Featured Articles

Biometric Authentication Platform for a Safe, Secure, and Convenient Society

—Public Biometrics Infrastructure—

Yosuke Kaga
Yusuke Matsuda
Kenta Takahashi, Ph.D.
Akio Nagasaka, Ph.D.

OVERVIEW: With the rise of issues such as cyber-crime and terrorist threats that have accompanied the growing use of information technology, biometric authentication has attracted attention as a means of identifying individuals to ensure security. However, biometric authentication is mainly used by individuals or individual organizations, and it has not reached a stage where it is available for widespread use as part of the infrastructure of society. This article considers the challenges associated with the wider use of biometric authentication as a basis for authenticating identity in social infrastructure, and describes the public biometrics infrastructure (PBI) and walkthrough-style finger vein authentication technology that can overcome these challenges. These technologies can be used to create a society with "empty-handed" safety and security.

INTRODUCTION

CORPORATE use of cloud computing and other forms of information and communication technology (ICT) is growing along with the adoption around the world of technology like national identity (ID) systems and electronic systems for government services, but accompanying these developments has been a rise in the damage done by cyber-crime. Meanwhile, the importance of physical security in cities is increasing as various countries face increased terrorist threats. Identity authentication to prevent unauthorized access or spoofing is a core technology for use in security for social infrastructure, which includes cyber and physical systems such as these. Among the technologies for authenticating identity, biometric authentication has attracted attention for its ability to combine a high level of both security and convenience. Biometric authentication is a way of confirming the identity of a person by acquiring information on their biological or behavioral characteristics, such as their finger veins or fingerprints, and comparing it against stored data. It provides a very convenient way to verify identity, with a lower risk of identification information being lost, stolen, or forgotten compared to conventional methods like passwords and smartcards. The use of biometric authentication to provide the basis for identity authentication in various services associated with social infrastructure makes possible a society in which safety and security can be achieved with an "empty-handed" style, without the need for smartcards or passwords.

However, three challenges in particular will need to be overcome if biometric authentication is to become a more widely used part of the social infrastructure. These are: getting various different services to adopt a sharable platform, ensuring the privacy and security of biometric information, and improving the convenience of authentication.

(1) Sharing a platform among various different services

Biometric authentication systems in current use ensure security by managing the biometric information in a standalone system. The problem with this model is that, when biometric authentication systems are used by a variety of different services, each system needs to record its own biometric information. And because this need to record information is one of the obstacles to wider use of biometric authentication, getting a wide variety of different services to adopt it as a means of verifying identity will require the development of a sharable authentication platform that these services can all use.

(2) Ensuring the use of biometric information

Because biometric information is of a sensitive nature, with the potential to identify a person's race, ethnicity or state of health, for example, it needs to be

kept secure to maintain privacy. Furthermore, because one's biometric information is a lifelong attribute that cannot be discarded or updated, it is very difficult to restore security once leaked, being vulnerable to use in forgery, replay attacks*1, or other forms of spoofing. Preventing leaks of biometric information is essential to protect users from such security threats.

(3) Improving the convenience of authentication

If biometric authentication is to be made a routine part of the social infrastructure, its use must not impose inconvenience. Accordingly, its operation must be sufficiently intuitive, easy-to-understand, and simple enough that anyone will be comfortable using it. For use in public places where large numbers of people congregate, such as major event venues or large facilities like railway stations or office buildings, the technology must combine both the accuracy needed to reliably identify individuals and the high throughput needed to ensure a smooth flow of people without queuing.

To deal with the first and second challenges of shared use and of privacy and security, Hitachi has put forward the concept of a public biometrics infrastructure (PBI) and implemented it by developing biometric signature technology[(1), (2)]. Hitachi is also working on the research and development of walkthrough-style finger vein authentication technology to overcome the third challenge of improving convenience[(3)].

*1 An attack involving the interception of authentication data such as a user identity (ID) and password and its use for spoofing.

PUBLIC BIOMETRICS INFRASTRUCTURE (PBI)

This section describes the concept of a PBI[(1)] that is intended to realize a sharable authentication platform across a variety of services and ensure the privacy and security of biometric information, and its implementation in the form of biometric signature technology[(2)].

