Biometric Authentication Technology Facilitating Protection and Management of Biometric Data

● Shigefumi Yamada ● Takahiro Aoki ● Takeshi Shimoyama ● Shigehisa Mori

Recently, amendments to laws such as the Amended Act on the Protection of Personal Information (implemented in May 2017) in Japan and the General Data Protection Regulation in the EU (GDPR, implemented in May 2018) have been increasing the need for safe management of personal data, with biometric data used for biometric authentication also falling under this scope. In utilizing biometric data, biometric data protection technology that allows for the easy handling of data while strengthening biometric data protections is attracting attention. However, there is a problem with this technology, with it difficult to achieve both security against biometric data leaks and accuracy in the provided biometric authentication. To deal with this issue, Fujitsu Laboratories has taken advantage of its palm vein authentication technology, one of its strength, to develop a biometric data protection technology that is robust against vein pattern deformation. This technology facilitates the protection and management of biometric data and is expected to contribute to the expansion of personal authentication services that make use of hands-free authentication, which requires centralized management of biometric data in the system instead of the need for entering IDs. This paper presents an overview of Fujitsu Laboratories' proprietary biometric data protection technology and examples of use of palm vein authentication technology and hands-free authentication.

1. Introduction

Recently, use of biometric authentication has become more widespread and the technology is in use in many different fields, such as various types of settlement, ATM transactions, immigration control, logins to PCs, and single sign-on (SSO). In Japan, feature data for registration and matching used for this biometric authentication have been clearly defined as personal data (Individual Identification Codes) under the Amended Act on the Protection of Personal Information enforced in May 2017 and require consideration when handling. In Europe, the General Data Protection Regulation (GDPR),[1] which went into effect in May 2018, is intended to protect personal data, including biometric data. In response to the enforcement of these laws, biometric data protection technology, which utilizes biometric data while strengthening the protections, is attracting attention.[2] With the ISO/IEC JTC 1/SC 37 (Biometrics), which internationally standardizes biometric technologies, a new standard has been established in the form of ISO/IEC 30136 for testing biometric data protection technologies.[3]

Against this backdrop, Fujitsu Laboratories has developed a palm vein authentication technology that strengthens the protections of the biometric data. This technology facilitates the protection and management of biometric data, allowing the burden and risk involved in the centralized management of biometric data in the system to be reduced. This raises expectations for contribution of the technology to the diffusion of identity authentication services based on hands-free authentication that can be used without the need for smartphones or cards.

This paper first describes Fujitsu Laboratories' proprietary biometric data protection technology for facilitating the protection of biometric data. Then, as applications of the technology, it presents examples of the utilization of identity authentication solutions making use of palm vain authentication such as hands-free authentication, which is becoming increasingly widespread because of its convenience as society is going increasingly cardless and cashless.

2. Needs of biometric data protection

As use of biometric authentication becomes increasingly widespread, the needs are increasing for safer and more secure handling of biometric data in authentication systems. System providers usually manage biometric data safely through measures such as encryption. On the other hand, as biometric authentication algorithms become more popular, any unlikely leakage of registration data in a system that uses the same biometric authentication algorithm poses a concern for the impact on the other systems.

From the viewpoint of users, the diffusion of biometric authentication allows it to be used in various other places, which in turn improves convenience. At the same time, the registration of personal biometric data in various systems may create feelings of anxiety. Accordingly, we expect biometric authentication to become available with more security and safety to both system providers and users.

In this context, biometric data protection technology is proposed as biometric authentication technology intended for handling biometric data with more security and safety.[4] The following four ideas can be considered requirements for safety and performance of biometric data protection.

- Requirement 1: Irreversibility

It is impossible to analogize the original biometric data from the feature data generated for registration and matching.

- Requirement 2: Un-likability

To safeguard the privacy of users, it is impossible to make use of feature data used in a system to match feature data in another biometric authentication system.

- Requirement 3: Diversity (renewability)

Different feature data can be generated from the same biometric data. Leaked feature data can be disabled and new feature data can be re-registered.

