A Novel Length-Flexible Lightweight Cancelable Fingerprint Template for Privacy-Preserving Authentication Systems in Resource-Constrained IoT Applications

Xuefei Yin, Song Wang, Yanming Zhu, and Jiankun Hu, *Senior Member, IEEE*

***Abstract*—Fingerprint authentication techniques have been employed in various Internet of Things (IoT) applications for access control to protect private data, but raw fingerprint template leakage in unprotected IoT applications may render the authentication system insecure. Cancelable fingerprint templates can effectively prevent privacy breaches and provide strong protection to the original templates. However, to suit resource-constrained IoT devices, oversimplified templates would compromise authentication performance significantly. In addition, the length of existing cancelable fingerprint templates is usually fixed, making them difficult to be deployed in various memory-limited IoT devices. To address these issues, we propose a novel length-flexible lightweight cancelable fingerprint template for privacy-preserving authentication systems in various resource-constrained IoT applications. The proposed cancelable template design primarily consists of two components: 1) length-flexible partial-cancelable feature generation based on the designed reindexing scheme and 2) lightweight cancelable feature generation based on the designed encoding nested difference XOR scheme. Comprehensive experimental results on public databases FVC2002 DB1–DB4 and FVC2004 DB1–DB4 demonstrate that the proposed cancelable fingerprint template achieves equivalent authentication performance to state-of-the-art methods in IoT environments, but our design substantially reduces template storage space and computational cost. More importantly, the proposed length-flexible lightweight cancelable template is suitable for a variety of commercial smart cards (e.g., C5-M.O.S.T. Card Contact Microprocessor Smart Cards CLXSU064KC5). To the best of our knowledge, the proposed method is the first length-flexible lightweight, high-performing cancelable fingerprint template design for resource-constrained IoT applications.**

***Index Terms*—Cancelable fingerprint template, fingerprint authentication, Internet of Things (IoT), length-flexible, lightweight cancelable template, privacy-preserving.**

Manuscript received 20 June 2022; accepted 1 September 2022. Date of publication 5 September 2022; date of current version 22 December 2022. This work was supported in part by the Australian Research Council (ARC) Discovery under Grant DP190103660 and Grant DP200103207, and in part by the ARC Linkage under Grant LP180100663. *(Corresponding author: Jiankun Hu.)*

Xuefei Yin and Jiankun Hu are with the School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia (e-mail: xuefei.yin@unsw.edu.au; j.hu@adfa.edu.au).

Song Wang is with the Department of Engineering, La Trobe University, Australia, VIC 3086, Australia (e-mail: song.wang@latrobe.edu.au).

Yanming Zhu is with the School of Computer Science and Engineering, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: yanming.zhu@unsw.edu.au).

Digital Object Identifier 10.1109/JIOT.2022.3204246

I. Introduction

With rapid technological advancements, the Internet of Things (IoT) has emerged as a network connecting various sensors or smart devices via the Internet or other communication channels [1]. The "things" connected in the IoT may perform functions of data collection, data processing, or information communication. However, these functions are vulnerable to privacy leakage [2], [3], [4], especially during data collection and data processing, if there is no protection to raw information. Therefore, identity authentication has been one of the promising options for access control in IoT applications [5], [6]. An identity authentication system usually consists of two procedures: 1) enrollment and 2) verification. The enrollment procedure is aimed at registering a user by generating and storing the user's template, while the verification procedure attempts to match the template generated for a query against the enrolled template.

Fingerprints have proven to be one of the most popular and efficient biometric traits and have been pervasively used for identity authentication [7], [8]. Compared to traditional token-based identity authentication [9], [10], [11], fingerprint-based authentication systems are user-friendly because, unlike passwords, fingerprints won't be forgotten. Along with convenience, however, fingerprint-based authentication systems without any protection also expose IoT applications to privacy breaches and security risks. First and foremost, raw fingerprint data leakage in unprotected IoT applications may render the authentication system insecure, because the raw fingerprint data can be repeatedly utilized to spoof the authentication system. Simultaneously, a finger would be "lost" forever once its raw fingerprint data is compromised. Another issue is regarding legal regulations on data privacy around the world. For example, to protect personal private information, specific laws, and legal regulations have been formulated in many regions and countries, such as the *General Data Protection Regulation*[1] in European Union, the *Personal Information Protection Law of the People's Republic of China* in China, and the *California Privacy Rights Act*[2] in the United States. Therefore, it is essential to implement protection schemes to fingerprint authentication systems in IoT applications.

[1] https://gdpr-info.eu

[2] https://oag.ca.gov/privacy/ccpa

Fingerprint protection can be typically divided into two categories: 1) cryptography-based approaches and 2) cancelable fingerprint template approaches. In cryptography-based approaches, cryptographic techniques (e.g., symmetric/asymmetric encryption and homomorphic encryption) are commonly utilized to encrypt fingerprint templates so as to avoid original template leakage [12], [13], [14]. The benefit is that encrypted templates tend to be very secure and cannot easily cracked. The downside is that the encryption and decryption processes are usually time-consuming. Therefore, the cryptography-based methods are unsuitable for resource-constrained IoT devices [13].

Cancelable biometrics is another template protection technique [15], [16], [17], [18], [19], [20]. The core idea of cancelable fingerprint templates is to irreversibly transform the raw fingerprint template into a new template to avoid privacy leakage. Four objectives are demanded in the design of cancelable fingerprint templates [15], [21]: 1) diversity: different unrelated fingerprint templates can be obtained with disparate distortions; 2) revocability: a new template can be issued to replace the compromised template; 3) noninvertibility: it should be computationally infeasible to retrieve the original fingerprint template from the transformed (cancelable) template; and 4) accuracy: cancelable fingerprint templates should not significantly deteriorate the accuracy of fingerprint recognition. Therefore, cancelable fingerprint templates can effectively avoid privacy leakage and provide strong protection to the original templates. However, to suit resource-constrained IoT devices, oversimplified cancelable fingerprint templates deployed in resource-constrained IoT applications would compromise authentication performance significantly. In addition, the length of existing cancelable fingerprint templates is usually fixed, making them difficult to be implemented in various resource-constrained IoT devices. Moreover, designing cancelable fingerprint templates that meet the above four objectives is challenging, especially for IoT applications.

To address these issues, we design a length-flexible lightweight, high-performing cancelable fingerprint template for privacy-preserving authentication systems with applications to resource-constrained IoT devices. The proposed cancelable fingerprint template is based on the state-of-the-art minutia cylinder-code (MCC) [22], which is a robust minutia-based local descriptor with excellent authentication performance on public fingerprint databases. However, the original MCC is not designed for resource-constrained IoT devices. More importantly, the original MCC has no template protection function. The proposed cancelable fingerprint template design consists of two components: 1) length-flexible partial-cancelable feature generation and 2) lightweight cancelable feature generation. For the first component, we propose a simple, efficient yet effective method to flexibly reindex the original MCC feature. For the second component, we develop an encoding-nested-difference-XOR scheme. The novel cancelable template possesses four advantages: 1) flexible length: the template length can be flexibly adjusted to suit various memory-limited IoT devices; 2) lightweight: this makes the proposed template further applicable to memory- and computation-constrained IoT devices; 3) cancelablility: this protects raw fingerprint data against privacy leakage; and 4) high performance: extensive experiments demonstrate the satisfactory performance of the proposed cancelable template on eight public fingerprint data sets.

The main contributions of this study are summarized as follows.

1) To the best of our knowledge, this study proposes the first length-flexible, high-performing privacy-preserving fingerprint template suited to various memory-limited IoT devices. As IoT devices are usually embedded with varying storage space, it is essential to provide length-flexible but high-performing fingerprint templates.
2) We propose an innovative lightweight cancelable fingerprint template based on the reindexing operation and the encoding-nested-difference-XOR operation. The template size is reduced by up to 85% (around 64 K bits) while achieving superior verification performance in the privacy-preserving IoT environment. The cancelable characteristic can also protect the original fingerprint data against hill-climbing and preimage attacks, thus making the proposed template appropriate for resource-constrained IoT applications.
3) Comprehensive experimental results obtained on eight public benchmark data sets FVC2002 DB1–DB4[3] [23] and FVC2004 DB1–DB4[4] [24] demonstrate that the proposed template achieves equivalent authentication accuracy to the state-of-the-art cancelable fingerprint templates in IoT settings, but our design significantly reduces template storage space and computational cost.

The remainder of this article is organized as follows. We review state-of-the-art studies on privacy-preserving fingerprint templates and lightweight fingerprint authentication systems for IoT applications in Section II. We detail the proposed cancelable template in Section III. We present the experimental setting and analyze the experimental results in Section IV. We conclude this article in Section V.

II. Related Work

Cryptographic techniques (e.g., symmetric/asymmetric encryption and homomorphic encryption) have been used to protect original fingerprint templates by encrypting them [12], [25], [26]. Xi and Hu [25] reviewed topical cryptographic techniques and fingerprint biometrics and discussed the applications of the cryptographic technique in fingerprint-based authentication systems. Kim *et al.* [12] proposed using fully homomorphic encryption to protect the original fingerprint image by encrypting its features. This method can provide strong protection to the original template. However, this method is time-consuming and unsuitable for resource-constrained IoT devices. Yang *et al.* [26] introduced a similar homomorphic encryption-based fingerprint authentication method, in which minutiae pairs are used as original features. However, the authentication accuracy (EER = 8.25%) of this method is unsatisfactory. Azzaz *et al.* [27] proposed a symmetric encryption-based method to encrypt a fingerprint image

[3] http://bias.csr.unibo.it/fvc2002/

[4] http://bias.csr.unibo.it/fvc2004/

instead of its features (e.g., minutiae) to avoid privacy leakage. The disadvantage is that fingerprints could be lost forever once the cipher key is leaked. Besides, the encryption and decryption would increase computational complexity. Liu *et al.* [28] presented a fingerprint encryption-based online fingerprint authentication scheme, in which homomorphic addition is used to encrypt fingerprint data. However, this method is cloud oriented and unsuitable for IoT applications. In summary, cryptography-based fingerprint authentication methods tend to be time-consuming and resource-intensive due to the encryption and decryption operations. Besides, original fingerprint information is still at risk to privacy breaches due to key-related hacking.

Another popular protection scheme is cancelable fingerprint template techniques, which are aimed to irreversibly transform the raw fingerprint template into a new one to avoid privacy breaches [15]. Kho *et al.* [29] proposed a cancelable fingerprint template design based on the local minutia descriptor and permutated randomized nonnegative least square. Wu *et al.* [30] designed a privacy-preserving cancelable pseudo-template based on a random distance transformation technique. Kavati *et al.* [31] proposed a cancelable fingerprint template protection scheme using elliptical structures guided by fingerprint minutiae. Although this method provides strong protection to the raw fingerprint template, the authentication accuracy is poor with equal-error rate (EER) of 7.3% and 5.13% for FVC2002 DB1 and DB2, respectively. Tran and Hu [21] proposed a multifilter matching framework for cancelable fingerprint template design and achieved good authentication performance. Bedari *et al.* [32] presented an alignment-free cancelable MCC-based fingerprint template design. Similarly, Yin *et al.* [33] proposed an IoT-oriented cancelable fingerprint template based on the MCC feature and achieved state-of-the-art authentication performance in an IoT environment. Unlike aforementioned methods, Lee *et al.* [34] developed a tokenless cancelable template for multimodal biometric systems, where the real-valued face and fingerprint vectors are fused into a cancelable template. In summary, compared to cryptography-based fingerprint template protection methods, cancelable fingerprint templates can effectively protect raw fingerprint data because the cancelable template instead of the raw template is stored in the authentication system. However, most of these approaches are designed for cloud applications or powerful devices rather than resource-constrained IoT applications. Besides, most of these cancelable templates are usually of fixed length, making them unsuitable for resource-constrained IoT devices.

