Integrated Biometric Authentication Technology to Support a Cashless Society

● Narishige Abe ● Hajime Nada ● Tomoaki Matsunami ● Hidetsugu Uchida

In order to realize and promote a cashless society, payment using only the biometric information of an individual without the need for identification by ID card or smartphone is attracting attention. In cases where authentication on a scale of one million users is assumed, such as payments at brick-and-mortar stores and admission to event venues, it is necessary to search for and authenticate a single individual from a huge volume of personal data. However, high-speed searches of large volumes of data were difficult with one biometric modality alone. For that reason, inputting additional information such as IDs and personal identification numbers (PINs) was necessary, which compromised user convenience. Accordingly, Fujitsu Laboratories has developed an integrated biometric authentication technology that combines palm vein and face recognition. This technology uses facial images effortlessly captured during payment terminal use to narrow down the possible matches, thereby allowing the number of system users to be increased without the need for the input of information other than biometric data. This paper describes the present state and issues of payments using biometric authentication, and the integrated biometric authentication technology developed.

1. Introduction

Cashless payment is spreading among brick-and-mortar retail stores such as convenience stores and supermarkets. This trend is prominent particularly outside Japan, where unmanned stores that have deliberately eschewed the use of cash registers, such as Amazon Go in the United States and BingoBox in China, have appeared. This is not only for the convenience of consumers, who do not have to carry cash, but also for the stores, which benefit by reducing opportunity loss as consumers can purchase whatever they want without cash on hand at any time.

However, according to a report from the Ministry of Economy, Trade and Industry,[1] while the proportion of cashless payments is 89.1% in Korea and 60.0% in China, it is only 18.4% in Japan. Even today, preference for cash is strong in Japan, and one of the reasons for this is the low reliability of cashless payment. For cashless payment to gain trust, it must achieve both the convenience of being easy to use at any time and the accuracy that makes it safe and secure to use by ensuring correct recognition of who the users are at all times.

Credit cards have been widely used as a means of cashless payment. However, since such means of payment may be lost or stolen, biometric authentication that performs personal identification using human biometric information is attracting attention. Since 2004, Fujitsu has been developing palm vein authentication technology, a biometric authentication technology that uses a person's palm vein pattern, to identify individuals. This technology has been applied to bank ATMs, entrance/exit management, and management of access to personal terminals such as PCs, among other things. As of the end of 2018, over 82 million people in some 60 countries around the world are using this technology, and its use is expanding.

This paper describes Fujitsu's integrated biometric authentication technology,[2] which can authenticate an individual using only biometric data consisting of palm vein and facial data, from a database of about one million people. This technology facilitates cashless payment without the need to input additional information such as IDs.

2. Authentication methods supporting cashless society and related issues

Credit cards, mobile phones and smartphones are the most commonly used means of cashless payment. In particular, services linked to identity verification methods using FIDO (Fast IDentity Online)[3] are increasing in number. However, things such as credit cards and phones may be lost or stolen, making them unavailable for use when needed.

Therefore, as a means of cashless payment that does not depend on such things, attention has been focused on so-called "ID-less authentication technology" that identifies users based solely on their biometric information. Biometric information is convenient because it can be used at any time without loss being a concern, and accuracy is assured by biometric authentication technology that can distinguish one person from others with a high degree of accuracy. Thus, highly reliable cashless payment can be realized through the use of ID-less authentication technology.

Figure 1 shows a possible deployment path of ID-less authentication and the respective user scales. In systems where tens of thousands to hundreds of thousands of people are registered, such as bank ATMs, performing ID-less authentication and payment through palm vein authentication requires efficient and accurate comparison and matching of the newly acquired data with the registered data. Traditionally, by inputting non-biometric information such as an ID, the candidate data could be narrowed down from the whole, speeding up the authentication process while maintaining accuracy by comparing and matching the candidate's data with the biometric information of the user. For the sake of even greater convenience, there is also demand for payment methods that do not require the user to consciously enter any additional information, such as methods whereby payment can be completed by having the user simply hover the palm of his or her hand over a sensor. In the case of ID-less payment, chain stores with more than one million users are also targeted. Efficient comparison and matching in the case of such huge user base requires even faster authentication processing and higher authentication accuracy.