Problems with Existing Biometric Authentication

Existing biometric authentication works by storing the biometric information obtained from users when they register and then using this information to confirm their identity by comparing it against the information obtained at the time of authentication. Biometric authentication systems can be broadly divided into a number of different models based on where they store and check the biometric information (see Fig. 1). The following section gives an overview of these models and describes the problems associated with each of them.

(1) Perform authentication in a smartcard

This involves storing the biometric information in a smartcard, such as the debit cards used in bank automated teller machines (ATMs). Storing the biometric information in a secure region on the smartcard enables robust security. However, because it requires smartcards to be issued to users, and that users have the smartcard with them when

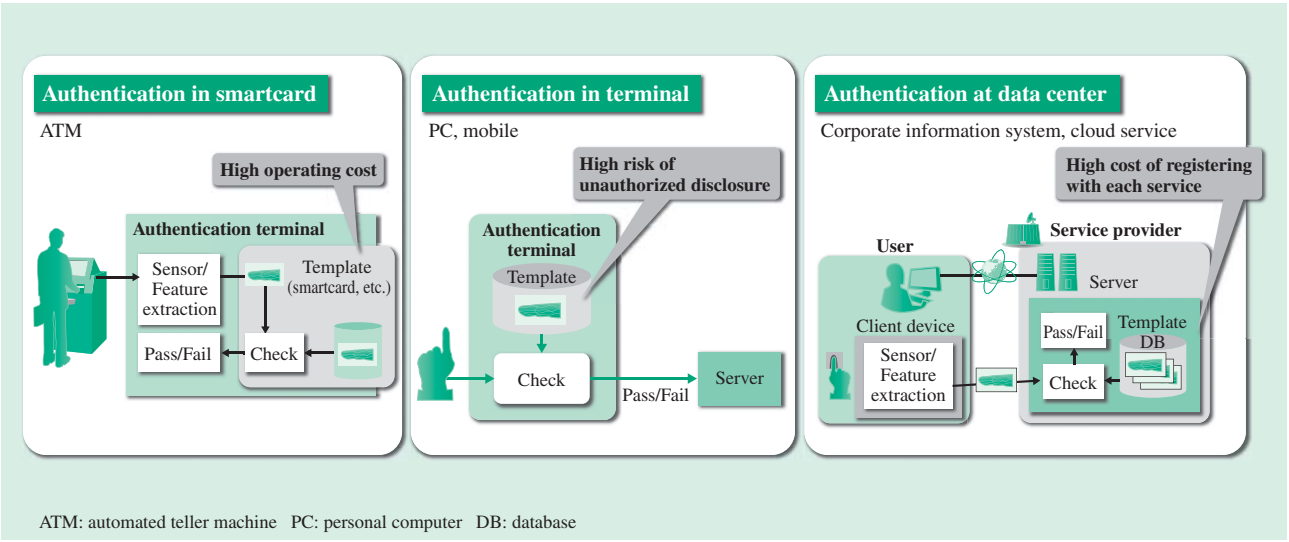

Fig. 1—System Model for Biometric Authentication.
The three existing system models for biometric authentication involve performing authentication in the smartcard, in the terminal, or at the data center. All of these suffer from problems that include operating costs, risk of unauthorized disclosure, and registration costs.