Fingerprint-based authentication systems in IoT environments have been explored in [35], [36], and [37]. Habib *et al.* [38] introduced an authentication framework based on biometric and radio fingerprinting for the IoT in an eHealth application. Through the embedded authentication system, the framework can guarantee that the monitored private data is associated with the correct patient. Punithavathi *et al.* [36] proposed a lightweight fingerprint authentication system based on machine learning for smart IoT devices in a cloud computing environment. However, the authentication accuracy evaluated on public data sets FVC2002 DB1–DB2 and FVC2004 DB1–DB2 is poor. Golec *et al.* [39] introduced a fingerprint-based authentication system in an IoT environment, where the fingerprint data in the communication channel and database is protected by the AES-128-bit key encryption method. Sabri *et al.* [40] developed a fingerprint-based authentication framework for match-on-card and match-on-host applications, but the fingerprint template is unprotected. Kumar [41] utilized a fingerprint authentication system in an IoT environment to defend communication channels against black hole attacks. However, the fingerprint template used in the authentication system is vulnerable to privacy breaches. In summary, fingerprints or fingerprint features have been used for identity authentication in various IoT applications and even on resource-constrained IoT devices, such as smart cards. However, the original fingerprint data in these studies faces privacy leakage issues.

III. Proposed Lightweight Cancelable Fingerprint Template

A fingerprint authentication system typically consists of two procedures: 1) enrollment and 2) verification. The enrollment procedure is aimed at registering a user by generating and storing the user's template, while the verification procedure is aimed at generating a template for a query user and matching the template against the enrolled one. The enrollment procedure usually consists of fingerprint acquisition via a fingerprint sensor, template generation, and template storage. The verification procedure usually consists of fingerprint acquisition, template generation, and template matching. In cloud-based applications, a fingerprint is captured on the end-user side and then transferred to the cloud for template generation, template storage, and template matching. Thus, the end-user is responsible for capturing a fingerprint, transferring it to the cloud, and then receiving the verification result from the cloud. The security issue here is that the private fingerprint data are held by the cloud. This may cause privacy leakage due to security concerns in relation to cloud servers or attackers. In the IoT applications discussed in this work, the fingerprint data does not leave the IoT. The IoT application takes responsibility for fingerprint acquisition, template generation, template storage, and template verification. As opposed to cloud-based applications where the raw fingerprint needs to be transferred to the cloud, in IoT applications, a cancelable template stays in the IoT. As an advantage, the raw fingerprint enrolled in the IoT application is securely protected because a compromised cancelable template would not reveal the raw fingerprint information.

The core step in both enrollment and verification is template generation. This work proposes a novel method for generating a lightweight cancelable fingerprint template for resource-constrained privacy-preserving IoT applications. In the rest of this section, we first introduce the preliminary procedure about minutia extraction and minutia-based MCC feature extraction in Section III-A. Then, we describe the details of partial-cancelable feature generation in Section III-B and lightweight cancelable feature generation in Section III-C. Finally, we present template matching in Section III-D.

A. Preliminary Procedure

1) Minutia Extraction: Minutiae as a popular feature starting point have been widely used in fingerprint biometrics. In this article, minutiae are also utilized to generate the proposed IoT-oriented cancelable fingerprint template. Given a fingerprint image captured by the embedding fingerprint sensor, n minutiae are extracted to represent this fingerprint, denoted by $\mathbf{T} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n\}$. Each minutia is in the format of ISO/IEC 19794-2,[5] defined by $\mathbf{m}_i = \{x_i, y_i, \theta_i\}$ where x_i and y_i are the coordinates in pixels and $\theta_i \in [0, 2\pi]$ stands for the minutia orientation. In the proposed IoT-oriented fingerprint authentication system, minutia extraction is conducted upon the minutia extraction algorithm, Mindtct [42], from the open-source NIST biometric image software.[6]

2) MCC Template: The MCC template [22] is a robust minutia-based local feature representation and has been proved successful in fingerprint authentication. As the MCC feature is defined by the relative relationship between a minutia and its neighboring minutiae, the MCC feature possesses some desirable properties, such as translation- and rotation-invariance, and fixed length. The MCC feature is defined for each minutia and represented by a cylinder which is discretized into cube-like cells. The value for each cell is used to measure the relative distance contribution between the cell and neighboring minutiae, as well as to measure the relative orientation contribution between the cell, the reference minutia, and neighboring minutiae.

The MCC feature for each minutia contains two vectors: 1) the cell value vector and 2) the cell validity vector. The cell value is calculated by the distance and orientation contributions, while the cell validity is used to indicate the cell status. An MCC feature is represented by

$$\mathbf{v} = [\mathbf{c}, \mathbf{b}]$$

where $\mathbf{c}$ denotes the cell value vector and $\mathbf{b}$ denotes the cell validity vector [22]. According to the parameter settings for the MCC feature in [22], the cylinder diameter is set to $N_S = 16$ cells and the height of the cylinder is set to $N_D = 5$ cells. Therefore, the length of the cell value vector $\mathbf{c}$ is represented by $L_\mathbf{c} = 1,280$ (i.e., $N_S \times N_S \times N_D$), while the length of the cell validity vector $\mathbf{b}$ is represented by $L_\mathbf{b} = 256$ (i.e., $N_S \times N_S$).

B. Length-Flexible Partial-Cancelable Features

A simple, efficient yet effective scheme is proposed to generate the partial-cancelable feature by reindexing the original MCC feature. The new feature contains two parts: 1) the cell value part and 2) the cell validity part. To design a lightweight feature, we assign a percentage value $p \in [50\%, 100\%]$ to control the length of the new cancelable feature. Given the MCC feature vector $\mathbf{v}$ with the length $L_\mathbf{c}$, its index set $\mathbf{I}$ is defined by

$$\mathbf{I} = \{1, 2, \ldots, L_\mathbf{c}\} \tag{1}$$

its cell value part $\mathbf{c}$ is represented by

$$\mathbf{c} = \left(c_1, c_2, \ldots, c_{L_\mathbf{c}}\right) \tag{2}$$

and its cell validity part can be easily obtained by replicating the base mask for each cell section in the cylinder because each section shares the same base mask, without causing ambiguity, represented by

$$\mathbf{b} = \left(b_1, b_2, \ldots, b_{L_\mathbf{c}}\right) \tag{3}$$

where the ith bit b_i denotes the validity of the ith value in the cell value part $\mathbf{c}$.

A reindexing set $\mathbf{I}'$ is generated by randomly selecting l unique integers from the set $\mathbf{I}$, represented by

$$\mathbf{I}' = \{t_i | t_i \in \mathbf{I}, 1 \le i \le l\} \tag{4}$$

where $l = \lfloor p * L_\mathbf{c} \rfloor - \text{mod}(\lfloor p * L_\mathbf{c} \rfloor, 8)$.[7] l is set to a multiple of eight to facilitate the subsequent feature extraction. For convenience, we alternatively denote $l = 8\text{K}$. The new cell value vector is then obtained by collecting the corresponding values from $\mathbf{c}$ with the index in $\mathbf{I}'$, expressed as

$$\mathbf{c}' = \left(c_{t_1}, c_{t_2}, \ldots, c_{t_{8k}}\right) \tag{5}$$

and the cell validity vector is similarly obtained from $\mathbf{b}$, given by

$$\mathbf{b}' = \left(b_{t_1}, b_{t_2}, \ldots, b_{t_{8k}}\right). \tag{6}$$

In summary, the partial-cancelable feature is formulated by

$$\mathbf{v}' = [\mathbf{c}', \mathbf{b}']. \tag{7}$$

This is a partial-cancelable feature, because it satisfies three of the four objectives of cancelable templates: 1) diversity; 2) revocability; and 3) accuracy. The diversity is guaranteed by many reindexing sets that exist, namely, $[L_c!/((L_c - l)!)]$.[8] Regarding the revocability, as the reindexing process is controlled by a random generator, a new template can be easily obtained by choosing a different random seed. The accuracy is also not much affected by this new feature. Especially, setting $p = 100\%$ maintains the same accuracy, because the similarity between two features defined in [22] is order-invariant to the feature elements. At this stage, the feature in (7) does not achieve noninvertibility, because the original template may be retrieved by gathering the features and the corresponding index sets. In Section III-C, we will propose a scheme to attain noninvertibility and a lightweight design.

C. Lightweight Cancelable Features

To achieve the noninvertibility objective as well as the lightweight design, we propose an encoding-nested-difference-XOR scheme, which contains three operations: 1) the nested-difference operation; 2) the encoding operation; and 3) the bitwise XOR Boolean operation. As a notable benefit to resource-constrained IoT devices, the new feature will save approximately 87.5% storage space when $p = 50\%$ compared to the bit-MCC feature [22]. For example, for the partial-cancelable feature with $p = 50\%$ containing 8K cell values, the proposed lightweight cancelable feature will result in 2K bits.

[5] https://www.iso.org/standard/50864.html

[6] https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis

[7] The operator $\lfloor x \rfloor$ rounds x to the nearest integer less than or equal to x, and *mod* is the modulo operation.

[8] The ! is the factorial operator, which returns the product of all positive integers less than or equal to a positive integer.

1) Nested-Difference Operation: This operation is to calculate the nested difference of four neighboring cell values in the partial-cancelable vector. For clarity, we define the first-layer nested difference by vector $\mathbf{e}^{\mathbf{L_1}}$, whose ith element $e_i^{L_1}$, formulated by (8), is calculated upon the partial-cancelable vector $\mathbf{c}'$ in (5)

$$e_i^{L_1} = c_{t_{2i-1}} - c_{t_{2i}} \tag{8}$$

where $1 \leq i \leq 4k$. The second-layer nested difference vector $\mathbf{e}^{\mathbf{L_2}}$ is then calculated upon the first-layer nested difference, represented by

$$\mathbf{e}^{\mathbf{L_2}} = \left(e_1^{L_2}, e_2^{L_2}, \ldots, e_{2k}^{L_2}\right) \tag{9}$$

where the ith element

$$\begin{aligned} e_i^{L_2} &= e_{2i-1}^{L_1} - e_{2i}^{L_1} \\ &= \left(c_{t_{4i-3}} - c_{t_{4i-2}}\right) - \left(c_{t_{4i-1}} - c_{t_{4i}}\right) \end{aligned}$$

and $1 \leq i \leq 2k$. For convenience and without causing ambiguity, we use $\mathbf{e}$ to represent $\mathbf{e}^{\mathbf{L_2}}$ and use e_i to represent the ith element in $\mathbf{e}$. As c_i is in the range [0, 1], e_i is therefore in the range [−2, 2]. For the cell validity part, we use the OR Boolean operator to concatenate four neighboring cell masks so that valid cells can remain. The new validity vector is formulated by

$$\mathbf{d} = (d_1, d_2, \ldots, d_{2k}) \tag{10}$$

where the ith element $d_i = b_{t_{4i-3}} | b_{t_{4i-2}} | b_{t_{4i-1}} | b_{t_{4i}}$, $1 \leq i \leq 2k$, and | denotes the OR Boolean operator.

This procedure has three advantages: 1) the nested difference can significantly reduce the number of elements because it can incorporate four values; 2) the proposed operation increases the difficulty to revert to the original feature; and 3) the simple relationship between four values can effectively identify the distinguishability of the original feature, which is also supported by the experimental results in Sections IV-D and IV-E.

2) Encoding Operation: The encoding operation is using two bits to encode the relationship between the nested difference and a threshold. For a well-defined threshold, this relationship can effectively model the original feature information without significantly deteriorating the matching accuracy. Given a nested difference e and a threshold τ (τ is optimally set to 0.2 in our experiments), the encoding table is shown in Table I. By encoding the vector $\mathbf{e}$ [in (9)] according to Table I, a new vector $\bar{\mathbf{e}}$ in bits is obtained as

$$\bar{\mathbf{e}} = (\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{2k}) \tag{11}$$

where each unit $\bar{e}_i$ contains two bits. Its validity vector is the same as $\mathbf{d}$ in (10).

The encoding procedure has two key advantages: 1) the threshold in the encoding operation can enhance the privacy of the original feature, thus making it impossible to revert to the original MCC feature and 2) the encoding that converts float values into bits can significantly reduce the storage space.

