AVET: A Novel Transform Function to Improve Cancellable Biometrics Security

Thao Mai Dang, Thuc Dinh Nguyen, Thang Hoang, *Member, IEEE*, Hyunseok Kim, Andrew Beng Jin Teoh, *Senior Member, IEEE*, and Deokjai Choi

***Abstract*— Similarity preserving is a key ingredient of cancellable biometric scheme design. The notion ensures the accuracy performance of the biometric systems can be preserved after the cancellable biometric technique is applied. Random Projection is among the most commonly adopted method in cancellable biometric schemes. However, it is reversible subject to certain conditions, which disrupts the template irreversibility criterion. This invites vulnerabilities for random projection-based schemes. In this paper, we propose a novel transform function, namely Absolute Value Equations Transform (AVET), which non-linearly projects feature vectors to another domain. The transformed templates hold two main merits ensuring the user's privacy, and maintaining the system's performance simultaneously. First, by relying on the hardness of the Absolute Value Equations problem, we guarantee that AVET satisfies irreversibility. Second, by using Johnson–Lindenstrauss lemma and the inverse triangle inequality, we prove that the proposed approach has the similarity preserving property. Notably, rigorous theoretical proofs and empirical experiments are provided. The efficacy of AVET is comprehensively evaluated on both physiological and behavioral biometrics including face, ear, fingerprint, and gait. With unimodal approach, we achieve competitive performances compared to related algorithms on eight public datasets. Regarding bimodal mode, the AVET surpasses the state-of-the-art technique on all three observed datasets. To the best of our knowledge, this is the first study that attempts to develop a secure transformation to augment the role of Random Projection in the existing cancellable biometric schemes.**

Manuscript received 21 June 2022; revised 15 October 2022; accepted 29 November 2022. Date of publication 16 December 2022; date of current version 23 December 2022. This work was supported in part by the Institute for Information and Communication Technology Planning and Evaluation (IITP) Grant funded by the Korea Government [Ministry of Science and ICT (MSIT)] (Regional Strategic Industry Convergence Security Core Talent Training Business) under Grant 2022-0-01203; in part by the University of Science, Vietnam National University-Ho Chi Minh City (VNU-HCM), under Grant CNTT2021-17; in part by an Unrestricted Gift from Robert Bosch; and in part by the Commonwealth Cyber Initiative (CCI), an investment in the advancement of cyber research and development, innovation, and workforce development. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Zhen Lei. *(Corresponding authors: Deokjai Choi; Thao Mai Dang.)*

Thao Mai Dang, Hyunseok Kim, and Deokjai Choi are with the Department of Artificial Intelligence Convergence, Chonnam National University, Gwangju 61186, South Korea (e-mail: thaomaidang@gmail.com; dchoi@jnu.ac.kr).

Thuc Dinh Nguyen is with the Decentralized Applied Crypto Laboratory, University of Science, VNU-HCMC, Ho Chi Minh City 700000, Vietnam (e-mail: ndthuc@fit.hcmus.edu.vn).

Thang Hoang is with the Department of Computer Science, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: thanghoang@vt.edu).

Andrew Beng Jin Teoh is with the School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: bjteoh@yonsei.ac.kr).

Digital Object Identifier 10.1109/TIFS.2022.3230212

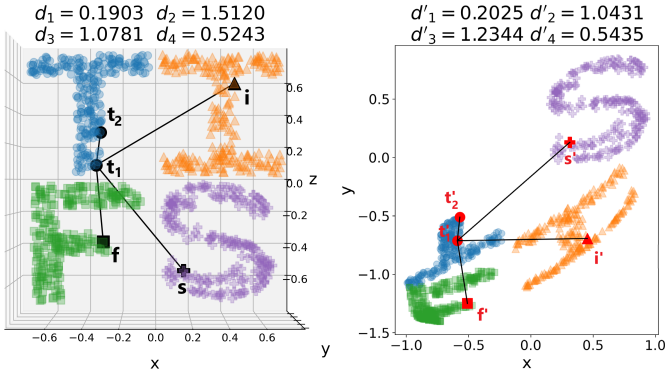
***Index Terms*— Cancelablle biometrics, similarity preserving, irreversible transformation, absolute value equations transform.**

I. Introduction

BIOMETRICS, human biological or behavioral traits, are appropriate for recognizing or verifying the identity of an individual due to its uniqueness. The main advantage of using biometrics over passwords or user-specific tokens is its convenience which enables people to get rid of remembering complicated random strings or carrying physical devices. While the connection between passwords/tokens and its holder is vague, the question "who I am" can be answered perfectly with biometrics, yielding irrefutable evidence in proof of liability. This leads to the sharp growth of biometrics-based solutions for defense, forensics, banking, and unlocking smart devices. However, biometric data is permanently associated with the user and cannot be modified; thus when a biometric template is disclosed, it would be lost eternally. Therefore, biometric template protection (BTP) schemes must meet the following criteria [1]:

- Revocability: The protected templates could be revoked at any time whenever required.
- Unlinkability: There is no correlation between protected templates (i.e., not cross-matching).
- Irreversibility: It should be computationally infeasible to trace back the original biometric templates from the corresponding compromised information.
- Performance preservation: The performance of the biometric systems should not be degraded when applying BTP methods.

To address the concern of BTP, the notion of *Cancellable Biometrics* (CB) was first introduced by Ratha et al. [2]. In general, CB refers to the irreversible transform that can generate a protected biometric template. While CB design mainly focuses on the security protection of the biometric templates, decent similarity preserving is a necessity to meet the performance preservation criterion. Random Projection (RP) is one of the most popular similarity preserving notions for CB design. The similarity preservation nature of the RP is guaranteed by the Johnson–Lindenstrauss (JL) lemma [36]. The RP is often found in data retrieval problems such as locality sensitive hashing (LSH) [3] and for privacy enhancement [4]. Random Projection has been implemented in many CB schemes for various biometrics modalities such as face [8], fingerprint [7], iris [12], palmprint [13], signature [10], gait [14], finger



(a) Original domain (b) Transformed domain

Fig. 1. Proposed AVET has both security and similarity preserving properties. The given toy dataset is irreversibly projected into another domain via AVET, i.e., $\mathbf{t}_1 \mapsto \mathbf{t}'_1$. The input data is drastically changed while the overall topology of the data points remains relatively stable, with d_1 (d_2, d_3, d_4) is Euclidean distance from $\mathbf{t}_1$ to $\mathbf{t}_2$ ($\mathbf{t}_1 \rightarrow \mathbf{i}$, $\mathbf{t}_1 \rightarrow \mathbf{s}$, $\mathbf{t}_1 \rightarrow \mathbf{f}$) and d'_1 (d'_2, d'_3, d'_4) is Euclidean distance from $\mathbf{t}'_1$ to $\mathbf{t}'_2$ ($\mathbf{t}'_1 \rightarrow \mathbf{i}'$, $\mathbf{t}'_1 \rightarrow \mathbf{s}'$, $\mathbf{t}'_1 \rightarrow \mathbf{f}'$).

TABLE I
NOTATIONS

Notation	Description
$dist(\cdot)$	Calculating distance function
$avet(\cdot)$	The proposed AVET transform function
$\phi(\cdot)$	Projection function
$sgn(\cdot)$	Sign function
$\delta, \varepsilon, \Delta$	Non-negative real number
$\mathbf{a}$ / a_i	Vector / Element i-th of vector $\mathbf{a}$
a / A	Scalar, number / Matrix
$\mathbf{A}$ / $\lvert\mathbf{A}\rvert_c$	Set / Cardinality of set $\mathbf{A}$
$\lvert\cdot\rvert$	Absolute value number / vector
$\lvert\lvert\cdot\rvert\rvert$	Euclidean distance
$\mathbf{a} \simeq_\varepsilon \mathbf{b}$	Euclidean distance between vectors $\mathbf{a}$ and $\mathbf{b}$ is smaller than the real number ε
i.i.d.	Independent and identically distributed
$[n]$	For a number $n \in \mathbb{N}^*$, $[n]$ denotes $\{1, ..., n\}$
$\lfloor\cdot\rfloor$	Floor operation
$\mathbf{a}\lvert\lvert\mathbf{b}$	Concatenation of vector $\mathbf{a}$ and vector $\mathbf{b}$

vein [15], speech [16], and electrocardiogram (ECG) [17] since early 2000s until today. Even though those CB schemes have distinct designs and extensions according to different biometric traits, the role of RP is entrenched due to its simplicity and effectiveness. However, many researches point out that RP is insecure on its own where the attackers can recover the original user's template partially [11] and particularly vulnerable to some dedicated attacks such as pre-image attack [18] and known-sample attack [19].

To remedy the limitations of RP, we propose a generic solution dubbed Absolute Value Equations Transform (AVET), which can be adapted to diverse biometric modalities yet satisfies revocability, unlinkability, and irreversibility criteria. Besides that, AVET also preserves the manifold structure among data points, before and after the transformation, within a certain small error with respect to the Euclidean metric. To intuitively show the promising performance of AVET, we demonstrate the method over a 4-dimensional toy dataset with 1000 data instances and illustrate the 2-dimensional transformed results in Fig. 1. Every character of "TIFS" is made by 250 data points. After applying AVET, despite distortions, the shape of the transformed characters "T", "I", "F", "S" remain recognizable. This suggests the distance relationship between data points is largely kept, thus can approximately preserve the accuracy performance after transformation.

For the upcoming parts of this paper, the existing similarity preserving methods are reviewed in Section II, as well as our motivation and contributions of this research are highlighted. We briefly present the background knowledge and introduce the proposed transformation function in Section III. Next, the experimental validations are performed in Section IV. Further, security, privacy and revocability analysis are described in Section V. Finally, Section VII is conclusions.

II. Literature Review

A. Related Work

In this section, we focus on reviewing state-of-the-art *generic* cancellable biometrics schemes. As mentioned above, all cancellable biometric schemes are to leverage certain similarity preserving notion to ensure performance preservation criterion can be satisfied. Most of the schemes can be subsumed under two broad categories: 1) non Random Projection and 2) Random Projection based. By generic, we refer to CB schemes that can be adapted to various biometric modalities such as face, iris, fingerprint, etc. For convenience of reference, we summarize all the key notations in Table I.

1) Generic Cancellable Biometrics Techniques: We first present several relevant CB schemes which do not follow the RP notion. Morphing technique was the first CB scheme proposed by [2] and [5] for fingerprint and face. The authors distort the biometric data with an user-specific morphing function that enables revocability. However, Dabbah et al. [20] revealed that the original data can be easily recovered due to the high correlation between the morphed data and its original counterpart.

Bloom filter notion is adapted for biometric template protection purpose and it is applied to iris [21], face [22], and fingerprint [23]. Bloom filter was first applied for iris template protection by Rathgeb et al. [21]. Bloom filter-based transforms have been claimed to achieve irreversibility due to the many-to-one adopted mapping. However, Hermans et al. [24] argued that Bloom filter violates the unlinkability requirement by providing a simple attack scheme that was able to distinguish whether two templates are extracted from the identical biometric sample or not. In addition, Bringer et al. [25] claimed that there exists a leakage in the Bloom filter-based schemes [21] when l is small (i.e., $l = \{16, 32\}$) by exploiting the Hamming distance between the reconstructed IrisCode and the compromised one.

Recently, Kaur and Khanna put forward Random Distance Method (RDM) [26] which is suitable for both unimodal and bimodal biometric systems. If the distance vector D and all of helper data are compromised, recovering the original features is feasible [26, Section V-C]. Later, Kaur and Khanna presented Random Slope Method (RSM) [27] that follows the outline in [26] but computes slope values between feature and synthetic points instead. Noticeably, the similarity preserving property of both RDM and RSM is established theoretically under a strong assumption than that of the RP-based methods. This issue will be discussed more in Section IV.

2) Random Projection-Based Techniques: In CB, the RP notion is widely adopted due to its simplicity and effectiveness in distance-related preserving.