- Requirement 4: Performance

In satisfying the above conditions, authentication accuracy and processing performance as biometric authentication are not degraded.

In the R&D of biometric data protection technology, "cancelable biometrics," introduced by Ratha et al. of IBM in the U.S. in 2001, is well known. It allows multiple types of feature data for registration and matching to be generated from one piece of biometric data.[5] In Europe, the TrUsted Revocable Biometric IdeNtitiEs (TURBINE) research project for the R&D of biometric data protection technology was conducted from 2007 to 2010 in the framework of a European FP7 project.

While many biometric data protection technologies have been proposed, practical technologies are limited to those that use fingerprints and finger veins.[6),7)] Many of the technologies developed assume binary codes consisting of 0 and 1 as the feature data to be protected. Though the patterns of biometric data themselves are unchangeable through life, biometric data acquired through sensors may see fluctuations for reasons such as deformation and the inclusion of noise. Therefore, binary codes extracted from biometric data never match perfectly. In comparison with existing authentication algorithms based on pattern matching, which evaluate the degree of coincidence by image pattern comparison, the effect of fluctuations in biometric data on the authentication accuracy is more significant with authentication algorithms that use binary codes. The improvement of authentication accuracy poses an issue for practical application.

3. Fujitsu Laboratories' proprietary biometric data protection technology

As an authentication technology to support a connected society, Fujitsu Laboratories has worked on the R&D of biometric data protection technology facilitating the protection of biometric data. By combining palm vein authentication, Fujitsu's strength, with encryption technology, we have realized a new palm vein authentication technology that allows for the following:

- the registration and matching of vein data as they remain encrypted (requirement 1 of the previous section)
- the generation of different feature data for registration and matching from one palm (requirements 2 and 3)
- the provision of authentication accuracy and processing performance equivalent to those of conventional product technology (requirement 4)

We have developed a technique for extracting feature data as binary codes represented by 0 and 1 from palm vein images and a biometric data protection function that makes use of existing cryptography so that patterns of biometric data can be matched by using existing encryption technology.

The following describes the features of this technology.

3.1 Stable codes generated from fluctuating palm vein patterns

We have developed a binary feature data generation technology that absorbs fluctuations in palm vein images acquired using a vein sensor. It is based on a palm vein authentication technology with the world's highest-level authentication accuracy—a false rejection rate of 0.01% (including a single retry attempt) and a false acceptance rate of less than 0.00001%.

The procedure for generating binary feature data based on palm vein images is shown in **Figure 1**. First, the rounding of the palm (three-dimensional deformation) is fit to a quadratic surface, which is spread out to fit a plane and corrected to normalize the image. This allows the inclination and rounding of the palm to be corrected. Next, the normalized palm vein image is subjected to vein extraction. A current product technology is used to detect multiple characteristic regions of the palm vein. Then, feature components are identified from each region and converted into binary codes.

When these processes are performed, the reproducibility of the generated binary codes can be improved by excluding the regions where the feature components have low reliability. Finally, binary codes generated from multiple regions are put together as binary feature data. The encryption process, which will be described later, is then applied to these binary codes. In the matching process, partial deformation can be absorbed by associating and comparing multiple binary codes obtained in registration and matching processes respectively.

The effects of deformation in the palm can be reduced and high authentication accuracy can be achieved with the above technology.

3.2 Realization of biometric data protection

We have realized a process for encrypting registration and matching data based on auxiliary information (equivalent to the seed of an encryption key) at the time of their generation by using the existing encryption technology. We have also realized a matching process through a comparison operation (Hamming distance) of codes as they remain encrypted with existing encryption technology (**Figure 2**). The generation of multiple different encryption feature data from the same biometric data has now been made possible by switching the auxiliary information to be input as the seed of an encryption key for every authentication system {**Figure 3 (a)**}.

