

A Proposal of One-Time Biometric Authentication

Yoshifumi Ueshige*

*Institute of Systems & Information Technologies/
KYUSHU
Fukuoka City, Fukuoka Pref., JAPAN

Kouichi Sakurai*+

+The Graduate School of Information Science and
Electrical Engineering, Kyushu University
Fukuoka City, Fukuoka Pref., JAPAN

Abstract - *In biometric authentication, feature information of each enrolled person's biometric information is enrolled as templates. Secure databases or anti-tampered devices store the templates in general. The biometric information, however, is irreplaceable information, when it is compromised. Thereby, one must give a special attention to protection of such information. On the other hands, increasing internet economical services causes a motivation of implementing online biometric authentication. We propose a novel protection technique for the biometric information, especially the feature information and the templates. The point of our proposal is that the extracted features and the enrolled templates are transformed by one-time transformation that is generated in each authentication. The transformed features and templates travel through insecure communication line like the internet, and they are used in matching process. This technique causes security against eavesdropping and replay attacks on the internet, because the transmitted feature information and the templates are different every time.*

Keywords: biometric authentication, one-time, template protection, nonlinear transform, security

1 Introduction

1.1 Background

Biometric authentication is well known with both of knowledge-based authentication like passwords, and possession-based authentication like cards (magnetic cards, IC cards, etc.). Because the biological features (fingerprint, vein, iris, facial image, voice, etc.) are unique for each person, production of the biometric techniques is encouraged. In facts, facilities for finance and immigration authorities [1] have already introduced the biometric authentication in many countries. In addition, some products of personal computers include the biometric authentication systems. The biometrics rapidly prevails in society like this. In these examples, the biometric systems are applied in closed environments, however, there are fervent social demand about the biometric systems applied to the authentication on internet services such as internet banking, electrical government, approval in company, etc.

On the other hands, the biometric system causes some privacy issues. That is, in some cases, significant privacy information like a medical history is compromised from the biometric information which is including biometric raw data acquired from biometric sensor devices, the feature information extracted from the corresponding biometric raw data, and enrolled templates. For example, one can know a person's diabetes from retina data. When biometric authentication system as shown in figure 1 leaks enrolled biometric templates, these templates are unable to re-enroll, because the corresponding biometric data is irreplaceable. This point is seriously different from the same situation of password system and public-key encryption. In the case that encrypted data is transmitted on each line connecting between any processes in figure 1, one needs the management of the encryption (and decryption) keys among the biometric authentication systems. Furthermore, if one biometric authentication system consists of distributed equipments, the cost of the key management becomes expensive. In addition, it is possible for adversaries to perform replay attack by using encrypted biometric information eavesdropped. Therefore, we need to protect the biometric information strictly. In this viewpoint, Ratha et al.[2] and Tulys et al.[3], [4] proposed some protection techniques as biometric template protection techniques. Next subsection, we will briefly introduce them.

1.2 Related Work

We can roughly classify the concepts of template protection into following two categories:

- 1) Geometrical transformation or irreversible mapping transforms the enrolled templates into strained templates separately [2].
- 2) One-way function with helper data transforms the enrolled templates into some corresponding unique parameter [3], [4].

According to the former concept, the biometric templates are blockwise scrambled, or geometrically distorted like morphing as shown in figure 2. In this figure, the number in the cells denotes indices of the sub blocks. The stars in these sub blocks denote the points of features. It is difficult for any adversaries to extract the information of enrolled templates from the transformed templates. Thus, the ref [2] states one can protect the enrolled templates. Because this method, however, causes decrease of the template quality in

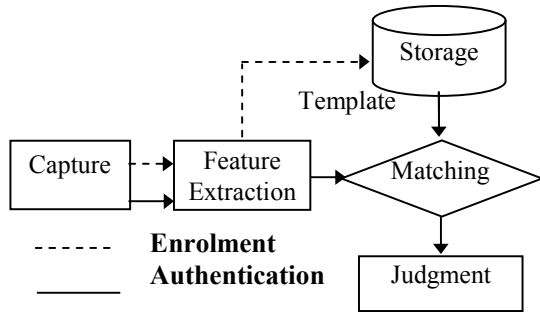


Figure 1. Basic model of biometric authentication system

matching process, we are not able to expect high accuracy of authentication.

