Security and Efficiency of Biometric Template Protection for Identification

Wataru Nakamura,* Yosuke Kaga,* Masakazu Fujio,* and Kenta Takahashi*
* Research & Development Group, Hitachi Ltd., Japan
E-mail: {wataru.nakamura.va, yosuke.kaga.dc, masakazu.fujio.kz, kenta.takahashi.bw}@hitachi.com

***Abstract*—The Biometric Template Protection (BTP) Technology includes Cancelable Biometrics(CB), Biometric Cryptosystem (BC), and Biometric Signature (BS). CB schemes cannot satisfy security requirements on irreversibility and spoofing difficulty if enrolled data leak from multiple entities. On the other hand, it is considered that well-implemented BC schemes such as fuzzy extractor or BS schemes such as fuzzy signature satisfy the security requirements. However, when these schemes are naively applied to identification, computation and communication cost increases. In this paper, we define efficiency requirements based on computation and communication cost for Biometric Template Protection for Identification (BTPI). Then, we show that BTPI schemes based on conventional BTP schemes cannot satisfy requirements on security and efficiency simultaneously. Next, we propose a novel BTPI scheme obtained by combining fast CB and secure BC or BS. The proposed scheme achieves both requirements under certain assumptions on the publicity of biometric features used for the proposed scheme.**

I. Introduction

As fintech market expands and ICT for governmental and medical services grows, online user authentication becomes more and more important. As a technology which enables reliable and convenient user authentication, biometrics has attracted attention. A general online biometric authentication system generates a biometric template from biometric feature acquired by the enrollment client, and stores the template in the authentication server. During the authentication, the authentication client acquires the biometric feature once more, and the authentication server performs a matching process.

In biometrics, it is necessary to minimize the risk of biometric feature leakage. This is because biometric features such as fingerprints and veins cannot be changed for life. In addition, a leak might lead to a spoofing risk by physically creating fake biometric features or electronically altering information transmitted from the authentication client. Therefore, biometric features must not be accessible by an attacker.

An approach to prevent biometric feature leakage is the Biometric Template Protection (BTP) technology, which protects biometric features by algorithms without requiring a special tamper-resistant region. Research and international standardization of BTP is actively conducted. International standard ISO30136 [1] on performance evaluation indices of BTP technology defines the BTP process model as Figure 1. During the enrollment, the system generates a pair of auxiliary data[1] AD and pseudonymous identity[2] PI, and stores (AD, PI) in association with the user ID. During the authentication, the system generates PI^* from AD and the biometric feature acquired once more (this process is called PIR), and verifies the user by matching PI with PI^* (this process is called PIC).

The BTP technology includes Cancelable Biometrics (CB) [2] schemes such as Correlation Invariant Random Filtering (CIRF) [3], Biometric Cryptosystem (BC) [4] schemes such as Fuzzy Extractor (FE) [5], and Biometric Signature (BS) schemes such as Fuzzy Signature (FS) [6] [7]. In CB schemes, if both AD and PI leak, the original biometric feature can be restored, and it can lead to spoofing attacks. On the other hand, it is considered that when implementing appropriately BC schemes such as FE or BS schemes such as FS, the biometric feature cannot be restored and spoofing is difficult even if both of AD and PI leak. Therefore, it is desirable to use BC or BS schemes to achieve higher security.

Here, biometric authentication is classified into 1:1 authentication and 1:N authentication (identification). In 1:1 authentication, the user ID is used together with the biometric feature during the authentication, and the system matches the biometric template of the input user ID. On the other hand, in 1:N authentication, only the biometric feature is inputted, and the system identifies the user among N enrolled users. For the application to hands-free payment or national ID systems, 1:N authentication is preferred for the convenience of users.

Consider BTP for Identification (BTPI). For stronger security, it is desirable to apply BC or BS schemes for identification. However, if the number N of enrolled users increases, the following problems on the amount of calculation or communication occur. When applying BC schemes to identification, Takahashi et al. [8] points out that in order to satisfy the security requirements, PIR processes for all enrolled users have to be done in the authentication client, but it requires calculation capabilities proportional to N in the authentication client and communication capabilities proportional to N between the authentication client and the servers. Generally, the calculation resource of the authentication client and the communication resource are limited, so when N is large, the identification process in an acceptable time becomes difficult. On the other

[1]Auxiliary Data (AD) is the information used for generating PI from biometric feature.

[2]Pseudonymous Identity (PI) is the identification information in which biometric feature is concealed so that it is difficult to reverse.

