Privacy-Preserving Multi-Biometric Indexing Based on Frequent Binary Patterns

Dailé Osorio-Roig, Lázaro Janier González-Soler, Christian Rathgeb, and Christoph Busch, *Senior Member, IEEE*

***Abstract*— The development of large-scale identification systems that ensure the privacy protection of enrolled subjects represents a major challenge. Biometric deployments that provide interoperability and usability by including efficient multi-biometric solutions are a recent requirement. In the context of privacy protection, several template protection schemes have been proposed in the past. However, these schemes seem inadequate for indexing (workload reduction) in biometric identification systems. More specifically, they have been used in identification systems that perform exhaustive searches, leading to a degradation of computational efficiency. To overcome these limitations, we present an efficient privacy-preserving multi-biometric identification system that retrieves protected deep cancelable templates and is agnostic with respect to biometric characteristics and biometric template protection schemes. To this end, a multi-biometric binning scheme is designed to exploit the low intra-class variation properties contained in the frequent binary patterns extracted from different types of biometric characteristics. Experimental results reported on publicly available databases using state-of-the-art Deep Neural Network (DNN)-based embedding extractors show that the protected multi-biometric identification system can reduce the computational workload to approximately 57% (indexing up to three types of biometric characteristics) and 53% (indexing up to two types of biometric characteristics), while simultaneously improving the biometric performance of the baseline biometric system at the high-security thresholds. Code is available at https://github.com/dosorior/FBP-Multi-biometric-Indexing.**

***Index Terms*— Multi-biometric indexing, workload reduction, biometric identification, cancelable template protection, fusion, face, iris, fingerprint.**

I. Introduction

BIOMETRIC technologies are rapidly gaining popularity due to their wide applicability. Biometric recognition of individuals based on distinctive biometric characteristics (BCs), *e.g.* face or iris, is successfully deployed in many personal, commercial, and governmental identity management systems around the world, *e.g.* border control, and national ID systems. A report on the global biometric market concerns the annual growth rate in biometric technologies by estimating 45.96 billion dollars in 2024 [1]. In addition, biometrics vendors demand interoperability and deployment assuring maximum usability by including multimodal biometric solutions, *e.g.* fight against fraud in banks [2] and border and immigration [3] processes. These requirements (*i.e.* interoperability and usability) motivate the development of BC-agnostic systems, in particular solutions that achieve high biometric performance and at the same time can be extended to multiple BCs.

According to ISO-IEC-2382-37:2022 [4], biometric systems can typically operate in two modes *verification* and *identification*. Biometric verification is "the process of confirming a biometric claim through a one-to-one biometric comparison". In contrast, biometric identification refers to the "process of searching against an enrolment database to find and return the biometric reference identifier(s) attributable to a single individual". That is, biometric identification does not require any biometric claim, *e.g.* name or ID, which yields certain benefits and enables different use-cases:

- *Usability*: Biometric identification offers a high level of user-friendliness. Since no biometric claim has to be additionally presented, the user can be authenticated by solely presenting his/her biometric characteristic(s).
- *De-duplication*: In case new subjects are enrolled into a biometric database, it is checked whether this subject has already been registered beforehand. To this end, biometric identification is used to detect potential duplicates.[1]
- *Forensics*: In forensic investigations, biometric information can be employed to determine the identity of a subject. This is done by performing biometric identification transactions on databases of known identities.

The above-listed scenarios cannot be realised in biometric verification systems that utilize biometric claims, *e.g.* unique subject IDs used as indexes pointing to biometric records in a relational database, based on which a user is verified efficiently in a single comparison. However, biometric identification is more challenging from a practical point of view, especially in large-scale systems. On the one hand, the probability of

Manuscript received 22 October 2023; revised 1 February 2024, 8 March 2024, and 27 March 2024; accepted 27 March 2024. Date of publication 8 April 2024; date of current version 7 May 2024. This work was supported in part by the German Federal Ministry of Education and Research; in part by the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity (ATHENE); and in part by the European Union's Horizon 2020 Research and Innovation Program under the Marie Skłodowska-Curie Grant [TRaining in Secure and PrivAcy-preserving biometricS-*Early Training Networks* (TReSPAsS-ETN)] under Agreement 860813. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Zhen Lei. *(Corresponding author: Christian Rathgeb.)*

The authors are with the da/sec–Biometrics and Security Research Group, Department of Computer Science, Hochschule Darmstadt, 64295 Darmstadt, Germany (e-mail: christian.rathgeb@h-da.de).

This article has supplementary downloadable material available at https://doi.org/10.1109/TIFS.2024.3386310, provided by the authors.

Digital Object Identifier 10.1109/TIFS.2024.3386310

[1] De-duplication checks based on non-biometric data provided by the user are not considered reliable.

running into false positives increases with the number of enrolled subjects; large-scale biometric systems usually make use of multiple BCs to minimise error rates (*e.g.* [5]). On the other hand, a biometric identification transaction requires an exhaustive search (*i.e.* comparing a biometric probe against all the enrolled subjects) to reach a decision and, consequentially, computational bottlenecks occur in large-scale biometric systems where millions of subjects are enrolled (*e.g.* [6]). As hardware-based accelerations only provide an expensive short-term solution to this issue, scalable algorithmic solutions are necessary, which effectively reduce the number of comparisons required for biometric identification and hence lower the overall computational workload.

In response to the above-mentioned issue, significant research efforts have been devoted to investigating *workload reduction* (WR) methods [7], often referred to as *biometric indexing schemes*. To process large amounts of biometric data with reasonable transaction times, some of these methods are designed to extract indexes directly from biometric data. Thus, the search can be reduced to subspaces of a database pointed to by the extracted index. This means, that during enrolment, the biometric database can be organised according to obtained indexes (similar to relational databases), while no identity claims are required at the time of authentication. Note that WR methods proposed in the scientific literature are commonly designed for systems based on a single BC.

In addition to the emerging topic of accelerating searches within large-scale biometric databases, data privacy is of utmost importance in the aforementioned use cases. Note that biometric data is considered sensitive information by privacy regulations, *e.g.* the European Union (EU) General Data Protection Regulation 2016/679 (GDPR) [8]. That is, unprotected storage of biometric references could lead to different privacy threats such as identity theft, linking across databases, or limited renewability [9]. However, the privacy protection of biometric data is highly non-trivial due to its natural intra-class variance. Conventional cryptographic methods would require the decryption of protected biometric data prior to the comparison step in order to prevent the effect of biometric variance in the encrypted domain. This is not the case with *biometric template protection* schemes [10], [11] which enable a comparison of biometric data in the transformed domain (encrypted) and hence a permanent protection of biometric data. They are usually distinguished in the literature as *cancelable biometrics* and *biometric cryptosystems*. Generally, the latter category is not suggested in identification scenarios, as they require complex comparison methods (*e.g.* [12], [13]), in contrast to cancelable schemes (*e.g.* [14]). Moreover, it is well-known that a single BC, *e.g.* a single fingerprint or face, contains an insufficient amount of effective entropy to achieve high recognition accuracy in large-scale identification systems and to resist against attacks. Therefore, several researchers have proposed multi-biometric template protection systems [15]. However, so far no privacy-preserving multi-biometric indexing scheme has been proposed in the scientific literature (to the best of the authors' knowledge), which is necessary to enable efficient, accurate and privacy-preserving identification transactions in large-scale biometric systems.

Recently, Osorio-Roig et al. [16] introduced the proof-of-concept of *frequent binary patterns* for indexing deep cancelable face templates. This privacy-preserving solution allowed working on different cancelable protection schemes (*e.g.* so-called BioHashing [17] and variants of Index-of-Maximum Hashing [18]) ensuring a trade-off between computational workload and biometric performance for protected biometric identification systems. Motivated by our previous study (see [16]), we present in this work the *first privacy-preserving multi-biometric indexing system* based on the search of frequent binary patterns over cancelable biometric templates. The main contributions of the article are:

- An overview that delves into the area of computational WR for the indexing of protected biometric templates in identification systems based on a single BC. Tab. I shows a general overview of the different types of BCs, *i.e.* face, iris, finger-vein, and fingerprint.
- The successful application of the proof-of-concept of *frequent binary patterns* on individual BCs, *i.e.* face, iris, and fingerprint. In previous work presented by Osorio-Roig et al. [16], the proof-of-concept was applied to the face only.
- An efficient privacy-preserving multi-biometric system that is agnostic across cancelable biometric template protection schemes (with binary representation) and BCs. This solution is able to operate on the most secure processing step (*i.e.* feature level) in a biometric system by enabling fusion strategies on the concept of frequent binary patterns at two steps: The representation- and feature-based step. The fusion in the representation-step retrieval and indexing shows that the WR and the biometric performance are irrespective of the ranking (*i.e.* order of priority) of the BCs. This contrasts with the fusion in the feature-step retrieval and indexing. It is worth noting that privacy-preserving systems have mostly been designed and applied only to a single BC, *e.g.* the face in Osorio-Roig et al. [16], see Tab. I.
- A thorough theoretical and empirical analysis of the trade-off between computational WR and biometric performance of the proposed identification system on multi-modal large-scale datasets with state-of-the-art biometric recognition systems. Experimental evaluations compliant with the metrics defined in the ISO-IEC-2382-37:2022 [4] show that a protected multi-biometric identification system can reduce the computational workload to approximately 57% (indexing up to three types of BCs) and 53% (indexing up to two types of BCs). This can be achieved while simultaneously improving the biometric performance at the high-security thresholds of a baseline biometric system.