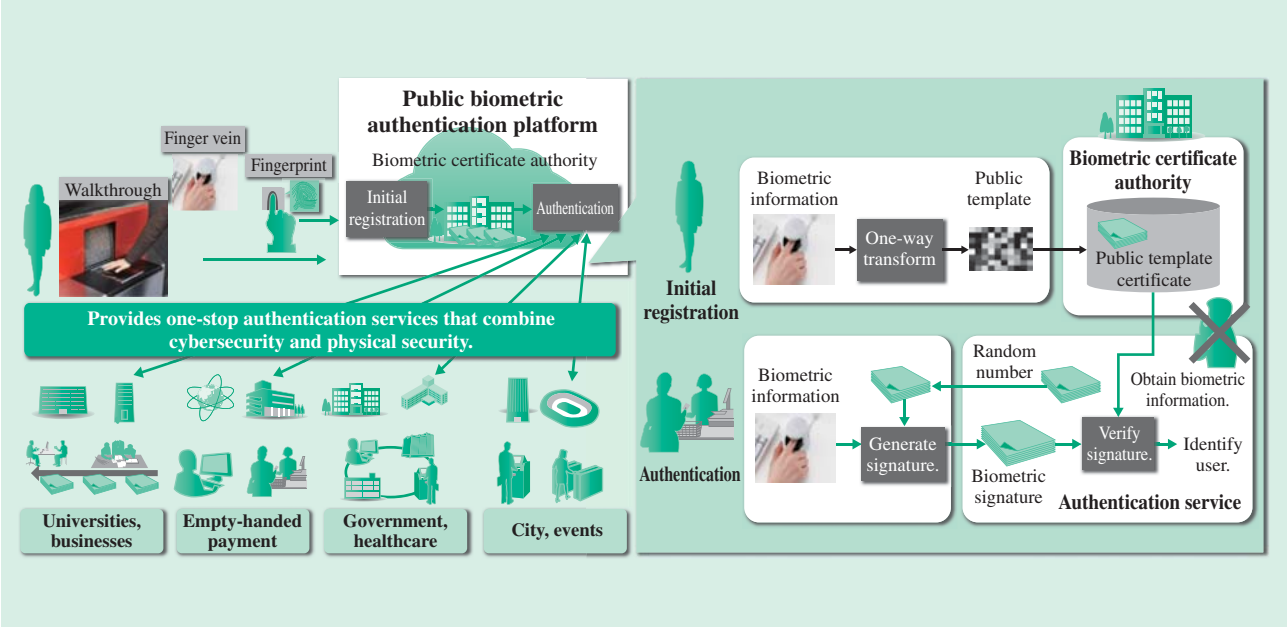

Fig. 2—Overview of Public Biometrics Infrastructure.
The user only needs to register once by providing their public template certificate to the certification authority. Because the same public template certificate can be used by different services, the user is able to access various services without having to repeat the registration process.

they perform authentication, the cost of issuing and managing user-specific smartcards is greater than for the other models.

(2) Perform authentication in a terminal

This involves storing the biometric information in the sensor used as the biometric reader, or in a personal computer or mobile device connected to the sensor. Because it is the responsibility of users to keep their terminals secure, risks include infection by malware due to the difficulty of ensuring that these terminals are always kept safe. If biometric information is stored on terminals like these with poor security, there is a strong risk of it being leaked.

(3) Perform authentication at a data center

This involves storing the biometric information at a data center that is linked to terminals via a network. This is more troublesome for users because each service saves the biometric information in its own data center, meaning users must register for each service separately. Because biometric information for a large number of users is stored in the same place, the damage resulting from any leak is likely to be large.

Accordingly, because existing biometric authentication requires the biometric information obtained from users when they register for services to be stored securely, its problems include the cost of registering biometric information and the risk of it being leaked. The following sections describe a biometric authentication platform that reduces the cost of registering biometric information by overcoming the first challenge of shared use, and a biometric signature technology that reduces the risk of biometric information being leaked by overcoming the second challenge of privacy and security.

Sharable Biometric Authentication Platform

This section describes a sharable biometric authentication platform that can be used by a number of different services. Fig. 2 shows an overview of the PBI.

The PBI provides the platform for incorporating identity authentication into the social infrastructure, including the establishment of new biometric certificate authorities for issuing and managing public template certificates. By making this identity authentication platform available for general use, biometric authentication can be used in applications such as a national ID system, “empty-handed” payment services, password-less authentication in the cloud, and physical security in cities without users having to register separately with each service.