In latter one [3], [4], the framework is shown in figure 3. We enroll both of a one-way function $F(\cdot)$ and correction term named helper data W so that the function $F(\cdot)$ generate same values when extracted feature Y for verification are close original templates X . That is, enrollment data consists of $F(\cdot)$, $F(X)$ and W . In verification, a user calculates $F(Y)$ with helper data W . If $F(X)=F(Y)$, the user is authenticated. This scheme has a characteristic, of which X or Y does not directly travel through open networks. Because this scheme is the authentication by using output of $F(\cdot)$ with W , this scheme has no compatibility with popular biometric authentication systems as shown in figure 1. Furthermore, authentication accuracy seems to rely on the value W susceptibly.

1.3 Our contribution

In this paper, we propose a novel compatible scheme with the popular biometric systems. Our main idea is biometric authentication by using one-time characteristics. That is, communicated data of the features and the templates is different every authentication session for even unique person, as shown in one-time password [9]. This scheme has following properties:

- 1) The extracted features and the enrolled templates are transformed by a common nonlinear function, and matching is done by using the transformed features and the transformed templates in order to ensure the one-time feature.
- 2) Our scheme needs no concern about compromising the transformed information in the communication through arbitrary lines, because of changeable authentication data for each authentication session.

In every session, some TTP generates the common function by using an authentication session ID with a time-stamp and some credential. The generating algorithm of the function ensures one-time characteristic of it. In this paper, we suppose the generating algorithm exists, we discuss the privacy protection and the biometric authentication scheme. If this requirement is satisfied, even though eavesdroppers

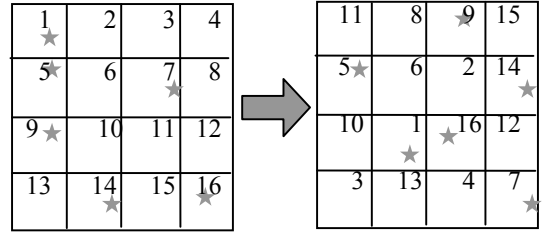


Figure 2. Transform of template by scrambling blockwise

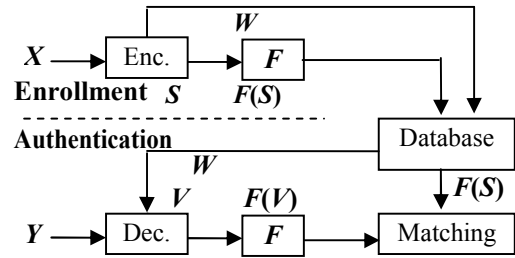


Figure 3. Biometric authentication with one way function and helper data

collect communication data between the biometric authentication processes, they cannot obtain the enrolled templates and the extracted features. When they monitor some person's entire authentication, they obtain only transformed data which has no correlation with other authentication sessions. An authentication server which performs matching process obtain the transformed data that are the transformed template, and the transformed features. We can expect the one-time characteristic of the transform causes high security of biometrics from the view of privacy protection. In this work, we call this transform "one-time transform (OTT)".

In the rest, section 2 describes what information should be protected in the biometric authentication. In section 3, we propose a definition of OTT, consideration of generating OTT, and authentication protocol. Section 4 gives a discussion of security in proposed scheme. Finally, section 5 concludes this paper.

2 Problems in this work

Biometric authentication has two flows of processing, that is, enrollment and authentication. Enrollment process is performed through the broken arrow lines in figure 1. Sensor device acquires a user's biometric raw data. Next step is feature extraction of the biometric raw data. The obtained features are enrolled as templates in the database.

On the other hands, there are authentication processes along straight arrow lines in figure 1. In the authentication, capture process and feature extraction process are in common with enrollment. The matching process performs

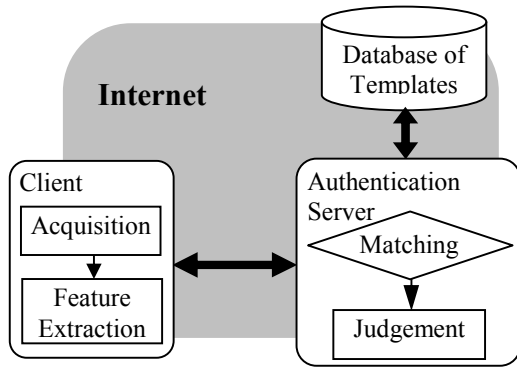


Figure 4. The server authentication model on the internet application

comparison between the extracted features and the enrolled templates. The judgment process evaluates the matching result (matching score) and calls the user accept or reject referring authentication policy.