To summarize the main contributions of this work, this novel privacy-preserving solution experimentally shows the feasibility of the concept of frequent binary patterns to be applied to protected biometric templates corresponding to different types of BCs, in contrast to the approach proposed by Osorio-Roig et al. [16]. Most importantly, a multi-biometric

privacy-preserving system is proposed which introduces novel fusion techniques based on frequent binary patterns that are extracted and designed agnostically with respect to types of BCs and template protection schemes. Extensive experimental evaluations demonstrate that design-agnostic multi-biometric systems based on frequent binary patterns preserve biometric security and performance while allowing different BCs to be searched efficiently in a single biometric identification transaction.

The remainder of this work is organised as follows: Related works summarising concepts related to information fusion, workload reduction and biometric template protection are revisited in Sect. II. In Sect. III, the proposed system is described in detail. Sect. IV presents the experimental evaluations and results are reported and discussed in Sect V. Finally, conclusions are drawn in Sect. VI.

II. Related Work

This section describes the background and related work on reducing computational workload in protected biometric identification systems. Whereas Sect. II-A introduces the fusion strategies commonly used in biometrics, Sect. II-B addresses the problem of WR on biometric systems. Finally, key work related to the *workload-reduction* and *biometric identification systems* areas on biometric template protection is summarised in Sect. II-C.

A. Biometric Information Fusion

Biometric information fusion allows combining biometric data at different levels of processing in a biometric system. Those systems which enable biometric information fusion are known in the literature as multi-biometric systems. Generally, multi-biometric schemes combine or fuse multiple sources of information to improve the overall discriminative power of a single biometric recognition system [19]. The fusion strategies can be categorised in the biometric context as multi-types, multi-sensorial, multi-algorithms, multi-instances, and multi-presentations [20], [21].

The system proposed in this work relates to the first scenario, *i.e.* multi-type, which relies on the fusion of different types of BCs (*e.g.* facial and iris images). Specifically, three types of BCs are selected and subsequently utilised in a binning and fusion scheme. Note that given the simplicity of the proposed scheme, other fusion categories, such as multi-sensorial, multi-instances and multi-presentations can be also employed. In addition to the general categories above, several levels of biometric processing can be distinguished at which information fusion can take place [20], [21]: Sensor, feature, score, rank, and decision.

In the scope of this article, the fusion of information from multiple features and at the score level is of major interest, as the proposed scheme in Sect. III is designed to operate at those levels of the biometric processing pipeline. The feature-level fusion has been also considered, as it is among the most convenient techniques contributing to the highest privacy protection and security level, respectively [10], [22].

Information fusion in biometrics has been widely addressed in the scientific literature. An interested reader is therefore referred to, *e.g.* Ross et al. [20] for a general introduction to this topic and Paul et al. [23] for score-level fusion specifically, as well as Dinca and Hancke [24], Singh et al. [25], and ISO/IEC TR 24722 [21] for more recent works relating to the general topic of biometric information fusion.

B. Computational Workload Reduction

Biometric identification systems require fast response times, as the typical exhaustive search-based retrieval method demands high computational costs. Thus, the computational complexity tends to grow linearly with the number of enrolled data subjects [26]. As expected, the investment in expensive hardware that contributes to the parallel processing/distribution can be used to maintain a quick response time in a biometric identification transaction. Whereas many companies spend high monetary costs to achieve the desired times, one possibility that is often overlooked is the optimisation of the underlying software and/or algorithms. In this context, a solution to said problems (*i.e.* high computational and monetary costs) is the research field of *computational workload reduction* which allows decreasing the dependence on the investment of the physical infrastructure and focusing more attention on the software and/or algorithms. WR-based methods work directly on the optimisation of the number of computations required for some specific tasks in the biometric processing pipeline. For instance, for a biometric identification transaction, the computational costs at the biometric template comparison level typically dominate the computational effort of the entire system. Thus, most of these methods have been categorised in [7] as *pre-selection* approaches. These methods seek to reduce the number of biometric template comparisons (*i.e.* reducing the search space (see *e.g.* [27])), and *feature transformation*, aimed at accelerating the computational cost produced in a one-to-one comparison (see *e.g.* [28]). The former is of interest in the context of this article. For further information on such methods, the reader can be referred to [7].

Naturally, those WR-based techniques (*i.e.* pre-selection methods) have achieved decreasing the search spaces w.r.t. the typical exhaustive searches. Conceptually, such approaches are mostly custom-built for specific biometric systems, *e.g.* single BCs or feature extractors introducing specific representations. They are not expected to be applicable within other systems, *e.g.* containing different types of BCs to be processed. In addition, they are primarily designed to facilitate the reduction of the computational workload associated with biometric identification transactions in unprotected biometric systems (*i.e.* unprotected template indexing), which are prone to unauthorised attacks. The latter has motivated the scientific literature to investigate new customised procedures capable of performing the protected template indexing while reducing the overall computational effort per biometric identification transaction.

TABLE I
MOST RELEVANT APPROACHES ON BIOMETRIC TEMPLATE PROTECTION FOR BIOMETRIC IDENTIFICATION SYSTEMS BASED ON A SINGLE BC. RESULTS REPORTED FOR BEST CONFIGURATIONS AND SCENARIOS

Approach	WR category	BTP category	Biometric characteristics	Biometric performance	Efficient comparison
Wang *et al.* [29]	Pre-selection, Feature transformation	Non-traditional BTP	Face	95% H-R	(✓)
Murakami *et al.* [30]	Feature transformation	Cancelable biometrics	Face	0.1% FRR, 0.022% FAR	(✓)
Dong *et al.* [14]	Feature transformation	Cancelable biometrics	Face	99.75% R-1	(✓)
Osorio-Roig *et al.* [16]	Pre-selection	Cancelable biometrics	Face	∼99.00% H-R	✓
Drozdowski *et al.* [31]	Pre-selection	Cancelable biometrics	Iris	0.1% FPIR,93.21–97.50% FNIR	✓
Choudhary *et al.* [32]	Feature transformation	Cancelable biometrics	Finger-Vein	99.70%R-1	(✓)
Sardar *et al.* [33]	Feature transformation	Cancelable biometrics	Face	99.85% CRR-1	(✓)
Drozdowski *et al.* [34]	Feature transformation	Homomorphic encryption	Face	∼5% FNIR, 1% FPIR	(✓)
Engelsma *et al.* [35]	Feature transformation	Homomorphic encryption	Face	81.4% R-1	(✓)
Osorio-Roig *et al.* [36]	Pre-selection	Homomorphic encryption	Face	1.0% FPIR, 2.5% FNIR	✓
Drozdowski *et al.* [37]	Pre-selection	Homomorphic encryption	Face	0.1% FPIR, 0.42% FNIR	✓
Kolberg *et al.* [38]	Feature transformation	Homomorphic encryption	Iris	98.08% R-1	(✓)
Bauspiess *et al.* [39]	Pre-selection	Homomorphic encryption	Face	0.1% FPIR, 1.2% FNIR	✓
Engelsma *et al.* [40]	Pre-selection, Feature transformation	Homomorphic encryption	Fingerprint	99.93% H-R	✓
Dong *et al.* [41]	Feature transformation	Fuzzy vault	Face	99.86% R-1	(✓)

H-R: Hit Rate, FRR: False Rejection Rate, FAR: False Acceptance Rate, R-1: Rank-1 Identification Rate, DIR: Detection and Identification Rate, CRR: Correct Recognition Rate at Rank-1, FPIR:False Positive Identification Rates, FNIR: False Negative Identification Rates, ✓: Property fulfilled, (✓): Property partially fulfilled.

C. Biometric Template Protection

Biometric template protection schemes allow protecting biometric references (*i.e.* biometric templates) in an unprotected storage environment of a biometric system. Once they are protected, a set of properties are expected to be inherent to the transformed or protected templates, constraining the flexibility of the biometric processing pipeline compared to unprotected templates. Comprehensive surveys on this field can be found in [10], [11], and [42]. Generally, template protection methods are categorised as *cancelable biometrics* and *biometric cryptosystems*. The former employ transformations in the signal or feature domain that allow biometric comparison in the transformed (encrypted) domain [43]. The latter (*e.g.* fuzzy vault schemes [13]) usually bind a key to a biometric feature vector, resulting in a protected template. Thus, the biometric comparison is then performed indirectly by verifying the correctness of a retrieved key [44]. In particular, homomorphic encryption-based template protection schemes are distinguished as biometric cryptosystems whose specific designs allow computing operations directly in the encrypted domain with results comparable to those in the plaintext domain (*i.e.* unprotected domain) [45]. The challenge of unprotected templates being replaced by protected templates leads to requirements or properties which must be fulfilled according to ISO/IEC IS 24745 [42]:

Irreversibility: The infeasibility of reconstructing the original biometric sample given a protected template. This type of property guarantees the privacy of the users' data (*e.g.* avoiding dislocating the subject's ethnic information) and additionally, the security of the system is increased against *e.g.* presentation attacks and face reconstruction from deep templates.