Users confirm their identity with a biometric certificate authority in order to obtain their initial registration. It is envisaged that biometric certificate authorities will include local government in the case of a national ID system, bank branches in the case of payment services, or the information technology

(IT) department of the relevant organization in the case of cloud authentication. When obtaining initial registration, the user's biometric information is supplied to the biometric certificate authority after first being converted into a public template using a one-way transform[*2]. The biometric certificate authority with whom the user is registering affixes a signature to this public template to issue a public template certificate. Because the public template is stored in a form from which the original biometric information cannot be recovered (due to use of the one-way transform), there is no risk of anyone obtaining the biometric information if the template is disclosed. This means that numerous different services can use the same public template.

The following section considers the advantages of using a biometric authentication platform like this. The biometric authentication platform works on a model whereby the biometric certificate authority acts as a repository for certificates that are distributed to services as required, meaning that the information obtained when a user registers can be reused by multiple different services. This overcomes the first challenge of providing a sharable platform.

Digital Signature Technique Using Biometric Information Key (Biometric Signature Technology)

Challenge and response authentication[*3] is one way of preventing the use of replay attacks for spoofing (as described above in the section on the second challenge of privacy and security). While using this method for authentication ensures security, a conventional digital signature requires that a secret key be stored in a smartcard or other device. Accordingly, the problems with this method include the risk of loss or theft of the card and the cost of administration.

Hitachi has developed biometric signature technology that uses biometric information as the secret key, meaning that the secret key is securely stored in the form of the user's own person rather than on a smartcard. The biggest problem with using biometric information as a key is that the data contains a level of error. In the conventional public key infrastructure (PKI), even a single incorrect bit will prevent identity and signature verification. Biometric information, on the other hand, is analog and therefore an allowance for errors is needed. Hitachi developed its biometric signature technology to solve this problem (see Fig. 3).

The biometric signature technology works by extracting a fuzzy key (a stable feature vector with a low level of error) from the biometric information during initial registration and generates the public template from this fuzzy key using a fuzzy signature.

When this public template is subsequently used for authentication, the fuzzy key is extracted from the biometric information in the same way as at initial registration, and then this fuzzy key is used to generate a biometric signature from a random number. The identity of the person can then be confirmed by using their public template to verify their biometric signature.

The following sections describe the steps performed during initial registration and during authentication in more detail.

Initial Registration

First, the fuzzy key extraction algorithm is used to generate the feature vector by extracting features from the biometric information. While biometric information typically contains a large number of errors, feature extraction obtains data with a low level of errors. Next a salt (random number) is added to the feature vector to convert it into the secret key data (fuzzy key) (Step 1).

Next, the key generation algorithm for the fuzzy signature is used to generate the public template, using the fuzzy key as input. Key generation generates a key pair (public key and secret key) (Step 2), and the secret key is embedded in the fuzzy key (Step 3). The key pair generation step is performed using an existing digital signature technique (S) that satisfies the criteria of key homomorphism (such as a Waters signature[*4]). Finally, with the secret key and fuzzy key having been transformed in such a way that they cannot be recovered, an error correction code[*5] is added to create the public template along with the public key (Step 4).

Authentication

First, following the same procedure as initial registration, the fuzzy key extraction algorithm is used to generate the fuzzy key from the user's biometric information (Step 1).

Next, challenge and response authentication is performed using the signature algorithm and verification algorithm from the fuzzy signature method.

*2 A conversion for which there is a mathematical proof that the original information cannot be recovered.

*3 An authentication technique with low vulnerability to replay and similar attacks and that can be implemented using digital signatures based on public key encryption.

*4 The ability to perform operations such as addition and multiplication while still in encrypted form.

*5 Additional data added to enable data errors to be corrected.