TABLE I
ENCODING TABLE

Relationship	Encoding bits
$\frac{e_i}{2} \geqslant \tau$	10
$\frac{e_i}{2} \leqslant -\tau$	01
otherwise	00

TABLE II
COMPARISON OF THE FEATURE LENGTH IN THE CASE OF $N_S = 16, N_D = 5$, AND $p = 50\%$

	Cell value vector	Cell validity vector
The original MCC feature	$L_c = 1,280$	$L_b = 256$
The proposed feature	$\frac{p}{4} L_c = 160$	$\frac{p}{8} N_D L_b = 80$

3) Bitwise XOR *Boolean Operation:* The XOR Boolean operation conducts the bitwise XOR between two neighboring units $\bar{e}_i$ and $\bar{e}_{i+1}$. Given the encoded vector $\bar{\mathbf{e}} = (\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{2k})$, the new feature vector $\hat{\mathbf{e}}$ in bits is formulated by

$$\hat{\mathbf{e}} = \left(\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_k\right) \tag{12}$$

where $\hat{e}_i = \bar{e}_{2i-1} \oplus \bar{e}_{2i}$, $1 \leq i \leq k$, and $\oplus$ denotes the bitwise XOR Boolean operator. For example, given $\bar{e}_1 = 10$ and $\bar{e}_2 = 00$, we obtain $\hat{e}_1 = 10 \oplus 00 = 10$. The corresponding validity vector is obtained by

$$\hat{\mathbf{d}} = \left(\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_k\right) \tag{13}$$

where the ith element $\hat{d}_i = d_{2i-1} | d_{2i}$, $1 \leq i \leq k$, and | denotes the OR Boolean operator. The proposed lightweight cancelable feature vector is then represented by $\hat{\mathbf{v}} = [\hat{\mathbf{d}}, \hat{\mathbf{e}}]$. The comparison of the feature length between the original MCC feature and the proposed lightweight cancelable feature is summarized in Table II. When $p = 50\%$, the length of the proposed cell value vector is approximately $(L_c/8)$. When $N_D < (8/p) \in [8, 16]$, the length of the proposed cell validity vector is less than that of the original cell validity vector; otherwise, we can alternatively use the base mask to easily obtain the cell validity vector without increasing extra storage costs.

D. Template Matching

Template matching is to decide whether two templates are matched, which is an essential process in biometric authentication. This procedure comprises two steps: 1) computation of the similarity between two feature vectors and 2) computation of the decision score.

1) Computation of the Similarity Between Two Feature Vectors: Given two feature vectors $\mathbf{v}_q = [\hat{\mathbf{e}}_q, \hat{\mathbf{d}}_q]$ and $\mathbf{v}_p = [\hat{\mathbf{e}}_p, \hat{\mathbf{d}}_p]$ coming from the query template and the enrolled template, respectively, the intersection between the two cell validity vectors is defined by

$$\mathbf{d}_{qp} = \hat{\mathbf{d}}_q \otimes \hat{\mathbf{d}}_p \tag{14}$$

where $\otimes$ denotes the bitwise AND Boolean operator. To facilitate the subsequent computation, we must align the intersected validity vector with the cell value vectors. The aligned validity vector $\hat{\mathbf{d}}_{qp}$ is obtained by duplicating each bit of $\mathbf{d}_{qp}$, represented by

$$\hat{\mathbf{d}}_{qp} = \left(d_{qp,1}, d_{qp,1}, \ldots, d_{qp,k}, d_{qp,k}\right). \tag{15}$$

The similarity between two features is calculated by

$$s_{qp} = 1 - \frac{\left\|\hat{\mathbf{e}}_{q|p} \oplus \hat{\mathbf{e}}_{p|q}\right\|}{\left\|\hat{\mathbf{e}}_{q|p}\right\| + \left\|\hat{\mathbf{e}}_{p|q}\right\|} \tag{16}$$

where

$$\begin{cases} \hat{\mathbf{e}}_{q|p} = \hat{\mathbf{e}}_q \otimes \hat{\mathbf{d}}_{qp} \\ \hat{\mathbf{e}}_{p|q} = \hat{\mathbf{e}}_p \otimes \hat{\mathbf{d}}_{qp}. \end{cases}$$

The similarity is in the range [0,1], where the higher the value, the more similar the two features are.

2) Computation of the Decision Score: The decision score is used to measure the matching probability between a query template and an enrolled template. Given a query template containing n feature vectors and an enrolled template containing m feature vectors, a score matrix $\mathbf{s}$ of size $n \times m$ is obtained by calculating the similarity of each pair of feature vectors from the query and enrolled templates. The element s_{qp} of the score matrix $\mathbf{s}$ is given by (16). The decision score is then calculated upon the score matrix $\mathbf{s}$ using the local greedy similarity (LGS) algorithm in [43]. The decision score is in the range [0, 1], with a larger value indicating a higher matching probability between the query and enrolled templates.

IV. Experiments

In this section, we evaluate the proposed template in an IoT environment in terms of matching accuracy and efficiency. First, we present the experimental setting in Section IV-A, including the benchmark data sets, the evaluation protocol, and the measurement metrics. Next, we evaluate the effect of the feature length using different values of p in Section IV-B. Then, we comprehensively compare the proposed lightweight cancelable template with state-of-the-art methods in Section IV-D, and implement an IoT prototype system to evaluate the authentication performance on eight benchmark data sets in Section IV-E. Finally, security analysis is conducted in Section IV-F.

A. Experimental Setting

1) Benchmark Data Sets: Eight benchmark data sets are used in the experiments, including four from FVC2002 [23] and four from FVC2004 [24]. Each data set is composed of eight hundred fingerprint images collected from one hundred fingers, with eight images per finger. Details about the FVC2002 data sets and FVC2004 data sets are shown in Tables III and IV, respectively.

2) Evaluation Protocol: The widely used FVC evaluation protocol is adopted to assess the performance of the proposed template. In this protocol, genuine scores and imposter scores are calculated to evaluate the performance. The genuine scores are obtained by matching each fingerprint image of a finger against the remaining ones of the same finger. If the matching of P against Q is performed, the symmetric one (i.e., Q against P) is not tested to avoid correlation. For each data set, the total number of genuine scores is therefore 2800 (i.e., $(8 \times 7)/2 \times 100$). The imposter scores are obtained by matching the first fingerprint image of each finger against the first one of remaining fingers. Similarly, repeating tests are not performed. For each database, the total number of imposter scores is therefore 4950 [i.e., $(100 \times 99)/2$].

TABLE III
Details About Data Sets FVC2002 DB1–DB4

	Fingers	Images per finger	Image size	DPI
FVC2002 DB1	100	8	388 × 374	500
FVC2002 DB2	100	8	296 × 560	569
FVC2002 DB3	100	8	300 × 300	500
FVC2002 DB4	100	8	288 × 384	500

TABLE IV
Information About Data Sets FVC2004 DB1–DB4

	Fingers	Images per finger	Image size	DPI
FVC2004 DB1	100	8	640 × 480	500
FVC2004 DB2	100	8	328 × 364	500
FVC2004 DB3	100	8	300 × 480	512
FVC2004 DB4	100	8	288 × 384	500

3) Measurement Metrics: The following metrics, which are commonly used in biometric authentication, are adopted to evaluate the authentication accuracy of the proposed template.

1) *False Matching Rate (FMR):* The rate of a pair of fingerprints not from the same finger falsely decided as a match.
2) *False Nonmatching Rate (FNMR):* The rate of a pair of fingerprints from the same finger falsely decided as a nonmatch.
3) *FMR$_{1000}$:* The lowest FNMR for a threshold at which the FMR $\leq$ 1%.
4) *Equal-Error Rate:* The value at which the FNMR is equal to the FMR. The lower the EER, the better.
5) *Detection Error Tradeoff (DET) Curve:* The DET curve plots the FNMR against the FMR for a series of varying thresholds.

B. Authentication Accuracy With Different Values of p

In this experiment, we evaluate the effect of the feature length, controlled by p in (4), on the authentication accuracy in terms of the DET curve, the EER, and the FMR$_{1000}$. To avoid redundant computation, we evaluate three feature lengths, namely, $(1/4)L_c$, $(1/6)L_c$, and $(1/8)L_c$, with $p = 1$, $p = 2/3$, and $p = 1/2$, respectively. For convenience, we use "eMCC$_1$", "eMCC$_{2/3}$," and "eMCC$_{1/2}$" to indicate these three features, respectively. Table V summarizes the relationship between the feature length and the parameter p as well as the comparison of the length between these three features and the original MCC feature.

TABLE V

COMPARISON OF THE FEATURE LENGTH WITH DIFFERENT VALUES OF p IN THE CASE OF $N_S = 16$ AND $N_D = 5$

	Cell value vector	**Cell validity vector**
The original MCC feature	$L_c = 1,280$	$L_b = 256$
eMCC_1 with $p = 1$	$\frac{p}{4}L_c = 320$	$\frac{p}{8}N_D L_b = 160$
$\text{eMCC}_{2/3}$ with $p = \frac{2}{3}$	$\frac{p}{4}L_c = 212$	$\frac{p}{8}N_D L_b = 106$
$\text{eMCC}_{1/2}$ with $p = \frac{1}{2}$	$\frac{p}{4}L_c = 160$	$\frac{p}{8}N_D L_b = 80$

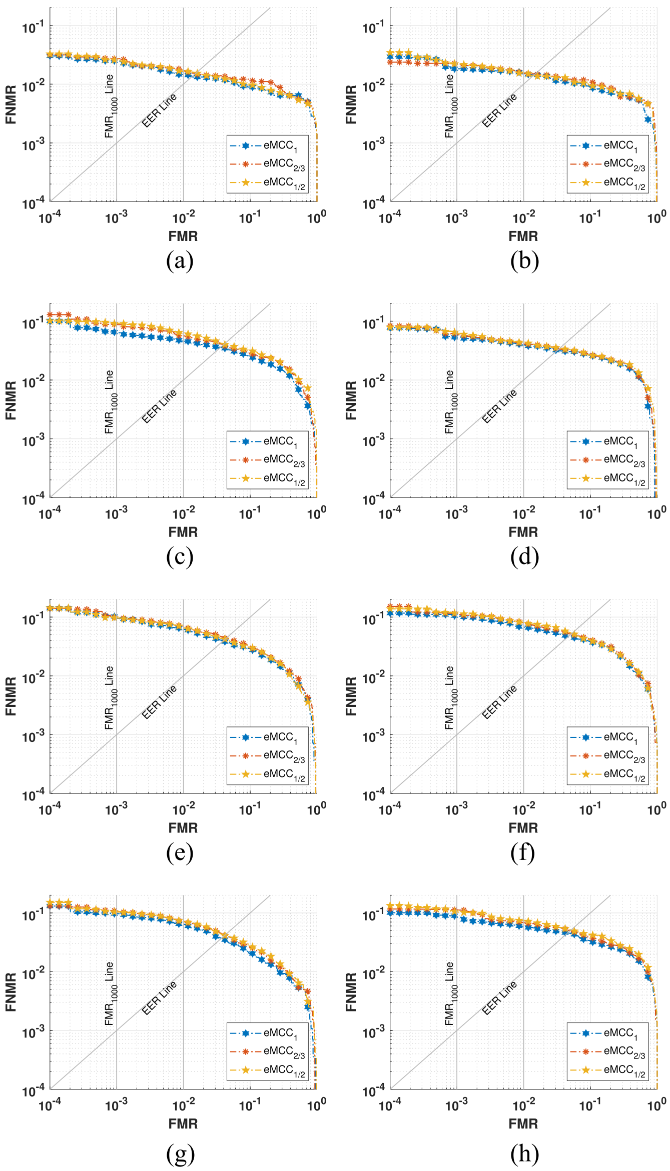
TABLE VI

COMPARISON OF VERIFICATION ACCURACY IN TERMS OF THE EER AND FMR_{1000} OBTAINED BY eMCC_1, $\text{eMCC}_{2/3}$, AND $\text{eMCC}_{1/2}$ ON FVC2002 DB1–DB4 AND FVC2004 DB1–DB4

Dateset		**EER (%)**			**FMR_{1000} (%)**		
		eMCC_1	$\text{eMCC}_{2/3}$	$\text{eMCC}_{1/2}$	eMCC_1	$\text{eMCC}_{2/3}$	$\text{eMCC}_{1/2}$
FVC2002	DB1	1.35	1.46	1.55	2.50	2.71	2.57
	DB2	1.43	1.47	1.40	1.83	2.26	2.22
	DB3	3.61	3.97	4.04	6.53	8.79	9.12
	DB4	3.18	3.33	3.50	5.33	6.15	6.48
FVC2004	DB1	3.89	4.32	4.21	10.21	9.97	9.75
	DB2	4.72	5.20	5.28	10.52	11.53	11.61
	DB3	3.71	4.15	4.11	9.71	10.92	10.38
	DB4	4.54	5.01	5.12	8.95	11.32	10.55

To minimize the side effects caused by missing and spurious minutiae, the commercial software Verifinger 12.1[9] is employed in this experiment to extract minutiae. The LGS algorithm mentioned in Section III-D is used to perform the template matching.