Usually biometric information such as a face, fingerprint, or vein pattern is used for biometric authentication. For example, Liquid Inc., which develops biometric authentication terminals, has conducted with Panasonic a demonstration experiment in which a vending machine is equipped with a fingerprint authentication function to sell products unattended.[4] However, in a system that identifies persons only from a single type of biometric information, there is a limit as to the maximum size of the group for which identification accuracy can be achieved, and this limit is commonly held

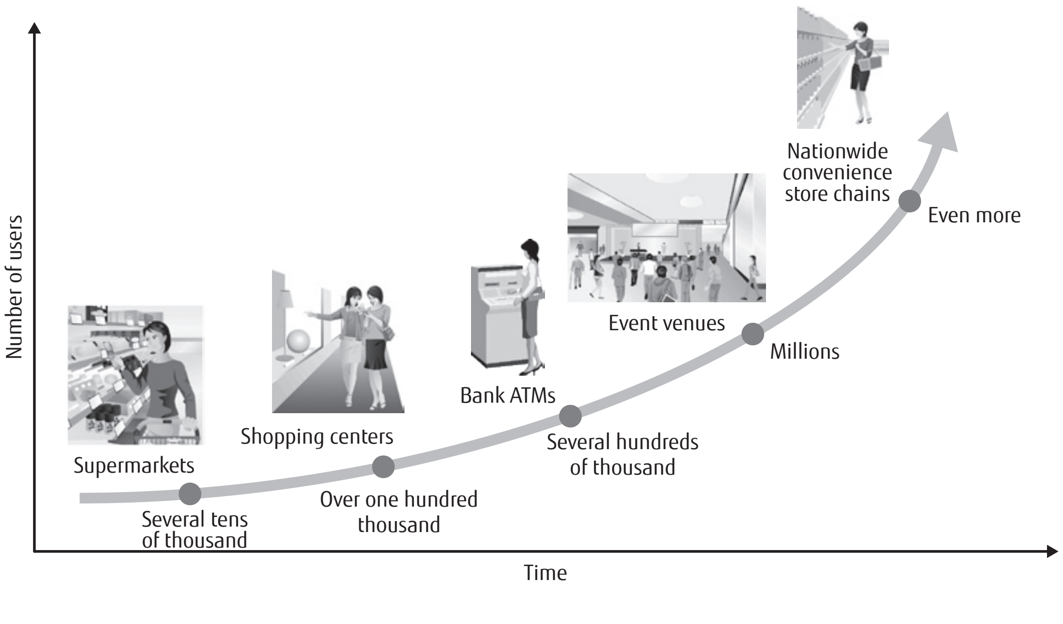

Figure 1
Potential deployment path of ID-less authentication and respective user scales.

to be about 10,000 people.[5] In other words, when authentication using a single type of biometric information is attempted for a group on the order of one million people, problems such as an increase in the number of erroneous identifications becomes apparent.

To remedy this, technologies that use not a single but rather multiple types of biometric information have been proposed to enable accurate identity verification even when the number of users increases, thereby realizing safe and secure authentication. For example, KDDI and Hitachi have jointly developed ID-less authentication technology that combines face and palm print recognition for use for payment at stores.[6] In this way, ID-less authentication has the advantage that it allows authentication without having to use a device dedicated to that application alone.

However, such technology presents convenience-related issues such as the following.

1) Increased processing time required for comparison and matching

When multiple types of biometric information are acquired and compared, comparison processing is performed independently for each type of biometric information, which increases processing time. To maintain overall throughput, it is necessary to increase the number of servers, which increases cost.

2) Increased user input load

As described above, to accommodate a greater number of registered users, users need to provide additional information. However, this is for the convenience of the system service side while imposing an additional burden on users to achieve the same purpose of personal authentication. Furthermore, to maintain high authentication accuracy, onerous input methods such as facial capture photography that require the user to position his or her face according to markers may also be needed. Passing such burdens as is on to users will directly reduce user convenience.

Solutions that improve user convenience yet remain to be established, and this is an issue that affects all ID-less payment systems. Fujitsu's aim is to solve these issues and realize ID-less authentication that combines convenience, safety, and security. To that end, high-speed and high-accuracy biometric authentication technology is required.