Unlinkability: The infeasibility of determining if two or more protected templates were derived from the same biometric instance, e.g. face. By fulfilling this property, cross-matching across different databases is prevented.

Renewability: The possibility of revoking old protected templates and creating new ones from the same biometric instance and/or sample, *e.g.* face image. With this property fulfilled, it is possible to revoke and re-generate new templates in case the database is compromised.

Performance preservation: The requirement of the biometric performance not being significantly impaired by the protection scheme.

Tab. I lists the most relevant scientific works on biometric template protection for biometric identification systems based on a single BC. The approaches have been analysed in terms of efficient comparison (*i.e.* WR) and biometric performance. Scientific works on biometric cryptosystems for identification [34], [35], [38] have been commonly focused on providing evidence of practical applicability. The majority of them have contributed to reducing the effort at a one-to-one comparison level by feature transformation while other approaches [36], [39] worked on the reduction of one-to-many comparisons. It is well-known that cancelable schemes appeared to be more suitable in an identification scenario [16], in contrast to biometric cryptosystems (*e.g.* [41]). That is because the design of cancelable biometrics does not require comparison strategies that usually enable the non-flexibility of launching non-arithmetic operations [46] or verifying the correctness of a retrieved key [44]. From

a practical perspective, cancelable approaches have been therefore successfully considered to be applied in identification scenarios for different BCs (*e.g.* face, iris, and fingerprint). As mentioned above, these schemes introduce non-invertible transformations at the feature level, which typically allow retaining efficient biometric comparators of the corresponding unprotected systems. This way, the majority of published cancelable schemes applied transformations in the feature domain while maintaining acceptable biometric performance and low computational workload. Over the past years, some feature transformations (*e.g.* BioHashing [33]) covered discriminative power-based gaps addressing the indexing protected templates with an identification rate at the rank 1 (R-1). Also, the locality sensitive hashing (LSH) [47] nature has recently been exploited and designed to obtain compact non-invertible features (*e.g.* [14], [32]). Similarly, protected templates are more likely to have the same hash collision compared to dissimilar ones.

The described solutions applied WR through an acceleration of a one-to-one comparison. In contrast, other researchers (*e.g.* [16], [31]) have explored computational WR to decrease the number of one-to-many comparisons, which dominates the overall computational effort in biometric identification transactions [37]. More precisely, Osorio-Roig et al. [16] proposed recently the retrieval of cancelable deep face templates based on their frequent binary patterns. The design of this type of retrieval enabled the use of different cancelable biometric template protection schemes. To sum up, all published works on cancelable biometric template protection for biometric identification worked on an exhaustive search when only feature transformation was employed. Whereas other works reduced the one-to-many search (*i.e.* pre-selection-based approaches), such schemes are usually not flexible or not designed to work on different BCs. In addition, some generic multi-biometric indexing methods suitable to work only on unprotected domains have been proposed *e.g.* in [19], [48], and [49].

III. Proposed System

Consider a biometric enrolment database containing references protected by cancelable schemes[2] of N data subjects for m different BCs or instances. A trivial search process for a single biometric identification transaction would be to conduct the comparisons exhaustively, *i.e.* the workload (W) of a baseline system is estimated as $W_{baseline} = N \cdot m$ comparisons for all BCs. In fact, for an improvement of the biometric performance or WR (see [19]), *e.g.* fusing the scores using one of the traditional strategies (such as score or rank level fusion) mentioned in Sect. II-A, the workload would be dominated by comparisons done exhaustively. As an alternative to the multi-biometric exhaustive search in the protected domain, this work extends the proof-of-concept of frequent binary patterns [16] to indexing multi-biometric cancelable references by employing strategies of biometric information fusion described in the Sect. II-A. In a nutshell, the concept of frequent binary patterns is employed as a multi-biometric efficient binning scheme. Each bin (*i.e.* a single frequent binary pattern) is built by fusing m representations from protected reference templates and allows for indexing them in a single biometric identification transaction. Fig. 1 presents a conceptual overview of the proposed scheme. The design of the multi-biometric binning scheme is template-protection-scheme and BC-agnostic, which makes it easy to work across different cancelable biometrics extracting binary representations. Sect. III-A discusses representation types of biometric feature vectors, Sect. III-B provides details on the approach that computes frequent binary patterns, Sect. III-C describes three strategies of information fusion that result in stable frequent binary patterns for indexing, Sect. III-D describes the retrieval process for each type of information fusion. Sect. III-E discusses the obtained WR. Sect. III-F elaborates on privacy and security aspects.

[2]We assume these schemes yield features containing binary representations.

A. Biometric Feature Representation

Biometric feature vectors may be of different representations depending on the type of feature elements (real, integer, or binary), their dimension and if they are fixed-length or variable-length. Common feature representations have been established for unprotected feature vectors of different BCs, *e.g.* minutiae sets for fingerprints or binary codes for iris. The use of DNN-based feature extractors usually results in real-valued vectors of fixed dimension since DCNNs are commonly trained using differentiable loss functions, *e.g.* Euclidean distance.

In the proposed system, it is assumed that cancelable schemes extract binary representations from DNN-based feature vectors. This is a reasonable assumption, since many cancelable biometric schemes are designed to obtain protected binary representations, *e.g.* in [50]. However, other representations can be easily transformed to binary vectors using common procedures [51]. Real-valued feature representations can be mapped to integers through quantisation. To obtain a binary feature vector, integers can be mapped to binary strings. In this context, different binary encoding methods have been suggested in the scientific literature [51]. The employed binarisation may result in a loss of biometric performance due to information loss caused by coarse quantisation. However, if parameters are chosen appropriately biometric performance may be maintained, see [28]. Alternatively, compact binary representations can also be extracted by deep learning techniques. Deep hashing has been coined as an umbrella term for methods which aim at extracting compact and stable representations with deep learning techniques [52]. In the recent past, deep hashes have been extracted from different BCs in various ways, *e.g.* in [53] and [54].

B. Frequent Binary Pattern Extraction

Frequent binary patterns can be defined in a general concept for the enrolment and retrieval processes, respectively. Formally, the frequent binary patterns can be extracted from a binary representation as follows: Let $f \in \{0, 1\}^n$ be a bit-string of size n and $k < n$ a given frequent pattern length. A set of

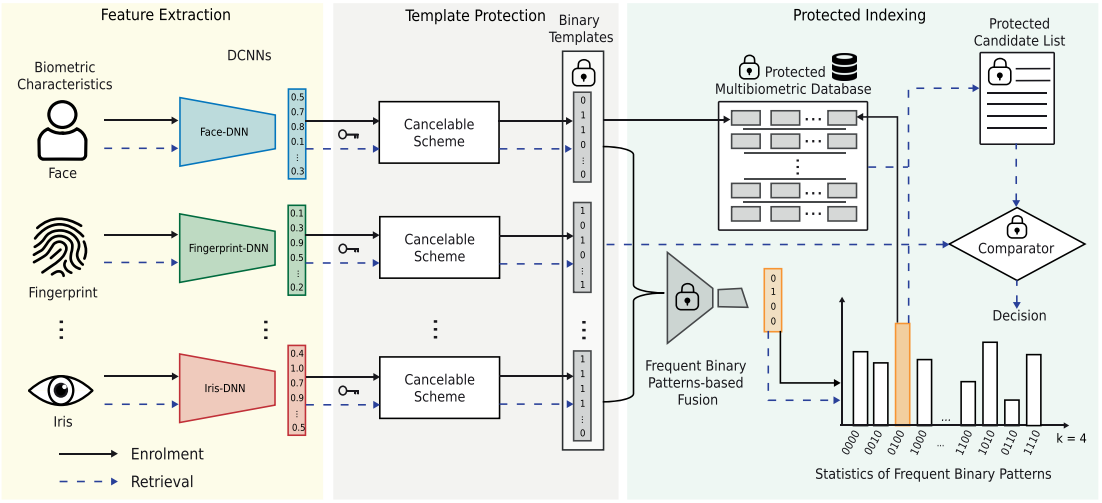

Fig. 1. Conceptual overview of the proposed multi-biometric scheme. Firstly, the system receives different BCs or instances which are processed by state-of-the-art DNN-based embedding extractors. Subsequently, feature vectors of equal size are protected and encoded in a binary representation by well-established cancelable schemes. Techniques of information fusion are then applied to the protected features along with the concept of frequent binary patterns for the indexing and retrieval steps. Finally, a protected candidate list can be returned taking into account the statistics of their frequent patterns.

unique binary patterns $\mathbf{P} = \{p_1, \ldots, p_L\}$, each of length k can be computed over f by sampling in a sliding window the consecutive k bits starting from positions $[0, \ldots, n-k]$ with stride 1. In addition, let $\mathbf{O} = \{o_1, \ldots, o_L\}$ be the set of occurrences of each $p_i \in \mathbf{P}$. There is a direct relation between $\mathbf{O}$ and $\mathbf{P}$: For each $p_i \in \mathbf{P}$ there exists an $o_i \in \mathbf{O}$ which denotes the number of occurrences of p_i in f. Therefore, for a general retrieval process, consider a function $\mathbf{FP}(\cdot)$ that extracts the set $\mathbf{P}$ ordered descending according to $\mathbf{O}$.