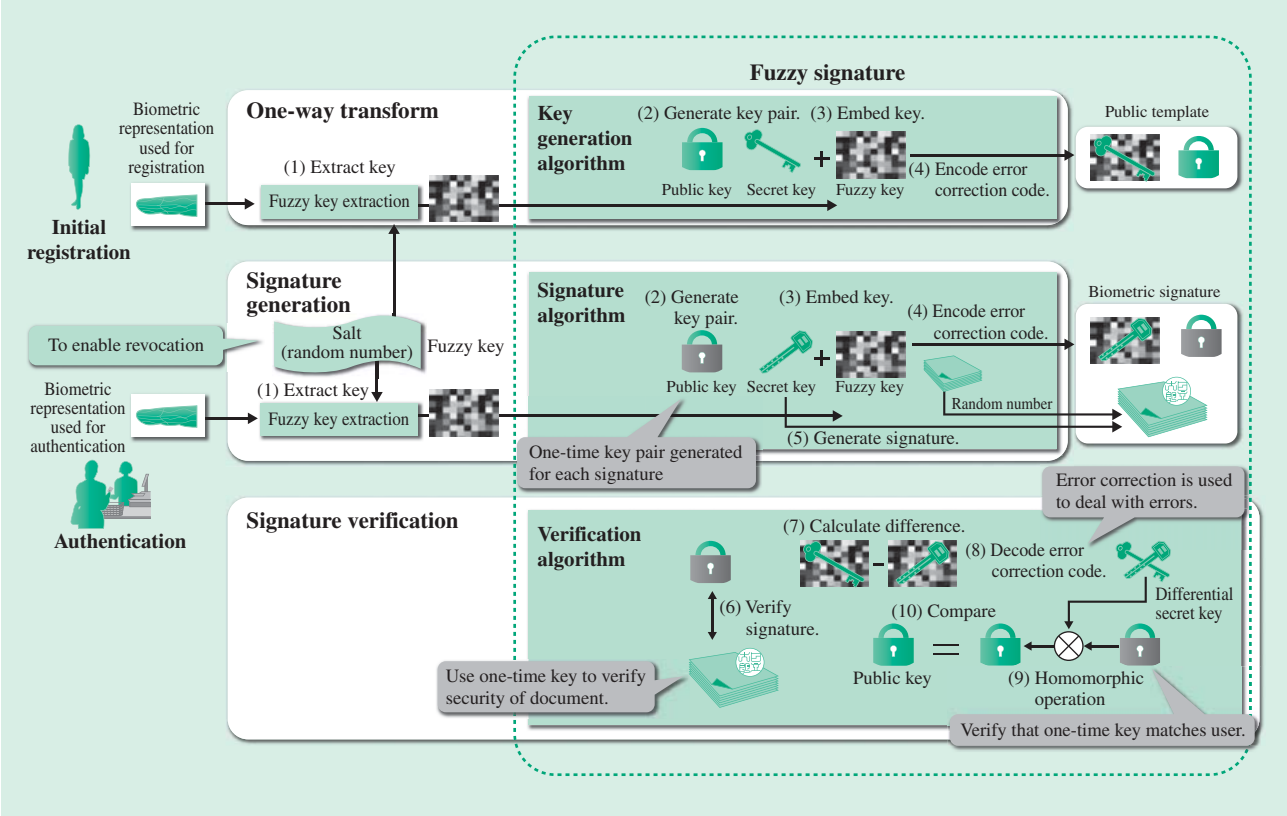

Fig. 3—Overview of Biometric Signature Technology.
To register a user, the fuzzy key is extracted from the biometric representation being used for registration and the key generation algorithm for the fuzzy signature method is used to generate the public template. To perform authentication, the fuzzy key is extracted from the biometric representation being used for authentication and then challenge and response authentication is performed using the signature algorithm and verification algorithm for the fuzzy signature method.

The signature algorithm generates a biometric signature using a random number sent by the server. First, a one-time key pair (secret key and public key) is generated based on the digital signature method (S) (Step 2). Because this one-time key pair is generated at random, the resulting data is different each time. Next, the one-time secret key is embedded in the fuzzy key (Step 3). With this secret key and fuzzy key having been transformed in such a way that they cannot be recovered, an error correction code is added (Step 4). A signature is then generated from a random number using the one-time secret key for the digital signature method (S) (Step 5), resulting in a biometric signature that combines the fuzzy key (which includes the embedded one-time secret key) and the one-time public key.

The verification algorithm checks the validity of the biometric signature. First, the signature generated from the random number is verified using the one-time public key (Step 6). Next, the difference between the fuzzy key that includes the embedded secret key from the public template and the fuzzy key that includes the one-time secret key from the biometric signature is calculated (Step 7). This generates a differential secret key, using error correction to allow for any errors between the biometric information at the time of registration and at the time of authentication (Step 8). The one-time public key is converted by performing a homomorphic operation based on this differential secret key (Step 9), and if the result of this conversion matches the public key in the public template, the biometric signature is deemed to be valid (Step 10).