3. Fujitsu's ID-less authentication achieving convenience, safety, and security

This section describes ID-less authentication technology that achieves convenience, safety, and security. First, it looks at integrated biometric authentication technology that achieves high authentication accuracy by integrating palm vein authentication technology and face recognition technology. It then looks at face recognition technology that uses the facial image captured during terminal use to quickly narrow down the matching target, and thus achieve high convenience.

3.1 Integrated biometric authentication technology

As mentioned in the previous section, expanding the scale of biometric users requires the input of additional information. However, as the burden on the user regarding the input of information increases, user convenience decreases. Therefore, we developed technology that uses facial data acquired from a camera during user terminal operation to narrow down the group of potential targets from a database of registered users. The user then simply hovers the palm of one hand over a sensor and is authenticated from out of that narrowed down group when payment is required (**Figure 2**).

This technology has the effect of stabilizing the authentication result by combining two different pieces of biological information, palm vein and facial data. Specifically, while it is difficult to distinguish similar faces such as those of twins with an ordinary web camera, the user can be correctly identified through the input of palm vein data at a later stage. On the other hand, with palm vein authentication, the accuracy of personal authentication may be insufficient due to fluctuations in the palm vein pattern caused by input operations, such as misalignment of the palm and changes in palm shape when the hand is held over the sensor (**Figure 3**). Even in such cases, the information required for authentication can be supplemented with the facial data acquired in the previous stage. Thus, by combining two types of biometric information, as opposed to using only a single type of information, it is possible to achieve more accurate authentication and improve the reliability of the biometric authentication technology.

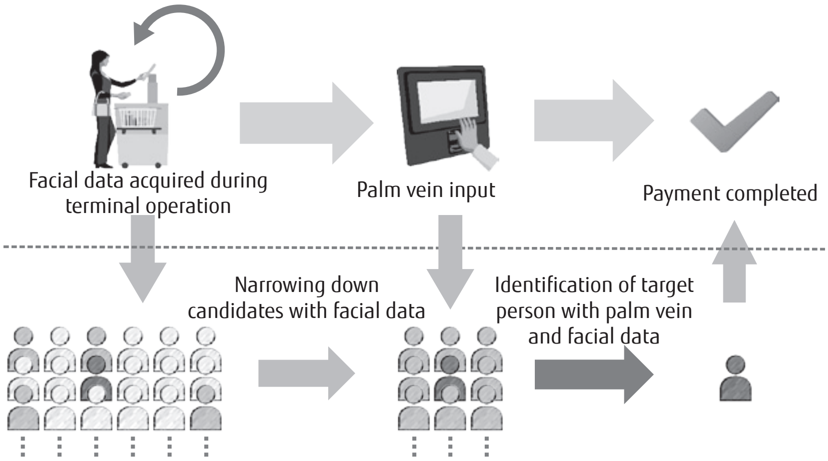

Figure 2
Flow of ID-less payment.

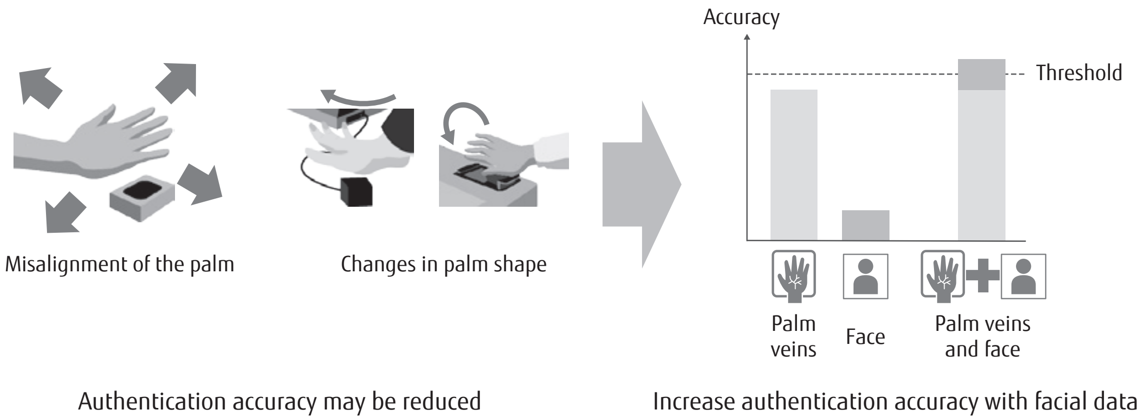

Figure 3
Improving the accuracy of authentication with integrated biometric authentication technology.