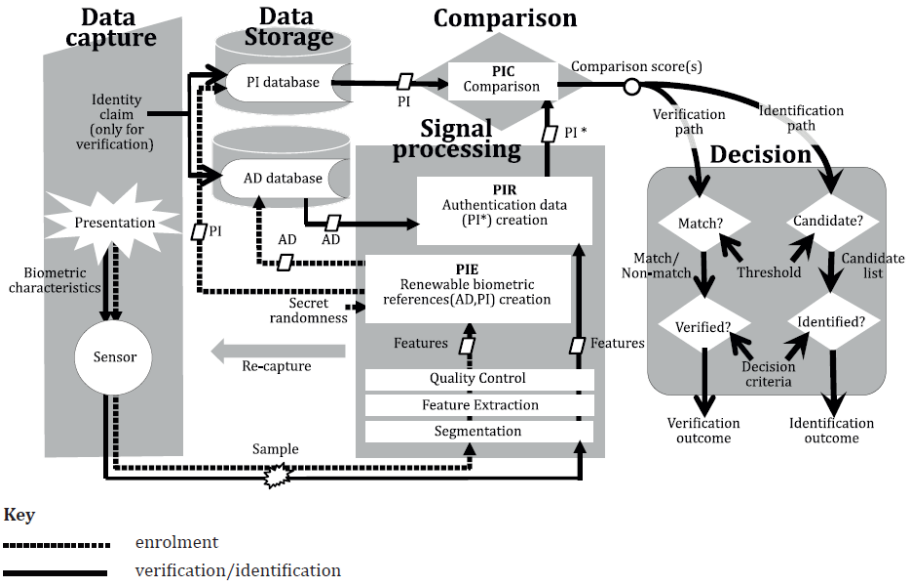

Fig. 1. BTP process model [1].

hand, when applying BS schemes to identification, the heavy process of N times PIC becomes a problem. Indeed, in currently known 1:1 BS schemes such as ones in [6][7], the PIC process includes an exponentiation calculation on a large order finite field, which takes much more computation time than a normal matching process. Therefore, if these 1:1 BS schemes are applied to identification for large-scale N, it is difficult to perform the identification in a realistic time even though N times PIC can be performed at the authentication server.

In this paper, we aim at constructing a BTPI scheme which is as secure as BC and BS and solves the problem on the amount of required calculation and communication. First, we define efficiency requirements[3] based on the amount of calculation and communication needed. Then, we evaluate BTPI schemes obtained by naively applying conventional BTP schemes to identification from security and efficiency requirements. Security requires irreversibility and resistance against spoofing attacks[4]. We show that these schemes do not satisfy all requirements. Next, we propose a novel BTPI scheme obtained by combining CB, which is fast for identification, and either of BC or BS, which has higher security. The proposed scheme achieves both security and efficiency requirements under certain assumptions on the publicity of biometric features used for the proposed scheme.

The rest of this paper is organized as follows. In Section II, we define the BTPI system model, assumptions, and requirements. In Section III, we evaluate BTPI schemes obtained by naively applying conventional BTP schemes to identification. In Section IV, we propose a novel BTPI scheme. In Section V, we conclude this paper.

II. System Model and Requirements

In this section, we describe the BTPI system model, assumptions on entities and requirements.

A. BTPI System Model

We consider a biometric identification system in which an enrollment client, multiple authentication clients[5], an authentication server, and an auxiliary server[6] are connected to the network (Figure 2). Also, we assume that N users $u_1, u_2, \ldots, u_N$ are enrolled to the system, and for a user u_i ($i \in \{1, \ldots, N\}$), we call i the user ID.

During the enrollment for the user u_i ($i \in \{1, \ldots, N\}$), the enrollment client acquires the biometric feature X_i. Then, the process by the enrollment client, the authentication server, and the auxiliary server with communication among them generates (AD_i, PI_i)[7]. AD_i is stored in the auxiliary server, and PI_i is stored in the authentication server.

During the identification, an authentication client acquires the biometric feature X' from an enrolled user. Then, the process by the authentication client, authentication server, and the auxiliary server with communication among them identi-

[3]Efficiency requirements are originally defined in [8]. However, in [8], the amount of calculation is considered only for an authentication client. We define efficiency requirements for not only calculation on the authentication client and communication but also calculation on the servers.

[4]Although resistance against spoofing attacks is not included in security requirements in ISO30136, we think it is an important requirement, so we include it in the security requirements.

[5]The assumption that the system has multiple authentication clients is appropriate, for example, in the case of a hands-free payment system in which POS (Point of Sales) terminals are installed in multiple stores.

[6]For some BTP schemes such as CIRF[3], if both of AD and PI leak, the original biometric feature can be restored. Therefore, it is desirable to store AD and PI in different servers as [10, Section 1.5]. Considering this, we assume that the BTPI system has two servers.

[7]$AD_1, \ldots, AD_N$ may be equal as in CB.