BioHashing (BH) is the first RP-based CB scheme proposed by Teoh et al. [6]. In BH, the feature vector $\mathbf{x} \in \mathbb{R}^m$ is projected via $\mathbf{y} = R \cdot \mathbf{x}$, where R is an user-specific orthogonal random matrix in $\mathbb{R}^{g \times m}$, with $g \leqslant m$. The matrix R can be generated from the password or token. The intermediate vector $\mathbf{y}$ is then discretized based on a pre-defined threshold τ to return a binary code $\mathbf{z}$. The value $\tau = 0$ is usually used in the literature, so a function that computes the hash code can be written briefly as $\mathbf{z} = sgn(\mathbf{y})$, where $sgn(\cdot)$ is a sign function. The BH was regarded as non-invertible due to the usage of a rectangular RP matrix ($g \leqslant m$) and thresholding operation. However, from a single stolen hash code $\mathbf{z}$, Lee et al. [28] introduced an attack scheme to find a pre-image $\mathbf{x}'$, such that $sgn(R \cdot \mathbf{x}). = sgn(R \cdot \mathbf{x}')$. Later, Lacharme et al. [29] proposed a genetic algorithm-based method that can approximate the original biometrics template $\mathbf{x}$ from the compromised binary hash code $\mathbf{z}$ and projection matrix R. Thus, it is shown that BH is not pre-image resistant [28], [29]. Besides that, in an event of *multiple* pairs of $(\mathbf{y}, R)$ are known to the attackers (i.e., linkage attacks), exact $\mathbf{x}$ recovery is possible since the attackers can collect enough $\mathbf{y}$ and R to solve a linear equation system formed by $\mathbf{y} = R \cdot \mathbf{x}$.

Based on BH, several CB schemes were put forward to address the stolen-token issue. For instance, multispace random projections presented in [9] and sectored random projections proposed in [12] are the variants of BH. Lumini and Nanni [10] proposed two solutions, namely, space augmentation and features permutation in order to improve the performance of BH. Wang and Plataniotis [11] introduced the secret translation vector notion to strengthen the security and the performance of the system.

The native BH was applicable only to a fixed size ordered feature vector but did not fit to the non-ordered varying size template such as fingerprint minutia. To address this limitation and to protect the projection matrix R from being revealed, Yang et al. proposed Dynamic Random Projection (DRP) [30]. Later, Jin et al. introduced two ranking-based CB schemes for fingerprint, namely Gaussian Random Projection-based and Uniformly Random Permutation-based Index-of-Max hashing [7] (abbreviation as GRP-IoM and URP-IoM). In this paper, we only compare our proposed method with GRP-IoM because URP-IoM does not utilize the RP function in its operation. Ghammam et al. [31] pointed out that this technique was vulnerable against Authentication and Nearby Reversibility attacks.

To ameliorate the trade-off of security and accuracy performance, Feng et al. [8] presented a hybrid approach which inherits advantages of both bio-cryptosystem and CB-based strategy. In their scheme, the biometric feature vector is perturbed with RP for revocation purposes. Next, the transformed template is binarized by a method called Discriminability Preserving Transform (DPT). Since DPT is vulnerable against masquerade attacks, the binary template is protected by Fuzzy Commitment Scheme [32], which is a classic biometric encryption scheme.

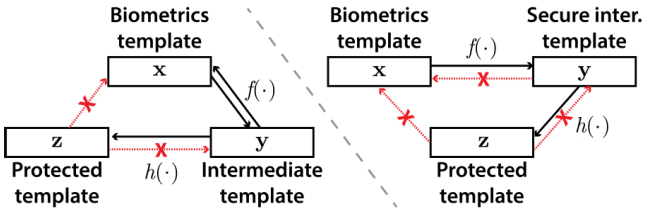


Fig. 2. Block diagrams generate protected templates of (left) RP-based techniques and (right) our strategy, with $f(\cdot)$ is projection function and $h(\cdot)$ is protection function. The reversibility of function $f(\cdot)$ in RP-based approaches is the weakness of this design.

To derive unpredictable hash codes from biometric inputs, Dang et al. proposed Full Entropy Hash (FEHash) [33]. This encodes the user's feature vectors to pre-defined full entropy binary strings which are, finally, protected by the SHA-512 cryptographic hash function to meet the requirement of irreversibility. We focus on the projection step in FEHash only and refer the readers to [33] for more details. Particularly, to obtain one bit of the hash code, the original vector $\mathbf{x} \in \mathbb{R}^m$ is projected to another domain with RFF transformation, i.e., $\mathbf{y} = \sqrt{2/g}\cos(\mathbf{\Omega} \cdot \mathbf{x} + \mathbf{r})$, with random value $\mathbf{r} \in [0, 2\pi]^g$ and a random matrix $\mathbf{\Omega} \in \mathbb{R}^{g \times m}$. We assume that $\mathbf{y}$ and all the projection parameters are known by the attackers. Clearly, reversing $\mathbf{x}$ from RFF is much more complicated than from RP since `arccos` is a *multivalued* function. However, if attackers also have knowledge about the value range of $\mathbf{x}$, the number of the inversion solutions can be greatly reduced and hence shrunken the solution searching space.

B. Motivation

From the literature, we observe that RP-based schemes share a common general design to generate protected templates, which is depicted in Fig. 2. First, the original template is projected to another subspace by using projection function $f(\cdot)$ to yield a random and *changeable* intermediate template (revocability). The protection function $h(\cdot)$ is then applied on this returned value to output the non-invertible template which has no correlation with the input (irreversibility).

To generate a new template, the projection step is repeated with distinct projection helper data, and thus users can reissue as many different templates as they require. This procedure (of RP-based approaches) is described explicitly as follows:

$$\begin{cases} R_1 \cdot \mathbf{x} = \mathbf{y}_1 \\ R_2 \cdot \mathbf{x} = \mathbf{y}_2 \\ \vdots \\ R_k \cdot \mathbf{x} = \mathbf{y}_k, \end{cases} \tag{1}$$

with $R \in \mathbb{R}^{n \times m}$ is random matrix and $n < m$. In the worst scenario when both template $\mathbf{y}$ and matrix R are leaked multiple times, RP function $f(\mathbf{x}) = R \cdot \mathbf{x} = \mathbf{y}$ becomes reversible (i.e., solving Eq. 1 is possible). Hence, the secret biometric template can be recovered completely. This assumption could be used in the cross-matching attack [11] which might be feasible if there were *mistakes* in the system architecture. Let a lightweight RP-based framework proposed by Punithavathi et al. [46] in 2019 be our example. Under

the mentioned attack, the framework would be undoubtedly broken due to its careless construction (see Eq. 10, Fig. 4, and Section 5.2 [46] for more details). Besides, the linear characteristic of RP was usually *exploited* to weaken the security guarantees of protection functions (i.e., reversibility attacks [31] on GRP-IoM were performed by solving linearly constrained quadratic equations). Thus, despite fascinating and irreversible protection functions, the conspicuous fragility of RP-based approaches lies in their projection method. Therefore, it is critical and deserves immediate attention to develop a secure alternative to RP, which motivates us to conduct this research.

C. Contribution

Concisely, our contributions are summarized as follows:

1) Some of the afore-discussed transform approaches are reversible (i.e., morphing technique [5], RDM [26], RP [6]); therefore, we introduce a secure transformation method called AVET. The proposed approach is a NP-hard problem yielding a convincing security level even in the worst scenario.

2) The proposed function can mitigate the long-standing problem of RP-based cancellable biometrics methods. Particularly, AVET is compatible with RP-based systems, which helps to reuse those schemes, reducing development time and avoiding massive modifications during reconstruction. To demonstrate its adaptability, we apply AVET into two existing techniques, namely, BH and GRP-IoM.

3) Some of transform functions are tailored for one specific modality such as iris [34] and fingerprint [35]. The state-of-the-art transformation technique, RDM, used only one feature extraction method (i.e., log-Gabor) to derive bio-features for all 5 different physiological modalities, which partly limits the full understanding about RDM. To claim that AVET is generic, universal, and easy to implement to various existing systems, we carry out experiments on eight datasets for both physiological and behavioural biometrics and extract feature vectors by using an appropriate method for each of them.

4) We provide comprehensive theoretical proof to prove that AVET holds both security and similarity preserving properties and meets all four requirements of biometrics protection. Besides, the major privacy and security attacks, i.e., brute force attacks, false acceptance attacks, and ARM attacks are described in detail.

III. Methodology

In Section III-A, we briefly present the concept of absolute value vector, introduce the definition of *closeness* between data points, and recall the JL lemma. In Section III-B, we describe our proposed method and provide theoretical proof to prove its privacy and similarity preserving properties.

A. Preliminaries

Following are some definitions used frequently in this paper.

Definition 1 (Distance Relationship Between Two Vectors): Given vectors $\mathbf{c}$, $\mathbf{d} \in \mathbb{R}^m$ *and a small number* $\varepsilon \geqslant 0$.

$$\textit{If } dist(\mathbf{c}, \mathbf{d}) = ||\mathbf{c} - \mathbf{d}|| \leqslant \varepsilon, \textit{ then } \mathbf{c} \simeq_\varepsilon \mathbf{d}.$$

We could interpret the definition 1 as that two high-dimensional data points are considered as *close* to each other if the Euclidean distance between them is smaller than a factor ε. This concept is widely implemented to minimize various loss functions in machine learning, based on the fact that the derived feature vectors from the same person are more akin than those from different individuals.

Definition 2 (Absolute Value Vector): Given $\mathbf{x} \in \mathbb{R}^m$, *absolute value of vector* $\mathbf{x}$ *is*:

$$|\mathbf{x}| = (|x_1|, \ldots, |x_m|).$$

We denote the absolute value vector of $\mathbf{x}$, the vector with absolute values of each component of $\mathbf{x}$, as $|\mathbf{x}|$.

Lemma 1 (Johnson–Lindenstrauss [36]): For any $0 < \delta < 1$ *and any integer p, let n be a positive integer such that* $n \geqslant 4(\delta^2/2 - \delta^3/3)^{-1}\ln(p)$. *Then, for any set S of p points in* $\mathbb{R}^m$, *there is a map* f_R: $\mathbb{R}^m \to \mathbb{R}^n$ *such that, for all* $\mathbf{c}, \mathbf{d} \in S$, $(1-\delta)||\mathbf{c} - \mathbf{d}||^2 \leqslant ||f_R(\mathbf{c}) - f_R(\mathbf{d})||^2 \leqslant (1+\delta)||\mathbf{c} - \mathbf{d}||^2$.

JL lemma implies that we can choose a random matrix $R \in \mathbb{R}^{n \times m}$, where each entry is sampled i.i.d. from a Gaussian distribution $\mathcal{N}(0, I)$. Such that, with high probability, for any vector $\mathbf{x} \in \mathbb{R}^m$, $\frac{1}{\sqrt{n}}||f_R(\mathbf{x})||^2$ is a $1 \pm \delta$ approximation to $||\mathbf{x}||^2$, where $f_R(\mathbf{x}) = R \cdot \mathbf{x}$ and δ is a small distortion value. In short, the JL lemma is used to prove that RP is a similarity preserving method; thus, the relationship between projected data points remains unchanged with respect to Euclidean distance. For the sake of simplicity, in this paper, we assume $\delta = 0$, which means the RP function following the JL lemma can map high-dimensional data to other spaces with zero distortion.

B. AVET: Absolute Value Equations Transform

The concept of *general* Absolute Value Equations (GAVE) was first introduced by Mangasarian [37]; the form of this problem is written as follows:

$$A \cdot \mathbf{x} + B \cdot |\mathbf{x}| = \mathbf{y}, \tag{2}$$

where input vector $\mathbf{x} \in \mathbb{R}^m$, matrices $A, B \in \mathbb{R}^{n \times m}$, and vector $\mathbf{y} \in \mathbb{R}^n$. By reducing the NP-hard Knapsack Feasibility Problem to the GAVE form, Mangasarian proved that solving Eq. 2 is an NP-hard problem [37, proposition 2] (i.e., given $A, B, \mathbf{y}$, find $\mathbf{x}$). Based on GAVE, we easily prove that:

$$A \cdot \mathbf{u} + B \cdot |\mathbf{v}| = \mathbf{y} \tag{3}$$

is also an NP-hard problem, where $\mathbf{u}$ and $\mathbf{v}$ are same length vectors derived from $\mathbf{x}$ (i.e., the concatenation of $\mathbf{u}$ with $\mathbf{v}$ equals $\mathbf{x}$). Since vector $\mathbf{u}$ can always be represented via $\mathbf{u} = \mathbf{v} + \mathbf{p}$ where $\mathbf{p}$ is a random vector; hence, Eq. 3 can be rewritten as: $A \cdot \mathbf{v} + B \cdot |\mathbf{v}| = \mathbf{y} - A \cdot \mathbf{p}$, which has the form of GAVE. Because vector $\mathbf{p}$ is unknown, attackers have no information about the value of $\mathbf{y} - A \cdot \mathbf{p}$. Therefore, the NP-hard problem, Eq. 3, is infeasible to solve.

Obviously, if we can combine GAVE with biometrics, then the security of bio-systems is ensured definitively thanks to the NP-hard problem of absolute equations. However, we cannot use directly neither the original GAVE algorithm nor its variant (i.e., Eq. 3) as a means to transform biometric template $\mathbf{x}$.