3.2 Fast and high-precision face recognition technology

If the input facial data is somehow insufficient and the target person is not included in the selection of people to be verified, authentication of the person will not be successful even when palm vein data is input in the latter stage. For this reason, it is necessary to use technology for narrowing down the selection with high accuracy using facial data characteristics that are less affected by changes in facial orientation and facial expression. On the other hand, simply increasing the accuracy complicates calculation processing, making real-time processing difficult in the case of a large one million user scale database.

To meet these challenges, we developed face recognition technology that narrows down the selection for verification with high speed and high accuracy. Face recognition technology with high speed is composed of facial feature extraction technology implemented on the client side and comparison and matching technology implemented on the server side. This subsection describes the facial feature extraction technology.

1) Facial feature extraction technology using distillation technology

Realizing a highly convenient narrowing-down process using face images requires facial features extraction that is robust with regard to changes in the user's facial orientation relative to the camera and facial expressions. To solve the issues described in Section 2, Fujitsu Laboratories developed feature extraction technology that uses deep learning.

Deep learning is a machine learning method that uses a multilayer neural network. In recent years, especially in the field of image processing, deep learning has achieved remarkable growth with results that surpass the accuracy of conventional methods.[7) On the other hand, to improve the accuracy of the feature extraction model with deep learning, it is necessary to construct complex models, for example by deepening the layer structure of the model. Since extracting features from a complex model is very time consuming, it is common to use a graphics processing unit (GPU) for this task. However, often the processing mechanism on the client side, such as a point-of-sale (POS) terminal, is not equipped with a GPU, and if installation of a GPU is essential, the cost of the terminal will increase, hindering the spread of facial feature extraction technology.

We solved this issue by utilizing distillation technology, which is a way to reduce model size while maintaining accuracy. In general learning algorithms, only correct data is learned as training data. By contrast, in addition to correct data, distillation technology also uses the output results of a model (teacher) that has already been learned and has high accuracy but a complicated structure. As a result, the amount of information that can be obtained by the model (student) to be learned increases, and it is possible to generate a student that has a simpler structure than that of the teacher and has high accuracy on a par with that of the teacher.

As shown in **Figure 4**, the process consists of two steps. First, by learning a complex network with many parameters, a sophisticated model (teacher) that outputs highly accurate feature vectors with emphasized layers and parameters for the extraction of important features is generated. High-accuracy feature vectors realize high-accuracy authentication so that even if the target person presents changes in face orientation or facial expression, that person is not omitted from the selection of people to be verified, and further, that person is given a higher search ranking.

Next, a simpler network with fewer parameters is learned by adding conditions to simulate the output of a sophisticated model. This creates a lightweight model (student) that can output feature vectors with high accuracy yet has a small number of network layers and parameters.[8) By simulating the important layers and parameters of a sophisticated model, we succeeded in generating a highly accurate and lightweight facial feature extraction model that is about 1/10 the model size and approximately 5 times faster in processing speed while maintaining the same authentication accuracy.

2) Feature value binarization technology

Usually, the feature value obtained by deep learning is a floating point vector, and similarity is calculated by calculating the distance between the relevant vectors. Although the processing load of a single comparison operation is small, when processing 1 million people, the processing must be performed 1 million times, so total processing time of several tens of seconds to several minutes is required.