C. Indexing Multi-Biometric Frequent Binary Patterns

Conceptually, as mentioned above, frequent binary patterns can be extracted only from binary representations. Therefore, deciding which type of information to fuse from the protected references before or after extracting the patterns could impact the efficacy of the proposed binning scheme. Introducing known and simple fusion strategies (*e.g.* concatenation) in intelligent and convenient steps increases the stability and the discriminative power of the procedure of frequent binary pattern extraction. Thus, the overall results of the proposed system in terms of biometric performance and computational workload are improved.

Formally, let $\mathbf{R}_i = \{r_i^1, \ldots, r_i^m\}$ be the set of data of the subject $i \in \{1, \ldots, N\}$ in the enrolment database, where each r_i^j denotes a protected binary reference associated with the BC $j \in \{1, \ldots, m\}$. Given a fixed frequent binary pattern length of k bits, the goal is to build a multi-biometric and efficient binning scheme over the base of stable frequent binary patterns successfully extracted on $\mathbf{R}_i$. For enrolment, this work considered the fusion strategies at two levels based on the concept of frequent binary patterns: Feature and representation level. The former pipeline introduces the concatenation of protected binary references corresponding to different m BCs. Here, the concatenation acts as doubling the feature dimension by keeping all the elements from the input features. The latter shows the fusion across the maximum binary patterns successfully mapped from individual protected binary references corresponding to m BCs.

Feature-level Indexing each $r_i^j \in \mathbf{R}_i$ of size d is concatenated with the remaining elements in $\mathbf{R}_i$ yielding a protected feature of size $d \cdot m$ bits. Let $\mathbf{B}_i = \left[r_i^1 \| \ldots \| r_i^m\right]$ be the concatenation of m protected binary references of the i-th subject. $\mathbf{B}_i$ can be then mapped to an individual bin b_i which is computed by $\max(\mathbf{FP}(\mathbf{B}_i)) \rightarrow b_i$ given a fixed k, as explained in Sect. III-B. That is, the set of data subjects is indexed with at most 2^k bins.

Representation-level Indexing each $r_i^j \in \mathbf{R}_i$ can be independently mapped by the function $\mathbf{FP}(r_i^j) \rightarrow \mathbf{P}_i^j$, resulting in at most 2^k patterns. In this context, two fusion approaches are considered:

1) Ranked-codes: $\max(\mathbf{P}_i^j) \rightarrow b_i$ a single binary pattern resulting in the most ranked frequent binary pattern extracted from the set $\{\mathbf{P}_i^j\}_{j=1}^m$ is considered as a stable bin for indexing.
2) XOR-codes: The bin b_i is constructed from the bitwise **XOR** operation between the binary patterns with the maximum occurrence in each $\mathbf{P}_i^j$ with $1 \leq j \leq m$, *i.e.* $\mathbf{XOR}(\max(\mathbf{P}_i^j)) \rightarrow b_i$.

D. Multi-Biometric Retrieval by Fusion Strategy

As explained in Sect. III-B, for a general retrieval process, frequent binary patterns are extracted preserving their order of occurrence. It is expected that the pattern with the highest occurrence provides a better chance to find the correct candidate subject than patterns leading with low occurrence, as showcased in [16]. In a retrieval step, this parameter (*i.e.* pattern with the highest occurrence) would be estimated on an incremental search for those p patterns with the highest occurrence. For a concrete example, consider 2^3 patterns: $\mathbf{P} = \{p_1, p_2, \ldots, p_8\}$, extracted by the function $\mathbf{FP}(\cdot)$ given $k = 3$. A threshold t with $1 \leq t \leq 2^k$ is determined on $\mathbf{P}$ and represents the maximum number of bins that can be visited

for a biometric probe. Note that this parameter (t) can easily be controlled by the binning scheme and is independent of the retrieval strategy employed. Also, extracted patterns can only take advantage of their orderings, which can be influenced by the retrieval strategy employed (*e.g.* type of fusion). In this regard, all proposed retrieval strategies employ a score-level fusion in a multi-biometric identification transaction once a corresponding bin is determined. In particular, a sum-rule fusion is applied among normalised similarity scores computed from each BC. This type of fusion has been utilised in multi-biometric indexing schemes (*e.g.* [19]) and has also contributed to very good biometric performance in general (see [55] and ISO/IEC TR 24722 [21]).

In this work, three retrieval strategies, one for each type of information fusion, are proposed. Firstly, we consider the fact that a binning scheme can be created using one of the strategies described in Sect. III-C. In a retrieval scenario, let $\mathbf{Z} = \{z_1, \ldots, z_m\}$ be the set of protected biometric templates for a probe subject, where each z_j denotes a binary representation for each of the m BCs. The key idea is that the proposed retrieval schemes offer different orderings and representations of the extracted frequent binary patterns. Subsequently, a parameter t can be empirically computed in a multi-biometric identification transaction (see Sect. V-B), thereby reducing the system workload while preserving a trade-off between biometric performance, efficiency, and privacy.

Feature-level Retrieval we follow a similar idea to that of feature-level indexing, as explained above in Sect. III-C. Let $\mathbf{B} = \left[z_1 \parallel \ldots \parallel z_m \right]$ be the concatenation of all $z_j \in \mathbf{Z}$ and a fixed k, the retrieval strategy searches the database for bins belonging to the ordered set $\mathbf{P} \leftarrow \mathbf{FP}(\mathbf{B})$. The final candidate list is therefore composed of the identities associated with the retrieved bins in $\mathbf{P}$.

Representation-level Retrieval in contrast to the feature-level based retrieval, this retrieval pipeline allows searching a t by handling the binary patterns extracted per BC. Said patterns are computed as follows:

1) Ranked-codes: The database is searched for the highest ranked binary patterns of each $\mathbf{P}_j \leftarrow \mathbf{FP}(z_j)$ and the identities associated with those existing patterns make up the final candidate list.
2) XOR-codes: The database is searched for those binary patterns resulting from the bitwise **XOR** operation among all possible pairs of binary patterns that belong to different $\mathbf{P}_j$. Note that the bitwise **XOR** operations are computed over at most $m \cdot 2^k$ number of pattern pairings that can be constructed from $\{\mathbf{P}_j\}_{j=1}^{m}$.

E. Computational Workload Reduction

Our design, which is agnostic with respect to the type of BCs and cancelable schemes, allows searching different BCs in a single biometric transaction. Therefore, the number of bins visited as well as the number of protected templates stored at each bin is expected to be the same per BC. To that end, as mentioned in Sect. III-D, a threshold t may be defined across m types of BCs used. Although this parameter is easily managed by the multi-biometric binning scheme, a computational workload cost may be noticed depending on the BCs involved (*e.g.* face and iris, or face and fingerprint), the workload of the individual BCs, and the strategy of fusion used for retrieval and indexing, respectively.

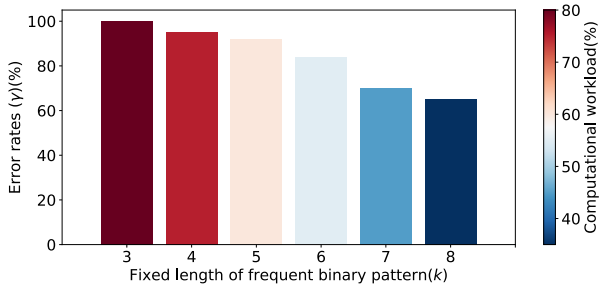

Fig. 2. Effect of k on the trade-off between the biometric performance (γ) and the computational workload ($W_{proposed}$). Consider that a biometric performance can be computed in any biometric identification transaction (*e.g.* $\gamma \rightarrow$ hit-rate).

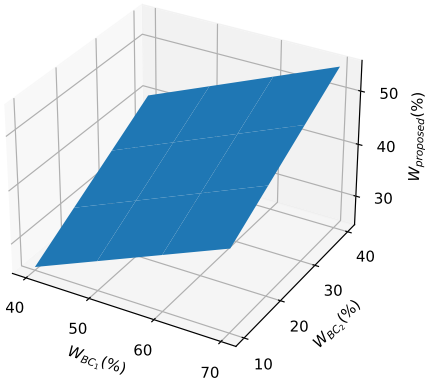

Fig. 3. Relation between the overall computational workload (*i.e.* $W_{proposed}$) of the multi-biometric approach with respect to the individual workload by type of BCs involved (*i.e.* W_{BC_1} and W_{BC_2}).

The computational workload $W_{proposed}$ of an identification transaction (measured in terms of the number of necessary template comparisons) in the proposed scheme, can be expressed as follows:

$$W_{proposed} = \sum_{i=1}^{t} |b_i| \cdot m, \tag{1}$$

where $1 \leq t \leq 2^k$ denotes a threshold for the maximum number of bins or frequent binary patterns visited in a retrieval step for a fixed k and $|b_i|$ the number of protected templates associated with the m BCs involved. Note that k implicitly is included in the Eq. 1 describing a fixed length in the search for frequent binary patterns (Sect. III-B), and is expected to affect the computational workload along with the biometric performance (see Sect. V). This trend is shown theoretically in Fig. 2. According to Fig. 2, it should be observed that larger k appears to provide a discriminating effect on the built bins, reducing the number of protected templates stored within a bin and thus the overall computational workload. However, some deterioration in biometric performance is observed while

maintaining a low workload. Additionally, Eq. 1 shows the relation between the computation of the overall computational workload and the types of BCs involved in the multi-biometric binning scheme. Fig. 3 theoretically visualizes said relation for *e.g.* two BCs involved (BC_1 and BC_2) in a range of computed individual workloads. Note that individual workloads can be computed on the proposed scheme using a single BC (*i.e.* uni-modal biometric system). As observed, the overall computational workload appears to be directly proportional to the individual workloads corresponding to each BC: $W_{proposed}$ increases with the workloads of the types of BCs involved. Also, this trend allows some BCs to take advantage of the unbalanced workloads among individual BCs, *e.g.* BC_1 over BC_2 in this case. However, an improvement in overall biometric performance is expected to be achieved, albeit with a slight increase in the overall computational workload.