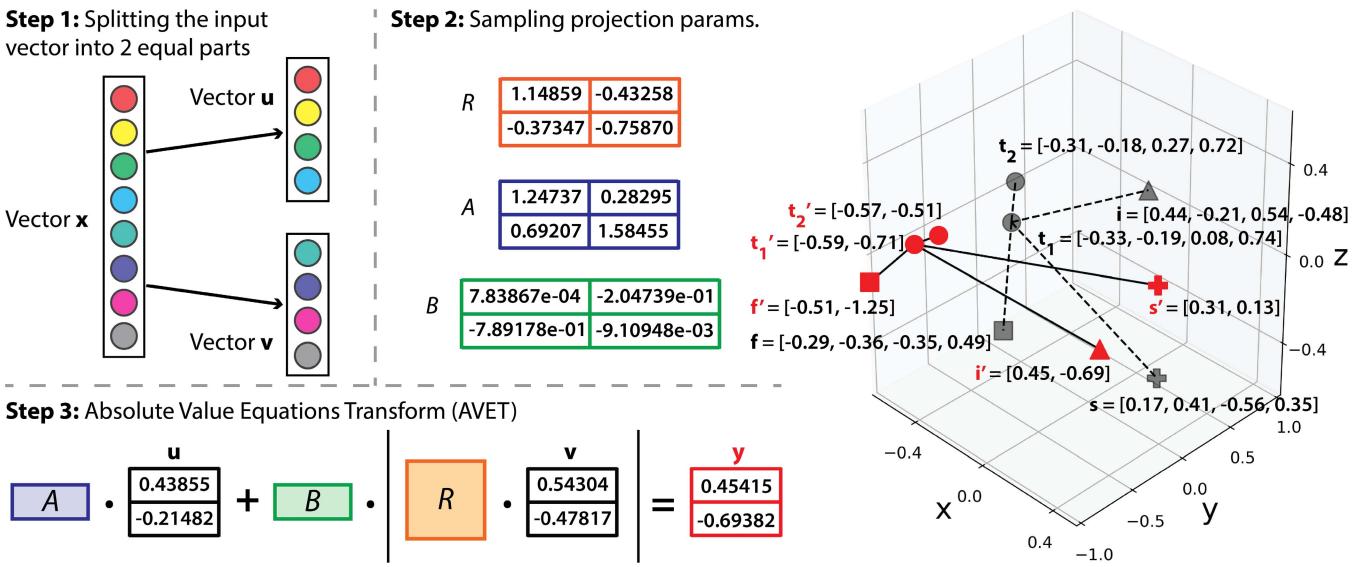


Fig. 3. The intuition of the proposed method: (left) AVET function with input is point **i** in the above toy dataset. (right) Before and after applying AVET: black points indicate original templates and red points are transformed outputs.

In Section Appendix-A, we provide a simple example to explain why those two equations 2-3 could be broken by using linkage attacks. To address this problem, an intuitive idea is projecting vector $\mathbf{v} \mapsto \phi(\mathbf{v})$, which allows us to separate the linkage information into *disconnected* data (i.e., creating multiple GAVE problems). Therefore, Eq. 3 is updated to: $A \cdot \mathbf{u} + B \cdot |\phi(\mathbf{v})| = \mathbf{y}$, where $\phi(\cdot)$ is any mapping function that has distance preservation nature (i.e., linear function: RP; non-linear function: Random Fourier Features).

Putting all together, we define our AVET function $avet_{R,A,B}(\cdot) : \mathbb{R}^m \to \mathbb{R}^n$ via:

$$avet(\mathbf{x}) = A \cdot \mathbf{u} + B \cdot |R \cdot \mathbf{v}|, \tag{4}$$

where $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ are two sub-vectors derived from biometric template $\mathbf{x} \in \mathbb{R}^m$, with $n = \lfloor m/2 \rfloor$. Particularly, the first half of vector $\mathbf{x}$ is set as $\mathbf{u}$ and vector $\mathbf{v}$ is the later half of the input template. Random matrices $R, A, B \in \mathbb{R}^{n \times n}$ are sampled i.i.d. from normal Gaussian distribution $\mathcal{N}\left(0, \frac{1}{n}\right)$. In addition, there is a constraint, i.e., $R \cdot \mathbf{v} \neq \mathbf{u}$, which prevents AVET from being converted back into the original GAVE problem. Figure 3 illustrates the workflow of AVET and Algorithm 1 summarizes the procedure of generating a secure intermediate template.

Remark 1: To avoid linkage attacks, matrix R must be unique, independent, and non-repetitive every time users revoke their protected templates.

AVET and Existing Cancellable Biometrics Systems:

To show the compatibility between AVET and existing CB schemes, RP function in BH and GRP-IoM algorithms would be replaced by our proposed transformation. The two variants are dubbed as Bi-AVET and In-AVET.

1) Bi-AVET: Like the structure of BH, we apply a threshold-based method that can binarize the returned value of $avet(\mathbf{x})$ without affecting the accuracy significantly. The Bi-AVET function is defined as follows:

$$b\_avet(\mathbf{x}) = sgn(avet(\mathbf{x})). \tag{5}$$

Algorithm 1 Absolute Value Equations Transform (AVET)

Input: Biometric feature vector $\mathbf{x} \in \mathbb{R}^m$
Output: Transformed vector $\mathbf{y} \in \mathbb{R}^n$ and helper data (R, A, B)
Workflow:
1: $n = \lfloor m/2 \rfloor$
2: $\mathbf{u} \leftarrow \mathbf{x}[:n]$; $\mathbf{v} \leftarrow \mathbf{x}[n:2n]$;
3: $R, A, B \overset{i.i.d.}{\sim} \mathcal{N}\left(0, \frac{1}{n}\right)$ such that $R \cdot \mathbf{v} \neq \mathbf{u}$;
4: $\mathbf{y} \leftarrow A \cdot \mathbf{u} + B \cdot |R \cdot \mathbf{v}|$;
return $\mathbf{y}, R, A, B$;

2) In-AVET: Multiple different triplets $\{(R, A, B)_i\}_{i=1}^k$ are generated. Without loss of generality, matrices A, B have a size of $g \times n$ in In-AVET. For each triplet, the intermediate vector $\mathbf{y}_i = avet_{R_i,A_i,B_i}(\mathbf{x})$ is calculated, and its max element $y_{ij} = max(\mathbf{y}_i)$ is found, with $j \in [g]$. The index of that max element (i.e., value j) is then appended to the protected template $\mathbf{z} \in \{1, \ldots, g\}^k$.

C. Privacy Preserving

In this section, we provide the security proof of AVET. The proposition 1 shows that even in the worst situation, it is computationally hard for attackers to retrieve the original feature vector. To find $\mathbf{x}$, they must solve an underdetermined system, which has infinitely many solutions.

Proposition 1: According Algorithm 1, let $\mathbf{x} = (x_1, \ldots, x_m)$ *be a solution of the system*:

$$A \cdot \mathbf{u} + B \cdot |R \cdot \mathbf{v}| = \mathbf{y},$$

where vector $\mathbf{u} = (x_1, \ldots, x_n)$ *and* $\mathbf{v} = (x_{n+1}, \ldots, x_m)$, *matrices* $R, A, B \in \mathbb{R}^{n \times n}$, *and vector* $\mathbf{y} \in \mathbb{R}^n$. *Given a set of k compromised quadruplets* $\{(R, A, B, \mathbf{y})_i\}_{i=1}^k$ *of the same vector* $\mathbf{x}$, *with* $n, m, k \in \mathbb{N}^*$ *and* $m = 2n$. *Finding* $\mathbf{x}$, *the solution of Eq. 4, is computational infeasible.*

Proof: - Case $k = 1$: With absolute term $|R \cdot \mathbf{v}|$, we set vector $\mathbf{t} = |R \cdot \mathbf{v}| = (|\mathbf{r}_1 \cdot \mathbf{v}|, \ldots, |\mathbf{r}_n \cdot \mathbf{v}|)$, with $i \in [n]$. Thus, the system becomes $A \cdot \mathbf{u} + B \cdot \mathbf{t} = \mathbf{y}$, which can be written as:

$$\begin{cases} a_{11}u_1 + \cdots + a_{1n}u_n + b_{11}t_1 + \cdots + b_{1n}t_n = y_1 \\ \vdots \\ a_{n1}u_1 + \cdots + a_{nn}u_n + b_{n1}t_1 + \cdots + b_{nn}t_n = y_n \end{cases} \tag{6}$$

The system (6) is a system of n equations of $2n$ unknowns.

- Case $k + 1$: We have:

$$\begin{cases} a_{11}^1u_1 + \cdots + a_{1n}^1u_n + b_{11}^1t_1^1 + \cdots + b_{1n}^1t_n^1 = y_1^1 \\ \vdots \\ a_{n1}^1u_1 + \cdots + a_{nn}^1u_n + b_{n1}^1t_1^1 + \cdots + b_{nn}^1t_n^1 = y_n^1 \\ \vdots \\ a_{11}^{k+1}u_1 + \cdots + a_{1n}^{k+1}u_n + b_{11}^{k+1}t_1^{k+1} \\ \quad + \cdots + b_{1n}^{k+1}t_n^{k+1} = y_1^{k+1} \\ \vdots \\ a_{n1}^{k+1}u_1 + \cdots + a_{nn}^{k+1}u_n + b_{n1}^{k+1}t_1^{k+1} \\ \quad + \cdots + b_{nn}^{k+1}t_n^{k+1} = y_n^{k+1} \end{cases} \tag{7}$$

The system (7) is an underdetermined system of $(k + 1) \times n$ equations with $(k + 2) \times n$ unknowns.

Conclusion: Given k distinct sets $\{(R, A, B, \mathbf{y})_i\}_{i=1}^k$, we can establish a system of $k \times n$ equations with $(k+1) \times n$ unknowns. Therefore, reversing $\mathbf{x}$ from those leaked information is equivalent to solving an underdetermined system, which yields infinitely many solutions. □

In the worst case, the proposition 1 implies that it is impossible for attackers to learn the actual values of all entries in $\mathbf{x}$. Note that both AVET and RP rely on information loss via dimensional reduction to prove irreversibility. However, with RP, attackers can collect enough information over time and then *obtain* exactly the biometric template $\mathbf{x}$, i.e., solving a system in which the number of equations is equal to that of unknowns. By contrast, AVET is always an underdetermined system thanks to additive absolute terms.

From the above discussion, the soundness of our method is confirmed. Particularly, in normal cases, if attackers have no knowledge of the structure of AVET, they gain no fruitful information from disclosed $\{(R, A, B, \mathbf{y})_i\}_{i=1}^k$. In the worse case when one quadruplet $(R, A, B, \mathbf{y})$ and AVET algorithm are both known by adversaries, solving Eq. 4 from the compromised data is as hard as solving NP-hard problem. Even in the worst scenario, attackers cannot find exactly the biometric template $\mathbf{x}$ because AVET remains permanently underdetermined.

D. Similarity Preserving

In this section, we prove that our proposed method has distance preservation property via lemma 2. First, we prove that if the feature vectors are *close*, then their corresponding absolute vectors are close to each other also.

Proposition 2: For all $\mathbf{c}, \mathbf{d} \in \mathbb{R}^m$ *and a non-negative real number* ε. *If* $\mathbf{c} \simeq_\varepsilon \mathbf{d}$, *then* $|\mathbf{c}| \simeq_\varepsilon |\mathbf{d}|$.

Proof: Let $\mathbf{c} \simeq_\varepsilon \mathbf{d}$

$\iff ||\mathbf{c} - \mathbf{d}||^2 \leqslant \varepsilon^2$

$\iff \sum_{i=1}^m (c_i - d_i)^2 \leqslant \varepsilon^2$ $(*)$

By the Reverse triangle inequality, we have:

$||c| - |d|| \leqslant |c - d|$

$\iff (|c| - |d|)^2 \leqslant (c - d)^2$ $(**)$

By $(*)$ and $(**)$, we have:

$$dist(|\mathbf{c}|, |\mathbf{d}|) = \sqrt{\sum_{i=1}^m (|c_i| - |d_i|)^2} \leqslant \sqrt{\sum_{i=1}^m (c_i - d_i)^2} \leqslant \varepsilon$$

Thus, $|\mathbf{c}| \simeq_\varepsilon |\mathbf{d}|$. □

In this paper, we assume that if feature vectors $\mathbf{c}$ and $\mathbf{d}$ are close, then their sub-vectors are also close to each other, i.e., $\mathbf{u}_c \simeq_\varepsilon \mathbf{u}_d$ and $\mathbf{v}_c \simeq_\varepsilon \mathbf{v}_d$. We prove that if $\mathbf{c} \simeq_\varepsilon \mathbf{d}$, then the Euclidean distance between transformed vectors is never exceed 2ε.