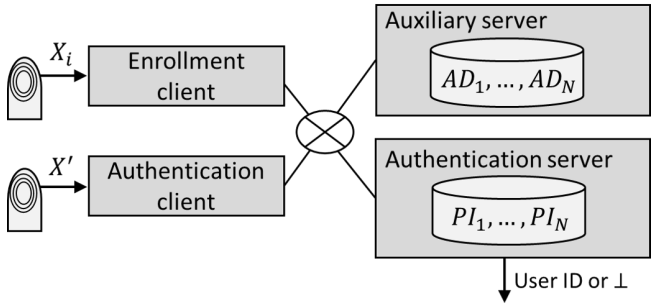

Fig. 2. BTPI System Configuration

fies the user[8]. If the identification process has succeeded, the authentication server outputs the identified user ID. Otherwise, it outputs a special symbol $\perp$ which represents the failure of identification.

We classify the information used for identification processes at each entity into the following two.

- *Static information*: information generated during the enrollment and stored in the entity.
- *Dynamic information*: information which appears in memory temporarily during an enrollment or identification process and is discarded at the end of the process. Note that information communicated with other entities is included in dynamic information.

B. Assumptions

We make the following assumptions (A)–(E).

(A) Prior to an enrollment or identification process, the entities mutually perform equipment certification. Because of this, the risk that an attacker fraudulently installs an entity and performs enrollment or identification process is sufficiently low. In addition, communication between the entities is independently encrypted by SSL etc., so the risk that attackers acquire communication information by sniffing attack is sufficiently low.

(B) The enrollment client is operated safely, meaning the risk that the program is tampered with, leading to dynamic information leak when an enrollment process is performed, is sufficiently low.

(C) The authentication client does not have static information. We make this assumption because otherwise, multiple authentication clients would need to keep static information of all users (or common to all users). This would lead to the high cost of management such as addition, deletion, and update, and would increase the risk of leakage of the static information.

(D) Authentication clients do *not* have a tamper-resistant[9] region, but are tamper-evident[10]. Therefore, in order to spoof an authorized user, an attacker may modify the program of an authentication client and execute an unauthorized identification process. Also, the attacker may obtain dynamic information during the unauthorized identification process. On the other hand, due to tamper-evidence, authorized users can check whether the program has been modified in an unauthorized way before an identification. Therefore, the risk of dynamic information leak from the authentication client during an identification by an authorized user (e.g., biometric feature of an authorized user, secret key in BC) is sufficiently low.

(E) From the authentication server and auxiliary server, both static and dynamic information may leak. We make this assumption because identification processes are continuously performed in response to identification trials at many authentication clients, so the servers may be attacked during an identification process, leading to dynamic information leak. Also, dynamic information might also leak because of the server administrator's fraud. On the other hand, an attacker can*not* modify the program and perform an unauthorized identification process. We make this assumption because in general, the servers are more strongly protected from the modification of program in an unauthorized way[11].

C. Requirements on BTPI

Next, we define security and efficiency requirements for BTPI.

1) Security Requirements: In order to define security requirements, we consider possible capabilities based on the above assumptions (A)–(E).

First, we consider attacks on the authentication server or the auxiliary server. From the assumption (E), we consider an attacker who can obtain both dynamic and static information. On the other hand, the attacker can*not* perform an unauthorized identification.

Next, we consider attacks on an authentication client. From the assumptions (C)(D), an attacker can*not* obtain neither dynamic information during an authorized identification process nor static information. On the other hand, we consider an attacker who can modify the program of an authentication client and perform unauthorized identification processes as described in the assumption (D).

To summarize the above, we consider the following (a)–(c) as the attacker capabilities.

(a) The attacker can acquire static and dynamic information from the authentication server.

[8]An example of the identification process is as follows. The auxiliary server sends $AD_1, \ldots, AD_N$ to the authentication client. The authentication client generates $PI_1^*, \ldots, PI_N^*$ by the PIR process using $AD_1, \ldots, AD_N$ and X', and sends $PI_1^*, \ldots, PI_N^*$ to the authentication server. The authentication server identifies the user ID by the PIC process using $PI_1, \ldots, PI_N$ and $PI_1^*, \ldots, PI_N^*$.

[9]Tamper-resistance stands for the property that performance such as acquisition of biometric feature, PIR, and communication can be done secretly.

[10]Tamper-evidence stands for the property that evidence remains when an attacker accesses dynamic information or modifies the program. As described in [3], tamper-evidence can be realized by, for example, a digital signature that detects software tampering, so can be realized at the low cost compared to tamper-resistance.

[11]Since there are many authentication clients, some of them might be insufficiently managed. For this reason, we consider the risk that the program of any of the authentication clients is modified is higher than the risk that the program of the servers is modified.

(b) The attacker can acquire static and dynamic information from the auxiliary server.
(c) The attacker can modify the program of an authentication client and perform an unauthorized identification. By this ability, the attacker can try to acquire dynamic information during unauthorized authentication, and to spoof an authorized user.