By using this fuzzy key extraction and fuzzy signature technique, the biometric signature technology is able to be implemented using biometric information as a key.

The security of the biometric signature technology has been demonstrated by a mathematical proof that shows that breaking this method for the purpose of forgery or falsification is sufficiently difficult. Specifically, security has been demonstrated by showing that the unforgeability of the biometric signature is equivalent to that of a Waters signature[4], the unforgeability of which has already been proven

mathematically[2]. Accordingly, the second challenge of privacy and security can be overcome by using biometric signature technology as the one-way transform of the biometric authentication platform. By using this biometric signature technology, it is possible to provide signatures and other forms of authentication based on biometric authentication that does not use things like smartcards or passwords, with the same level of security as PKI that is already widely used for things like electronic payments and electronic-government (e-government) services.

Fig. 4—Walkthrough-style Finger Vein Authentication Unit.
The unobstructed access to the interface enables users to place their fingers on the reader and identify themselves as they walk past.

BIOMETRIC AUTHENTICATION THAT PROVIDES ACCURATE AND STRESS-FREE PERSONAL IDENTIFICATION

This section describes a biometric authentication technique that can provide accurate and stress-free personal identification, even at venues attended by large numbers of people.

Convenient Biometric Authentication

Hitachi has previously developed a biometric authentication technique that uses the pattern of veins in a person's fingers and deployed it in products for banking, access control and information security. This finger vein authentication technique can achieve a high level of authentication accuracy provided the body part in question is presented in the correct position. Also, finger veins are very difficult to forge because they are an internal characteristic.

A problem, however, is that it is difficult to make authentication quick and simple because it requires the user to stop and present their finger in the correct position. What is needed to combine high authentication accuracy with convenience is a quick and simple operation that can identify people accurately.

Accordingly, Hitachi has developed a biometric authentication technique that is still based on finger vein authentication but can identify people as they walk past, with finger vein authentication that is both accurate and has superior performance in terms of making forgery difficult.

Walkthrough-style Finger Vein Authentication Technology

The finger vein authentication technique uses a finger vein pattern obtained by shining near-infrared light onto the user's fingers and capturing an image of the light after it passes through the interior of the fingers. Hitachi has further enhanced the technique by developing walkthrough-style finger vein authentication technology that can identify people quickly and easily using simple and intuitive operation that consists of having them place their fingers on a reader as they walk past it (see Fig. 4).

Fig. 5 shows diagrams of the prototype authentication unit. In brief, the proposed method involves first using a ranging sensor [three-dimensional (3D) sensor] to detect the position and orientation of the user's fingers. The light sources are controlled based on this information and the finger vein images acquired.

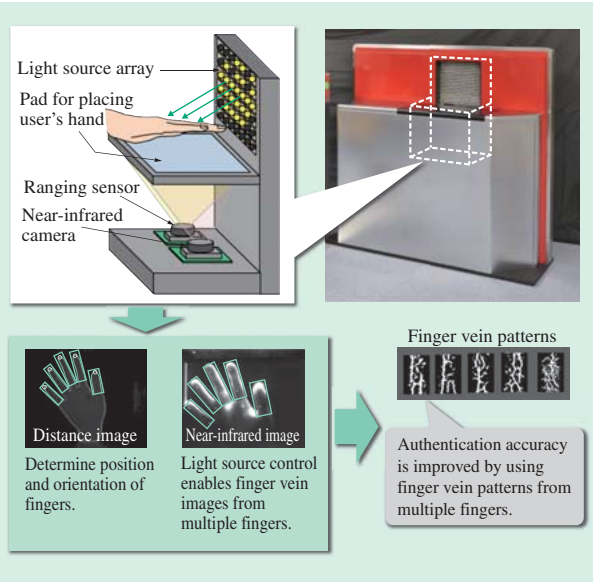

Fig. 5—Authentication Unit Components and Overview of Authentication Process.
A ranging sensor detects the position and orientation of the user's fingers, which are used for adaptive control of the light source array, enabling authentication to be performed using multiple finger vein patterns that are obtained instantaneously.