When we apply this biometric authentication to internet services, we must consider a part or all of the above five processes are included in separate entities distributed in internet. Because the biometrics on the internet services requires communication of the authentication information like the feature information, the template information, the authentication results etc. between the five processes through the internet. Since the internet is not secure against eavesdropping, substitution, and impersonation, we must appreciate that insufficient security for the above information compromises the user's biometric information as one of personal information. Because biometric information is irreplaceable in general, the user is unable to re-enroll to the biometric authentication system [5]. In addition, even if eavesdroppers obtained only encrypted biometric information, their replay attacks can menace the biometric system. Thereby, protection of the biometric information from these risks is one of the significant problems in the biometric authentication as a problem of privacy protection.

In the rest of this paper, we notice protection of the feature information and the template information in the server authentication model as shown in figure 4. This model seems to be a practical implementation as a remote biometric authentication. In this model, we must save the features and the templates as personal information from adversaries.

3 Proposals one-time transform

In this work, we propose the biometric authentication so that information transformed by a changeable common function, OTT is used as communication data on the internet. The OTT is nonlinear function and changes every

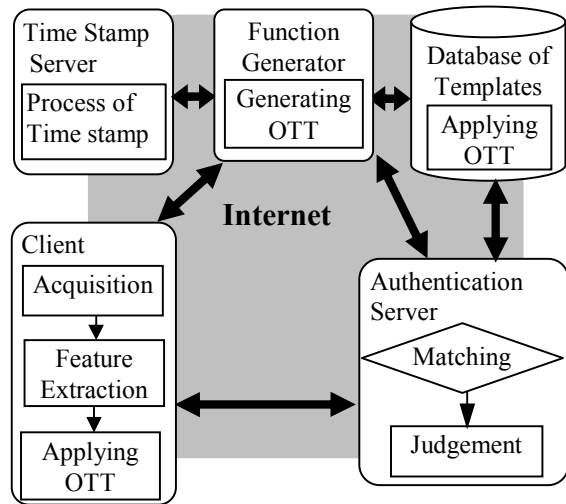


Figure 5. Proposed framework (The sever authentication model)

authentication session in order to prevent prediction of the functions by adversaries. A third trusted party generates the OTTs as shown in figure 5. In this paper, we apply the OTT to the feature information and the template information. Even if our proposal needs new entities for generating the OTTs, it is easy to extend the current popular biometric system because only software of application of OTT is added to the system.

We call our biometric authentication “*one-time biometric authentication (OTBA)*”. Following subsections precisely explain the OTBA in server authentication model.

3.1 Requirements of the authentication system using OTT

For construction of the OTBA system, we suppose five entities which are client, authentication server, database storing templates, function generator of OTT, and time-stamp server as shown in figure 5. In figure 5, the function generator and the time-stamp server are TTP.

Requirement of the function generator is followings: Algorithm and input values for generating the OTT is opened. In order to give time dependency to function generator, the input values are authentication session ID with time-stamp data signed by time-stamp server and secret value of function generator.

3.2 Requirements of the OTT functions

The goals of application of the OTT function are to protect enrolled original templates and to prevent replay attacks by using dishonest acquirement data of transformed information by OTT. For achievement of the goals, the OTTs need to satisfy the following conditions:

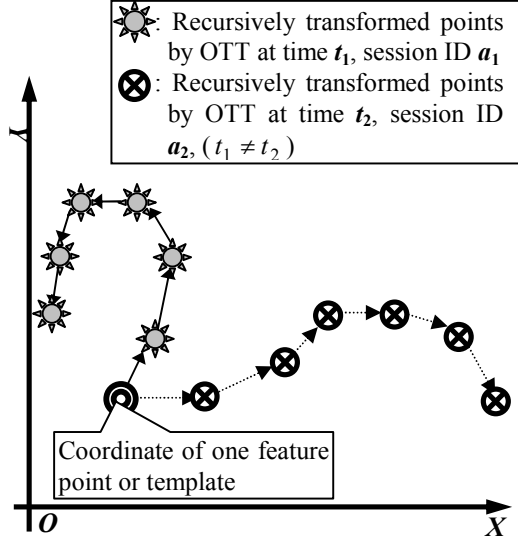


Figure 6 Image of OTT

1) One-to-one function

In the methods [3], and [4], the original templates and features are transformed into a different space which has no direct relationship with a space of these information. Therefore, the method [3] and [4] become low similarity to the current biometric systems. This point receives our attention. In our method, the original templates and features are transformed into same space in order to keep the similarity at the matching process.

2) Difficulty of prediction

It is extremely difficult for any adversary to guess the original templates and features from the transformed information.

3) Preservation of distance

This means that matching process can evaluate the distance between the transformed feature and the corresponding transformed template by using optimal distance function. Because OTTs are nonlinear mapping, OTTs may be contractive or expansile, locally. However, it is necessary to design OTTs so that every OTT transforms relative feature and template into close points.

We anticipate satisfying the above conditions may be difficult. We, however, expect a candidate of the OTTs is chaos mapping such as Henon's mapping:

$$\begin{cases} x_{t+1} = 1 - ax_t^2 + by_y \\ y_{t+1} = x_t \end{cases} \quad (1)$$

Because orbits of points recursively mapped by this function are strongly depend on the parameters a , b , and initial points (see figure 6), we expect the mapped points do not imply the information of initial points if a and b are securely protected. That is, it may be possible to construct the OTTs by generating and protecting the parameters of the OTTs. In addition, if these parameters are changeable at each generation of OTTs, even though adversaries obtain data of the identical user's authentication sessions, the adversaries cannot know even the identity. For example of Henon's mapping, we can represent generating the parameters a and b at function generator as following:

$$\begin{cases} a = f(H_{ID}, t_c, s) \\ b = g(H_{ID}, t_c, s) \end{cases} \quad (2)$$

where H_{ID} , t_c , and s denote hash value of session ID, time from the time-stamp data of the session ID, secret value, respectively. Function f and g need to be one-way functions.

3.3 Protocols of the biometric authentication using one-time transforms

We propose an authentication protocol using OTT. In the rest, (a) - (p) denote numeral notations shown in figure 7.

- 1) Processes from (a) to (c) denote negotiation for beginning the authentication. After these steps, the client and the authentication server share the authentication session ID
- 2) In (d), function generator receives requests of generating OTT with the session ID from both of the client and the authentication server. Process (e) is a verification concerning validity of the authentication session.
- 3) In (f) and (g), the function generator obtains time-stamped data of the above session ID. The time-stamped data is used for a parameter of OTT generation and an evidence of the session performed.
- 4) About process (h), please refer the discussion in subsection 3.1 and 3.2.
- 5) In (i), the function generator sends the generated OTT to both of the client and the database of enrolled templates.
- 6) In order to end the generation process, the function generator sends signal of the end to the authentication server in process (l).
- 7) In (j) and (k), the client and the database apply the OTT to the feature data and the corresponding template data, respectively. Because of common OTT used, the transformed data are used in matching process as is. For example, we can denote formally as following equation:

$$ftr_n = F^{*n}(ftr) \quad (3),$$

where $F(x)$, n , and ftr denote the OTT, the number of iteration, and the coordinate of the features,