We consider two levels of strength of attackers. We refer to an attacker who has only one ability of (a)–(c) as *a single attacker*, and refer to an attacker who has more than one ability as *a combined attacker*.

We consider the attacker aims to perform spoofing attacks or acquiring information on biometric features. Therefore, we consider the following (i)(ii) as security requirements.

(i) *Single/combined spoofing difficulty* aims to make difficult the obtention of a successful output from the authentication server when performing an unauthorized identification based on previously acquired information.
(ii) *Single/combined irreversibility* aims to make restoring biometric features based on the acquired information difficult.

In (i)(ii), "single/combined" stands for the attacker capabilities. For example, combined irreversibility means that it is difficult for an combined attacker to restore biometric features. Note that single spoofing difficulty means the attacker has only ability (c) because it is a necessary skill when attempting spoofing.

2) Efficiency Requirements: We consider the following (iii)-(v) as efficiency requirements[12].

(iii) *Client Efficiency* means that the amount of calculation in the authentication client during an identification process is constant order independent of N.
(iv) *Communication Efficiency* means that the amount of communication during an identification process is constant order independent of N.
(v) *Servers Efficiency* means that the identification process in the authentication and auxiliary servers are fast. In general, the servers can consume more computing resources than an authentication client, so it cannot be said immediately that the servers efficiency requirement is not satisfied even if the amount of calculation is proportional to N. On the other hand, if a time-intensive process is performed N times, it is difficult to perform an identification for large N in an acceptable time. Considering these, we evaluate relatively whether the servers efficiency requirement is satisfied.

III. Naive BTPI Schemes

In this section, we evaluate BTPI schemes obtained by naively applying conventional BTP schemes to identification from requirements (i)–(v) described in Section II-C, and show that these schemes cannot satisfy all the requirements.

A. Evaluation of Naive BTPI Schemes

We describe contents of naive BTPI schemes and evaluate them.

1) A 1:N Normal Encryption (NE) Scheme: Before treating BTPI, we consider an simpler identification scheme, which encrypt biometric feature X_i using a symmetric-key algorithm such as AES. We refer to this scheme as 1:N Normal Encryption (NE) scheme. Because this scheme is not included in BTPI, we describe the enrollment and identification processes without using AD or PI.

Prior to the enrollment, the auxiliary server generates and saves a cryptographic key K.

The enrollment process for a user u_i is as follows. The enrollment client sends X_i to the authentication server, and the auxiliary server sends K to the authentication server. Then, using K, the authentication server encrypts X_i into a ciphertext, denoted by C_i, and saves C_i.

The identification process is as follows. The authentication client sends biometric feature X' to the authentication server, and the auxiliary server sends K to the authentication server. Then, using K, the authentication server decrypts $C_1, \ldots, C_N$ into $X_1, \ldots, X_N$, and identifies the user by matching $X_1, \ldots, X_N$ with X'.

For this scheme, single irreversibility is not satisfied because an attacker with the ability (c) can obtain a decrypted version of $X_1, \ldots, X_N$ during the identification. The single spoofing difficulty is satisfied because an attacker with only the ability (c) cannot obtain any information generated during the authorized identification process or stored in the servers. However, the combined spoofing difficulty is not satisfied because a combined attacker can obtain $X_1, \ldots, X_N$ and can spoof a user u_i by inputting X_i to an unmodified authentication client. Client and communication efficiency requirements are satisfied trivially. Also, we evaluate that the servers efficiency requirement is satisfied because the process by the authentication server is decrypting $X_1, \ldots, X_N$ by a symmetric-key algorithm in addition to matching $X_1, \ldots, X_N$ with X', and decryption is sufficiently fast if an algorithm such as AES is used.

We note that we can consider schemes which manage the symmetric key K more safely using secret sharing schemes or others. However, if $X_1, \ldots, X_N$ are decrypted during the identification process, the security evaluation result is the same as above.

2) A 1:N CB Scheme: We consider a 1:N CB scheme obtained by applying CIRF [3][13] to identification and managing the cancelable parameter[14] by "parameter-server model" [10, Section 1.5.2.1].

[12]Efficiency is originally defined in [8] as the condition that the number of referred ADs and generated PI*s and the processes of PIR is constant independent of N. Under the assumption that PIR is performed at the authentication client, efficiency defined in [8] is equivalent to satisfying both client and communication efficiency requirements in our definition.

[13]We consider CIRF because the matching in CIRF can be done relatively fast.

[14]The cancelable parameter is a kind of secret key, which determines the functions for converting the biometric features as described later.

Prior to the enrollment, the auxiliary server (called the parameter server in [10]) generates the cancelable parameter K, and stores K in itself. Because K is the common auxiliary data for $u_1, \ldots, u_N$, i.e., $AD_1 = AD_2 = \cdots = AD_N = K$, we simply denote it as AD.