In summary, the key idea behind Eq. 1 is to reduce the computational workload dominated by the cost of comparisons carried out exhaustively. Hence, it is expected that $W_{proposed} \ll W_{baseline}$, reducing the penetration rate in the search. An upper bound of $W_{proposed}$ in Eq. 1 is reached, when the system retrieves all bins, resulting in an exhaustive search. In contrast, the best case is when the biometric probe is in the first bin retrieved (*i.e.* $t = 1$) and this contains the fewest number of protected multi-biometric templates.

F. Privacy and Security Aspects

The privacy protection and security provided by the proposed system are evaluated according to international standards that define metrics and attack models for the evaluation of biometric (template protection) schemes.

According to ISO/IEC 24754 [42], the privacy protection requirements of irreversibility, unlinkability and renewability have to be fulfilled. Irreversibility prevents from the attack where an adversary tries to reconstruct the original biometric data from the protected biometric template. Unlinkability prevents from the attack in which an adversary tries to determine whether two protected biometric templates stem from the same subject. If unlinkability is achieved, the requirement of renewability is met, too. To properly evaluate these requirements for a distinct template protection scheme, established metrics need to be applied, as defined in ISO/IEC 30136 [56]. In experiments, those established metrics will be applied to measure the privacy protection properties of the proposed system.

Further, different attack models for describing scenarios and assumptions of attacks on biometric template protection schemes are standardised in ISO/IEC 30136 [56]. The most restrictive model is referred to as the naïve model, in which an attacker has neither information of the template protection scheme, nor owns a large biometric database. However, it is common practise to analyse template protection schemes under Kerckhoffs' principle, which is referred to as *the general model*. In this model, an adversary is assumed to possess full knowledge of the template protection algorithm. In addition, the adversary may have access to one or more protected templates from one or more databases. However, the attacker is not in possession of the employed key. This attack model is considered in the privacy protection evaluation. Further, application-specific keys are applied, since subject-specific keys have been found to counterfeit the privacy protection capabilities in biometric template protection schemes [57].

TABLE II
SUMMARY OF THE DATASETS USED IN IDENTIFICATION EXPERIMENTS

Biometric characteristic	Dataset	#Instances	#Samples
Face	LFW [60]	1,120	4,126
Fingerprint	MCYT [61]	1,120	13,440
Iris	CASIA-Iris-Thousand [62]	916	3,369
	BioSecure [63]	204	757

Note that the proposed multi-biometric indexing scheme is largely agnostic with respect to the cancelable scheme employed for privacy protection. In other words, the privacy protection capabilities of the used cancelable scheme are transferred to the proposed multi-biometric indexing scheme. This means the privacy protection capability of the used cancelable biometric system is retained, which is a major advantage of the presented indexing method.

Further, it is important to note that the proposed scheme does not introduce any additional helper data that may cause information leakage. In the proposed system, indexing is performed on protected biometric templates. Obtaining indexes from these cancelable binary templates offers the advantage that the privacy protection of the underlying cancelable scheme is not impaired by the indexing scheme. Recently, it has been shown that indexing methods can leak sensitive information, in particular, if additional indexing data is extracted from unprotected biometric templates [58]. In contrast, the proposed scheme extracts the indexing data from the protected templates. The frequent binary patterns extracted from the protected templates do not comprise any additional sensitive information that could be leveraged by an attacker. In case an attacker estimates frequent binary patterns from a protected template, he/she could only learn the bin in which such a template would be stored. However, bins are expected to contain protected templates of more than one subject and, therefore, do not provide any useful information to the attacker.

As for any biometric (template protection) system, the security is directly related to the probability of false positives. More precisely, in an identification system the False Positive Identification Rate (FPIR) as defined in ISO/IEC 19795-1 [59] (see Sect. IV-E) reflects this probability. A low FPIR prevents from false accept attacks, in which the adversary iteratively simulates non-mated authentication trails until a false match is reached. It is generally known that biometric systems based on multiple BCs can operate at lower FPIRs [7] since false positives occur with lower probability if more biometric data is compared. This is also the case in the scheme proposed in this work. However, this also depends on other factors, *i.e.* the number of enrolled subjects in the database, used feature extraction techniques, or biometric sample quality.

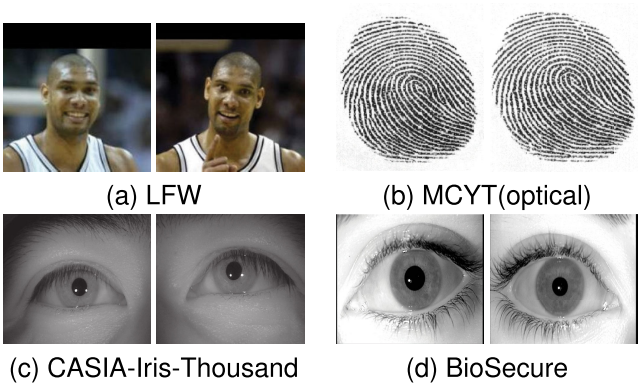

Fig. 4. Example images from the selected databases.

IV. Experimental Setup

This section describes a detailed setup of the experiments conducted on privacy-preserving multi-biometric indexing. Sect IV-A describes the datasets together with the different BCs employed in this investigation, Sect. IV-B provides details of the extraction process of deep templates, Sect. IV-C details the cancelable template protection schemes, while Sect. IV-E provides the metrics for the evaluation of the proposed system.

A. Databases

For biometric identification experiments where WR across indexing schemes is analysed, large-scale databases should be considered. Since large-scale databases are not available to researchers, we created a composite database using selected BCs. This type of database allows operational systems to work independently of the BCs and their feature representations. A similar concept was utilised in [19]. Tab. II shows an overview of the databases used in terms of the number of instances and samples. Note that we selected the three most common types of BCs, *i.e*. face, fingerprint, and iris for our research. Details of the selected BCs and their databases are described as follows:

Face: LFW [60] database is focusing on the large-scale unconstrained face recognition problem. It comprises 13,233 face images captured in the wild from 5,749 subjects collected from the web, where 1,680 subjects are represented with two or more images and 4,069 subjects are represented with a single sample. In our experiments, we used only 1,170 identities from the group containing more than one face sample. CR-FIQA(L)[3] as a quality measure has been utilised as a filtering step for selecting the subset of identities with their corresponding samples.

Fingerprint: MCYT [61] database containing only fingerprint images captured with an optical capture device is used. This dataset contains all 10 fingers from 330 subjects and 12 samples for each finger, for a total of 39,600 samples. For the experimental protocol, each fingerprint is considered a different biometric instance and is therefore treated as a separate subject. In particular, 1,170 identities are filtered out by using the quality factor NFIQ 2.0.[4]

Iris: A mixed iris database was designed to achieve a balanced number of identities with respect to the other BCs. CASIA-Iris-Thousand [62] database and BioSecure [63] database, both containing images captured in the near-infrared light spectrum, were used. The former contains 1,000 subjects with 2,000 instances, each one represented with 10 samples from each right and left eye. The latter comprises 210 subjects with 420 instances, each one containing 4 samples from each right and left eye. Similar to fingerprints, each iris instance was considered a separate identity. In our experiments, a mixed subset was constructed up to a total of 1,170 identities. Iris samples and instances were discarded taking into account different criteria: Segmentation errors that led to a bad normalisation step, samples containing glasses, critical images where the visible iris area did not represent more than 70% of the usable iris area, and other quality measures with less critical behaviour such as the iris-sclera, iris-pupil contrast, and the iris-pupil ratio. Note that all quality measures analysed were evaluated and interpreted according to ISO/IEC 29794-6 [64]. For the quality assessment of iris samples, an open-source software[5] BIQT-Iris was utilised, which reports all the quality measures described in ISO/IEC 29794-6.

Note that 50 identities of 1,170 per database are selected for the score normalisation process and the remaining 1,120 are selected for biometric identification experiments. It is worth noting that biometric identification scenarios are more challenging than verification scenarios, as the chance of a false positive can easily increase with the number of comparisons [26]. Thus, for the selection of identities per BC, the correlation between those biometric samples that produce worse similarity scores (highest chances of false positive in a critical operational point) and the different quality measures were also analysed. It should be noted that quality metrics were evaluated in order to keep only those samples with the best quality. To sum up, it is reasonable that biometric identification systems in real applications may operate with samples that provide acceptable quality in accordance with evaluation standards. Even more when biometric template protection and indexing schemes are employed. For the evaluations of the proposed multi-biometric systems, a database merged with the identities selected independently for each BC (*i.e*. , face, fingerprint, and iris) is constructed. Fig. 4 shows some example images from the databases selected per BC.