Proposition 3: For all $\mathbf{c}, \mathbf{d} \in \mathbb{R}^m$ *and a non-negative real number* ε. *If* $\mathbf{c} \simeq_\varepsilon \mathbf{d}$, *then* $avet(\mathbf{c}) \simeq_{2\varepsilon} avet(\mathbf{d})$.

Proof: Set:

$$avet(\mathbf{c}) = A \cdot \mathbf{u}_c + B \cdot |R \cdot \mathbf{v}_c| = \mathbf{e} + \mathbf{o}.$$
$$avet(\mathbf{d}) = A \cdot \mathbf{u}_d + B \cdot |R \cdot \mathbf{v}_d| = \mathbf{p} + \mathbf{q}.$$

By the lemma 1 (i.e., JL lemma with the zero-distortion assumption) and proposition 2, if $\mathbf{c} \simeq_\varepsilon \mathbf{d}$, we have:

$$\begin{cases} f_A(\mathbf{u}_c) \simeq_\varepsilon f_A(\mathbf{u}_d) \\ f_B(|f_R(\mathbf{v}_c)|) \simeq_\varepsilon f_B(|f_R(\mathbf{v}_d)|) \end{cases} \iff \begin{cases} \mathbf{e} \simeq_\varepsilon \mathbf{p} \\ \mathbf{o} \simeq_\varepsilon \mathbf{q}. \end{cases}$$

The Euclidean distance between two transformed vectors:

$$\begin{aligned} &dist(avet(\mathbf{c}), avet(\mathbf{d})) \\ &= \sqrt{\sum_{i=1}^m (e_i + o_i - p_i - q_i)^2} \\ &= \sqrt{\sum_{i=1}^m (e_i - p_i)^2 + (o_i - q_i)^2 + 2(e_i - p_i)(o_i - q_i)} \\ &\leqslant \sqrt{\sum_{i=1}^m 2\,(e_i - p_i)^2 + 2\,(o_i - q_i)^2} \text{ (Cauchy inequality)} \\ &\leqslant \sqrt{2\varepsilon^2 + 2\varepsilon^2} = 2\varepsilon. \end{aligned}$$

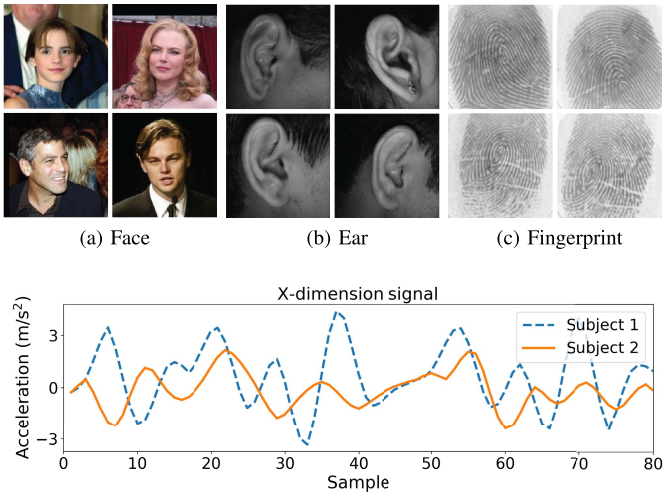
Thus, $avet(\mathbf{c}) \simeq_{2\varepsilon} avet(\mathbf{d})$. □

If feature vectors $\mathbf{c}$, $\mathbf{d}$ belong to different individuals, then the distance between them would be large, i.e., $||\mathbf{c} - \mathbf{d}|| \leqslant \Delta$, with $\Delta \gg \varepsilon$. By the same argument with propositions 2-3 we get $avet(\mathbf{c}) \simeq_{2\Delta} avet(\mathbf{d})$.

Lemma 2 (Upper Bound of AVET): Given transform function $avet(\cdot)$ *according to Eq. 4, for all inputs* $\mathbf{c}, \mathbf{d} \in \mathbb{R}^m$, *we have*:

$$||avet(\mathbf{c}) - avet(\mathbf{d})|| \leqslant 2||\mathbf{c} - \mathbf{d}||.$$

Based on propositions 2 and 3, the correctness of lemma 2 is proved, which says that the Euclidean distance between two projected templates is proportional to the distance between original vectors. Like the state-of-the-art transform function RDM, the lower bound of AVET is still an open question.



(a) Face (b) Ear (c) Fingerprint

(d) Inertial sensor-based gait signal

Fig. 4. Raw biometric examples from: (a) LFW, (b) IITD-Ear, (c) FVC2002-DB1, (d) CNU datasets.

However, the promising results obtained in the next section help to imply that inter and intra variations of the data are largely maintained after applying AVET.

IV. Experiments

A. Datasets

- Labeled Faces in the Wild (LFW) [38]: The dataset consists of 13,233 facial images of 5749 individuals gathered from the Internet. There are 423 subjects with more than four images. The first five images of those identities were used in the experiments.

- Celebrities in Frontal-Profile in the Wild (CFPW) [39]: The dataset contains images of 500 celebrities in frontal and profile views. Frontal-pose pictures were used in experiments so that each subject has 10 images.

- CASIA Face Image Database Ver. 5.0 (CASIA-V5) [40]: We used the cropped version of this dataset, which consists of 2500 color images of 500 subjects. All of the crops are considered to be used in the experiments.

- IIT Delhi Ear Image Database Ver. 1.0 (IITD-E) [41]: The database consists of two versions: raw and cropped ears. There are 31 subjects with more than four images. The first five raw images of those individuals were used in the experiments.

- Fingerprint Verification Competition (FVC2002) [42]: We used DB1, DB2, and DB3 datasets of FVC2002 for experiments. Each dataset contains images of 100 different individuals. For each subject, the first three finger images were used for training feature extraction model, the remaining 5 images were used in transformation experiments.

- The gait dataset of Chonnam National University (CNU) [43]: The dataset contains gait signals of 38 subjects captured using mobile phone sensors. The data were acquired during a long-time span of several days and under varied environmental conditions (i.e., shoes, clothes, road surfaces), thus this dataset is considered almost realistic. To obtain the same number of feature vectors, 10 gait cycles of each subject are taken, yielding a total of 380 feature embeddings.

TABLE II
Feature Extraction Methods for Different Modalities

Modality	Employed feature extraction techniques	Dim.
Face	- We applied the same preprocessing steps in [33] and the pretrained FaceNet model[2] to extract facial features.	$\mathbb{R}^{512}$
Ear	- We applied the pretrained CNN model in paper [44] to extract features.	$\mathbb{R}^{512}$
Fingerprint	- We applied the same preprocessing steps and Kernel Principal Component Analysis (KPCA) method in [45] to get fixed length feature vectors.	$\mathbb{R}^{299}$
Gait	- We used the framework in [43] to extract user's features on both time and frequency domains.	$\mathbb{R}^{289}$

B. Setup

Distinct human traits have distinct characteristics, thus we apply particular methods that were best fitted to extract different types of biometrics. Table II provides details of the extraction methods implemented and their corresponding output representations.

Matching experiments are performed with state-of-the-art CB schemes, namely, BH, GRP-IoM, and RDM. The three techniques are generic and can be applied to various human traits. Besides, the *original* matching results are also reported. With BH, we project feature vectors $\mathbf{x} \in \mathbb{R}^m$ using an orthogonal matrix of size $\lfloor m/2 \rfloor \times m$. In terms of the ranking-based method [7], the GRP-IoM variant was used in experiments. In RDM, the dimension of transformed features is always reduced to half because of the nature of this algorithm. Therefore, if the input vector's length is an odd number, we remove the last element of the vector before running RDM.

In the experiments, the proposed transformation function AVET and its two enabled CB methods (i.e., Bi- and In-AVET) are implemented. With AVET and Bi-AVET, matrices R, A, B have size $n \times n$, with $n = \lfloor m/2 \rfloor$. For In-AVET, we sample[1] $k = 300$ distinct triplets $\{(R, A, B)_i\}_{i=1}^{k}$, with $R \in \mathbb{R}^{n \times n}$ and $A, B \in \mathbb{R}^{g \times n}$, where $g = 16$.

C. Evaluation Metrics and Matching Method

Five metrics, namely, Equal Error Rate (EER), Decidability Index (DI), Recognition Index (RI), Receiver Operating Characteristic (ROC) curve, and Cumulative Match Characteristics (CMC) curve were used to evaluate the system performance. The experiment is repeated 5 times, each time with different enrolled (or gallery) images and helper data. The mean and standard deviation of EER, DI, and RI are reported. In this paper, the degree of closeness between protected templates is computed in a transformed domain with respect to Euclidean distance. Based on original published papers, distinct measurements are implemented for different transformation methods. Particularly, BH uses Hamming, GRP-IoM uses Jaccard, and RDM uses cosine distance to compute similarity scores.

In the verification task, one-shot enrollment was implemented. We randomly chose one image per user for enrollment

[1] $k = 300$ and $g = 16$ are optimal hyperparameters in the original paper.
[2] Available: https://github.com/davidsandberg/facenet

TABLE III
EER% FOR ORIGINAL AND TRANSFORMED TEMPLATES IN THE STOLEN HELPER DATA SCENARIO (LOWER IS BETTER)

Method	LFW	CFPW	CASIA-V5	IITD-E	2002-DB1	2002-DB2	2002-DB3	CNU
Without protection function								
Original	1.83±0.22	1.90±0.25	5.95±0.23	5.65±1.14	0.15±0.12	0.35±0.12	2.15±0.46	1.99±0.60
RP	2.27±0.10	2.30±0.18	6.47±0.30	6.61±1.56	0.35±0.34	0.90±0.49	4.95±0.83	2.28±0.75
RDM (no MF)	5.69±1.45	6.42±1.63	8.72±0.89	8.87±1.35	0.70±0.37	1.40±0.44	4.40±0.64	28.60±5.31
AVET	2.51±0.15	2.64±0.24	6.98±0.50	6.13±0.97	0.05±0.10	0.36±0.13	2.22±0.76	2.75±0.82
With protection function								
BH	2.72±0.23	2.81±0.27	7.64±0.40	6.61±1.72	0.35±0.25	1.12±0.56	5.30±1.01	11.81±1.32
GRP-IoM	2.25±0.24	2.33±0.33	7.07±0.30	6.13±0.97	0.20±0.19	0.50±0.27	2.95±0.73	5.20±1.13
RDM	13.50±2.49	15.45±2.42	14.12±1.72	12.10±1.52	2.45±0.66	5.40±0.51	7.75±1.13	49.77±1.30
Bi-AVET	3.85±0.11	4.60±0.33	9.22±0.47	7.90±0.14	0.2±0.18	0.60±0.33	3.40±0.87	15.93±2.20
In-AVET	2.51±0.18	2.53±0.25	7.16±0.12	6.13±0.90	0.05±0.17	0.39±0.18	1.55±0.37	6.24±1.30

TABLE IV
DI FOR ORIGINAL AND TRANSFORMED TEMPLATES IN THE STOLEN HELPER DATA SCENARIO (HIGHER IS BETTER)

Method	LFW	CFPW	CASIA-V5	IITD-E	2002-DB1	2002-DB2	2002-DB3	CNU
Without protection function								
Original	4.51±0.07	4.37±0.11	3.22±0.04	3.11±0.18	7.03±0.35	6.89±0.37	4.48±0.24	2.50±0.05
RP	4.25±0.06	4.12±0.08	3.11±0.05	3.09±0.18	5.98±0.28	5.44±0.35	3.65±0.18	2.49±0.08
RDM (no MF)	3.13±0.29	2.91±0.25	2.78±0.18	2.57±0.19	4.90±0.27	4.56±0.14	3.17±0.12	1.11±0.13
AVET	3.98±0.06	3.85±0.07	3.02±0.08	3.03±0.16	7.73±0.31	6.12±0.43	3.86±0.21	2.50±0.07
With protection function								
BH	3.87±0.03	3.71±0.08	2.84±0.05	2.77±0.16	4.95±0.18	4.56±0.16	3.25±0.18	1.97±0.09
GRP-IoM	3.37±0.06	3.11±0.08	2.73±0.04	2.34±0.25	4.22±0.16	3.93±0.22	2.82±0.10	2.51±0.10
RDM	2.29±0.24	2.09±0.21	2.21±0.18	2.29±0.21	3.68±0.25	2.96±0.08	2.79±0.15	0.05±0.04
Bi-AVET	3.39±0.04	3.20±0.05	2.63±0.08	2.58±0.12	3.89±0.27	5.44±0.31	3.71±0.23	1.96±0.21
In-AVET	3.93±0.04	3.90±0.03	2.92±0.03	2.98±0.14	7.51±0.16	6.27±0.25	4.54±0.14	2.26±0.12