1) Comparison of DET Curves for Different Values of p: Fig. 1 shows the comparison of DET curves evaluated by eMCC_1, $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$ on data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4. It is clearly shown that similar DET curves are obtained by eMCC_1, $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$ on these eight data sets, especially on data sets FVC2002 DB1, FVC2002 DB2, FVC2002 DB4, FVC2004 DB1, FVC2004 DB2, and FVC2004 DB3. We can also observe that there are no significant differences at the intersections between the DET curves and the FMR_{1000} line and the EER line. The DET curves obtained by eMCC_1 on these eight data sets are slightly better than those obtained by $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$, which is because eMCC_1 incorporates the whole information of the original MCC feature, while $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$ only utilize two thirds and half of the original MCC feature, respectively. It is worth noting that there are fewer differences between the DET curves obtained by $\text{eMCC}_{2/3}$ and those obtained by $\text{eMCC}_{1/2}$. In summary, eMCC_1 performs marginally better than $\text{eMCC}_{2/3}$ and $\text{eMCC}_{1/2}$, while $\text{eMCC}_{2/3}$ and $\text{eMCC}_{1/2}$ achieve much similar performance.



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 1. Comparison of DET curves by eMCC_1, $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$ evaluated on data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4. (a) DET curves on FVC2002 DB1. (b) DET curves on FVC2002 DB2. (c) DET curves on FVC2002 DB3. (d) DET curves on FVC2002 DB4. (e) DET curves on FVC2004 DB1. (f) DET curves on FVC2004 DB2. (g) DET curves on FVC2004 DB3. (h) DET curves on FVC2004 DB4.

2) Comparison of the EER and FMR_{1000} Evaluated With Different Values of p: Table VI demonstrates the comparison of verification accuracy in terms of the EER and FMR_{1000} evaluated by eMCC_1, $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$ on FVC2002 DB1–DB4 and FVC2004 DB1–DB4. As shown in Table VI, eMCC_1 achieves slightly better EER on most of these eight data sets than $\text{eMCC}_{2/3}$ and $\text{eMCC}_{1/2}$, except on FVC2002 DB2 where $\text{eMCC}_{1/2}$ achieves a slightly better EER than eMCC_1 and $\text{eMCC}_{2/3}$. On these eight data sets, $\text{eMCC}_{2/3}$ and $\text{eMCC}_{1/2}$ achieve comparable accuracy in terms of the EER, evidenced by $\text{eMCC}_{2/3}$ performing better on five of these eight data sets than $\text{eMCC}_{1/2}$, while $\text{eMCC}_{1/2}$ obtains better EER on the other three data sets than $\text{eMCC}_{2/3}$. Regarding FMR_{1000}, eMCC_1 performs better on seven of these eight data sets than $\text{eMCC}_{2/3}$ and $\text{eMCC}_{1/2}$, while on FVC2004 DB1, $\text{eMCC}_{1/2}$ achieves a slightly better result. $\text{eMCC}_{2/3}$ and $\text{eMCC}_{1/2}$ achieve comparable accuracy of FMR_{1000}, evidenced by $\text{eMCC}_{1/2}$ achieving better results on five of these

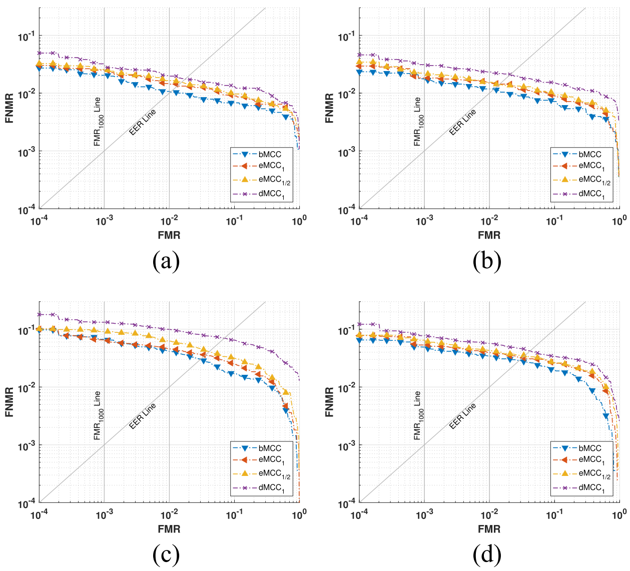
[9] https://www.neurotechnology.com/verifinger.html

TABLE VII
COMPARISON OF VERIFICATION ACCURACY IN TERMS OF THE EER AND FMR_{1000} OBTAINED BY bMCC, eMCC_1, $\mathrm{eMCC}_{1/2}$, AND dMCC_1 ON FVC2002 DB1–DB4

Dateset	**EER (%)**				**FMR_{1000} (%)**			
	bMCC	eMCC_1	$\mathrm{eMCC}_{1/2}$	dMCC_1	bMCC	eMCC_1	$\mathrm{eMCC}_{1/2}$	dMCC_1
DB1	1.04	1.35	1.55	1.75	2.04	2.50	2.57	3.22
DB2	1.15	1.43	1.40	2.11	1.77	1.83	2.22	3.11
DB3	3.00	3.61	4.04	6.99	6.69	6.53	9.12	13.24
DB4	2.86	3.18	3.50	4.23	4.92	5.33	6.48	7.75

TABLE VIII
COMPARISON OF THE PROPOSED TEMPLATE WITH bMCC IN THE CASE OF $N_S = 16$, $N_D = 5$ AND THE NUMBER OF MINUTIAE $n = 50$, WITH $L_c = N_S \times N_S \times N_D$ AND $L_b = N_S \times N_S$

	Template length (bits)
bMCC [22]	$n(L_c + L_b) = 76,800$
eMCC_1 with $p = 1$	$n(\frac{1}{4}L_c + \frac{1}{8}N_D L_b) = 24,000$
$\mathrm{eMCC}_{1/2}$ with $p = 1/2$	$n(\frac{1}{8}L_c + \frac{1}{16}N_D L_b) = 12,000$
dMCC_1 with $p = 1$	$n(\frac{1}{8}L_c + \frac{1}{16}N_D L_b) = 12,000$



(a) (b)

(c) (d)

Fig. 2. Comparison of DET curves obtained by bMCC, eMCC_1, $\mathrm{eMCC}_{1/2}$, and dMCC_1 on data sets FVC2002 DB1–DB4. (a) DET curves evaluated on DB1. (b) DET curves evaluated on DB2. (c) DET curves evaluated on DB3. (d) DET curves evaluated on DB4.

eight data sets than $\mathrm{eMCC}_{2/3}$, while $\mathrm{eMCC}_{2/3}$ performs better on the other three data sets than $\mathrm{eMCC}_{1/2}$. In summary, eMCC_1 performs better on most of these eight data sets than $\mathrm{eMCC}_{2/3}$ and $\mathrm{eMCC}_{1/2}$, while $\mathrm{eMCC}_{2/3}$ and $\mathrm{eMCC}_{1/2}$ achieve much similar performance.

C. Performance Against the Number of Nesting Layers

The main idea of our nested-difference operation is to extract discriminative features exhibiting the difference of neighboring feature cell pairs. So, in the first nesting layer $\mathbf{e}^{\mathbf{L_1}}$ in (8), a nested difference $e_i^{L_1}$ involves two cells of the cell vector. Four cell values contribute to the nested difference in the second layer $\mathbf{e}^{\mathbf{L_2}}$ in (9). Eight cells of the cell vector will contribute to the nested difference in the third layer $\mathbf{e}^{\mathbf{L_3}}$, where the ith element $e_i^{L_3}$is formulated by (17)

$$\begin{aligned} e_i^{L_3} &= e_{2i-1}^{L_2} - e_{2i}^{L_2} \\ &= \left(\left(c_{t_{8i-7}} - c_{t_{8i-6}}\right) - \left(c_{t_{8i-5}} - c_{t_{8i-4}}\right)\right) \\ &\quad - \left(\left(c_{t_{8i-3}} - c_{t_{8i-2}}\right) - \left(c_{t_{8i-1}} - c_{t_{8i}}\right)\right). \end{aligned} \tag{17}$$

We use dMCC_1 to denote the new template defined by (17) with $p = 1$. Experiments are conducted to show the performance against the number of nesting layers (i.e., number of cell vector values involved in the nested difference).

As shown in Table VII, Fig. 2 and Table VIII, compared to eMCC_1, dMCC_1 obtains much worse accuracy in terms of EER and FNMR_{1000}, although it saves half storage space. Compared to $\mathrm{eMCC}_{1/2}$ which has the same storage space, dMCC_1 still achieves much worse accuracy in terms of EER and FNMR_{1000} for all four data sets. Apparently, two layers of nesting can strike the best balance between the template size and authentication accuracy.

D. Comparison of the Proposed Lightweight Cancelable Template With State-of-the-Art Methods

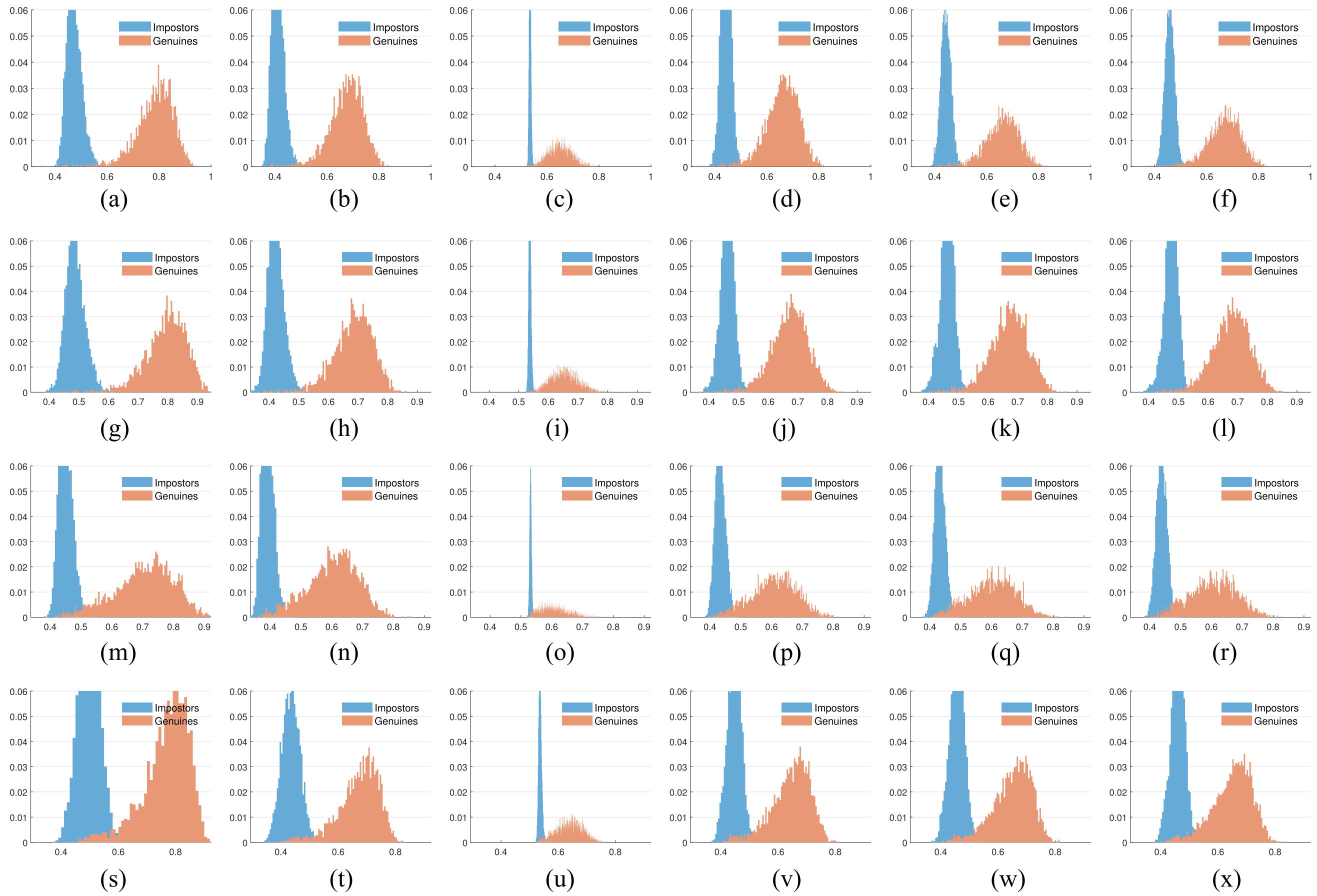
In this section, we comprehensively compare the proposed lightweight cancelable template with state-of-the-art methods in four essential aspects.