B. Deep Templates and Pre-Processing

For the experimental analysis, embeddings extracted by the current state-of-the-art DNN-based recognition systems per BC are considered. All embeddings utilised consist of 512 floating-point values. Note that the features extracted per BC are balanced in terms of the number of dimensions, which

[3]https://github.com/fdbtrs/CR-FIQA

[4]https://github.com/usnistgov/NFIQ2/

[5]https://github.com/mitre/biqt-iris

allows the indexing scheme to produce the same chances of binary pattern search when they are fused at *e.g.* the feature level. Details of the extraction process and pre-processing per BC are described as follows:

Face: ElasticFace represents a state-of-the-art face recognition system. Features are extracted from the pre-trained model ElasticFace made available by the authors.[6]

Fingerprint: Deep fingerprint fixed-length representations are extracted from the open-source software introduced in [65]. Note that fingerprint embeddings are extracted by using the training on the texture branch.

Iris: A deep iris representation extractor presented in [66] was used to extract iris embeddings. To that end, the approach proposed by [66] was trained on subsets of the CASIA-Iris-Thousand [62] and BioSecure [63] databases, respectively, from scratch. Note that those instances selected for training were not included in the set of instances for testing that contributed to the biometric identification experiments in this paper. Specifically, for the set of training, 200 instances[7] and 818 instances[8] from BioSecure [63] and CASIA-Iris-Thousand [62], respectively, were selected randomly. Iris images were pre-processed with the traditional approaches. Iris segmentation was applied by using the Viterbi algorithm available in the open-source OSIRIS [67], iris textures were normalised according to the rubbersheet model, and subsequently, enhanced by applying Contrast Limited Adaptive Histogram Equalization (CLAHE).

To sum up, it is important to note that any specific pre-processing like alignment, or type of input to the DNN was considered as described in their corresponding articles of reference. Furthermore, original embeddings extracted per BC are converted to 512 binary-values feature vectors (*i.e.* unprotected baseline system) by using a simple sign function with threshold 0. This trivial binarisation method was found to be the most effective since it did not cause any significant performance drops in the employed baseline systems. However, in case a performance degradation is observed, the use of a more sophisticated binarisation technique is recommended. Suitable approaches have been mentioned in Sect. III-A. The resulting binary representation is compatible with the proposed scheme and enables a one-to-one comparison via Hamming distance.

C. Cancelable Schemes

Biometric template protection approaches representing the current state-of-the-art for cancelable schemes have been used in these experiments. In particular, the so-called BioHashing [50] and a single instance of the Locality Sensitive Hashing [18] based on Index-of-Maximum Hashing with Gaussian Random Projection (IoM-GRP). The former yields output representations containing 512 binary-point values, while the latter comprises 512 integer-point values. To facilitate the design agnostic w.r.t. the output of the cancelable scheme (binary representation) before the application of the proposed indexing scheme, output representations of the IoM-GRP approach were binarised prior to the frequent binary pattern extraction process. To that end, each integer value is encoded in n bits which are computed on a one-hot encoding by using the maximum number of Gaussian Random Projection vectors (q) for all the IoM-GRP integer representations. Finally, a binary representation with length $n \cdot m$ bits, where m represents the number of Gaussian Random Matrices or length of the integer representation, can be obtained. In these experiments, we used $q = 16$ and $m = 512$ to obtain a binary vector of size 2,048 bits. Note that for the computation of the similarity score function for a single biometric identification transaction, this scheme employs its own comparator based on the number of collisions through integers. In particular, BioHashing [50] employs hamming distance. Overall, all protected templates have been used on stolen-token scenarios where non-mated comparisons have access to the genuine users' secret key and use this key with the impostors' deep features.

D. Proposed System Configurations

Biometric identification experiments including the exhaustive search, *i.e.* baseline workload ($W_{baseline}$), and the proposed indexing scheme (*i.e.* at the feature- and representation-level) were conducted using 10-fold cross-validation for closed-set and open-set scenarios, respectively. For each fold, two samples per instance are randomly selected, one for enrolment and the other for search. It should be noted that the same samples (same randomness) selected for enrolment and search for each fold are maintained across the configurations of the proposed indexing schemes. Note also that the proposed multi-biometric approach applies to all possible combinations of two types of BCs and to all three types of BCs together. Moreover, for the step of score normalisation, the Z-score method is utilised as done in [19], which uses the arithmetic mean and standard deviation of the score's data.

E. Evaluation Metrics

The experimental evaluation is conducted according to two key aspects which are considered using methods and metrics standardised from the ISO/IEC 19795-1 [59] and supported by others which are commonly reported in the scientific literature:

- **Biometric performance**: For the closed-set scenario, the hit-rate (H-R), the proportion of subjects for which the corresponding subject identifier is in the subset of candidates retrieved by the proposed indexing scheme; for the open-set scenario, the detection error trade-off (DET) curves between the false negative identification rate (FNIR) and false positive identification rate (FPIR).
- **Computational workload reduction**: Average proportion of the total number of references that are retrieved per identification transaction (denoted W) compared to a baseline workload (*i.e.* an exhaustive search). It is worth noting that W is theoretically defined in Sect. III-E.
- **Unlinkability**: To evaluate unlinkability of cancelable schemes, mated and non-mated comparisons are performed with sample-specific keys, and the general

[6] https://github.com/fdbtrs/ElasticFace

[7] Those instances containing more than 3 samples.

[8] Those instances containing more than 5 samples.

unlinkability measure introduced in [9] is estimated. The linkability of two templates is measured in terms of the difference of conditional probabilities of two hypotheses of being mated, H_m, and non-mated, H_{nm}, for a given comparison score s between two given templates:

$$\mathrm{D}_{\leftrightarrow}(s) = p(H_m|s) - p(H_{nm}|s). \quad (2)$$

Then, by finding conditional expectation of this local measure $\mathrm{D}_{\leftrightarrow}(s)$ over all comparison scores, results in a global measure, $\mathrm{D}_{\leftrightarrow}^{sys}$, which is considered as the system unlinkability measure:

$$\mathrm{D}_{\leftrightarrow}^{sys} = \int p(s|H_m)\mathrm{D}_{\leftrightarrow}(s)\mathrm{d}s. \quad (3)$$

The value of $\mathrm{D}_{\leftrightarrow}^{sys}$ is in the interval [0,1], with lower values indicating smaller possibilities to link templates of the same subject.

- **Irreversibility**: Irreversibility is measured in terms of mutual information (MI). It quantifies the amount of information related to the set of original (unprotected) biometric templates X that can be obtained from the set of protected biometric templates Y. The set Y is obtained with the application of cancelable schemes to the set of unprotected templates X. The calculation of MI requires as input the two sets of unprotected and protected templates and provides as output a non-negative score. The smaller this score, the better for irreversibility, with a value equal to zero when the two sets are independent. The computation of MI relies on the estimation of entropy. To simplify the computation of entropy and MI, Principal Component Analysis (PCA) is applied to the sets X and Y, which are matrices with initial dimensions $s \times u$ and $s \times p$ respectively, with s being the number of samples, u the number of features in unprotected templates, and p the number of features in protected templates. From the application of PCA to the matrices X and Y, the reduced matrices $X_r = PCA(X)$ and $Y_r = PCA(Y)$ are obtained, with dimensions $s \times r$, where r is the number of reduced features. While decreasing the number of features, PCA retains the most significant information of biometric templates. PCA is applied to the matrices of unprotected templates X and protected templates Y_i resulting from different cancelable schemes i, always considering a fixed number of features $r = 100$ for the reduced matrices. Then, we approximate to multivariate Gaussian the distribution of features of the reduced matrices. For each matrix Y_{ri}, the MI between X_r and Y_{ri} can be computed as follows:

$$MI(X_r, Y_{ri}) = H(X_r) + H(Y_{ri}) - H(X_r, Y_{ri}), \quad (4)$$

where $H(\cdot)$ is the measure of entropy, quantified with the Shannon's entropy formula.

V. Results and Discussion

In this section, the experimental results are described. Firstly, in Sect. V-A, the proof-of-concept of *frequent binary patterns* for indexing deep cancelable templates is empirically validated to work on a single-BC: Face, iris, and fingerprint, against a baseline workload (*i.e.* exhaustive search). Subsequently, Sect. V-B shows the results of indexing by combining different BCs at different levels. Finally, an analysis of the privacy protection is presented in Sect. V-C. It is worth noting that all the figures (plots) utilise nomenclatures to refer to the different types of BCs: FA (face), FP (fingerprint), and IR (iris). Also, different nomenclatures to refer to different statistical data computed in closed-set scenarios have been employed; #Comp: Average number of comparisons, Std_comp: Standard deviation across the comparisons done per subject, #Visited-patterns: Average number of binary patterns visited from the probe, Std_bins_v: Standard deviation across the bins visited per subject.