TABLE V
RI% FOR ORIGINAL AND TRANSFORMED TEMPLATES IN THE STOLEN HELPER DATA SCENARIO (HIGHER IS BETTER)

Method	LFW	CFPW	CASIA-V5	IITD-E	2002-DB1	2002-DB2	2002-DB3	CNU
Without protection function								
Original	91.90±0.66	89.58±1.22	74.44±2.20	95.32±0.79	99.85±0.12	99.75±0.00	95.65±0.96	95.38±2.18
RP	89.68±0.75	87.51±1.29	72.53±2.26	95.00±1.64	99.70±0.24	99.15±0.44	92.45±0.19	94.15±2.67
RDM (no MF)	81.90±4.11	76.76±5.16	69.33±2.20	94.52±1.09	99.35±0.37	97.55±1.20	89.15±1.86	67.72±3.40
AVET	88.11±0.87	86.05±1.39	70.65±2.03	94.68±1.39	99.85±0.12	99.75±0.16	94.50±1.08	93.04±2.16
With protection function								
BH	84.73±0.57	82.60±1.66	62.50±3.11	92.74±1.98	99.65±0.25	98.30±0.98	90.35±1.51	40.70±3.93
GRP-IoM	89.00±0.80	86.85±1.36	70.15±2.47	94.84±1.21	99.80±0.19	99.50±0.22	94.30±0.68	82.16±3.79
RDM	58.82±8.65	50.45±8.19	51.95±4.36	89.52±1.61	95.35±2.12	85.20±2.58	80.65±2.92	7.08±3.98
Bi-AVET	77.84±0.75	74.85±1.16	57.13±2.55	91.45±1.09	99.55±0.29	99.00±0.57	91.05±1.78	38.66±4.28
In-AVET	88.22±0.68	85.80±1.36	69.21±1.94	94.52±0.94	99.95±0.10	99.85±0.12	96.20±0.53	80.88±4.61

and the rest were used for testing. False Accept Rate (FAR) and False Reject Rate (FRR) are common metrics used to measure matching efficiency. EER is defined as a point where FAR equals FRR. The lower the EER value obtains, the better the system performance. The metric DI estimates how separable the genuine distribution is from its corresponding impostor one. Given genuine and impostor score populations, DI is calculated as follows: $DI = |\mu_g - \mu_i| / \sqrt{(\sigma_g^2 + \sigma_i^2)/2}$, with (μ_g, σ_g) and (μ_i, σ_i) are (mean, standard deviation) of genuine and impostor distributions, respectively. The higher DI implies the better discrimination between intra and inter classes, yielding lower error rates (i.e., EER, FAR, FRR). Besides, ROC curve plots display the overview of performance comparison between selected methods, supported by the AUC (area under the curve) score.

With the identification experiment, we used metric RI which is commonly called rank-1 identification rate (i.e., rank $r = 1$) to evaluate the identification ability of the system.

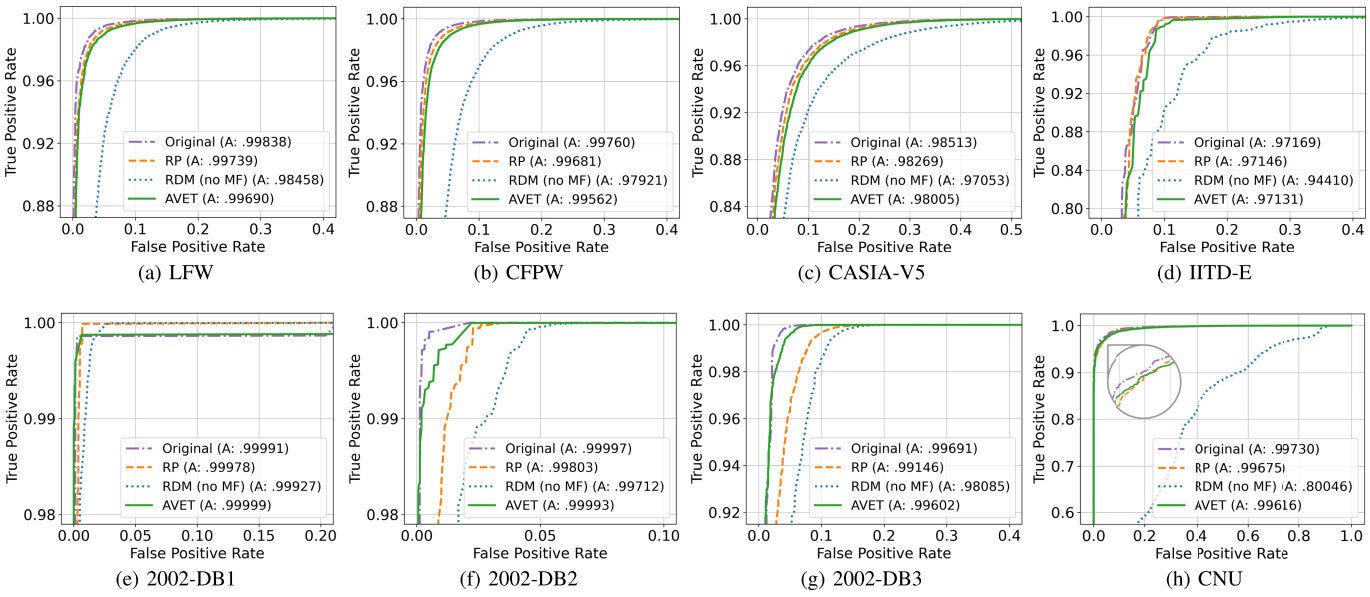


Fig. 5. ROC curves in the stolen helper data scenario; "A" denotes *Area under the curve* (best view in color).

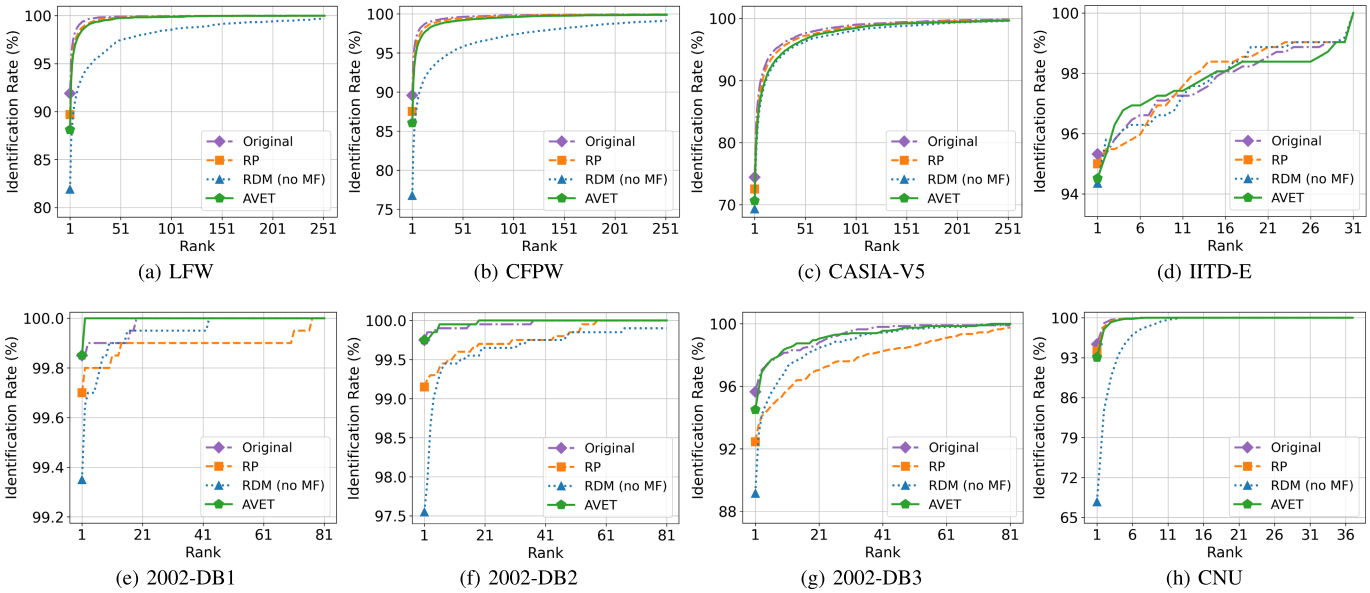


Fig. 6. CMC curves in the stolen helper data scenario (best view in color).

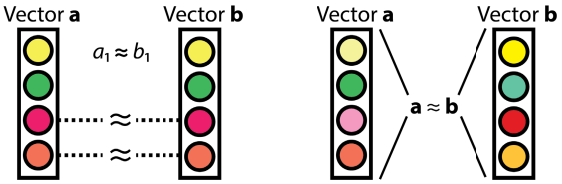
To criticize the ranking power of the system, we illustrated the identification rate with respect to rank r via CMC curves.

D. Results

1) Unimodal Cancellable Biometrics: Tables III, IV, V report evaluation results in terms of EER, DI, and RI respectively. Besides, the ROC and CMC curves are displayed in Fig. 5-6 to generally compare the performances of AVET to two state-of-the-art algorithms: RP and RDM (i.e., the term "RDM (no ML)" indicates the RDM transform method without its protection function - Median filter). Recall that, to show the real influence of transform functions, the simplest verification and identification schemes were used in experiments. In addition, the dimension of all transformed vectors generated by the three observed techniques was reduced with the same factor (i.e., 50%) so that the performances of those methods could be analyzed fairly. All results in this section were measured under the *stolen helper data* scenario, in which each subject was given the same projection parameters to transform the biometrics templates.

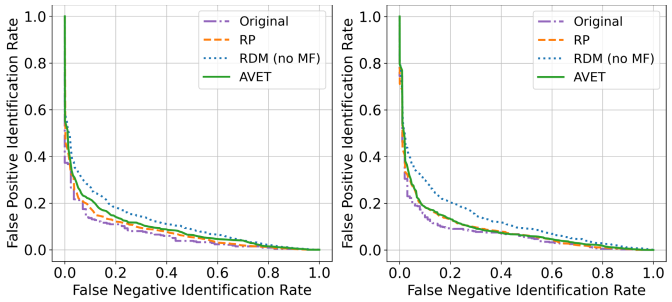
We observed that both RP and AVET can preserve, pretty well, the *baseline* performance that does not perform any transform function (i.e., original data). The results of AVET are slightly lower than RP on the majority of matching experiments, which is easy to explain since AVET gains more distortions than RP due to losing information for the purpose of privacy. It is a trade-off between accuracy and security; in turn, AVET is much more secure than RP, which is the dominant advantage of our proposed method.

In both verification and identification tasks, our proposed method exceeds RDM for all eight datasets. With *learned* features (i.e., the first seven datasets applied machine/ deep learning-based extraction methods), performances of RDM are quite close to those of AVET. For the *hand-crafted* gait



(a) Element-level similarity (b) Vector-level similarity

Fig. 7. Illustration of element and vector-level assumptions.



(a) LFW (b) CFPW

Fig. 8. Performance comparison under open-set condition.

features, RDM yields an uncommonly high EER value of about 28.60%, which is more than 10 times compared with our proposed method. The reason for this event is that RDM relies on a stronger assumption than the one adopted in this research. Particularly, RDM assumes that if two feature vectors **a** and **b** belong to the identical individual, then the dissimilarity between their pairwise elements would be small. In other words, the distance preservation property of RDM was proved based on an *element*-level assumption: $|a_i - b_i| < \varepsilon$, with $i \in [m]$. While, more generally, RP uses a *vector*-level one: $||\mathbf{a} - \mathbf{b}||_2 < \varepsilon$. So that the similarity preserving of AVET, loosely speaking, relies on the *hybrid* assumption (i.e., proposition 3) in the unimodal mode. The difference between two types of assumptions is illustrated in Fig. 7. Besides, like RP, RDM (without Median filters) is a reversible and insecure transform function in the worst case [26, Section V-C]. Thus, AVET outperforms RDM transform function regarding both accuracy and security perspectives.

As anticipated, after applying protection functions, both Bi-AVET and In-AVET achieve competitive performances compared with the original schemes (i.e., BH and GRP-IoM). This implies that the proposed method AVET is suitable with existing RP-based architectures. Notably, unlike the entirely provable cancellation schemes such as BH and GRP-IoM, the similarity preserving property of RDM was proved without including the protection step. It might be an explanation why the performance of RDM scheme reduces sharply after implementing the Median filters.