The enrollment process for a user u_i is as follows. The auxiliary server sends K to the enrollment client. The enrollment client generates PI_i by $PI_i := f_K(X_i)$, where f_K is a certain function determined by K. Then, PI_i is sent and stored in the authentication server.

The identification process is as follows. The auxiliary server sends K to the authentication client. The authentication client generates PI^* by $PI^* := g_K(X')$ and send it to the authentication server, where g_K is a certain function determined by K. We denote this process by $\mathrm{PIR}^{\mathrm{CB}}$. The authentication server identifies the user by matching $PI_1, \ldots, PI_N$ with PI^*[15]. We denote this process by $\mathrm{PIC}^{\mathrm{CB(1:N)}}$[16].

In later sections, we denote $AD^{\mathrm{CB}} := AD$, $PI_i^{\mathrm{CB}} := PI_i$ for $i \in \{1, \ldots, N\}$, and $PI^{*\mathrm{CB}} := PI^*$.

For this scheme, single irreversibility is satisfied because even if either of AD or $(PI_1, \ldots, PI_N, PI^*)$ leak, no information on $(X_1, \ldots, X_n)$ leaks [3]. However, combined irreversibility is not satisfied because an attacker with the abilities (a)(b) can recover $X_1, \ldots, X_N$ by obtaining AD and $PI_1, \ldots, PI_N$. As in the case of the 1:N NE scheme, single spoofing difficulty is satisfied but combined spoofing difficulty is not satisfied. Client and communication efficiency requirements are satisfied trivially. Also, we evaluate that servers efficiency requirement is satisfied because matching $PI_1, \ldots, PI_N$ with PI^* in CIRF can be done relatively fast[17].

3) A 1:N BC Scheme: We consider a 1:N BC scheme obtained by naively applying FE [5][18] to identification.

The enrollment process for a user u_i is as follows. The enrollment client generates a pair (sk_i, pk_i) of a secret key and a public key. Then, it generates AD_i from sk_i and X_i, and sets $PI_i := pk_i$. AD_i is stored in the auxiliary server, and PI_i is stored in the authentication server.

The identification process is as follows. The authentication server generates a random number m called a challenge code and sends m and $PI_1, \ldots, PI_N$ to the authentication client. The auxiliary server sends $AD_1, \ldots, AD_N$ to the authentication client. Next, the authentication client recovers the secret key $PI_i^* := sk_i^*$ using X' and the received AD_i for each $i \in \{1, \ldots, N\}$, and verifies sk_i^* using the received PI_i^{BC}. Then, for the user ID i' that has succeeded in the verification, the authentication client generates a signature $\sigma_{i'}$ for m using $sk_{i'}^*$, and sends $(i', \sigma_{i'})$ to the authentication server. We denote this process for the user i' by $\mathrm{PIR}_{i'}^{\mathrm{BC}}$. The authentication server verifies the pair $(m, \sigma_{i'}, pk_{i'})$. We denote this process by $\mathrm{PIC}^{\mathrm{BC}}$. If the verification is successful, the authentication server outputs i' as the user ID.

In later sections, we denote $(AD_i^{\mathrm{BC}}, PI_i^{\mathrm{BC}}) := (AD_i, PI_i)$ for $i \in \{1, \ldots, N\}$ and $PI^{*\mathrm{BC}} := PI^*$.

For this scheme, combined spoofing difficulty and combined irreversibility are satisfied because recovering $X_1, \ldots, X_N$ or spoofing is difficult even if all of $AD_1, \ldots, AD_N$, $PI_1, \ldots, PI_N$ and communication information during the identification process leak. Servers efficiency requirement is satisfied because the authentication server only verifies the signature once. However, as pointed out in [8], client and communication efficiency requirements are not satisfied because this scheme requires N iterations to recover the secret key in the authentication client, and transmission of $AD_1, \ldots, AD_N$.

We note that even if both of $(AD_1, \ldots, AD_N)$ and $(PI_1, \ldots, PI_N)$ are stored in the authentication server, the evaluation result is the same as the above.

4) A 1:N BS Scheme: We consider a 1:N BS scheme obtained by naively applying FS[6][7] to identification.

The enrollment process for a user u_i is as follows. The enrollment client generates PI_i from X_i. Then, PI_i is sent to and stored in the authentication server. On the other hand, this scheme does not require auxiliary data, i.e., $AD_1 = AD_2 = \cdots = AD_N = \emptyset$.

The identification process is as follows. The authentication server generates a challenge code m, and sends m to the authentication client. The authentication client generates a signature σ for m using X', and sends σ to the authentication server. We denote this process by $\mathrm{PIR}^{\mathrm{BS}}$. Then, the authentication server verifies the pair (m, σ, PI_i) for all $i \in \{1, \ldots, n\}$, and output the user ID i' that has succeeded in the verification. We denote this process for i' by $\mathrm{PIC}_{i'}^{\mathrm{BS}}$.