A. Single-Biometric Characteristic

Tab. III shows the effect of the length of the frequent pattern (k) in relation to the hit rate (H-R) and the system workload (W) empirically computed for a set of identification transactions over closed-set scenario. Note that k has been only shown for the best configuration and for a final value of k (*i.e.* k=8). In the context of the workload computation, two WR values representing a lower bound (W_l) and an upper bound (W_u) are estimated. The former considers the lowest number of comparisons equitably distributed among bins without considering their standard deviations, while the latter considers an increased workload taking into account the standard deviations. Note that for a realistic scenario (*e.g.* open-set scenario), the overall workload would be limited to the upper limit of computational workload (see W_u on Tab. III) that can be easily controlled by a fixed number of bins for a biometric identification transaction. In addition to the closed-set scenario evaluations, Tab. IV shows open-set results for the best parameter configurations in Tab. III. Note that for this scenario, a fixed number of bins representing the number of bins visited (see #Visited-patterns + Std_bins_v in Tab. III) is set for a set of biometric identification transactions. It should be noted that an exhaustive search represents the baseline workload ($W_{baseline} = 100\%$).

Tab. III shows that the proof-of-concept of *frequent binary patterns* for indexing deep cancelable templates outperforms the exhaustive search in terms of WR across different BCs for two well-known biometric template protection schemes: BioHashing and IoM-GRP. In particular, the lowest values observed for W_u are 30.43% and 43.87% for BioHashing and IoM-GRP, respectively, and are achieved by the fingerprint while maintaining a high hit rate (99%≤H-R≤100%). Then, a higher W value can be perceived for the face (*i.e.* $\mathrm{W}_u \geq 72\%$) and iris (*i.e.* $\mathrm{W}_u \geq 67\%$) on the same schemes.

Additionally, it can be observed that the workload is inversely proportional to the length of the frequent pattern: W decreases as k increases, while some H-R values are compromised. A similar trend is theoretically shown in Fig. 2 (Sect.III-E). This observation is to be expected, as bins constructed from longer lengths are more discriminative and can reduce the number of candidates in a comparison step. Therefore, this type of binning design makes the indexing

TABLE III

CLOSED-SET SCENARIO OVER SINGLE-BC. THE BASELINE REPRESENTS THE UNPROTECTED SYSTEM. BOLD VALUES SHOW A TRADE-OFF BETWEEN BIOMETRIC PERFORMANCE AND COMPUTATIONAL WR. THE DESCRIPTION OF THE NOMENCLATURE NAMED IN THE COLUMNS IS DETAILED BELOW THE TABLE

BC	Approach	k	#Comb	#Comp	Std_comp	$W_u(\%)$	$W_l(\%)$	#Visited-patterns	Std_bins_v	H-R
Face	Baseline	**5**	**32**	**451.1**	**282.18**	**72.75**	**44.75**	**13.48**	**9.72**	**100.0**
		8	256	378.25	199.97	57.36	37.53	92.97	55.03	64.53
	BioHashing	**5**	**32**	**473.97**	**292.14**	**76.00**	**47.02**	**14.68**	**9.82**	**100.0**
		8	256	383.66	201.97	58.1	38.06	94.96	54.46	64.29
	IoM-GRP	**7**	**128**	**439.47**	**292.45**	**72.61**	**43.60**	**54.45**	**39.02**	**99.99**
		8	256	444.35	288.28	72.68	44.08	110.46	76.06	99.65
Fingerprint	Baseline	**6**	**64**	**228.09**	**217.60**	**44.22**	**22.63**	**12.15**	**14.12**	**99.95**
		8	256	188.73	186.33	37.21	18.72	40.29	47.8	91.68
	Biohashing	**7**	**128**	**137.03**	**169.66**	**30.43**	**13.59**	**11.58**	**17.53**	**99.99**
		8	256	117.58	155.03	27.05	11.67	17.91	29.69	98.66
	IoM-GRP	**7**	**128**	**245.4**	**196.82**	**43.87**	**24.35**	**8.12**	**13.73**	**100.0**
		8	256	164.38	169.29	33.1	16.31	14.16	26.11	98.99
Iris	Baseline	**5**	**32**	**402.93**	**278.39**	**67.59**	**39.97**	**12.13**	**9.38**	**100.00**
		8	256	333.69	210.48	53.98	33.1	81.19	56.13	71.96
	BioHashing	**6**	**64**	**410.67**	**290.29**	**69.54**	**40.74**	**25.35**	**19.31**	**99.46**
		8	256	342.75	208.49	54.69	34.0	83.57	55.46	72.13
	IoM-GRP	**7**	**128**	**395.23**	**288.21**	**67.80**	**39.21**	**47.88**	**38.1**	**100.0**
		8	256	390.27	289.37	67.42	38.72	95.7	76.1	98.60

k: Length of the frequent binary pattern, #Comb: Number of possible combinations to be generated given a k, #Comp: Average number of comparisons, Std_comp: Standard deviation across the number of comparisons carried out per subject, W_l: Lower bound of the computational workload reduction estimated on the average number of comparisons computed per subject, W_u: Upper bound of the computational workload reduction, #Visited-patterns: Average number of binary patterns visited from the probe, Std_bins_v: Standard deviation across the bins visited per subject, H-R: Hit-Rate.

TABLE IV

OPEN-SET RESULTS OVER SINGLE-BC

BC	Approach	k	#Bins	W(%)	FPIR=0.01(%)	FPIR=0.1(%)
Face (exhaustive)	Baseline	-	-	100.00	21.07	17.85
	Biohashing	-	-	100.00	33.91	21.42
	IoM-GRP	-	-	100.00	15.44	14.09
Face (indexing)	Baseline	5	23	69.99	35.00	34.00
	Biohashing	5	25	75.52	36.21	33.15
	IoM-GRP	7	93	71.22	37.61	32.10
Fingerprint (exhaustive)	Baseline	-	-	100.00	20.06	15.79
	BioHashing	-	-	100.00	44.43	36.80
	IoM-GRP	-	-	100.00	16.92	13.47
Fingerprint (indexing)	Baseline	6	26	43.30	28.76	24.86
	BioHashing	7	29	32.23	39.57	31.21
	IoM-GRP	7	22	35.86	22.47	19.85
Iris (exhaustive)	Baseline	-	-	100.00	44.86	37.80
	BioHashing	-	-	100.00	44.60	32.52
	IoM-GRP	-	-	100.00	36.75	32.69
Iris (indexing)	Baseline	5	22	67.06	70.59	49.70
	BioHashing	6	45	69.04	74.42	49.42
	IoM-GRP	7	86	66.63	53.77	47.03

scheme highly dependent on the intra-class and inter-class variance of each BC.

Focusing on the open-set results in Tab. IV, at a fixed number of bins (see column #Bins in Tab. IV), it can be observed that indexing schemes for individual BCs do not achieve similar biometric performances with respect to their corresponding exhaustive searches. However, their WR values are remarkable with respect to the baseline workload. Also, the proposed multi-biometric indexing scheme is expected to outperform the biometric performance of the retrieved individual BCs, while maintaining the overall workload of the system.

TABLE V

CLOSED SCENARIO RESULTS OF THE PROPOSED MULTI-BIOMETRIC INDEXING SCHEMES ON BIO-HASHING FOR THE BEST PARAMETER K

Method	Combination	k	$W_u(\%)$	$W_l(\%)$	H-R
Feature-concatenation	Face-Fingerprint	6	57.63	31.79	100.00
	Iris-Fingerprint	6	52.04	27.63	100.00
	Face-Iris	6	71.35	43.04	100.00
	Face-Fingerprint-Iris	6	61.53	34.68	100.00
Ranked-codes	Face-Fingerprint	6	55.60	31.03	99.72
	Iris-Fingerprint	6	51.91	28.50	99.73
	Face-Iris	6	71.80	43.44	99.28
	Face-Fingerprint-Iris	6	60.78	34.70	99.43
XOR-codes	Face-Fingerprint	5	78.00	49.97	100.00
	Iris-Fingerprint	5	78.55	48.64	100.00
	Face-Iris	7	78.19	49.30	100.00
	Face-Fingerprint-Iris	7	78.77	51.18	100.00

B. Multi-Biometric Characteristics

While Sect. V-A validated the concept of *frequent binary patterns* as a solution agnostic w.r.t. types of BCs (*i.e.* face, iris, and fingerprint) and cancelable biometric template protection schemes (with binary representation), this section shows the evaluation of different fusion strategies presented in Sect. III. Note that the proposed schemes allow the retrieval of protected multi-biometric templates in a single biometric transaction. Initially, the multi-biometric indexing results in a closed-set scenario are depicted in Tab. V for the best k-combinations across the proposed indexing approaches for the BioHashing scheme. Similar to single-BC (Sect. V-A), the closed-set scenario evaluation allows estimating a threshold in terms of bins visited (see column #Bins in Tab. VI) which can

then be set in further open-set scenario evaluations. Since the order of the combinations between the BCs does not affect the final workload of the system in the closed-set scenario, a single combination for two and three BCs is shown.