Under the open-set condition, the efficiency of AVET with respect to false positive and false negative identification rates (i.e., FPIR and FNIR) was analyzed on eight distinct datasets. Particularly, we randomly selected 20 percent of subjects as unknown individuals, so the ratio of known to unknown subjects was 4:1 in each dataset. As expected, the open-set results followed the same pattern seen in previous experiments. We illustrate the typical "FPIR versus FNIR characteristics" over LFW and CFPW datasets in Fig. 8.

TABLE VI

COMPUTATIONAL SPEED COMPARISON WITH OTHER TRANSFORM FUNCTIONS REPORTED IN SECONDS

Dim.	RP	RDM	AVET
I: Generating helper data			
Helper data	Orthogonal matrix R	Random grid RG, random key K	Random matrices R, A, B
$\mathbb{R}^{512}$	2.1137±0.0070	0.00049±3.918e^{-7}	0.00516±0.00027
$\mathbb{R}^{299}$	0.2647±0.0127	0.0003±0.00022	0.00198±3.54e^{-7}
$\mathbb{R}^{289}$	0.2411±0.0091	9.92e^{-5}±0.000222	0.00178±0.00027
II: Computing an intermediate template **y**			
Algorithm	Reduce size of R; $R \cdot \mathbf{x}$	$fs = \mathbf{x} + RG$; $D \leftarrow fs, K$	$\mathbf{u}, \mathbf{v} \leftarrow \mathbf{x}$; $A \cdot \mathbf{u} + B \cdot \lvert R \cdot \mathbf{v} \rvert$
$\mathbb{R}^{512}$	0.0016±0.0022	0.00178±0.00027	0.00049±1.07e^{-7}
$\mathbb{R}^{299}$	0.0004±0.0004	0.00079±0.00027	9.92e^{-5}±0.00022
$\mathbb{R}^{289}$	0.0003±0.0003	0.00099±1.31e^{-7}	9.92e^{-5}±0.00022
$\sum$ = I + II: Total time			
$\mathbb{R}^{512}$	2.1139±0.0071	0.00188±0.00022	0.00565±0.00027
$\mathbb{R}^{299}$	0.2651±0.0128	0.00109±0.00022	0.00208±0.00022
$\mathbb{R}^{289}$	0.2414±0.0093	0.00099±1.31e^{-7}	0.00179±0.00027

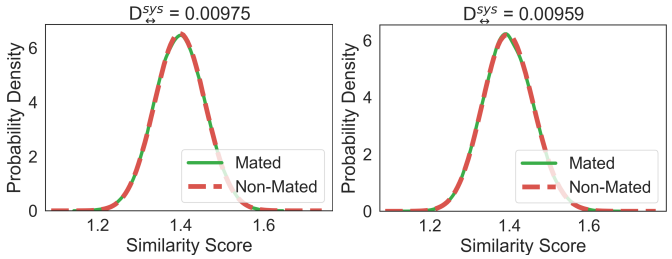
TABLE VII

ACCURACY PERFORMANCES FOR TRANSFORMED TEMPLATES (WITHOUT PROTECTION FUNCTION) IN THE STOLEN HELPER DATA SCENARIO

Metric	Method	LFW + IITD	CFPW + IITD	CASIA + IITD
EER%	Original	0.63±0.32	0.79±0.24	2.22±0.81
	RDM	4.88±2.22	4.79±1.97	4.65±2.37
	AVET	0.81±0.001	1.08±0.33	2.53±1.22
DI	Original	5.27±0.30	5.23±0.26	4.47±0.45
	RDM	3.44±0.51	3.46±0.58	3.50±0.57
	AVET	4.93±0.31	5.03±0.24	4.36±0.45
RI%	Original	99.19±0.94	99.68±0.65	98.55±1.72
	RDM	99.03±0.94	98.55±1.07	98.39±2.10
	AVET	99.19±0.72	99.19±0.51	98.55±1.79

To show the robustness of AVET, the speed of transforming a single feature vector into an intermediate template was computed and displayed in Table VI. This experiment was implemented in Python 3.7 and executed on a computer equipped with a Core i5-8500 3.00GHz processor, 32GB of RAM, and a SATA SSD of 1TB. We observed that both RDM and AVET are able to transform feature vectors in a very short time. By contrast, RP requires more effort since generating an orthogonal matrix is time-consuming.

2) Bimodal Cancellable Biometrics: Table VII reports the matching results for bimodal transformed vectors generated from the combination of face and ear biometrics. In this experiment, a raw facial vector is concatenated with an ear feature vector to produce an *original* bimodal embedding. With RDM, vectors fX and fY are face and ear biometric templates, respectively. Likewise, in AVET, vector **u** is facial features and vector **v** is filled up with ear features. Obviously, in the bimodal mode, the similarity preserving property of AVET can be proved with the vector-level assumption, while RDM still relies on the element-level one. It means RDM uses a stronger assumption than AVET, which may explain why our proposed algorithm achieves an extremely higher accuracy than that of RDM. As expected, the bimodal approach returns better performance compared to the unimodal method, which indicates that AVET is effective for generating both unimodal and bimodal cancellable templates.



(a) Without R (b) With R

Fig. 9. Unlinkability analysis on LFW dataset.

TABLE VIII

GLOBAL LINKABILITY SCORES $D_{\leftrightarrow}^{sys}$ FOR DIFFERENT DATASETS AND SETTINGS

Dataset	Without R	With R	Dataset	Without R	With R
LFW	0.00975	0.00959	02-DB1	0.02744	0.02323
CFPW	0.00736	0.00621	02-DB2	0.02763	0.02137
CASIA	0.01200	0.01069	02-DB3	0.02708	0.02517
IITD-E	0.05374	0.05222	CNU	0.05283	0.04837

V. ANALYSIS

A. Unlinkability

As mentioned above, irreversibility and unlinkability are the two most critical criteria in the CB field. Concerning irreversibility, projecting the feature vector via $\phi(\mathbf{x}) = R \cdot \mathbf{x}$ before transforming it with absolute equations is required to guarantee the security of the system. Regarding the latter requirement, we expect that function $\phi(\cdot)$ will also help in reducing linkability between templates. To examine our prediction and gain a full understanding of the role of $\phi(\cdot)$, we analyze the system's linkability degree in two conditions: "With R" and "Without R". Those settings reflect the unlinkability level achieved by AVET and Eq. 3, respectively.

In this section, the unlinkability of AVET is justified using the framework that was developed by Gomez-Barrero et al. [47]. Various secure intermediate templates are generated by using AVET with 10 distinct triplets (R, A, B). The *mated pairs* templates correspond to transformed templates derived from the same subject and the *non-mated pairs* are templates extracted from different samples. The linkability of the system is evaluated via the global score $D_{\leftrightarrow}^{sys} \in [0, 1]$; the closer the score to zero, the better the proposed method. We illustrate the unlinkability curves of *mated* and *non-mated* distributions over LFW dataset in Fig. 9. The two distributions are almost overlapped each other, yielding a significant low linkability score $D_{\leftrightarrow}^{sys} = 0.00959$ when using AVET. The $D_{\leftrightarrow}^{sys}$ scores of other datasets are displayed in Table VIII.

It is observed from Table VIII that the global linkability scores $D_{\leftrightarrow}^{sys}$ in both cases are negligible, which implies that AVET satisfies the stringent requirement of unlinkability. Furthermore, the linkability scores are slightly decreased on all eight datasets when projection function $\phi(\cdot)$ was applied. This means using matrix R not only plays an important position in irreversibility but also contributes to enhance unlinkability perspective.

TABLE IX

BF ATTACK ANALYSIS: PROBABILITY TO GUESS CORRECTLY SINGLE AND ENTIRE COMPONENTS OF THE ORIGINAL TEMPLATE $\mathbf{x}$

Dataset	Min value	Max value	$\mathbb{P}$ (single)	$\mathbb{P}$ (total)
LFW	-0.1857	0.1933	$1/3791 < 1/2^{11}$	$1/2^{11\times512}$
CFPW	-0.2156	0.2070	$1/4227 < 1/2^{12}$	$1/2^{12\times512}$
CASIA	-0.1896	0.1866	$1/3763 < 1/2^{11}$	$1/2^{11\times512}$
IITD-E	-0.1306	0.1748	$1/3055 < 1/2^{11}$	$1/2^{11\times512}$
02-DB1	-0.8031	0.6303	$1/14335 < 1/2^{13}$	$1/2^{13\times299}$
02-DB2	-0.7130	0.6831	$1/13962 < 1/2^{13}$	$1/2^{13\times299}$
02-DB3	-0.5224	0.5688	$1/10913 < 1/2^{13}$	$1/2^{13\times299}$
CNU	-0.0702	0.7649	$1/8352 < 1/2^{13}$	$1/2^{13\times289}$

B. Security

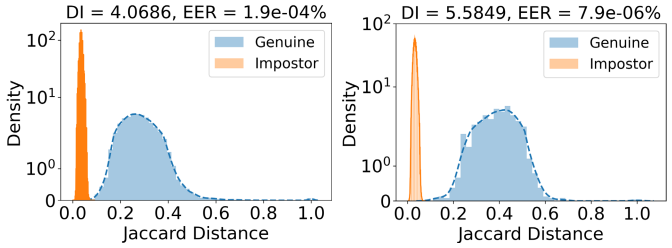
1) Brute Force Attack: In brute force (BF) attacks, attackers have no information about the system (i.e., procedure flow of execution, implemented techniques). They search exhaustively and try all possible combinations to find the original biometrics template $\mathbf{x}$. Since those templates are real-valued vectors, guessing exactly $\mathbf{x}$ is computationally hard. If the adversaries have knowledge about minimum and maximum values of the feature components of $\mathbf{x}$, they can reduce the search space. For instance, assume that attackers know the minimum and maximum values of CFPW dataset are -0.2156 and 0.2070, respectively. There are $4227 > 2^{12}$ possibilities to guess a *single* element of vector $\mathbf{x}$. Thus, the *entire* 512 feature components require around $2^{12\times512} = 2^{6144}$ attempts in total. The probabilities $\mathbb{P}$ to get the precise templates $\mathbf{x}$ are presented in Table IX; the minimum and maximum values are displayed with 4 decimal precision.

2) Pre-Image Attack: In this attack, adversaries try to find a template $\tilde{\mathbf{x}}$ that has a *specific* hash value, i.e., $h(\tilde{\mathbf{x}}) = h(\mathbf{x}_{genuine})$. On one hand, distance-preserving is an indispensable property that helps to maintain the performance and efficiency of CB schemes. But on the other hand, attackers can also rely on the leakage information inherent to this nature to perform pre-image attacks (or similarity-based attacks [19]). For instance, with BH, attackers attempt to find a pre-image $\tilde{\mathbf{x}} \in \mathbb{R}^m$ satisfying $sgn(R \cdot \tilde{\mathbf{x}}) = sgn(\tilde{\mathbf{y}}) = \mathbf{z}$. Lee et al. [28] proposed an attack scheme in which the pre-image could be generated easily. Fortunately, there are several security proposals to address this problem (i.e., designing a helper data management protocol to hide helper data [48], avoiding two-factor input [49], protecting helper data with bio-encryption techniques [50], designing a secure authentication structure [19]). Note that tailoring a complete bio-protection system, which is resilient against those threats, is out of scope in this research and is the topic of the next study.

3) False Acceptance Attack: The threshold-based decision approach is commonly implemented in biometric applications and systems. In the verification phase, the access can be granted when the matching score is lower (or higher) than the pre-defined threshold τ. In false acceptance (FA) attacks, attackers exploit the false positive rate of the system to gain illegitimate access to target accounts. To perform FA attacks, initially, adversaries gather and create a huge database of biometric images. Let the scheme In-AVET be our example, those forged samples are then verified to find

TABLE X
DATABASES USED FOR FA ATTACK EXPERIMENTATION

Database	Genuine	Impostor
Face-DB	CFPW dataset, total: 500 subjects	LFW + CASIA-V5 (5749 + 500), total: 6249 subjects
Finger-DB	02-DB1 dataset, total: 100 subjects	02-DB2, 02-DB3, 04-DB1, 04-DB2, 04-DB3 (100×5), total: 500 subjects



(a) Face-DB (b) Finger-DB

Fig. 10. FA attack analysis: Genuine and Impostor distributions.

a feature vector ω satisfying $matching(in\_avet(\omega), \mathbf{z}_s) \geqslant \tau$, with $\mathbf{z}_s$ is the stored protected template. Table X summarizes how we establish two large databases, namely, Face-DB and Finger-DB, which were used in this experiment. The *genuine* dataset corresponds to a set of authentic users of the system. Their transformed templates are stored in the system's storage as gallery images. The *impostor* dataset contains biometric images collected by attackers.