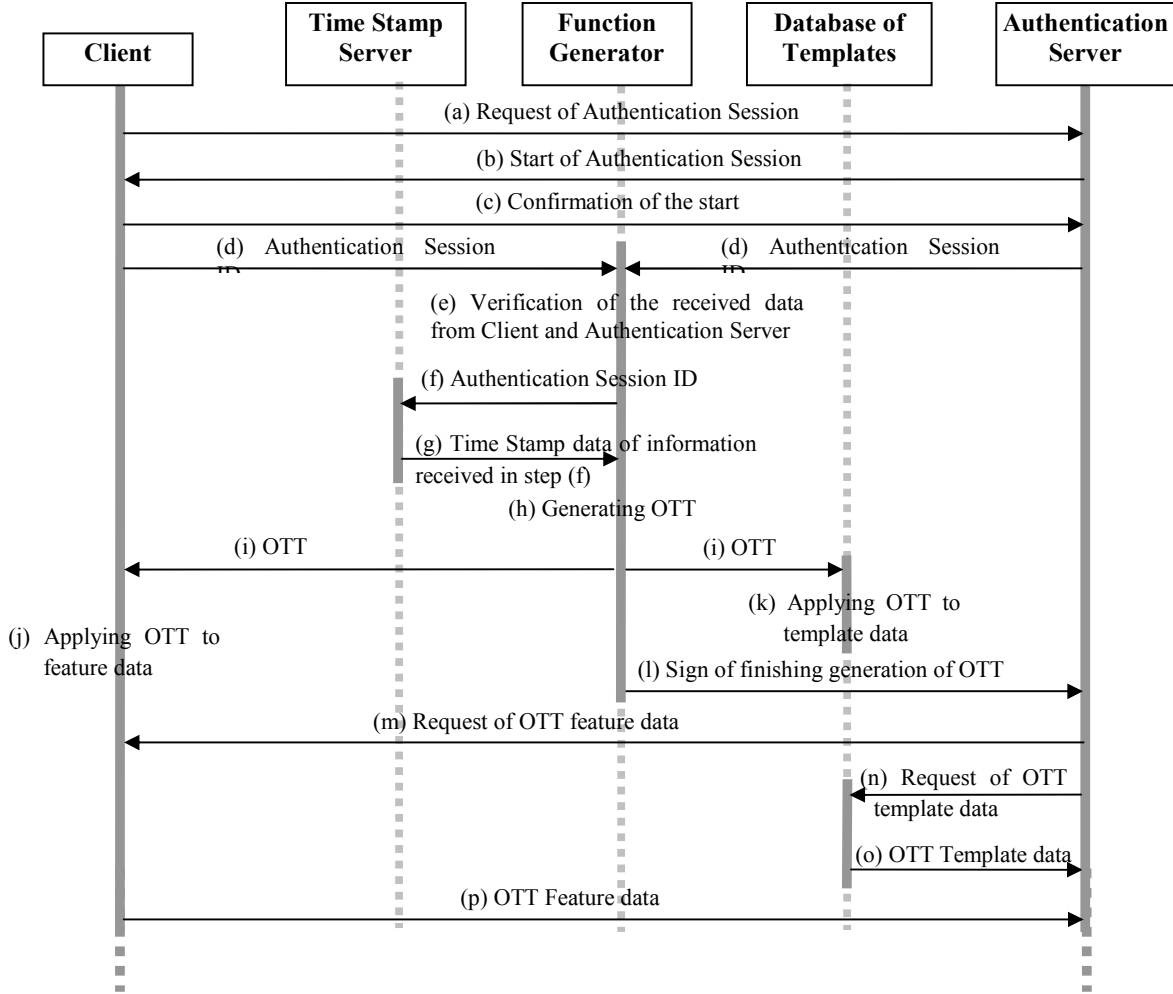


Figure 7. Protocol of starting authentication session to sending one-time transformed features and one-time transformed template

respectively. We can describe the transform of the templates as following:

$$tpl_n = F^{\circ n}(tpl) \quad (4),$$

where tpl denotes the coordinate of the templates.

- 8) In (n)-(q) the authentication server obtains the transformed data of templates and features. After the above protocols finished, the authentication server performs matching process and judgment process.
- 9) In matching process, the authentication server calculates distance between the set of transformed features and one of the transformed templates. For an example of distance function, we can find the Hausdorff distance [6]:

$$H(Tpl_n, Ftr_n) = \max \left\{ \max_{tpl_n \in Tpl_n} \min_{ftr_n \in Ftr_n} \{d(tpl_n, ftr_n)\}, \max_{ftr_n \in Ftr_n} \min_{tpl_n \in Tpl_n} \{d(tpl_n, ftr_n)\} \right\} \quad (5),$$

where Tpl_n, Ftr_n denote the set of OTT templates and one of the OTT features. Function $d(\cdot)$ denotes distance function between two points. We should choose the optimal distance function depending upon OTT.

- 10) The authentication server calculates the matching score based on $H(Tpl_n, Ftr_n)$. In judgment process, the authentication server decides accept or reject by comparing $H(Tpl_n, Ftr_n)$ with the corresponding threshold.