Even with encrypted feature data for the same person from other systems, they cannot be authenticated even if they are matched because they are encrypted with different auxiliary information. Furthermore, even in the event of data leakage, all of the registered data stored in the authentication system will be converted by collectively switching the auxiliary information {**Figure 3 (b)**}. Even if leaked data are used for spoofing, they will not be authenticated. In this way, eliminating the need for re-registration by users allows for continued, seamless operation of a large-scale authentication system where many use hands-free authentication.

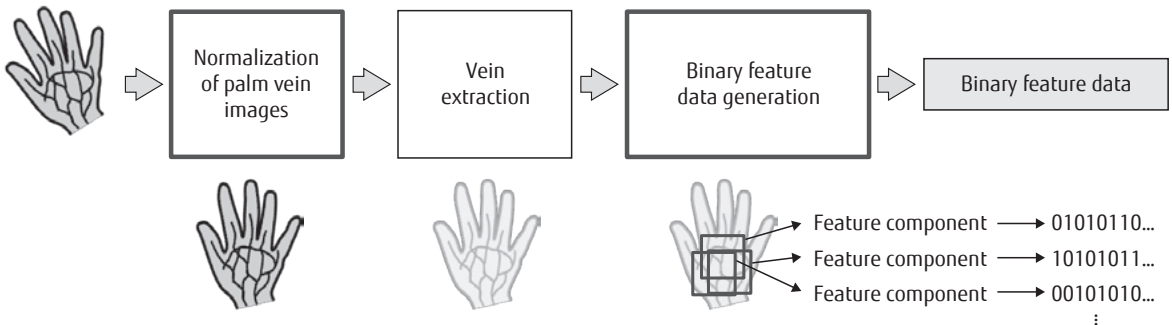

Figure 1
Binary feature data generation.

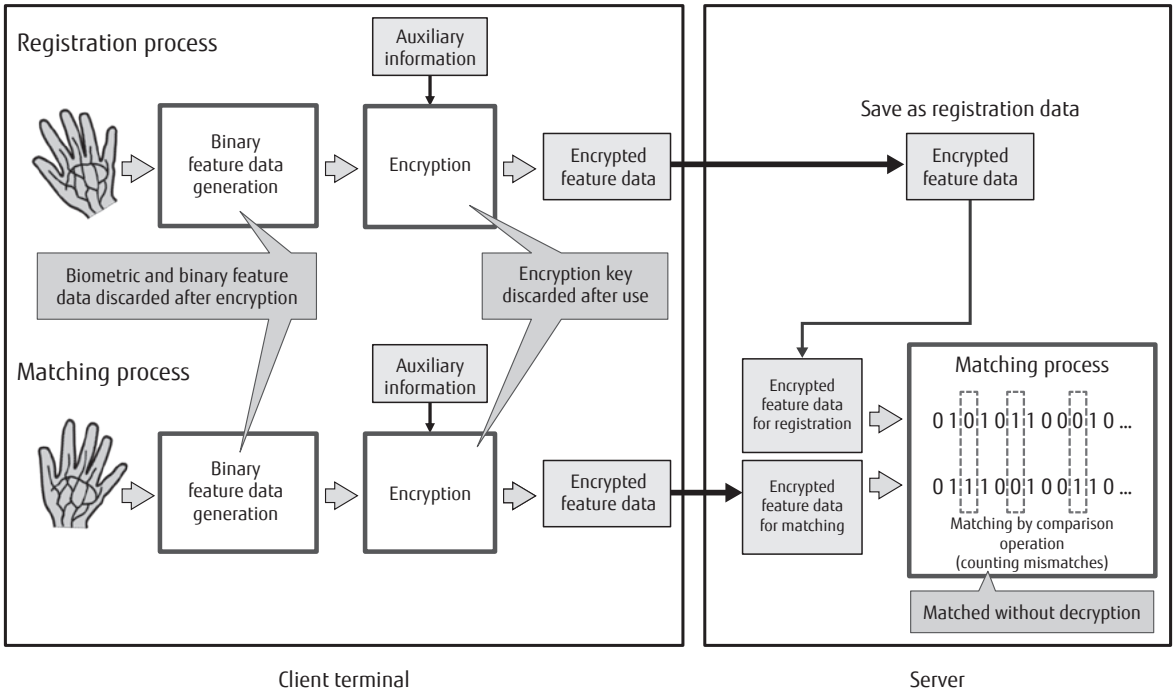

Figure 2
Biometric data protection mechanism.