In various applications and systems, there is a maximum number of entering wrong passwords to prevent attacks and security threats. Let's assume that there is no limitation about the number of wrong *querying* biometric samples, i.e., attackers can query forged biometric templates as many as they want. Thus, adversaries can use all their available images to run FA attacks. For experiments on Face-DB and Finger-DB, the achieved EER values equal to $1.9 \times 10^{-4}\%$ and $7.9 \times 10^{-6}\%$, respectively. Those low EERs indicate that our proposed approach can defend towards false acceptance attacks. We demonstrate the genuine and impostor distributions (with respect to matching score) under FA attacks in Fig. 10.

4) Attacks via Record Multiplicity: In attacks via record multiplicity (ARM), adversaries have more than one copy of transformed templates derived from the identical subject and attempt to trace back exactly the original template by linking those leaked data. We assume that attackers have multiple compromised user's information $\{(R, A, B, \mathbf{y})_i\}_{i=1}^{k}$.

• $k = 1$: Based on the hardness of absolute equations, we claim that solving AVET is an NP-hard problem, which is as hard as the Knapsack problem [37].

• $k > 1$: The proposition 1 proves that for every new stolen quadruplet $(R, A, B, \mathbf{y})$, attackers gain more n equations and n unknowns. Therefore, adversaries can only establish an underdetermined system of $k \times n$ equations with $(k + 1) \times n$ unknowns.

Another way to recover $\mathbf{x}$ is expanding the absolute terms correctly n times to construct a linear system in which the number of equations is equal to that of unknowns. However, the proposition 4 implies that the probability to guess exactly the sign of n inner products between the user's vector $\mathbf{v}$ and random generated matrix R is $\mathbb{P} = 1/2^n$, which is negligible.

Proposition 4: Let $\mathbf{v} \in \mathbb{R}^n$ *be a fixed vector and* $\mathbf{r} \in \mathbb{R}^n$ *be a random vector which is sampled i.i.d. from a normal distribution* $\mathcal{N}(0, s^2)$. *Let X be the event that an inner product of* $\mathbf{r}$ *and* $\mathbf{v}$ *is positive. The probability of event X to occur is* $\mathbb{P} = 0.5$.

Proof: We set $Y = \mathbf{r} \cdot \mathbf{v} = \sum_{i=1}^{n} r_i v_i$. Since $\mathbf{r} \sim \mathcal{N}(0, s^2)$, mean of Y equals to zero and $Var(Y)$ can be computed as:

$$Var(Y) = ||\sum_{i=1}^{n} r_i v_i||^2 = \sum_{i=1}^{n} r_i^2 v_i^2 = s^2 \sum_{i=1}^{n} v_i^2 = ||\mathbf{v}||^2 s^2.$$

Thus, Y is a normal random variable with mean $\mu = 0$ and variance $\sigma^2 = ||\mathbf{v}||^2 s^2$. By standardizing, the random variable Z defined by $Z = \dfrac{Y - \mu}{\sigma}$ has a standard normal distribution.

Therefore: $\mathbb{P}(Y \leqslant 0)$

$$= \mathbb{P}\left(\frac{Y - \mu}{\sigma} \leqslant \frac{0 - \mu}{\sigma}\right) = \mathbb{P}(Z \leqslant 0)$$
$$= \mathbb{P}(-\infty < Z \leqslant 0) = \mathcal{A}(0) - \mathcal{A}(-\infty) = \mathcal{A}(0) = 0.5,$$

with $\mathcal{A}$ is the area under the standard normal curve. Hence, $\mathbb{P}(Y \leqslant 0) = \mathbb{P}(Y > 0) = 0.5$. □

Thus, the proposed AVET is more resilient against ARM attacks compared to RP and RDM transform methods which are completely broken under this condition.

VI. DISCUSSION

Recently, it has witnessed several deep learning-based methods for cancellable biometrics, such as face [50], [51], [52], [53], [54] and EEG signals [55]. The two studies [51] and [52] share the same idea in the transforming step, in which a binary string is pre-defined to each user. A neural network learns to map the user's bio-features to that pre-assigned intermediate template. Hence, the network has to be re-trained whenever the user revokes his/her protected template. In [54], as there is no mention about the measures taken to re-issue protected templates, how the system satisfies the cancellability request is questionable. All of the three researches [50], [53], and [55] are non-generic CB schemes that were tailored for mere certain traits. Particularly, the projection and protection stages in [55] were designed and only suitable for EEG signals.

Recall that the objective of this work is not to introduce a novel bio-template protection scheme but the secure transform function. Bi-AVET and In-AVET were used to illustrate the compatibility of our proposed algorithm that helps to enhance the security level of existing RP-based systems. By comparing the performance of AVET-based methods with deep learning-based CB schemes, we add more evidence to support the claim that AVET provides sufficient security while maintaining usability.

To be fair, we used the same settings with previous studies [51], [52], [53], [54] on the CMU-PIE [56], which yields a dataset that consists of 7140 facial images of 68 subjects. Table XI reports the comparison results regarding the Genuine Acceptance Rate (GAR) against FAR. This shows that our proposed method achieves competitive performance compared to the state-of-the-art SecureFace [50].

TABLE XI
PERFORMANCE COMPARISON WITH DEEP LEARNING-BASED BIO-TEMPLATE PROTECTION SCHEMES ON CMU-PIE DATABASE

Method	Year	GAR@FAR
MEB Encoding [51]	2016	93.22%@0%
Deep CNN [52]	2018	91.91%@0.1%
Deep LDPC*[53]	2019	98.9%@0.1%
DH-NND [54]	2019	96.2%@0.01%
SecureFace [50]	2021	99.00%@0.1%
Bi-AVET	2022	99.70%@0.1% (97.35%@0.01%)
In-AVET	2022	99.95%@0.1% (98.90%@0.01%)

* The value of GAR@FAR is estimated based on the corresponding ROC curves reported in [53].

VII. CONCLUSION

In this paper, we propose the secure projection function, AVET, which can be used as an alternative of the highly efficient yet fragile Random Projection. In addition, AVET is compatible with RP-based approaches, which means it is easy to implement to existing bio-systems without changing much in terms of design and performance. Our proposed method is established based on the famous mathematics work called Absolute Value Equations. Therefore, solving AVET is as hard as solving the Knapsack NP-hard problem. Besides, both the security and similarity preserving properties of AVET are constructed and proved under realistic and reasonable assumptions. Unimodal and bimodal transformed templates generated by using AVET are compared with the original and other transform techniques for several modalities. By achieving promising accuracy on all observed datasets, we empirically show that AVET is stable, robust, and universal.

APPENDIX

In this section, we provides three examples to show that AVET is more reliable than both GAVE and its variant against linkage attacks. For the sake of convenience, we use integers in our examples.

A. Absolute Value Equations

Assume that attackers have multiple compromised user's information $\{(A, B, \mathbf{y})_i\}_{i=1}^{k}$. The attacker's purpose is reversing $\mathbf{x}$ from the given information (solution: $\mathbf{x} = (0, -5, -1, 2)$).

1) GAVE: $A \cdot \mathbf{x} + B \cdot |\mathbf{x}| = \mathbf{y}$

The 1st compromised $(A_1, B_1, \mathbf{y}_1)$: $\mathbf{y}_1 = (0, 5, 9, -32)$,

$$A_1 = \begin{bmatrix} 7 & 2 & -4 & -8 \\ -4 & -5 & 8 & -2 \\ 2 & 9 & -1 & 5 \\ -2 & 8 & 4 & -9 \end{bmatrix},$$

$$B_1 = \begin{bmatrix} -3 & 7 & -9 & -2 \\ -6 & -5 & 1 & 8 \\ 2 & 9 & -4 & 1 \\ -1 & 3 & 7 & 4 \end{bmatrix}.$$

The 2nd compromised information: $\mathbf{y}_2 = (-5, 16, -1, -9)$,

$$A_2 = \begin{bmatrix} -4 & 6 & -9 & 1 \\ 1 & 2 & -7 & 5 \\ -8 & -3 & -5 & 2 \\ 5 & -8 & 9 & -4 \end{bmatrix},$$

$$B_2 = \begin{bmatrix} -6 & 3 & -3 & 1 \\ 1 & 2 & 9 & -5 \\ -6 & -8 & 7 & 4 \\ 2 & -5 & -1 & -3 \end{bmatrix}.$$

Set $\mathbf{t} = (x_1, x_2, x_3, x_4, |x_1|, |x_2|, |x_3|, |x_4|)$, attackers can establish a valid system of equations as follows:

$$\begin{cases} 7t_1 + 2t_2 - 4t_3 - 8t_4 - 3t_5 + 7t_6 - 9t_7 - 2t_8 = 0 \\ -4t_1 - 5t_2 + 8t_3 - 2t_4 - 6t_5 - 5t_6 + 1t_7 + 8t_8 = 5 \\ 2t_1 + 9t_2 - 1t_3 + 5t_4 + 2t_5 + 9t_6 - 4t_7 + 1t_8 = 9 \\ -2t_1 + 8t_2 + 4t_3 - 9t_4 - 1t_5 + 3t_6 + 7t_7 + 4t_8 = -32 \\ -4t_1 + 6t_2 - 9t_3 + 1t_4 - 6t_5 + 3t_6 - 3t_7 + 1t_8 = -5 \\ 1t_1 + 2t_2 - 7t_3 + 5t_4 + 1t_5 + 2t_6 + 9t_7 - 5t_8 = 16 \\ -8t_1 - 3t_2 - 5t_3 + 2t_4 - 6t_5 - 8t_6 + 7t_7 + 4t_8 = -1 \\ 5t_1 - 8t_2 + 9t_3 - 4t_4 + 2t_5 - 5t_6 - 1t_7 - 3t_8 = -9 \end{cases} \tag{8}$$

By solving the system (8), attackers have the solution $\mathbf{t} = (0, -5, -1, 2, 0, 5, 1, 2)$; they easily find out the user's feature vector $\mathbf{x} = (0, -5, -1, 2)$.

2) Variant of GAVE: $A \cdot \mathbf{u} + B \cdot |\mathbf{v}| = \mathbf{y}$

The 1st compromised $(A_1, B_1, \mathbf{y}_1)$: $\mathbf{y}_1 = (-17, -57)$

$$A_1 = \begin{bmatrix} -7 & 5 \\ -4 & 8 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 2 & 3 \\ -9 & -4 \end{bmatrix}.$$

The 2nd compromised information: $\mathbf{y}_2 = (22, 27)$

$$A_2 = \begin{bmatrix} 2 & -5 \\ 1 & -8 \end{bmatrix}, \quad B_2 = \begin{bmatrix} -9 & 3 \\ 1 & -7 \end{bmatrix}.$$

Set $\mathbf{t} = (u_1, u_2, |v_1|, |v_2|)$, attackers can establish a valid system of equations as follows:

$$\begin{cases} -7t_1 + 5t_2 + 2t_3 + 3t_4 = -17 \\ -4t_1 + 8t_2 - 9t_3 - 4t_4 = -57 \\ 2t_1 - 5t_2 - 9t_3 + 3t_4 = 22 \\ 1t_1 - 8t_2 + 1t_3 - 7t_4 = 27 \end{cases} \tag{9}$$

By solving the system (9), attackers have the solution $\mathbf{t} = (0, -5, 1, 2)$. Even though adversaries cannot get exactly $\mathbf{x}$ due to absolute values, they are able to compute precisely new transformed templates based on the resultant vector $\mathbf{t}$.

B. Absolute Value Equations Transform

Assume that attackers have multiple compromised user's information $\{(R, A, B, \mathbf{y})_i\}_{i=1}^{k}$. Their purpose is obtaining $\mathbf{x}$ from the given information (solution: $\mathbf{x} = (0, -5, -1, 2)$).