In later sections, we denote $PI_i^{\mathrm{BS}} := PI_i$ for $i \in \{1, \ldots, N\}$ and $PI^{*\mathrm{BS}} := PI^*$.

For this scheme, combined spoofing difficulty and the combined irreversibility are satisfied from the property of FS. Also, as pointed out in [8], client and communication efficiency requirements are satisfied because the $\mathrm{PIR}^{\mathrm{BS}}$ is independent of N and the information transmitted during the identification process is only m and PI^*. However, we evaluate that servers efficiency requirement is not satisfied for the following reason. This scheme requires the authentication server to perform $\mathrm{PIC}_i^{\mathrm{BS}}$ for all $i \in \{1, \ldots, N\}$. However, $\mathrm{PIC}_i^{\mathrm{BS}}$ for each i requires exponentiation operation on a large-order finite field, which requires much more computational cost as compared to normal matching or matching by CB. Therefore, if N becomes large, $\mathrm{PIC}_i^{\mathrm{BS}}$ for all $i \in \{1, \ldots, N\}$ in an acceptable time becomes difficult.

[15] By defining f_K and g_K appropriately, the matching can be done without restoring the biometric features.

[16] In this scheme, AD^{CB} is simply sent to the authentication client. A more secure scheme is known, in which the identification process can be performed without the authentication client knowing AD^{CB} [10, Section 1.5.2.2]. However, the evaluation result is same as the above from requirements in this paper.

[17] The matching in CIRF can be done fast by Fast Fourier Transform (FFT). Also, for fastening identification of 1:N CB, indexing schemes such as in [11] can be used.

[18] We consider FE because it is considered that when implementing it appropriately, the biometric feature cannot be restored and spoofing is difficult even if both of AD and PI leak. On the other hand, we note that there are cases in which security is reduced because of bad implementation [12]. Therefore, implement should be done carefully.

TABLE I
EVALUATION OF NAIVE BTPI SCHEMES

Schemes	Efficiency requirements			Security requirements			
	Client	Communication	Server	Spoofing difficulty		Irreversibility	
				Single	Combined	Single	Combined
1:N NE	✓	✓	✓	✓	✗	✗	✗
1:N CB	✓	✓	✓	✓	✗	✓	✗
1:N BC	✗	✗	✓	✓	✓	✓	✓
1:N BS	✓	✓	✗	✓	✓	✓	✓

B. Problems of Naive BTPI Schemes

The evaluation results in Section III-A are summarized in Table I. As shown in Table I, the above BTPI schemes do not satisfy the efficiency and security requirements simultaneously.

IV. A BTPI SCHEME BY HIERARCHICAL MATCHING WITH TWO BIOMETRIC FEATURES

To solve the problems mentioned in the previous section, we propose a BTPI scheme which uses a hierarchical matching with two biometric features.

A. Assumptions and Requirements on Biometric Modalities

We assume that the modalities of biometric features are classified into the following two. We refer to modalities relatively easy to obtain, such as face and voice, as *public modalities*, and ones relatively hard to obtain except during biometric authentication, such as vein and retina, as *private modalities*. Private modalities should be more strongly protected because they tend to be used for use-cases in which strong security is required. Also, public modalities should be protected to some extent, because leakage of them might lead to privacy violation. In this paper, we require that private modalities are protected at the level of combined irreversibility, and public modalities are protected at the level of single irreversibility.

B. The Content of the Proposed BTPI Scheme

The proposed scheme uses two features. The 1st feature is selected from public modalities, and the 2nd feature is selected from private modalities. We assume that no information on the 2nd feature can be obtained from the 1st feature[19]. Then, by combining 1:N CB and either of 1:1 BC or 1:1 BS, we construct a scheme which satisfies security and efficiency requirements.

We describe the proposed scheme. Prior to the enrollment, the system generates AD^{CB} as described in Section III-A2.

The enrollment process for a user u_i is as follows. First, the enrollment client acquires two biometric features $X_i := (Y_i, Z_i)$. The 1st feature Y_i is selected from the public modalities, and the 2nd feature Z_i is selected from private modalities. Next, from Y_i, the BTPI system generates PI_i^{CB} as described in Section III-A2. Also, from Z_i, it generates $(AD_i^{\mathrm{BC}}, PI_i^{\mathrm{BC}})$ as described in Section III-A3, or PI_i^{BS} as described in Section III-A4. Then, the system sets $(AD_i, PI_i) := ((AD^{\mathrm{CB}}, AD_i^{\mathrm{BC}}), (PI_i^{\mathrm{CB}}, PI_i^{\mathrm{BC}}))$ or $(AD_i, PI_i) := (AD^{\mathrm{CB}}, (PI_i^{\mathrm{CB}}, PI_i^{\mathrm{BS}}))$.