To shorten this processing time, we have developed

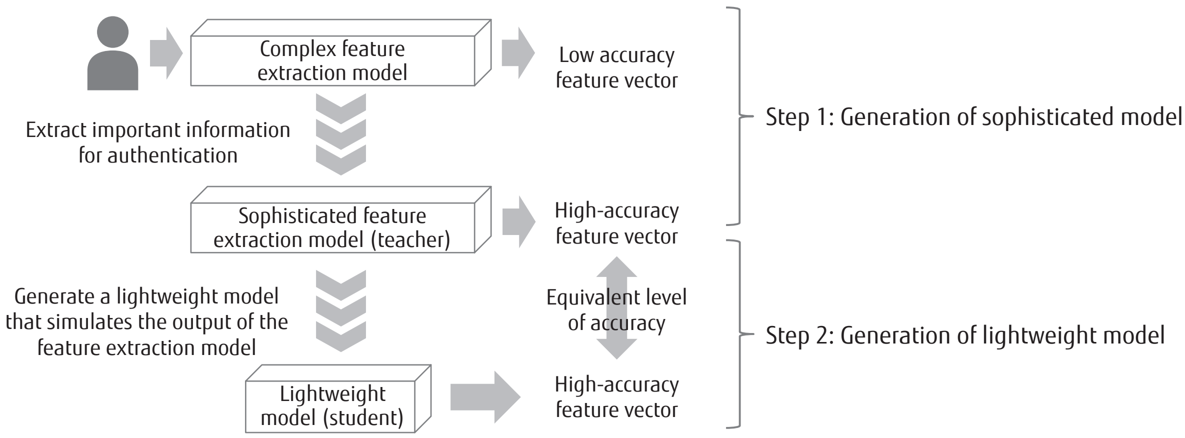

Figure 4
Facial feature extraction technology using distillation technology.

binarization technology that converts floating point vectors into binary value vectors represented by 0 or 1. Specifically, we took technology[9] developed by Fujitsu Laboratories in 2013 to extract and match a 2,048-bit binary string from palm veins, and applied it to facial images. This makes it possible to replace the comparison operation with the hamming distance calculation, which is easier to calculate, and even in the case of one million people, the comparison operation can be realized in about 1 second.

4. Usage scenarios

This section describes usage scenarios other than ID-less payment, picked out from various envisioned usage scenarios.

The technology introduced in Section 3 has made it possible to process payments using only biometric authentication in real time, even in a million-user scale system, without requiring users to input information such as IDs. Since facial data can be acquired even during terminal operation, for example, without the user needing to be aware of face recognition, the only action for authentication to be performed by the user is to simply hover the palm over the sensor. An additional advantage is that since both palm vein and facial data can be acquired without touching the sensor, it is easy to keep the sensor clean and this reduces user resistance. **Figure 5** shows usage scenarios for ID-less authentication that take advantage of these features.

At the entrance of venues such as concerts and sporting events, theme parks, and movie theaters, users need to present a paper ticket or an electronic ticket displayed on their smartphones. Use of this technology makes it possible to identify whether or not persons entering or leaving the site are ticket holders without checking tickets. Specifically, biometric information is registered at the time of ticket purchase. On the day of the event, the system automatically acquires facial data with a camera at the entrance of the venue and narrows down the candidates from the list of preregistered persons. Furthermore, the target user is authenticated from those narrowed-down candidates by hovering the palm of his or her hand over the sensor at the entrance gate. As a result, users can enter and exit smoothly without having to worry about ticket presentation or loss.

This technology registers and links biometric information and personal information in advance, so that the identity of persons can be confirmed using biometric information alone. This could be particularly useful in the case of an emergency such as a disaster, by allowing easy identification of individuals even if they do not carry an ID such as a driver's license or passport. Thus, this technology could be used for example for survival confirmation and to record the distribution of supplies,