The 1st compromised $(R_1, A_1, B_1, \mathbf{y}_1)$: $\mathbf{y}_1 = (51, -37)$

$$R_1 = \begin{bmatrix} -3 & 1 \\ 2 & 4 \end{bmatrix}, \quad A_1 = \begin{bmatrix} -1 & 1 \\ 9 & -2 \end{bmatrix}, B_1 = \begin{bmatrix} 4 & 6 \\ -7 & -2 \end{bmatrix}.$$

The 2nd compromised information: $\mathbf{y}_2 = (-54, 87)$

$$R_2 = \begin{bmatrix} -6 & -1 \\ 9 & 7 \end{bmatrix}, \ A_2 = \begin{bmatrix} -4 & 3 \\ -5 & -2 \end{bmatrix}, \ B_2 = \begin{bmatrix} -6 & -3 \\ 8 & 9 \end{bmatrix}.$$

The 3rd compromised information: $\mathbf{y}_3 = (52, 27)$

$$R_3 = \begin{bmatrix} -6 & 3 \\ 7 & -2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} -4 & 1 \\ 5 & -6 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 2 & 3 \\ 8 & -9 \end{bmatrix}.$$

Attackers can only establish an underdetermined system of equations as follows:

$$\begin{cases} -1u_1 + 1u_2 + 4| - 3v_1 + 1v_2| + 6|2v_1 + 4v_2| = 51 \\ 9u_1 - 2u_2 - 7| - 3v_1 + 1v_2| - 2|2v_1 + 4v_2| = -37 \\ -4u_1 + 3u_2 - 6| - 6v_1 - 1v_2| - 3|9v_1 + 7v_2| = -54 \\ -5u_1 - 2u_2 + 8| - 6v_1 - 1v_2| + 9|9v_1 + 7v_2| = 87 \\ -4u_1 + 1u_2 + 2| - 6v_1 + 3v_2| + 3|7v_1 - 2v_2| = 52 \\ 5u_1 - 6u_2 + 8| - 6v_1 + 3v_2| - 9|7v_1 - 2v_2| = 27 \end{cases} \tag{10}$$

Obviously, the system (10) is underdetermined so that it is computationally hard to obtain the actual $\mathbf{x}$.

ACKNOWLEDGMENT

The authors would like to thank for insightful comments Trinh Hieu Le, Khang Vinh Nguyen, and Thuc Anh Tran.

REFERENCES

[1] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancellable biometrics," *EURASIP J. Inf. Secur.* vol. 2011, no. 1, pp. 1–25, 2011.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.

[3] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, "Locality-sensitive hashing scheme based on P-stable distributions," in *Proc. 20th Annu. Symp. Comput. Geometry (SCG)*, 2004, pp. 253–262.

[4] K. Kenthapadi, A. Korolova, I. Mironov, and N. Mishra, "Privacy via the Johnson-Lindenstrauss transform," *J. Privacy Confidentiality*, vol. 5, no. 1, pp. 1–24, Aug. 2013.

[5] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, 2002.

[6] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Apr. 2004.

[7] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[8] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 103–117, Mar. 2010.

[9] A. B. J. Teoh and C. T. Yuang, "Cancellable biometrics realization with multispace random projections," *IEEE Trans. Syst., Man, Cybern., B*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.

[10] R. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.

[11] Y. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," *IEEE Trans. Syst., Man, Cybern., B*, vol. 40, no. 5, pp. 1280–1293, Oct. 2010.

[12] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2010, pp. 1838–1841.

[13] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: A novel approach for cancelable biometrics," *Inf. Process. Lett.*, vol. 93, no. 1, pp. 1–5, Jan. 2005.

[14] C. Ntantogian, S. Malliaros, and C. Xenakis, "Gaithashing: A two-factor authentication scheme based on gait features," *Comput. Secur.*, vol. 52, pp. 17–32, Jul. 2015.

[15] H. O. Shahreza and S. Marcel, "Deep auto-encoding and biohashing for secure finger vein recognition," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Jun. 2021, pp. 2585–2589.

[16] K. Y. Chee et al., "Cancellable speech template via random binary orthogonal matrices projection hashing," *Pattern Recognit.*, vol. 76, pp. 273–287, Apr. 2018.

[17] S.-C. Wu, P.-T. Chen, A. L. Swindlehurst, and P.-L. Hung, "Cancelable biometric recognition with ECGs: Subspace-based approaches," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1323–1336, May 2019.

[18] X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," 2019, *arXiv:1905.03021*.

[19] Y. Lai, Z. Jin, K. Wong, and M. Tistarelli, "Efficient known-sample attack for distance-preserving hashing biometric template protection schemes," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3170–3185, 2021.

[20] M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure authentication for face recognition," in *Proc. IEEE Symp. Comput. Intell. Image Signal Process.*, Apr. 2007, pp. 121–126.

[21] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On application of Bloom filters to iris biometrics," *IET Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.

[22] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, and C. Busch, "Protected facial biometric templates based on local Gabor patterns and adaptive Bloom filters," in *Proc. 22nd Int. Conf. Pattern Recognit.*, Aug. 2014, pp. 4483–4488.

[23] G. Li, B. Yang, C. Rathgeb, and C. Busch, "Towards generating protected fingerprint templates based on Bloom filters," in *Proc. 3rd Int. Workshop Biometrics Forensics (IWBF)*, Mar. 2015, pp. 1–6.

[24] J. Hermans, B. Mennink, and R. Peeters, "When a Bloom filter becomes a doom filter: Security assessment of a novel iris biometric template protection system," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2014, pp. 1–6.

[25] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis of Bloom filter-based iris biometric template protection," in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 527–534.

[26] H. Kaur and P. Khanna, "Random distance method for generating unimodal and multimodal cancellable biometric features," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 709–719, Mar. 2019.

[27] H. Kaur and P. Khanna, "Random slope method for generation of cancelable biometric features," *Pattern Recognit. Lett.*, vol. 126, pp. 31–40, Sep. 2019.

[28] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on BioHashing," in *Proc. IEEE Workshop Comput. Intell. Biometrics, Theory, Algorithms, Appl.*, Mar. 2009, pp. 92–97.

[29] P. Lacharme, E. Cherrier, and C. Rosenberger, "Preimage attack on BioHashing," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, 2013, pp. 1–8.

[30] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *Proc. 4th IEEE Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2010, pp. 1–7.

[31] L. Ghammam, K. Karabina, P. Lacharme, and K. Thiry-Atighehchi, "A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2869–2880, 2020.

[32] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur. (CCS)*, 1999, pp. 28–36.

[33] T. M. Dang, L. Tran, T. D. Nguyen, and D. Choi, "FEHash: Full entropy hash for face template protection," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2020, pp. 810–811.

[34] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancellable iris biometric," in *Proc. Int. Conf. Pattern Recognit. (ICPR)*, 2008, pp. 1–4.

[35] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancellable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[36] S. Dasgupta and A. Gupta, "An elementary proof of a theorem of Johnson and Lindenstrauss," *Random Struct. Algorithms*, vol. 22, no. 1, pp. 60–65, 2003.

[37] O. L. Mangasarian, "Absolute value programming," *Comput. Optim. Appl.*, vol. 36, no. 1, pp. 43–53, Jan. 2007.

[38] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Univ. Massachusetts Amherst, Amherst, MA, USA, Tech. Rep., 07–49, Dec. 2020. [Online]. Available: http://vis-www.cs.umass.edu/lfw/

[39] S. Sengupta, J.-C. Chen, C. Castillo, V. M. Patel, R. Chellappa, and D. W. Jacobs, "Frontal to profile face verification in the wild," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Mar. 2016, pp. 1–9.

[40] (Dec. 5, 2020). *CASIA Face Image Database Ver. 5.0 (CASIA-FaceV5)*. [Online]. Available: http://biometrics.idealtest.org

[41] A. Kumar and C. Wu, "Automated human identification using ear imaging," *Pattern Recognit.*, vol. 41, no. 5, pp. 956–968, 2012.

[42] (Dec. 5, 2020). *BioLab, FVC2002, FVC2004*. [Online]. Available: http://bias.csr.unibo.it/fvc2002/

[43] T. Hoang, D. Choi, and T. Nguyen, "On the instability of sensor orientation in gait verification on mobile phone," in *Proc. 12th Int. Conf. Secur. Cryptogr.*, 2015, pp. 148–159.

[44] E. E. Hansley, M. P. Segundo, and S. Sarkar, "Employing fusion of learned and handcrafted features for unconstrained ear recognition," *IET Biometrics*, vol. 7, no. 3, pp. 215–223, May 2018.
[45] Z. Jin, M.-H. Lim, A. B. J. Teoh, B.-M. Goi, and Y. H. Tay, "Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 10, pp. 1415–1428, Oct. 2016.
[46] P. Punithavathi, S. Geetha, M. Karuppiah, S. K. H. Islam, M. M. Hassan, and K.-K. R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," *Inf. Sci.*, vol. 484, pp. 255–268, May 2019.
[47] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.
[48] K. Takahashi and S. Hirata, "Parameter management schemes for cancelable biometrics," in *Proc. IEEE Workshop Comput. Intell. Biometrics Identity Manag. (CIBIM)*, Apr. 2011, pp. 145–151.
[49] J. Kim and A. B. Jin Teoh, "One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2018, pp. 3108–3113.
[50] G. Mai, K. Cao, X. Lan, and P. C. Yuen, "SecureFace: Face template protection," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 262–277, 2021.
[51] R. K. Pandey, Y. Zhou, B. U. Kota, and V. Govindaraju, "Deep secure encoding for face template protection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2016, pp. 77–83.
[52] A. K. Jindal, S. Chalamala, and S. K. Jami, "Face template protection using deep convolutional neural network," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2018, pp. 575–5758.
[53] L. Chen, G. Zhao, J. Zhou, A. T. S. Ho, and L. Cheng, "Face template protection using deep LDPC codes learning," *IET Biometrics*, vol. 8, no. 3, pp. 190–197, May 2019.
[54] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Zero-shot deep hashing and neural network based error correction for face template protection," in *Proc. IEEE 10th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2019, pp. 1–10.
[55] M. Wang, S. Wang, and J. Hu, "Cancellable template design for privacy-preserving EEG biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3350–3364, 2022.
[56] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression (PIE) database," in *Proc. 5th IEEE Int. Conf. Autom. Face Gesture Recognit.*, May 2002, pp. 53–58.

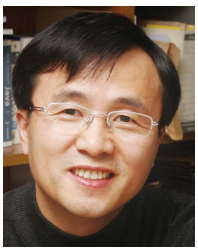
Thao Mai Dang received the B.S. degree in computer science from the Ho Chi Minh University of Science in 2017 and the M.S. degree from the Department of Electronics and Computer Engineering, Chonnam National University, Gwangju, South Korea, in 2020. Her research interests include face recognition, biometric cryptosystems, physics-informed neural networks, and medical image processing.

Thuc Dinh Nguyen received the B.S. degree from the Faculty of Information Technology, University of Science, Vietnam, in 1990, and the Ph.D. degree from the University of Science in 2000. He is currently an Associate Professor with the Department of Knowledge Engineering, Faculty of Information Technology, University of Science, VNU-HCMC. He is also the Leader of the Decentralized Crypto and IoT-Blockchain Research Group, Vietnam National University of Ho Chi Minh City. His research interests include bio-cryptology, database security, and the IoT-blockchain.

Thang Hoang (Member, IEEE) received the B.S. degree in computer science from the University of Science, VNU-HCMC, Vietnam, in 2010, the M.S. degree in computer science from Chonnam National University, South Korea, in 2014, and the Ph.D. degree in computer science from the University of South Florida in August 2020. He was a Post-Doctoral Fellow at Carnegie Mellon University from August 2020 to December 2020. He has been an Assistant Professor with the Department of Computer Science, Virginia Tech, since January 2021. His research interests include applied cryptography, secure computation, privacy-enhancing technologies, and biometrics.

Hyunseok Kim received the B.S. degree in software engineering from Chonnam University, Gwangju, South Korea, in 2020, and the M.S. degree from the Interdisciplinary Program of Information Security, Chonnam University, in 2022. His research interests include computer cryptography, network security, and information security.

Andrew Beng Jin Teoh (Senior Member, IEEE) is currently a Full Professor with the Department of Electrical and Electronic Engineering, College of Engineering, Yonsei University, South Korea. He has published more than 300 international refereed journal articles, conference papers, and editing books. His current research interests include machine learning and biometrics security. He is serving as an Associate Editor for IEEE TRANSACTION OF INFORMATION FORENSICS AND SECURITY, *Applied Sciences*, and *Machine Learning with Applications*.



Deokjai Choi received the B.S. degree from the Department of Computer Engineering, Seoul National University, in 1982, the M.S. degree from the Department of Computer Science, KAIST, South Korea, in 1984, and the Ph.D. degree from the Department of Computer Science and Telecommunications, University of Missouri–Kansas City, Kansas City, MO, USA, in 1995. He is currently a Full Professor with the Department of Artificial Intelligence Convergence, Chonnam National University, South Korea. His research interests include human activity recognition, biometric authentication, and network security.