1) Template characteristics, including template length, IoT oriented, binary, and cancelable.
2) Distributions of matching score.
3) DET curves.
4) EER and FMR_{1000} evaluation.

Similar to Section IV-B, to reduce the impact of missing and spurious minutiae, the commercial software Verifinger 12.1 is adopted in this experiment for minutia extraction. The LGS algorithm introduced in Section III-D is used to perform the template matching. The three state-of-the-art templates used as the baseline are summarized as follows: 1) the original MCC template [22] (denoted as "MCC"); 2) the original binary MCC template [22] (denoted as "bMCC") obtained by binarizing the MCC template; and 3) the latest IoT-oriented privacy-preserving template [33] (denoted as "cMCC") developed upon the MCC template. The experimental results for MCC, bMCC, and cMCC are provided by [33].

1) Comparison of the Template Characteristics: Table IX compares the template characteristics of the proposed lightweight cancelable template and the baseline (i.e., the aforementioned three state-of-the-art fingerprint templates MCC, bMCC, and cMCC). Compared with MCC and bMCC, the IoT-oriented binary cancelable template cMCC reduces half of the cell value part but does not save the cell validity part. By contrast, the proposed template achieves substantial storage savings in both the cell value part and the cell validity part.

2) Comparison of Matching Score Distributions: Figs. 3 and 4 show the comparison of matching score distributions



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

(m) (n) (o) (p) (q) (r)

(s) (t) (u) (v) (w) (x)

Fig. 3. Comparison of score distributions by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ evaluated on data sets FVC2002 DB1–DB4. The *x*-axis is the matching score, and the *y*-axis is the proportion of scores falling into each score bin. (a) MCC on DB1. (b) bMCC on DB1. (c) cMCC on DB1. (d) eMCC$_1$ on DB1. (e) eMCC$_{2/3}$ on DB1. (f) eMCC$_{1/2}$ on DB1. (g) MCC on DB2. (h) bMCC on DB2. (i) cMCC on DB2. (j) eMCC$_1$ on DB2. (k) eMCC$_{2/3}$ on DB2. (l) eMCC$_{1/2}$ on DB2. (m) MCC on DB3. (n) bMCC on DB3. (o) cMCC on DB3. (p) eMCC$_1$ on DB3. (q) eMCC$_{2/3}$ on DB3. (r) eMCC$_{1/2}$ on DB3. (s) MCC on DB4. (t) bMCC on DB4. (u) cMCC on DB4. (v) eMCC$_1$ on DB4. (w) eMCC$_{2/3}$ on DB4. (x) eMCC$_{1/2}$ on DB4.

between MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ evaluated on data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4, respectively. It is clear that the imposter scores of eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ mainly concentrate in the range [0.4, 0.5], while the genuine scores of the three templates mainly concentrated in the range [0.4, 0.8]. The imposter and genuine scores of MCC are mainly in the range [0.4, 0.6] and [0.4, 0.9], respectively. Similarly, the imposter and genuine scores of bMCC are mainly in the range [0.4, 0.5] and [0.5, 0.8], respectively, while cMCC's imposter scores are mainly clustered in the range [5.3, 5.5] and its genuine scores are mainly in the range [0.55, 75]. In summary, the proposed eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ have similar imposter and genuine score distributions in comparison with MCC and bMCC, but different distributions compared to cMCC.

3) DET Curves: Figs. 5 and 6 show the comparison of DET curves obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ on data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4, respectively. On FVC2002 DB4 and FVC2004 DB4, the proposed eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ show similar DET curves compared to MCC, bMCC, and cMCC. On FVC2002 DB1, FVC2002 DB3, FVC2004 DB1, and FVC2004 DB2, for FMR $<$ 10^{-3}, the proposed eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ achieve close FNMR values compared to MCC, bMCC, and cMCC. In summary, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ only have minor deterioration in authentication accuracy, but they make considerable savings in the storage space. This demonstrates the validity of the proposed template.

TABLE IX
TEMPLATE CHARACTERISTICS OF THE BASELINE AND PROPOSED TEMPLATES

	IoT-oriented	Binary	Cancelable	Template length
MCC [22]				$n(L_c + L_b)$
bMCC [22]		✓		$n(L_c + L_b)$
cMCC [33]	✓	✓	✓	$n(\frac{1}{2}L_c + \frac{1}{2}L_b)$
eMCC$_1$	✓	✓	✓	$n(\frac{1}{4}L_c + \frac{1}{8}N_D L_b)$
eMCC$_{2/3}$	✓	✓	✓	$n(\frac{1}{6}L_c + \frac{1}{12}N_D L_b)$
eMCC$_{1/2}$	✓	✓	✓	$n(\frac{1}{8}L_c + \frac{1}{16}N_D L_b)$

4) EER and FMR$_{1000}$: Table X compares the EER and FMR$_{1000}$ obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ on data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4. With a sizable reduction on

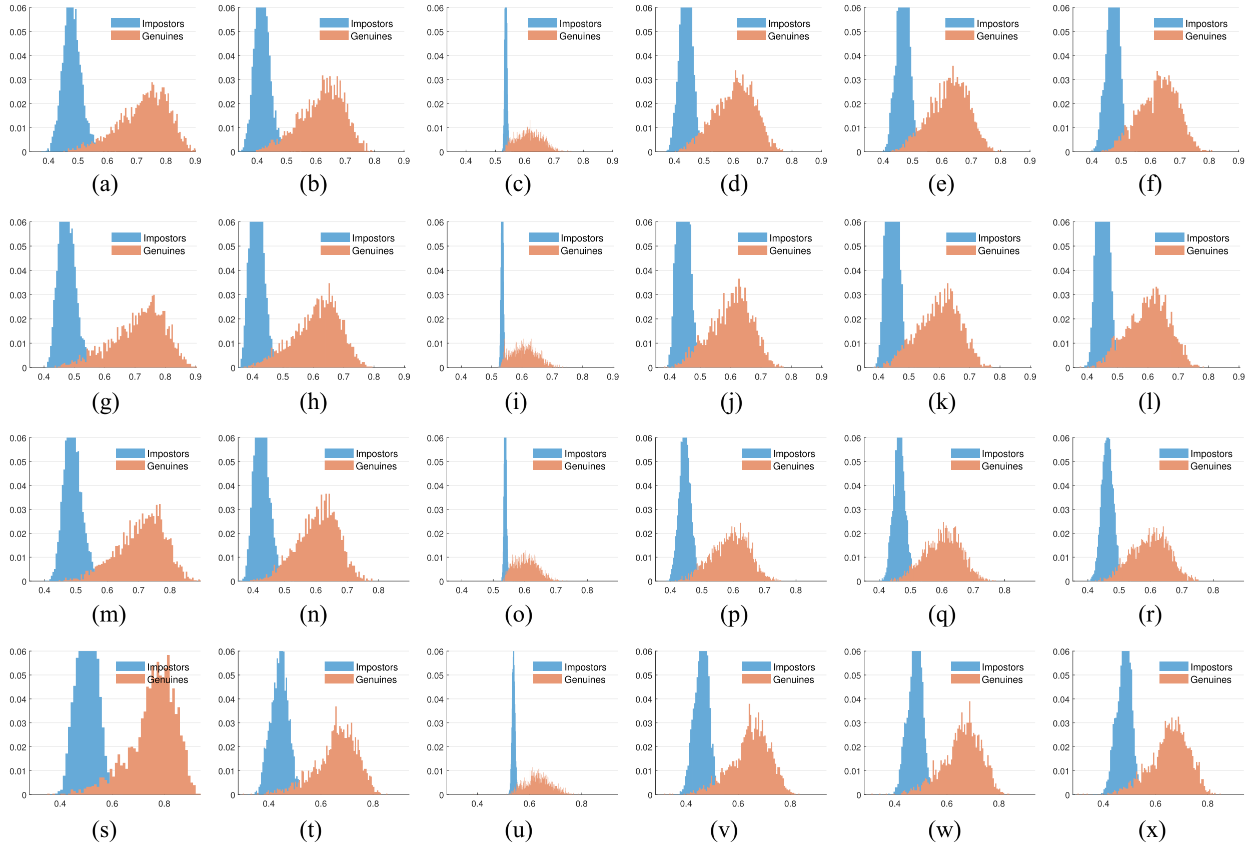

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k) (l) (m) (n) (o) (p) (q) (r) (s) (t) (u) (v) (w) (x)

Fig. 4. Comparison of score distributions by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ evaluated on data sets FVC2004 DB1–DB4. The *x*-axis is the matching score, and the *y*-axis is the proportion of scores falling into each score bin. (a) MCC on DB1. (b) bMCC on DB1. (c) cMCC on DB1. (d) eMCC$_1$ on DB1. (e) eMCC$_{2/3}$ on DB1. (f) eMCC$_{1/2}$ on DB1. (g) MCC on DB2. (h) bMCC on DB2. (i) cMCC on DB2. (j) eMCC$_1$ on DB2. (k) eMCC$_{2/3}$ on DB2. (l) eMCC$_{1/2}$ on DB2. (m) MCC on DB3. (n) bMCC on DB3. (o) cMCC on DB3. (p) eMCC$_1$ on DB3. (q) eMCC$_{2/3}$ on DB3. (r) eMCC$_{1/2}$ on DB3. (s) MCC on DB4. (t) bMCC on DB4. (u) cMCC on DB4. (v) eMCC$_1$ on DB4. (w) eMCC$_{2/3}$ on DB4. (x) eMCC$_{1/2}$ on DB4.

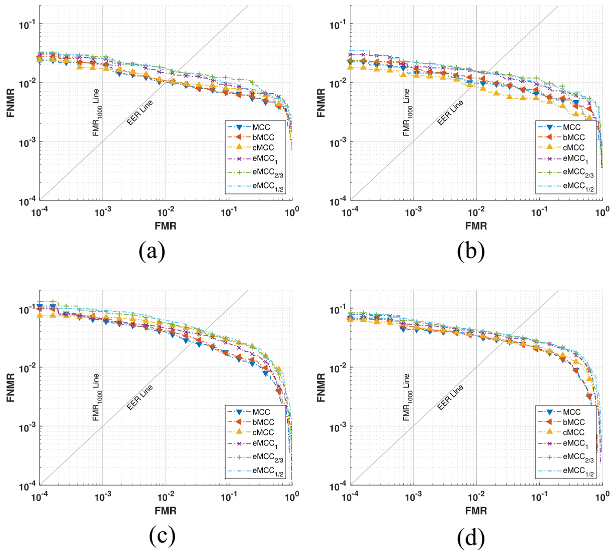

(a) (b) (c) (d)

Fig. 5. Comparison of DET curves obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ on data sets FVC2002 DB1–DB4. (a) DET curves evaluated on DB1. (b) DET curves evaluated on DB2. (c) DET curves evaluated on DB3. (d) DET curves evaluated on DB4.

