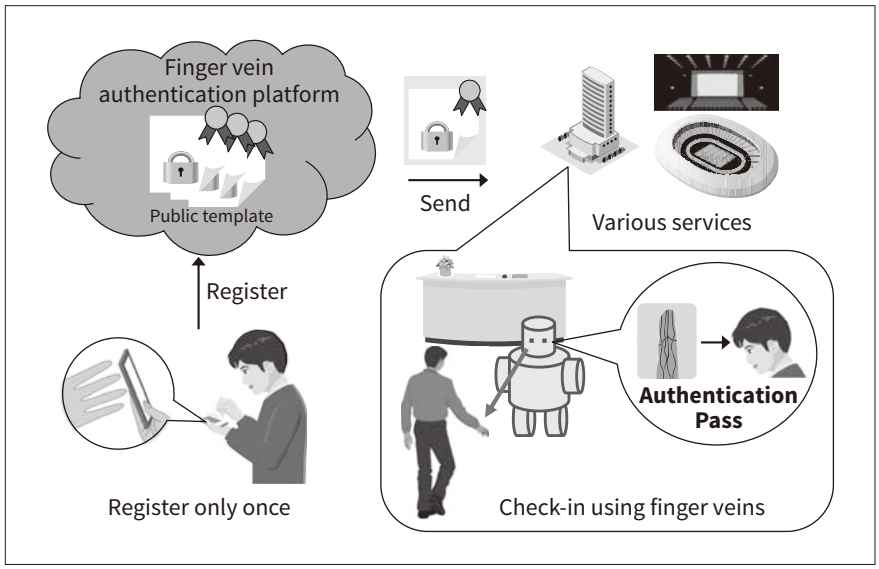


Figure 8 — One-stop Biometric Authentication at the Hotel

One-stop biometric authentication can be provided for everything from hotel reservations and check-in to accessing services by having users register their finger vein information on their own smartphones.

In this way, one-stop biometric authentication can be provided for everything from making hotel reservations to accessing services by having users register their finger vein information using their own smartphones.

4. 3
Enhanced Convenience through Government-Industry Partnership

Japan introduced a personal identification (ID) number system in January 2016, and the use of My Number cards that hold this ID number information in electronic form is continuing to increase. In addition to using the card as a certified public document, the electronic certificate for user authentication stored on the card's integrated circuit (IC) can also be used as personal identification in government administrative procedures or when accessing private services.

If a facility that issues PBI public templates linked to My Number certificates becomes available in the future at local government offices, for example, it will become possible to use finger vein authentication to verify personal identity in public on a wide variety of camera-equipped devices (see **Figure 9**).

Such a capability would enhance convenience in a variety of ways, including by making it possible for people to open bank accounts using their smartphones without having to physically visit a bank branch, or to certify official documents using a public terminal, such as at a convenience store, even if they do not have their My Number card with them.

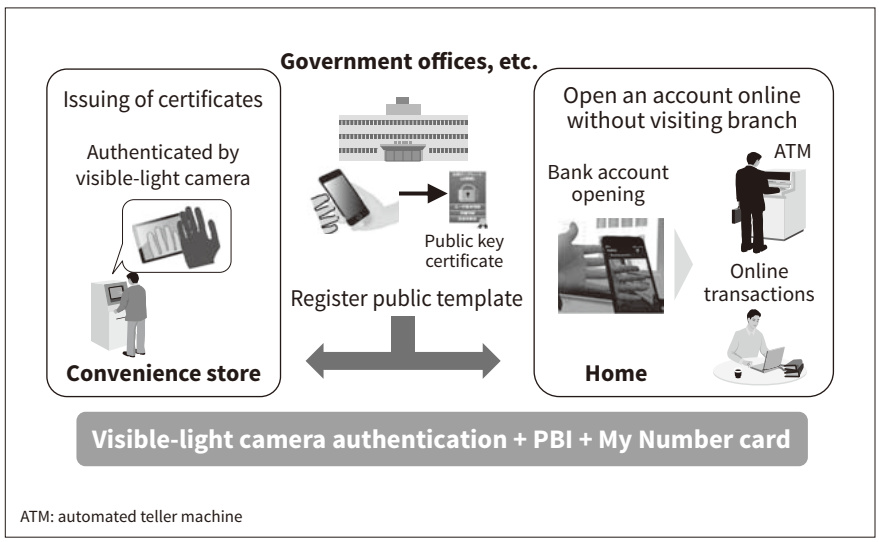


Figure 9 — Enhanced Convenience through Government-Industry Partnership

Using public services for verifying personal identity can be made available to a wide variety of camera-equipped devices by using the signature function of My Number cards to issue public key certificates for public finger vein templates.

5. Conclusions

This article described the technologies used to implement finger vein authentication using the visible-light cameras typically built into devices such as smartphones and tablets, and also described the future prospects for this technology.

This ability to use the technology on a large number of camera-equipped devices means these are now capable of performing finger vein authentication. Meanwhile, the article also described how using the technology together with PBI will open up potential applications in a wide variety of services, including automatic payment solutions for the banking and retail sectors.

In the future, Hitachi intends to contribute to creating a society that is safer and more secure by supplying personal identification solutions with high added-value that incorporate this technology.

References

1) S. Priya, "Forrester Data: Mobile Payments Forecast, 2016 To 2021 (US)," ForecastView Document (Jul. 2016).
2) Japanese Bankers Association Website, "Results of Survey on 'Illicit Deposit Withdrawals Using Internet Banking,' etc. (2008–2013)," (Nov. 2017), https://www.zenginkyo.or.jp/fileadmin/res/news/news291130_2.pdf in Japanese.
3) N. Miura et al., "Extraction of Finger-vein Patterns Using Maximum Curvature Points in Image Profiles," In MVA, pp. 347–350 (2005).
4) K. Takahashi et al., "A Provably Secure Digital Signature with Fuzzy Secret Key and its Application to Public Biometrics Infrastructure," The 30th Symposium on Cryptography and Information Security (SCIS2013) (2013) in Japanese.

Authors

Naoto Miura, Ph.D.
Center for Exploratory Research, Research & Development Group, Hitachi, Ltd. *Current work and research:* Research and development of biometric authentication systems, computer vision, and pattern recognition technologies. *Society memberships*: The Institute of Electronics, Information and Communication Engineers (IEICE).

Keiichiro Nakazaki
Media Intelligent Processing Research Department, Center for Technology Innovation – Digital Technology, Research & Development Group, Hitachi, Ltd. *Current work and research:* Research and development of biometric authentication systems, computer vision, and pattern recognition technologies.

Masakazu Fujio, Ph.D.
Security Research Department, Center for Technology Innovation, Research & Development Group, Hitachi, Ltd. *Current work and research:* Research and development of biometric authentication technology, crypto systems, and pattern recognition technologies. *Society memberships*: IEICE, the Information Processing Society of Japan (IPSJ), and The Japanese Society for Artificial Intelligence (JSAI).

Kenta Takahashi, Ph.D.
Security Research Department, Center for Technology Innovation, Research & Development Group, Hitachi, Ltd. *Current work and research:* Research and development of biometric authentication technology, cryptography, and information security. *Society memberships*: IEICE, and IPSJ.