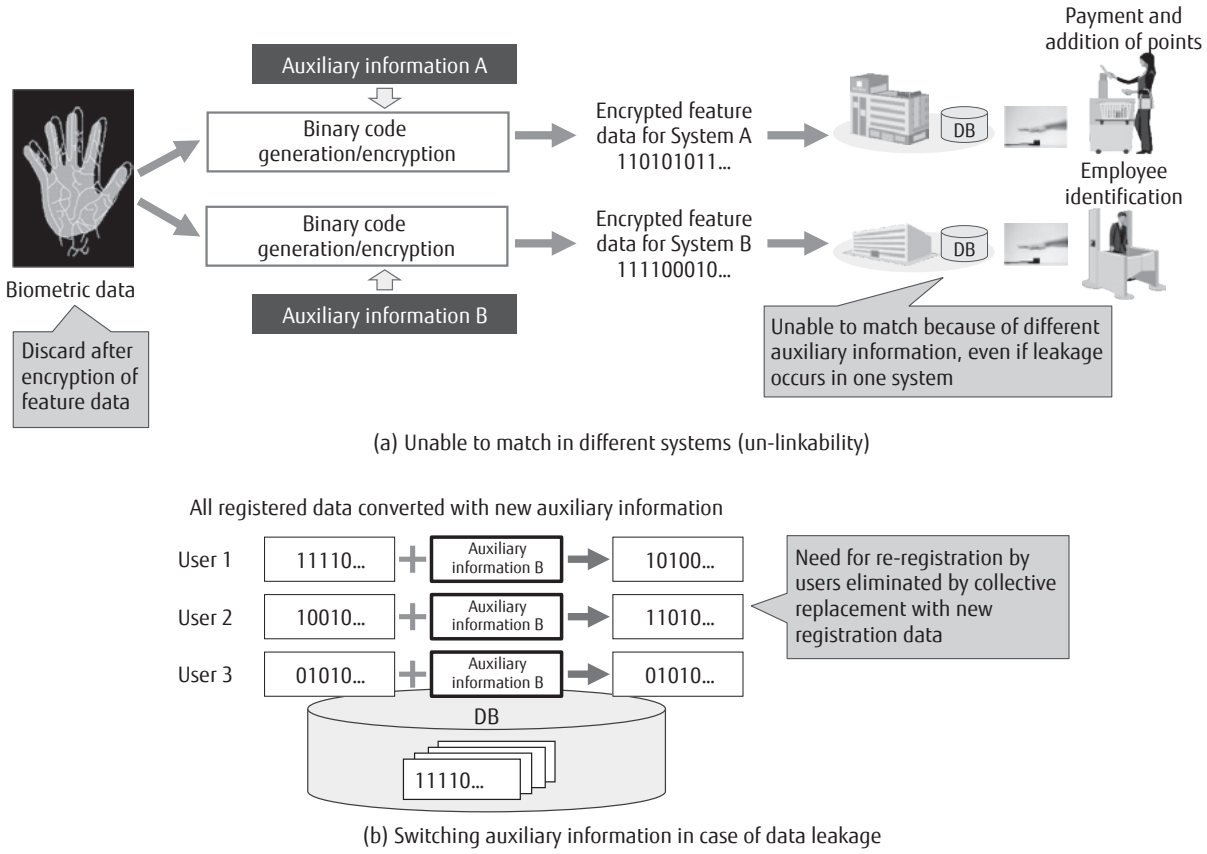

Figure 3
Effect of biometric data protection.

4. Examples of identity authentication solutions using palm vein authentication

This section introduces examples of ID-less authentication, such as hands-free payment using FUJITSU PalmSecure Palm Vein Authentication Technology.