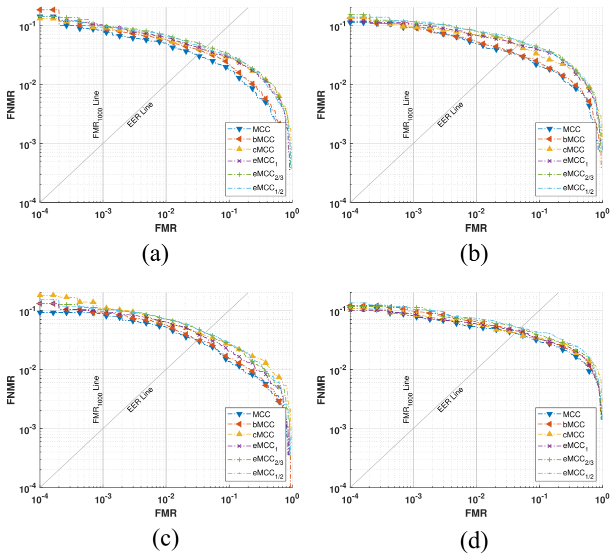

(a) (b) (c) (d)

Fig. 6. Comparison of DET curves obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ on data sets FVC2004 DB1–DB4. (a) DET curves evaluated on DB1. (b) DET curves evaluated on DB2. (c) DET curves evaluated on DB3. (d) DET curves evaluated on DB4.

the template length, the proposed eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ achieve relatively close EER on most of these eight data sets, and eMCC$_1$ even outperforms the IoT-oriented template cMCC on FVC2002 DB3 and FVC2004 DB3. Regarding FMR$_{1000}$, the proposed eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ also achieve similar accuracy on most of the eight

TABLE X
COMPARISON OF VERIFICATION ACCURACY IN TERMS OF THE EER AND FMR_{1000} OBTAINED BY MCC, bMCC, cMCC, eMCC_1, $\text{eMCC}_{2/3}$, AND $\text{eMCC}_{1/2}$ ON FVC2002 DB1–DB4 AND FVC2004 DB1–DB4

Dateset		**EER (%)**						**FMR_{1000} (%)**					
		MCC	bMCC	cMCC	eMCC_1	$\text{eMCC}_{2/3}$	$\text{eMCC}_{1/2}$	MCC	bMCC	cMCC	eMCC_1	$\text{eMCC}_{2/3}$	$\text{eMCC}_{1/2}$
FVC2002	DB1	1.00	1.04	1.07	1.35	1.46	1.55	2.11	2.04	1.70	2.50	2.71	2.57
	DB2	0.97	1.15	0.86	1.43	1.47	1.40	1.43	1.77	1.32	1.83	2.26	2.22
	DB3	2.68	3.00	3.90	3.61	3.97	4.04	6.34	6.69	6.98	6.53	8.79	9.12
	DB4	2.76	2.86	2.74	3.18	3.33	3.50	4.34	4.92	4.81	5.33	6.15	6.48
FVC2004	DB1	3.11	3.64	3.85	3.89	4.32	4.21	8.27	9.92	9.15	10.21	9.97	9.75
	DB2	3.51	3.55	4.51	4.72	5.20	5.28	9.20	9.29	9.39	10.52	11.53	11.61
	DB3	3.05	3.15	3.83	3.71	4.15	4.11	8.89	9.06	9.98	9.71	10.92	10.38
	DB4	4.08	4.48	4.15	4.54	5.01	5.12	8.23	9.74	8.69	8.95	11.32	10.55

TABLE XI
COMPARISON OF THE PROPOSED TEMPLATE WITH bMCC AND cMCC IN THE CASE OF $N_S = 16$, $N_D = 5$ AND THE NUMBER OF MINUTIAE $n = 50$, WITH $L_c = N_S \times N_S \times N_D$ AND $L_b = N_S \times N_S$

	Template length (bits)
bMCC [22]	$n(L_c + L_b) = 76,800$
cMCC [33]	$n(\frac{1}{2}L_c + \frac{1}{2}L_b) = 38,400$
eMCC_1 with $p = 1$	$n(\frac{1}{4}L_c + \frac{1}{8}N_D L_b) = 24,000$
$\text{eMCC}_{2/3}$ with $p = 2/3$	$n(\frac{1}{6}L_c + \frac{1}{12}N_D L_b) = 16,000$
$\text{eMCC}_{1/2}$ with $p = 1/2$	$n(\frac{1}{8}L_c + \frac{1}{16}N_D L_b) = 12,000$

data sets. On FVC2002 DB3, eMCC_1 even performs better than bMCC and cMCC. On FVC2004 DB4, eMCC_1 has a better FMR_{1000} than bMCC. On FVC2004 DB1, $\text{eMCC}_{1/2}$ achieves a better FMR_{1000} than bMCC. In summary, this demonstrates that with a significantly reduced template length, the proposed lightweight cancelable template shows no degradation in authentication accuracy.

E. Evaluation in an IoT Prototype System

In this section, we evaluate the proposed template on an IoT prototype system, implemented using the popular open-source software Open Virtual Platforms$^{\text{TM}}$[10] (OVP^{TM}, version 20210408.0) and the RISC-V instruction set architecture.[11]

1) Storage of eMCC Template and Runtime: Table XI shows the comparison of the proposed template with bMCC and cMCC in the case of $N_S = 16$, $N_D = 5$, and the number of minutiae $n = 50$, with $L_c = N_S \times N_S \times N_D$ and $L_b = N_S \times N_S$.

As shown in Table XI, eMCC_1 template requires 24K bits, saving 52.8K bits over bMCC and 14.4K bits over cMCC, while $\text{eMCC}_{1/2}$ template only requires 12K bits, saving 64.8K bits over bMCC and 26.4K bits over cMCC. This manifests that the proposed length-flexible template can remarkably reduce template storage space, which is highly beneficial to resource-constrained IoT devices. The prototype system requires about 12K bits, 16K bits, and 24K bits for the template storage of $\text{eMCC}_{1/2}$, $\text{eMCC}_{2/3}$, and eMCC_1, respectively. Therefore, they are applicable to commercial smart cards (e.g., C5-M.O.S.T. Card Contact Microprocessor Smart Cards CLXSU064KC5 32K Bits[12] and Atmel AT24C16C Memory Smart Card 16K Bits).[13]

The average time taken for fingerprint enrollment and verification is measured by evaluating the prototype system on FVC2002 DB1 with eight hundred fingerprints of size 388 × 374. The fingerprint enrollment process aims to extract minutiae in the format of ISO/IEC 19794-2 and to generate an eMCC template to be stored, so the original fingerprint image or feature is not stored to prevent privacy leakage. The fingerprint verification process sharing the common minutiae extraction and template generation aims to match a query template against the enrolled template. The open-source algorithm Mindtct [42] is utilized to implement the minutiae extraction in this simulation experiment. The average runtime of the minutiae extraction is around 2300 ms, which obviously can be optimized further. Since minutiae extraction is a relatively independent process, it is beyond the scope of this work. The average runtime of generating eMCC_1, $\text{eMCC}_{2/3}$, and $\text{eMCC}_{1/2}$ is approximately 255, 240, and 225 ms, respectively. Compared with minutiae extraction and template generation, template matching is time-efficient, with an average runtime of 70 ms for eMCC_1, 55 ms for $\text{eMCC}_{2/3}$, and 45 ms for $\text{eMCC}_{1/2}$. In summary, slightly depending on the parameter p, the average runtime of the enrollment process varies approximately from 2525 to 2555 ms, while the average runtime of the verification process varies approximately from 2570 to 2625 ms. Note that the enrollment and verification procedures require much more time on the time-consuming minutia

[10] https://www.ovpworld.org/

[11] https://www.ovpworld.org/dlp/

[12] https://www.cardlogix.com/product/contact-smart-card-most-c5-microproccessor-cards/

[13] https://www.cardlogix.com/product/atmel-at24c16c-memory-smart-chip-card-16k/

TABLE XII
EFFICIENCY COMPARISON BETWEEN THE PROPOSED AND STATE-OF-THE-ART CRYPTOGRAPHIC FINGERPRINT AUTHENTICATION METHODS

Methods	Cryptographic techniques	Cloud computing	Authentication time (ms)	Storage space (Bytes)	Communication cost (Bytes)
M1-2021 [44]	Homomorphic encryption	Yes	$\sim 7,168$	20K	20K
M2-2021 [28]	Homomorphic encryption	Yes	$\sim 7,413$	23.125K	20.0625K
M3-2020 [26]	Homomorphic encryption	Yes	$\sim 3,028$	unavailable	unavailable
eMCC$_{1/2}$	nil	No	$\sim 2,570$	$\sim$ 1.5K	nil

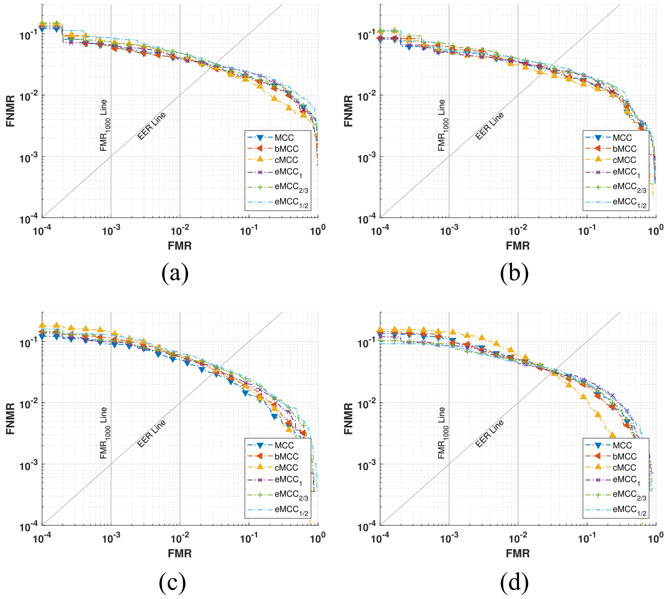
extraction. Therefore, there is much room for reducing the runtime by either optimizing the minutiae extraction process or integrating a time-saving minutiae extraction method.

Table XII shows the comparison of efficiency of the proposed eMCC$_{1/2}$ with state-of-the-art cryptographic fingerprint authentication methods, namely, M1-2021 [44], M2-2021 [28], and M3-2020 [26]. As shown in Table XII, compared with M1-2021 [44] and M2-2021 [28], even though they are based on cloud computing, the proposed eMCC$_{1/2}$ achieves better efficiency in terms of authentication time, storage space, and communication cost. Compared with the cloud-based method M3-2020 [26], the proposed eMCC$_{1/2}$ performs better in authentication time. In addition, the proposed eMCC$_{1/2}$ performs much faster than M3-2020 [26]. The proposed eMCC$_{1/2}$ costs about 2525 ms for a 12 000-bit template, while M3-2020 [26] needs about 123 537 ms for encrypting a 300-bit template. Besides, the proposed eMCC$_{1/2}$ achieves a better EER of 1.4% than M3-2020 [26] with an EER of 8.25% on FVC2002 DB2.

2) Comparison of DET Curves: Figs. 7 and 8 compare the DET curves obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ on data sets FVC2002 and FVC2004, respectively, evaluated using the implemented IoT prototype system.