[19]For example, if the two features are obtained from different parts such as a face and a finger, this assumption is satisfied.

The identification process is as follows (the identification process when 1:N BC is used for Z_i is shown in Figure 3). First, the authentication client acquires a pair $X' := (Y', Z')$ of the 1st feature and the 2nd feature. Also, the auxiliary server sends AD^{CB} to the authentication client. Next, the authentication client generates $PI^{*\mathrm{CB}}$ by applying $\mathrm{PIR}^{\mathrm{CB}}$ to Y', and sends it to the authentication server. Then, the authentication server identifies the user ID i' by $\mathrm{PIC}^{\mathrm{CB}(1:\mathrm{N})}$[20]. After that, the system operates $(\mathrm{PIR}_{i'}^{\mathrm{BC}}, \mathrm{PIC}^{\mathrm{BC}})$ or $(\mathrm{PIR}^{\mathrm{BS}}, \mathrm{PIC}_{i'}^{\mathrm{BS}})$ for Z'. When the verification is successful, the authentication server outputs the user ID i', and otherwise, it outputs $\perp$.

C. The Evaluation of the Proposed Scheme

First, we evaluate the proposed scheme from efficiency requirements. Client efficiency requirement is satisfied because the process in the authentication client is $\mathrm{PIR}^{\mathrm{CB}}$ for Y' and either of $\mathrm{PIR}_{i'}^{\mathrm{BC}}$ or $\mathrm{PIR}^{\mathrm{BS}}$ for Z'. Communication efficiency requirement is satisfied trivially. Servers efficiency requirement is satisfied because the process in the authentication server is $\mathrm{PIC}^{\mathrm{CB}(1:\mathrm{N})}$ and either of $\mathrm{PIC}^{\mathrm{BC}}$ or $\mathrm{PIC}_{i'}^{\mathrm{BS}}$.

Next, we evaluate the proposed scheme against security issues. For the 1st feature Y_i selected from public modalities, single irreversibility is satisfied but combined irreversibility is not satisfied because CB is used. On the other hand, for the 2nd feature Z_i selected from private modalities, combined irreversibility is satisfied because BC or BS is used. Also, combined spoofing difficulty is satisfied for the following reason. In order to succeed in spoofing, it is necessary to generate a forged signature $\tilde{\sigma}_{i'}$ for the received challenge code m passing the verification. From the assumption that no information on the 2nd feature can be obtained from the 1st feature, $(AD^{\mathrm{CB}}, PI_i^{\mathrm{CB}})$ has no information on the values of $\tilde{\sigma}_{i'}$ passing the verification. Therefore, an attacker has to generate $\tilde{\sigma}_{i'}$ passing the verification from $(AD_i^{\mathrm{BC}}, PI_i^{\mathrm{BC}})$ or PI_i^{BS}, which is difficult from the property of BC or BS.

The evaluation results of the proposed scheme is shown in Table II. In Table II, the proposed scheme is referred to as 1:N CB + (BC or BS) because in the identification process of the proposed scheme, after the candidate user is identified by 1:N CB, the authentication process of BC or BS is performed. Here, as a scheme which uses two features in order to satisfy client, servers, and communication efficiency requirements, and combined spoofing difficulty, we can consider the scheme

[20]For simplicity, we assume that only one candidate user is identified by $\mathrm{PIC}^{\mathrm{CB}(1:\mathrm{N})}$. However, practically, it is sufficient to narrow down the N enrolled users to a few candidates for which 1:N BC or 1:N BS can be performed in an practical time.