Finally, the multiple finger vein patterns obtained from these images are compared against existing vein patterns stored in a database to verify identity. The key features of the proposed method are as follows.
(1) Unobstructed interface that does not impede users as they walk past
(2) Control of light sources based on finger position and orientation when capturing finger vein images
(3) Enhanced accuracy through use of multiple finger vein patterns

Firstly, the unit was designed without any obstructions above or on the side where the user is passing to ensure that nothing gets in the way of the user placing their hand on the reader for authentication as they walk past.

To provide flexibility in the position and orientation of the user's fingers on the reader as they walk past and to ensure reliable vein pattern images under these conditions, the system uses an array of multiple light sources. Using a single light source would result in the light not reaching the user's fingers in some cases, depending on where they placed their hand, making it difficult to obtain clear finger vein images. Instead, the control function selects which of the multiple light sources to use based on the position and orientation of the user's fingers to obtain reliable finger vein images regardless of the position and orientation of the user's hand.

To improve authentication accuracy, the system uses multiple fingers. The authentication unit shown in Fig. 4 captures images from multiple fingers simultaneously and provides a larger region for the user to place their hand than previous models that only captured an image from a single finger. This means it achieves greater authentication accuracy by using images of multiple fingers.

Proof of concept testing conducted to demonstrate the throughput and authentication accuracy of the new technique using the prototype unit shown in Fig. 4 was able to identify a maximum of 70 people per minute. Furthermore, although accuracy has only been evaluated for a small sample size, the results indicate that the unit can achieve similar accuracy to current production models even when operating at the above maximum rate of throughput. Because the newly developed walkthrough-style finger vein authentication technology provides a higher level of convenience than previous security techniques, it has potential uses in a wide range of applications. In the future, Hitachi aims to expand its business by using the new technology as a core component of its security solutions.

CONCLUSIONS

This article has described a PBI and walkthrough-style finger vein authentication, two technologies that will be essential to the wider adoption of biometric authentication as a basis for identity authentication in social infrastructure. The use of this technology will make possible a society in which "empty-handed" safety and security can be achieved without the need to use cards or passwords.

In the future, Hitachi intends to proceed with further research and development of biometric authentication and other forms of cybersecurity and physical security to help create a safe and secure society with a high level of convenience.

REFERENCES

(1) K. Takahashi et al., "A New Security Infrastructure Based on Public Biometric Templates," 2012 Symposium on Cryptography and Information Security (SCIS 2012) (2012) in Japanese.
(2) K. Takahashi et al., "A Provably Secure Digital Signature with Fuzzy Secret Key and Its Application to Public Biometrics Infrastructure," 2013 Symposium on Cryptography and Information Security (SCIS 2013) (2013) in Japanese.
(3) Hitachi News Release, "Finger Vein Authentication Technology for Smooth and Accurate Walkthrough-style Personal Verification" (Dec. 2014), http://www.hitachi.com/New/cnews/month/2014/12/141208a.html
(4) B. Waters, "Efficient Identity-Based Encryption Without Random Oracles," EUROCRYPT 2005, Vol. 3494 of LNCS, pp. 114–127 (2005).

ABOUT THE AUTHORS

Yosuke Kaga

Center for Exploratory Research, Research & Development Group, Hitachi, Ltd. He is currently engaged in the development of biometric authentication technologies. Mr. Kaga is a member of The Institute of Electronics, Information and Communication Engineers (IEICE).

Kenta Takahashi, Ph.D.

Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the development of biometric authentication and information security technologies. Dr. Takahashi is a member of the IEICE and the Information Processing Society of Japan (IPSJ).

Yusuke Matsuda

Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the development of image recognition and biometric authentication. Mr. Matsuda is a member of the IEICE.

Akio Nagasaka, Ph.D.

Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the development of finger vein authentication technology. Dr. Nagasaka is a member of the IEICE.