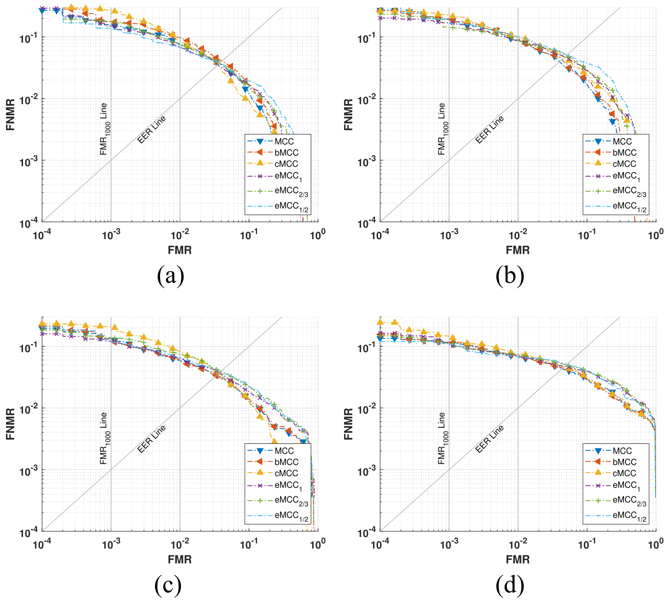
The results for MCC, bMCC, and cMCC are provided by [33]. The results for eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ are obtained using the implemented IoT system. As shown in Fig. 7, on FVC2002 DB1, FVC2002 DB2, and FVC2002 DB3, the DET curves are similar to each other. On the left side of the FMR$_{1000}$ line on FVC2002 DB1 and FVC2002 DB2, eMCC$_1$ show better DET curves than cMCC. We also observe that on the left side of the FMR$_{1000}$ line on FVC2002 DB3, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ perform better than cMCC. On FVC2002 DB4, it is shown that above the EER line, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ exhibit better DET curves than the other three templates. Similar experimental results are also observed on FVC2004, as can be seen in Fig. 8. This shows that the authentication accuracy of the proposed template is comparable to that of the state-of-the-art templates.

3) EER and FMR$_{1000}$: Table XIII compares the EER and FMR$_{1000}$ obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ on data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4, evaluated using the implemented IoT prototype system. As shown in Table XIII, compared with MCC, bMCC, and cMCC, the proposed templates eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ achieve comparable accuracy in terms of the EER and FMR$_{1000}$. eMCC$_1$ even performs better than MCC on FVC2002 DB4 and FVC2004 DB1. eMCC$_{2/3}$ and eMCC$_{1/2}$ also achieve better EER values than bMCC on FVC2004 DB1. Regarding the FMR$_{1000}$, the accuracy of eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ are close to that of MCC,



(a) (b)
(c) (d)

Fig. 7. Comparison of DET curves obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ based on the minutiae extraction presented in Section III-A1 on data sets FVC2002 DB1–DB4, evaluated using the implemented IoT prototype system. (a) DET curves evaluated on DB1. (b) DET curves evaluated on DB2. (c) DET curves evaluated on DB3. (d) DET curves evaluated on DB4.



(a) (b)
(c) (d)

Fig. 8. Comparison of DET curves obtained by MCC, bMCC, cMCC, eMCC$_1$, eMCC$_{2/3}$, and eMCC$_{1/2}$ based on the minutiae extraction presented in Section III-A1 on data sets FVC2004 DB1–DB4, evaluated using the implemented IoT prototype system. (a) DET curves evaluated on DB1. (b) DET curves evaluated on DB2. (c) DET curves evaluated on DB3. (d) DET curves evaluated on DB4.

TABLE XIII
COMPARISON OF VERIFICATION ACCURACY IN TERMS OF THE EER AND FMR_{1000} OBTAINED BY MCC, BMCC, CMCC, EMCC_1, $\text{EMCC}_{2/3}$, AND $\text{EMCC}_{1/2}$ ON FVC2002 DB1–DB4 AND FVC2004 DB1–DB4, EVALUATED USING THE IMPLEMENTED IoT PROTOTYPE SYSTEM

Dateset		**EER (%)**						**FMR_{1000} (%)**					
		MCC	bMCC	cMCC	eMCC_1	$\text{eMCC}_{2/3}$	$\text{eMCC}_{1/2}$	MCC	bMCC	cMCC	eMCC_1	$\text{eMCC}_{2/3}$	$\text{eMCC}_{1/2}$
FVC2002	DB1	2.96	2.78	2.89	3.03	3.17	3.25	6.50	6.41	7.39	6.64	7.46	8.64
	DB2	2.64	2.68	2.29	2.71	2.89	3.09	5.21	6.21	5.00	4.96	6.90	5.53
	DB3	3.07	3.29	3.43	3.57	3.71	3.83	9.07	11.56	14.48	9.90	10.40	12.92
	DB4	3.28	3.18	3.11	3.25	3.37	3.49	11.14	11.82	14.32	8.53	9.11	8.47
FVC2004	DB1	3.70	4.04	3.56	3.57	3.82	3.78	15.81	17.66	27.28	15.11	17.98	13.79
	DB2	4.00	4.32	4.64	4.82	5.03	5.13	19.26	19.89	22.78	16.95	14.45	19.29
	DB3	3.42	3.36	3.63	3.75	3.92	3.89	13.36	13.30	20.67	12.11	13.91	12.76
	DB4	4.33	4.44	4.69	4.72	4.90	5.07	11.28	11.67	14.68	11.63	11.35	11.02

bMCC, and cMCC. On FVC2002 DB2, $\text{eMCC}_{1/2}$ achieves a better FMR_{1000} than bMCC, and eMCC_1 outperforms MCC and bMCC. Similar results are also clearly observed on FVC2004. In summary, comparable authentication accuracy is demonstrated between the proposed and state-of-the-art templates.

F. Authentication Accuracy and Security Analysis

1) Authentication Accuracy Analysis: In authentication, there are two cases: 1) genuine matching and 2) imposter matching. For the genuine matching, because the query cancelable template and the enrolled cancelable template are processed by the same cancelable system, it is obviously clear that the authentication result of the query cancelable template against the enrolled cancelable template will be the same as the results of the original query and enrolled templates with a high probability. This is also supported by authentication accuracy results in Sections IV-D and IV-E.

Next, we analyze the authentication accuracy for the imposter matching case, As shown in Fig. 9, according to the distribution of $(e_i/2)$ (in Table I) collected from 18 539 valid MCC feature vectors from five hundred fingerprints, we have the following probabilities:

$$\begin{cases} P\left(-0.2 \le \frac{e_i}{2} \le 0.2\right) & \approx 0.75 \\ P\left(\frac{e_i}{2} \ge 0.2\right) & \approx 0.125 \\ P\left(\frac{e_i}{2} \le -0.2\right) & \approx 0.125. \end{cases}$$

Hence, for an eMCC_1 feature vector defined in (12) with $k = 160$, according to the encoding scheme in Table I, we have the following probabilities:

$$\begin{cases} P\left(\hat{e}_i = 00\right) & \approx 0.75 \\ P\left(\hat{e}_i = 10\right) & \approx 0.125 \\ P\left(\hat{e}_i = 01\right) & \approx 0.125. \end{cases}$$

Therefore, for a fake query cancelable template matching against the enrolled cancelable template, the probability that the authentication result is the same as the genuine result is about $0.75^{120} * 0.125^{20} * 0.125^{20} \approx 7.65 \times 10^{-52}$. In summary, there is near zero probability for a fake cancelable template to obtain a highly-close authentication accuracy as the genuine query cancelable template.

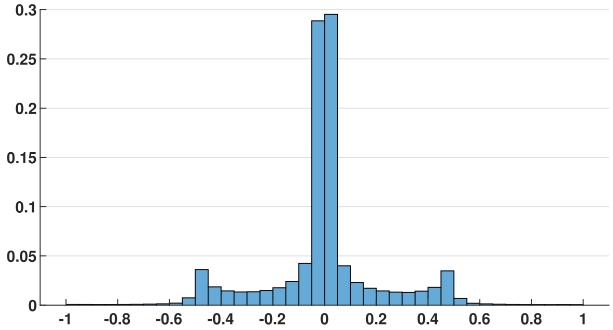


Fig. 9. Distribution of $(e_i/2)$ (in Table I) collected from 18 539 valid MCC feature vectors from five hundred fingerprints. The x-axis represents the values of $(e_i/2)$, and the y-axis is the proportion of the values falling into each bin.

2) Security Analysis on the Cancelable Template Design: The proposed template design meets the four objectives of cancelable biometrics: 1) diversity; 2) revocability; 3) accuracy; and 4) noninvertibility. The diversity is guaranteed by the reindexing scheme, as there exist numerous reindexing sets, that is $(L_c!/[(L_c - l)!])$ (e.g., $L_c = 1280$ in the experiments). Regarding the revocability, as the reindexing process is controlled by a random generator, a completely new template therefore can be easily obtained by choosing a different random seed. The accuracy of the proposed template is comparable to that of the state-of-the-art methods. Especially, when $p = 100\%$, equivalent authentication accuracy is achieved on eight public benchmark data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4 compared to the state-of-the-art templates. The noninvertibility of the proposed template is guaranteed by the irreversible mapping under two protection mechanisms: 1) the encoding of the nested-difference (Sections III-C1 and III-C2); and 2) the XOR operation on the encoded vector (Section III-C). As the first protection mechanism, the encoding of the nested-difference utilizes two bits to represent a nested difference of four float values. This process constitutes an infinite-to-one mapping, which is irreversible. Given the encoding bits, there is a near-zero probability to retrieve the original float values, because there exist infinite combinations of float values that can map to the same encoded bits. The second protection mechanism is the XOR Boolean operation on the encoded vector [in (11)]. The XOR operation makes it impossible to retrieve the true encoded vector $\bar{\mathbf{e}}$ [in (11)] from the resultant vector $\hat{\mathbf{e}}$ [in (12)]. For example, even with the most lightweight template with $p = 50\%$ for the case of $N_S = 16$ and $N_D = 15$, there exist up to 2^{160} possible candidate vectors $\bar{\mathbf{e}}$ [in (11)], which can be used as the input and return the same vector $\hat{\mathbf{e}}$ [in (12)]. In conclusion, the probability of retrieving the original template from the proposed lightweight cancelable template is almost zero. In addition, since the proposed template is revocable, if an enrolled template is compromised, it is easy to issue a completely different template (even of a different length) to ensure the security of the IoT authentication system.

3) Security Analysis Against Attacks: The proposed cancelable template is resistant to attacks via record multiplicity (ARM), which utilizes multiple compromised protected templates to recover the original template. This attack can be effectively prevented by the proposed encoding-nested-difference-XOR scheme through two layers of protection. The first layer of protection is the XOR operation (Section III-C). Because the inputs for each bit of the XOR output cannot be uniquely determined, the XOR operation provides computational infeasibility to retrieve the encoded binary feature vector $\bar{\mathbf{e}}$ in (11) in Section III-C2, as shown by the example in Section IV-F2. Taking $C = A\ XOR\ B$ as an example, according to the truth table of the XOR, $C = 1$ has two possible inputs: $A = 1, B = 0$ or $A = 0, B = 1$. The case of $C = 0$ is similar. Therefore, even though the adversary acquires multiple compromised protected templates, the encoded binary vectors $\bar{\mathbf{e}}$ in (11) cannot be uniquely determined. The second layer of protection is the encoding operation (Section III-C2), where a threshold is defined to binarize the nested difference. Evidently, given the threshold and binarized values, it is of zero probability to restore the nested differences in that infinite combinations of float values can result in the same encoded bits. In summary, the proposed cancelable template is resilient to the ARM.

The proposed cancelable template is secure against preimage attacks and optimization-based attacks. If the enrolled binary template is compromised, it is not computationally difficult to reconstruct or search for a possible input that can return the same binary vector. However, given that there exist infinite possible candidate inputs, it is of a near-zero probability for the reverted one to be the genuine fingerprint template. In other words, the reverted one cannot be used to generate another legitimate binary template. Therefore, these attacks can be effectively prevented by revoking the compromised binary template. In addition, attacks may also be launched through real-world fingerprint data sets. The impact of this attack can be assessed through authentication accuracy (e.g., the EER and FMR_{1000}). As demonstrated in Sections IV-D and IV-E, the proposed template achieves favorable authentication accuracy in terms of the EER and FMR_{1000} in a privacy-preserving IoT environment.

In case the template has been compromised by an adversary, it is infeasible for the attacker to retrieve the input feature due to the noninvertibility of our proposed template. Without this input feature, the attacker cannot launch an attack via the sensor interface which is the normal system interface. It is, however, possible for the attacker to get authenticated if the attacker can inject the compromised template into the matching module after bypassing the sensor and the built-in transformation module. This is exceedingly difficult but possible. Therefore, it is still difficult to attack a new device even if it has the same compromised template. Our cancelable template design offers further security protection by revoking the compromised template, like the revocation of a password.