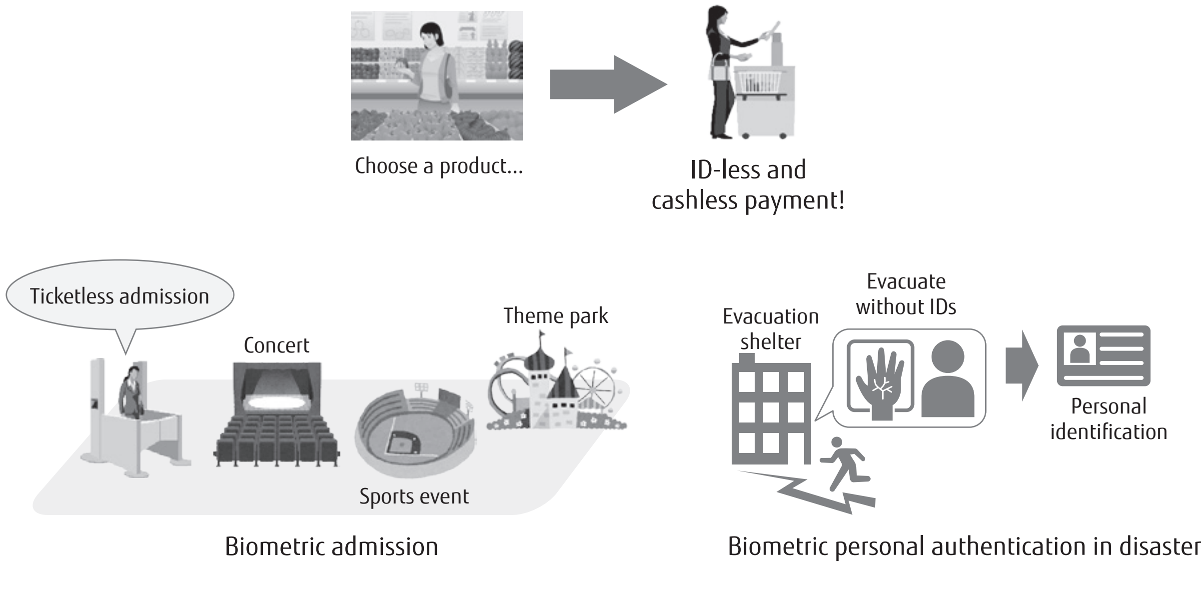

Figure 5
Examples of ID-less authentication usage scenarios.

thereby contributing to efforts for swift recovery.

5. Conclusion

This paper introduced integrated biometric authentication technology for personal authentication on a scale of one million users using only palm vein and facial data. This technology enables ID-less payment not requiring users to present things such as credit cards and phones.

It also realizes simple, high-speed and high-accuracy authentication without burdening the user. Further, since input is possible without touching the sensor, it is easy to maintain cleanliness, making this technology easy to introduce in large-scale systems.

Future issues for practical application include the establishment of operational procedures in accordance with applicable laws and regulations such as the Amended Act on the Protection of Personal Information, and the selection of an organization that provides guarantees in the event of unauthorized payment due to system failure. We aim to carry out demonstration tests and put this technology into practical use in FY2020 to promote the realization of a more safe, secure, and convenient cashless society.

References

1) Ministry of Economy, Trade and Industry in Japan: Current status of cashless payment and future initiatives (May 2018) (in Japanese).
https://www.kantei.go.jp/jp/singi/it2/senmon/dai14/siryou2-1.pdf
2) Fujitsu Laboratories: Fujitsu Develops Non-contact Biometric Integration Technology as an Optimal Solution for a Cashless Society.
https://www.fujitsu.com/global/about/resources/news/press-releases/2018/1004-01.html
3) FIDO Alliance.
https://fidoalliance.org/
4) Panasonic, Liquid: Launch of demonstration experiment of unmanned sales showcase using biometric authentication and RFID (in Japanese).
https://news.panasonic.com/jp/press/data/2019/02/jn190201-1/jn190201-1.html
5) Fujitsu Frontech: PalmSecure-F Pro (in Japanese).
https://www.fujitsu.com/jp/group/frontech/solutions/business-technology/security/palmsecure/f-pro/
6) KDDI Research, Hitachi: Realization of safe and secure biometric-enabled payment with palm and face without use of dedicated devices (in Japanese).
https://www.kddi-research.jp/newsrelease/2018/101101.html
7) ImageNet Large Scale Visual Recognition Challenge (ILSVRC) 2017.
http://image-net.org/challenges/talks_2017/ILSVRC2017_overview.pdf
8) M. Wang et al.: Discover the Effective Strategy for Face Recognition Model Compression by Improved Knowledge Distillation. 2018 25th IEEE International Conference on Image Processing (ICIP), (2018).
https://ieeexplore.ieee.org/document/8451808
9) Fujitsu Laboratories: Fujitsu Develops World's First Authentication Technology to Extract and Match 2,048-bit Feature Codes from Palm Vein Images.
https://www.fujitsu.com/global/about/resources/news/press-releases/2013/0805-01.html

Narishige Abe
Fujitsu Laboratories Ltd.
Mr. Abe is currently engaged in research and development of biometric authentication technology.

Hajime Nada
Fujitsu Laboratories Ltd.
Mr. Nada is currently engaged in research and development of biometric authentication technology.

Tomoaki Matsunami
Fujitsu Laboratories Ltd.
Mr. Matsunami is currently engaged in research and development of biometric authentication technology.

Hidetsugu Uchida
Fujitsu Laboratories Ltd.
Dr. Uchida is currently engaged in research and development of biometric authentication technology.