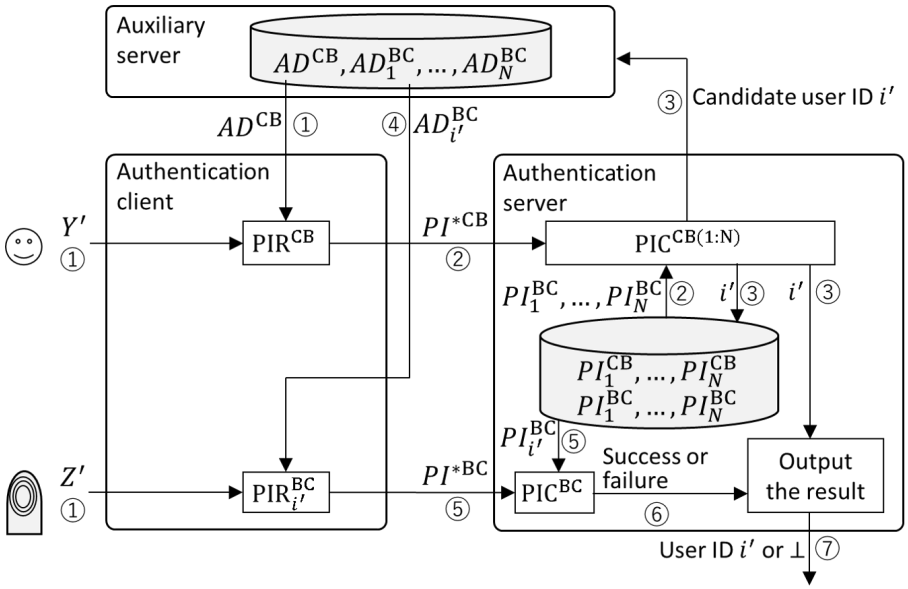

Fig. 3. The Identification Process of the Proposed Scheme

obtained by replacing 1:N CB in the proposed scheme with 1:N NE. We refer to this scheme as 1:N NE + (BC or BS), and show the evaluation result of this scheme in Table II for reference. This scheme does not satisfy single irreversibility, and other properties can be shown by the same way as the proposed scheme.

The proposed scheme has the following properties as compared to others. First, we can show from Table II that the proposed scheme satisfies client, servers, and communication efficiency requirements, and combined spoofing difficulty simultaneously. As shown in Table I, the BTPI schemes based on conventional BTP schemes cannot satisfy these requirements simultaneously. Next, on irreversibility, the following can be said. The 2nd feature should be strongly protected because it is selected from private modalities. By the proposed scheme, it is protected at the level of combined irreversibility. Also, the 1st feature, which is selected from public modalities, is protected at the level of single irreversibility.

The proposed scheme realizes BTPI which satisfies efficiency requirements, is protected against spoofing attacks by attackers who can have access to multiple entities, and can protect biometric features at a sufficient level.

V. Conclusion

In this paper, we evaluated some BTPI schemes based on conventional BTP schemes, and showed that they did not satisfy efficiency and security requirements simultaneously. Also, we proposed a BTPI scheme which used two features and performed a hierarchical matching by CB and either of BC or BS. The proposed scheme satisfies efficiency requirements and combined spoofing difficulty, and can protect biometric feature at sufficient level.

The following future work remains:

- To evaluate experimentally the proposed scheme efficiency server-side.
- To categorize public and private modalities more reasonably.

References

[1] "Information technology — performance testing of biometric template protection schemes," *ISO/IEC 30136,* 2018.
[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometric-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.
[3] K. Takahashi and S. Hirata, "Cancelable biometrics with provable security and its application to fingerprint verification," *IEICE Transaction on Fundamentals*, vol. 94-A, no. 1, pp. 233–244, 2011.
[4] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems: Issues and challenges," vol. 92, no. 6, pp. 948–960, 2004.
[5] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.
[6] K. Takahashi, T. Matsuda, T. Murakami, G. Hanaoka, and M. Nishigaki, "A signature scheme with a fuzzy private key", *Proc. of 13th International Conference on Applied Cryptography and Network Security (ACNS2015)* LNCS9092, pp. 105–126, 2015.
[7] T. Matsuda, K. Takahashi, T. Murakami, and G. Hanaoka, "Fuzzy signatures: relaxing requirements and a new construction," *Proc. of 14th International Conference on Applied Cryptography and Network Security (ACNS2016)* LNCS9696, pp.97–116, 2016.
[8] K. Takahashi, T. Matsuda, T. Murakami, and G. Hanaoka, "On the security and efficiency of template protected biometric identification," *Proc. of 2017 Symposium on Cryptography and Information Security (SCIS2017)*, 3B1-6, 2017 (in Japanese).
[9] K. Takahashi, S. Hirata, M. Mimura, and S. Tezuka, "A protocol for secure remote authentication using biometrics," *IPSJ Journal*, vol. 49, no. 9, pp. 3016–3027, 2008 (in Japanese).
[10] D. C. L. Nao, A. B. J. Teoh, and J. Hu, *Biometric security*, Cambridge Scholars, 2015.
[11] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio, and K. Takahashi, "Cancelable permutation-based indexing for secure and efficient biometric identification," *IEEE Access*, vol. 7, pp. 45563–45582, 2019.
[12] S. Hidano, T. Ohki, and K. Takahashi, "Evaluation of security for protected template in biometric cryptosystem using fuzzy commitment scheme," *IPSJ Journal*, vol. 54, no. 11, pp. 2383–2391, 2013 (in Japanese).

TABLE II
EVALUATION OF THE PROPOSED SCHEME AND A RELATED SCHEME

	Efficiency requirements			Security requirements					
						Irreversibility			
	Client	Communication	Server	Spoofing difficulty		1st biometric feature (public modality)		2nd biometric feature (private modality)	
				Single	Combined	Single	Combined	Single	Combined
[Proposed] 1:N CB + (BC or BS)	✓	✓	✓	✓	✓	✓	✗	✓	✓
[For reference] 1:N NE + (BC or BS)	✓	✓	✓	✓	✓	✗	✗	✓	✓