V. Conclusion

In this article, we proposed a length-flexible lightweight cancelable fingerprint template design for privacy-preserving authentication systems in resource-constrained IoT applications. The proposed template design consists of two components: 1) length-flexible partial-cancelable feature generation based on the reindexing scheme and 2) lightweight cancelable feature generation based on the encoding-nested-difference-XOR scheme. Our template design has a number of benefits to IoT applications, such as flexible feature lengths, lightweight, cancelability, and high performance. Comprehensive experimental results evaluated on eight benchmark data sets FVC2002 DB1–DB4 and FVC2004 DB1–DB4 demonstrate that the proposed cancelable fingerprint template achieves equivalent authentication performance compared to the state-of-the-art methods, but our design significantly reduces storage space and computational cost. More importantly, the proposed length-flexible lightweight cancelable template is suitable for various resource-constrained IoT devices, evidenced by its implementation using a real-world IoT prototype system. To the best of our knowledge, it is the first length-flexible lightweight, high-performing cancelable fingerprint template design for resource-constrained IoT applications.

Acknowledgment

This research was undertaken with the assistance of resources and services from the National Computational Infrastructure (NCI), which is supported by the Australian Government.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, no. 1, pp. 82721–82743, 2019.

[2] N. N. Tran, H. R. Pota, Q. N. Tran, and J. Hu, "Designing constraint-based false data injection attacks against the unbalanced distribution smart grids," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9422–9435, Jun. 2021.

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[5] K. Riad, R. Hamza, and H. Yan, “Sensitive and energetic IoT access control for managing cloud electronic health records,” *IEEE Access*, vol. 7, pp. 86384–86393, 2019.

[6] O. J. A. Pinno, A. R. A. Grégio, and L. C. De Bona, “ControlChain: A new stage on the IoT access control authorization,” *Concurrency Comput. Pract. Exp.*, vol. 32, no. 12, p. e5238, 2020.

[7] A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[8] X. F. Yin, Y. M. Zhu, and J. K. Hu, “Contactless fingerprint recognition based on global minutia topology and loose genetic algorithm,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 28–41, 2020.

[9] M. S. Obaidat, S. P. Rana, T. Maitra, D. Giri, and S. Dutta, “Biometric security and Internet of Things (IoT),” in *Biometric-Based Physical and Cybersecurity Systems*. Cham, Switzerland: Springer, 2019, pp. 477–509.

[10] C.-X. Ren, Y.-B. Gong, F. Hao, X.-Y. Cai, and Y.-X. Wu, “When biometrics meet IoT: A survey,” in *Proc. Int. Asia Conf. Ind. Eng. Manage. Innov.*, 2016, pp. 635–643.

[11] X. Jiang *et al.*, “Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture,” *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16535–16547, Nov. 2021.

[12] T. Kim, Y. Oh, and H. Kim, “Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption,” *Security Commun. Netw.*, vol. 2020, Feb. 2020, Art. no. 4195852.

[13] M. Barni *et al.*, “A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates,” in *Proc. IEEE Int. Conf. Biometrics Theory, Appl. Syst.*, 2010, pp. 1–7.

[14] Z. Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, “Encryption node design in Internet of Things based on fingerprint features and cc2530,” in *Proc. IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber Phys. Soc. Comput.*, 2013, pp. 1454–1457.

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

[16] 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, Jan. 2001.

[17] P. Punithavathi and S. Geetha, “Partial DCT-based cancelable biometric authentication with security and privacy preservation for IoT applications,” *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 25487–25514, 2019.

[18] H. Kaur and P. Khanna, “Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing,” *Future Gener. Comput. Syst.*, vol. 102, pp. 30–41, Jan. 2020.

[19] X. Jiang *et al.*, “Cancelable HD-sEMG-based biometrics for cross-application discrepant personal identification,” *IEEE J. Biomed. Health Inform.*, vol. 25, no. 4, pp. 1070–1079, Apr. 2021.

[20] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable biometrics: A review,” *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[21] Q. N. Tran and J. Hu, “A multi-filter fingerprint matching framework for cancelable template design,” *IEEE Trans. Inf. Forensics Security*, vol. 16, no. 1, pp. 2926–2940, 2021.

[22] R. Cappelli, M. Ferrara, and D. Maltoni, “Minutia cylinder-code: A new representation and matching technique for fingerprint recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[23] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2002: Second fingerprint verification competition,” in *Proc. ICPR*, vol. 3, 2002, pp. 811–814.

[24] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2004: Third fingerprint verification competition,” in *Proc. Int. Conf. Biometric Authentication*, 2004, pp. 1–7.

[25] K. Xi and J. Hu, *Bio-Cryptography*. Berlin, Germany: Springer, 2010, ch. 7, pp. 129–157.

[26] W. Yang, S. Wang, K. Yu, J. J. Kang, and M. N. Johnstone, “Secure fingerprint authentication with homomorphic encryption,” in *Proc. Digit. Image Comput. Techn. Appl.*, 2020, pp. 1–6.

[27] M. S. Azzaz, C. Tanougast, A. Maali, and M. Benssalah, “An efficient and lightweight multi-scroll chaos-based hardware solution for protecting fingerprint biometric templates,” *Int. J. Commun. Syst.*, vol. 33, no. 10, p.e4211, 2020.

[28] Y. Liu *et al.*, “Secure and efficient online fingerprint authentication scheme based on cloud computing,” *IEEE Trans. Cloud Comput.*, early access, Aug. 10, 2021, doi: 10.1109/TCC.2021.3103546.

[29] J. B. Kho, J. Kim, I.-J. Kim, and A. B. Teoh, “Cancelable fingerprint template design with randomized non-negative least squares,” *Pattern Recognit.*, vol. 91, pp. 245–260, Jul. 2019.

[30] L. Wu, L. Meng, S. Zhao, X. Wei, and H. Wang, “Privacy-preserving cancelable biometric authentication based on RDM and ECC,” *IEEE Access*, vol. 9, pp. 90989–91000, 2021.

[31] I. Kavati, A. M. Reddy, E. S. Babu, K. S. Reddy, and R. S. Cheruku, “Design of a fingerprint template protection scheme using elliptical structures,” *ICT Exp.*, vol. 7, no. 4, pp. 497–500, 2021.

[32] A. Bedari, S. Wang, and W. Yang, “Design of cancelable MCC-based fingerprint templates using Dyno-key model,” *Pattern Recognit.*, vol. 119, Nov. 2021, Art. no. 108074.

[33] X. Yin, S. Wang, M. Shahzad, and J. Hu, “An IoT-oriented privacy-preserving fingerprint authentication system,” *IEEE Internet Things J.*, vol. 9, no. 14, pp. 11760–11771, Jul. 2022.

[34] M. J. Lee, A. B. J. Teoh, A. Uhl, S.-N. Liang, and Z. Jin, “A tokenless cancellable scheme for multimodal biometric systems,” *Comput. Security*, vol. 108, Sep. 2021, Art. no. 102350.

[35] F. Benhammadi and K. B. Bey, “Embedded fingerprint matching on smart card,” *Int. J. Pattern Recognit. Artif. Intell.*, vol. 27, no. 2, 2013, Art. no. 1350006.

[36] 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, no. 1, pp. 255–268, 2019.

[37] C. T. Pang, W.-Y. Yau, R. Mueller, and L. Yih, *Biometric System-On-Card*. Boston, MA, USA: Springer, 2014, pp. 1–6.

[38] K. Habib, A. Torjusen, and W. Leister, “A novel authentication framework based on biometric and radio fingerprinting for the iot in ehealth,” in *Proc. Int. Conf. Smart Syst. Devices Technol.*, 2014, pp. 32–37.

[39] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, “BioSec: A biometric authentication framework for secure and private communication among edge devices in Iot and industry 4.0,” *IEEE Consum. Electron. Mag.*, vol. 11, no. 2, pp. 51–56, Mar. 2022.

[40] M. Sabri, M.-S. Moin, and F. Razzazi, “A new framework for match on card and match on host quality based multimodal biometric authentication,” *J. Signal Process. Syst.*, vol. 91, no. 2, pp. 163–177, 2019.

[41] R. Kumar, “Internet of Things for the prevention of black hole using fingerprint authentication and genetic algorithm optimization,” *Int. J. Comput. Netw. Inf. Security*, vol. 10, no. 8, pp. 17–26, 2018.

[42] C. I. Watson *et al.*, “User’s guide to nist biometric image software (NBIS),” Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. 7392, 2007.

[43] R. Cappelli, M. Ferrara, D. Maltoni, and M. Tistarelli, “MCC: A baseline algorithm for fingerprint verification in FVC-onGoing,” in *Proc. Int. Conf. Control Autom. Robot. Vis.*, 2010, pp. 19–23.

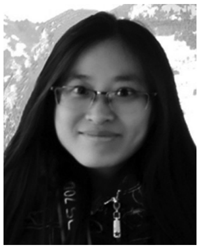
[44] H. Zhu, Q. Wei, X. Yang, R. Lu, and H. Li, “Efficient and privacy-preserving Online fingerprint authentication scheme over Outsourced data,” *IEEE Trans. Cloud Comput.*, vol. 9, no. 2, pp. 576–586, Apr.-Jun. 2021.

Xuefei Yin received the B.S. degree from Liaoning University, Liaoning, Shenyang, China, in 2011, the M.E. degree from Tianjin University, Tianjin, China, in 2014, and the Ph.D. degree from the University of New South Wales, Canberra, ACT, Australia, in 2019.

He is currently a Research Associate with the University of New South Wales. He has published articles in top journals, including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *ACM Computing Surveys*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE INTERNET OF THINGS JOURNAL. His research interests include biometrics, pattern recognition, privacy-preserving, and intrusion detection.

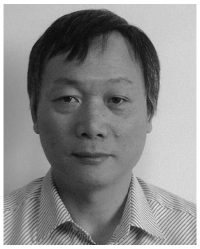
Song Wang received the B.Eng. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1991, and the Ph.D. degree from the University of Melbourne, Melbourne, VIC, Australia, in 2001.

Since January 2005, she has been with the Department of Engineering, La Trobe University, Melbourne, where she is currently a Senior Lecturer. She has published numerous articles in highly ranked journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY AND PATTERN RECOGNITION. Her research areas include biometric security, pattern recognition, and blind channel estimation.



Yanming Zhu received the B.E. degree from Shandong Agricultural University, Tai'an, China, in 2010, the M.E. degree from Tianjin University, Tianjin, China, in 2014, and the Ph.D. degree from the University of New South Wales, Canberra, ACT, Australia, in 2019.

She is currently a Research Fellow with the University of New South Wales, Sydney, NSW, Australia. She has published articles in top journals, including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, *Pattern Recognition*, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *ACM Computing Surveys*, and *Bioinformatics*. Her research interests include deep learning, biometrics, and biomedical image analysis.



Jiankun Hu (Senior Member, IEEE) received the B.E. degree from Hunan University, Changsha, China, in 1983, the Ph.D. degree in control engineering from Harbin Institute of Technology, Harbin, China, in 1993, and the Masters by Research degree in computer science and software engineering from Monash University, Melbourne, VIC, Australia, in 2000.

He has worked with Ruhr University, Bochum, Germany, on the prestigious German Alexander von Humboldt Fellowship from 1995 to 1996, and a Research Fellow with Melbourne University, Melbourne, from 1998 to 1999. He is currently a Full Professor with the School of Engineering and Information Technology, University of New South Wales, Canberra, ACT, Australia. He has published many articles in top venues, including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *Pattern Recognition*, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. His research interest is in the field of cybersecurity covering intrusion detection, sensor key management, and biometrics authentication.

Prof. Hu is an invited expert of the Australia Attorney-Generals Office assisting the draft of the Australia National Identity Management Policy. He has received nine Australian Research Council Grants and has served at the Panel of Mathematics, Information and Computing Sciences, Australian Research Council ERA (The Excellence in Research for Australia) Evaluation Committee 2012. He has served on the editorial board for up to seven international journals, including IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.