4 Argument of Security of OTBA

We discuss the security of the above proposal. First, we mention the security of the framework of the OTBA. If adversaries success to steal this value s stored in the function generator, they can become impostor of the function generator. After that, the function generator loses trust from other entities in figure 5. However, even if adversaries hijack the function generator, because it receives no personal information, of course including the

original template and the extracted feature, the takeover does not threaten the user's privacy. Then we consider the case of a malicious authentication server collects information. In this framework, it receives transformed features and templates. As aforementioned, they imply no information before transform. Furthermore, the malicious sever cannot know the corresponding OTT. Hence, the malicious server obtains no information about original templates and extracted features.

Next, we consider security of the information transformed by OTT against hill-climbing attack [7], [8], replay attack, collusion attack. Hill-climbing attack uses of replied matching score in order to make a fake. When the application server sends the matching score to client (adversary) in figure 5, the adversary transforms feature data selected from database which the adversary constructs. The adversary sends the transformed features to the authentication server. Because this system changes the calculation algorithm of matching score and threshold for it according to selected distance function $d(\cdot)$, it is difficult for the adversary to improve the fake from the replied matching score. Therefore, the probability of the adversary's success on the OTBA becomes less than conventional biometric authentication like figure 4.

In general, replay attack is impossible, if previously obtained information is not reusable. When adversaries eavesdrop on the communication between the client and the authentication server, they obtain only transformed features which are not reusable. Hence, no adversary successes replay attack on the OTBA. If the adversaries can listen to the communication from the function generator, they obtain the information of OTT. When they reuse this information, the client and the database can detect replay attack by verifying the difference among the information of OTT used in former authentication sessions.

Two cases of collusion attack establish possibly. The one of case is that the client conspires with the function generator. In this case, the client can obtain not only OTT but also information of evaluation function. Hence, adversaries who can perform normal hill-climbing attack success the collusion attack. The other one is that the authentication server stands in with the function generator. The manner of attack is same as the above one.

5 Conclusions

In this paper, we pointed out the problems of the current studies of the template protection. As a countermeasure, we proposed the OTBA to protect the biometric templates and the extracted features. The main concept of the OTBA is that stolen biometric information is not reusable by changeable transform, OTT every authentication for even same person. We described recursive transform as a candidate of OTT. As a result, we obtained the view of the security of the OTBA against hill-climbing attack and replay attack during the function generator keeps security.

This paper described only concept of the OTBA. As future works, we should study optimal function of the OTTs, and practical generating algorithm of the OTTs. In addition, we should research formal analysis of information theoretic security and time of calculation in the OTBA.

Acknowledgement

This research was supported by Strategic International Cooperative Program, Japan Science and Technology Agency (JST).

References

- [1] ISO/JTC1/SC17/WG3/TF1 for ICAO-NTWG, "Supplement 9303", International Civil Aviation Organization (ICAO), 2005. (URL: http://www.icao.int/mrtd/download/documents/FTT_Supplement%20to%20Doc%209303.pdf)
- [2] N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing Security and Privacy in Biometric-based Authentication Systems", IBM Systems Journal, Vol. 40, No. 3, pp. 614-634, 2001.
- [3] P. Tuyls, J. Goseling, "Capacity and Example of Template-Protecting Biometric Authentication Systems", ECCV Workshop BioAW, no. 77, pp. 158-170, 2004.
- [4] J.-P. Linnartz, P. Tuyls "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates", AVBPA 2003, pp. 393-402, 2003.
- [5] P. Reid, "Biometrics for Network Security", Prentice Hall, 2004.
- [6] M. F. Barnsley, "Fractals Everywhere second edition", Academic Press Professional, 1993.
- [7] C. Soutar, "Biometric System Security", Secure No. 5, pp. 46-49, 2002 (URL: http://www.silicontrust.com/pdf/secure_5/46_techno_4.pdf)
- [8] A. Dimovski, D. Gilgoroski, "Generating highly nonlinear Boolean function using a genetic algorithm", 1st Balkan Conference on Informatics, 2003
- [9] PKCS #11 v2.20 Amendment 1, "PKCS #11 mechanisms for One-Time Password Tokens", RSA Security Inc. (URL: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20a1.pdf>)