1) Cardless ATM: Ogaki Kyoritsu Bank[8)]

This is the first case in Japan in which cardless ATMs that use palm vein authentication have been realized, and its operation started in September 2012. At the time of the Great East Japan Earthquake that occurred in 2011, many victims lost their passbooks and cash cards, which rendered them unable to withdraw necessary funds immediately. Ogaki Kyoritsu Bank saw this as an issue to be addressed by the industry and considered a financial service that could be used without the need of any object associating the person with the account such as a passbook and a card as necessary.

Biometric authentication used in conventional ATMs had a role with more focus on the security enhancement of IC cards. In this case, biometric data was stored in IC chips. With cardless ATMs, on the other hand, the vein data are stored and managed in the system, making it possible to identify the person's account and carry out transactions on ATMs even if there is no passbook or card. Because no physical objects, such as a passbook and a card, are required, ATM services can now be continued even in times of disaster or evacuation, which has been impossible until now.

2) Lotte Card/7-Eleven Korea[9)]

This is an example of 7-Eleven Korea launching hands-free shopping "Hand Pay" for Lotte Card members, and its operation started in May 2017. Hand Pay is a highly convenient service that allows for identity authentication and payment via one's own body and telephone number alone without the need for carrying cash, a card, or a smartphone. Since palm vein authentication utilizes biometric data, falsification and spoofing are very difficult. The vein data are registered in the system, making payment across stores possible. An increase in the number of stores accepting Hand Pay will lead to further improvements in convenience.

This technology allows biometric data to be managed easily and is suited for hands-free authentication, which requires centralized management of biometric data in the system. This technology will contribute to more widespread hands-free authentication.

5. Conclusion

This paper described Fujitsu Laboratories' proprietary biometric data protection technology for facilitating the protection of biometric data. It has also presented examples of utilization of identity authentication solutions making use of palm vein authentication such as hands-free authentication, which leads to improved convenience in the form of cardless and cashless payments and so on.

In the future, we intend to study various use cases that make use of this technology for demonstration. Through demonstration, we will improve the authentication accuracy and security functions and in turn enhance peripheral technologies required for system application.

References

1) European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en*
2) International Organization for Standardization (ISO): ISO/IEC 24745:2011: Information technology -- Security techniques -- Biometric information protection. *https://www.iso.org/standard/52946.html*
3) International Organization for Standardization (ISO): ISO/IEC 30136:2018: Information technology -- Performance testing of biometric template protection schemes. *https://www.iso.org/standard/53256.html*
4) A. K. Jain et al.: Biometric Template Security. EURASIP Journal on Advances in Signal Processing, 2008.
5) N. K. Ratha et al.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, pp. 61–634, 2001.
6) Genkey: BioHASH. *https://www.genkey.com/privacy-by-design/*
7) Hitachi Systems, Ltd.: SHIELD PBI Finger Vein Authentication Service. (in Japanese). *https://www.hitachi-systems.com/solution/s0307/pbi/*
8) Fujitsu, Fujitsu Frontech: Fujitsu Builds Japan's First Palm Vein Authentication System for ATMs—First ATMs in Japan that require no passbook or ATM card begin operations at Ogaki Kyoritsu Bank. *https://www.fujitsu.com/global/about/resources/news/press-releases/2012/0926-01.html*

9) Fujitsu: Lotte Card established a highly reliable and user-friendly authentication payment solution with PalmSecure.
https://www.fujitsu.com/global/about/resources/case-studies/cs-2017aug-lottecard.html

Shigefumi Yamada
Fujitsu Laboratories Ltd.
Mr. Yamada is currently engaged in the research and development of biometric authentication technology.

Takahiro Aoki
Fujitsu Laboratories Ltd.
Mr. Aoki is currently engaged in the research and development of biometric authentication technology.

Takeshi Shimoyama
Fujitsu Laboratories Ltd.
Dr. Shimoyama is currently engaged in the research and development of encryption technology.

Shigehisa Mori
Fujitsu Ltd.
Mr. Mori is currently engaged in the sales promotion of palm vein authentication PalmSecure.