As observed in Tab. V, the computational workload required by the proposed multi-biometric techniques increases slightly or greatly depending on the type of strategy and the level at which the data are merged. The proposed multi-biometric approaches based on the highest-ranked code and feature-concatenation indexing improve the overall workload of some independent BCs, while slightly increasing the individual workload of others. More specifically, this trend is generally observed when designing combinations of types of BCs centred on the fingerprint. In other words, the Face-Fingerprint combination results in an approximate average of W_I=∼31%, which represents 16 percentage points lower than the workload of the face as a single BC (*i.e.* W_I=∼47% in Tab. III) and approximately 18 percentage points more than the workload yielded individually by the fingerprint (*i.e.* W_I=∼13% in Tab. III). Similar trends can be also observed for the combinations with Iris, *e.g.* Face-Fingerprint and Face-Iris. The above observations have also been modelled theoretically in Fig. 3 and Sect. III-E. We believe that these gaps or imbalances in terms of overall workloads across the BC combinations are due to the fact that single-BCs (*e.g.* face or fingerprint) may exhibit different biometric variances (intra- and inter-class). Note that some variations are nearly inevitable and specific for some BCs, *e.g.* for fingerprint, environmental conditions during the sample acquisition process and for iris, distance, and angle from the sensor.

Subsequently, the evaluation of the open-set scenario is shown in Tab. VI across the proposed multi-biometric indexing approaches for BioHashing. For convenience, the evaluation of each of the individual BCs indexing systems is also presented. In these experiments, all possible combinations of types of BCs and orderings are analysed.

Note that, on the one hand, the overall computational workload (*i.e.* , W) of the different multi-biometric approaches proposed is not affected by the order of the BCs involved in the combination, *e.g.* Face-Iris or Iris-Face. On the other hand, W generally depends on the type of BCs used in the combination process, similar to what was observed for the closed-set scenario, *e.g.* Face-Iris results in a higher W than the Fingerprint-Iris. Furthermore, the presented multi-biometric schemes outperform single-BC indexing pipelines in terms of biometric performance, while producing an approximate average W of the individual BCs. Note the imbalances in terms of W between multi-biometric and single-BC systems. In particular, and depending on the multi-biometric strategy, the FNIR produced by the single-BC approaches is reduced down to 19.81% for high-security thresholds (*i.e.* FPIR = 0.01%). With regard to the above results, we also observe that the best trade-off between W and biometric performance is achieved by combining three BCs, *e.g.* the ranked-codes approach results in an FNIR = 21.55% at an FPIR = 0.01%, which is approximately up to 53 percentage points less than the FNIR yielded *e.g.* for Iris at the same operating point (FNIR = 74.42%). These performance trends are confirmed in Fig. 5: The blue DET curves, representing the multi-biometric scheme merging three BCs, significantly outperform the remaining curves associated with the individual BCs for higher security thresholds.

TABLE VI
OPEN-SET RESULTS OVER BIOHASHING ACROSS DIFFERENT INDEXING-SCHEMES

	BC	k	#Bins	W(%)	FPIR=0.01(%)	FPIR=0.1(%)
Single	Face(indexing)	5	25	75.52	36.21	33.15
	Fingerprint(indexing)	7	29	32.23	39.57	31.21
	Iris(indexing)	6	45	69.04	74.42	49.42
Feature-concatenation	Face-Fingerprint	6	32	53.98	23.60	21.78
	Fingerprint-Face	6	32	53.91	25.46	23.17
	Iris-Fingerprint	6	31	53.07	32.20	24.69
	Fingerprint-Iris	6	31	53.11	29.92	26.81
	Face-Iris	6	46	70.22	27.73	24.56
	Iris-Face	6	46	70.27	26.82	23.70
	Face-Fingerprint-Iris	6	38	61.61	19.81	19.36
	Face-Iris-Fingerprint	6	38	61.63	20.02	19.32
	Fingerprint-Face-Iris	6	38	61.63	20.47	18.38
	Fingerprint-Iris-Face	6	38	61.63	20.56	19.00
	Iris-Face-Fingerprint	6	38	61.59	22.57	18.84
	Iris-Fingerprint-Face	6	38	61.59	19.98	18.38
Ranked-codes	Face-Fingerprint	6	32	56.02	20.37	19.73
	Fingerprint-Face	6	32	56.02	20.37	19.73
	Iris-Fingerprint	6	30	53.40	32.14	25.36
	Fingerprint-Iris	6	30	53.40	32.14	25.36
	Face-Iris	6	46	72.92	26.16	23.49
	Iris-Face	6	46	72.92	26.16	23.49
	Face-Fingerprint-Iris	6	33	57.40	21.55	20.81
	Face-Iris-Fingerprint	6	33	57.40	21.55	20.81
	Fingerprint-Face-Iris	6	33	57.40	21.55	20.81
	Fingerprint-Iris-Face	6	33	57.40	21.55	20.81
	Iris-Face-Fingerprint	6	33	57.40	21.55	20.81
	Iris-Fingerprint-Face	6	33	57.40	21.55	20.81
XOR-codes	Face-Fingerprint	5	25	78.05	28.11	24.53
	Fingerprint-Face	5	25	78.05	28.11	24.53
	Iris-Fingerprint	5	25	78.03	35.25	29.36
	Fingerprint-Iris	5	25	78.03	35.25	29.36
	Face-Iris	7	100	78.13	28.93	26.67
	Iris-Face	7	100	78.13	28.93	26.67
	Face-Fingerprint-Iris	7	63	81.55	26.24	22.38
	Face-Iris-Fingerprint	7	63	81.55	26.24	22.38
	Fingerprint-Face-Iris	7	63	81.55	26.24	22.38
	Fingerprint-Iris-Face	7	63	81.55	26.24	22.38
	Iris-Face-Fingerprint	7	63	81.55	26.24	22.38
	Iris-Fingerprint-Face	7	63	81.55	26.24	22.38

C. Privacy Protection Analysis

As mentioned earlier, the privacy protection capabilities of the underlying cancelable biometric schemes are retained in the indexing schemes. Hence, the privacy protection in terms of unlinkability and irreversibility (see Sect. IV-E) is estimated for the BioHashing and IoM-GRP schemes for the different employed BCs under the general attack model (as suggested in [56]). Obtained results are presented in Tab. VII.

The measure used to evaluate the unlinkability of protected templates analyses the overlap between the distribution of scores of mated templates and the distribution of scores of non-mated templates protected with different keys. Therefore, if the distribution of scores of mated templates and the distribution of scores of non-mated templates largely overlap, based on the hypothesis test in this measure, it is hard to link templates. Therefore, protected templates are considered to be unlinkable and the global measure $D_{\leftrightarrow}^{sys}$ will be close to zero. Accordingly, all cancelable schemes obtain low values for $D_{\leftrightarrow}^{sys}$, *i.e.* protected templates that are hardly linkable for different BCs.

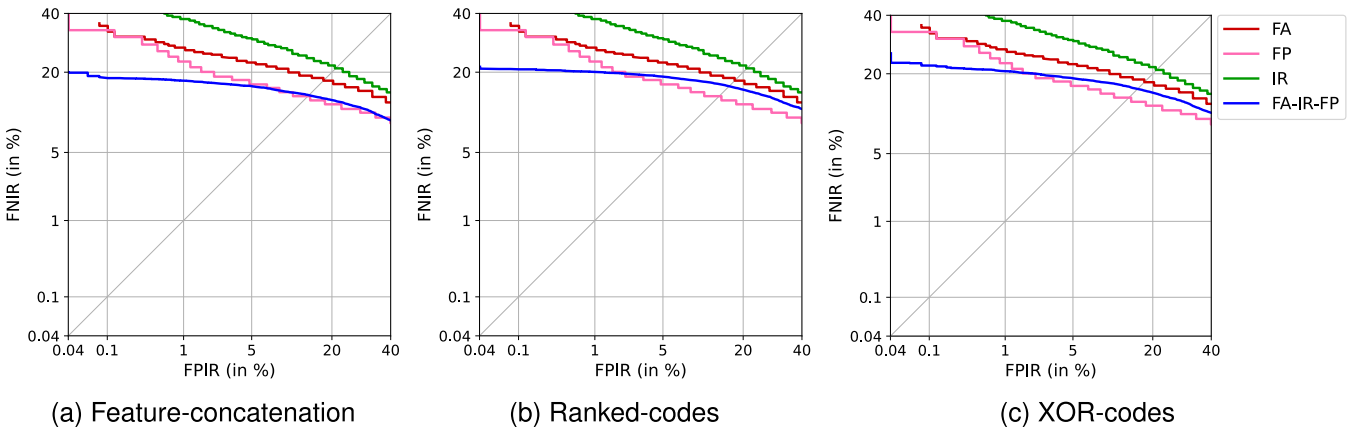

Fig. 5. Best results over open-set scenario are reported on the BioHashing for different multi-biometric approaches w.r.t. their uni-modal approaches.

TABLE VII
EVALUATION OF PRIVACY PROTECTION OF USED CANCELABLE BIOMETRIC SCHEMES

BC	Approach	Unlinkability ($D_{\leftrightarrow}^{sys}$)	Irreversibility (MI)
Face	BioHashing	0.0058	79.05
	IoM-GRP	0.0059	25.98
Fingerprint	BioHashing	0.0048	39.76
	IoM-GRP	0.0026	43.21
Iris	BioHashing	0.0014	98.26
	IoM-GRP	0.0061	36.52

The MI values obtained for the different cancelable schemes for the considered characteristics are more difficult to interpret. Obviously, there is certain mutual information between unprotected and protected templates. Nevertheless, the MI values are comparable to those achieved in other benchmarks on cancelable biometrics, *e.g.* in [68]. Therefore, it can be concluded that reconstructing the original template from the protected ones is not feasible.

VI. CONCLUSION

A multi-biometric indexing scheme for binning and retrieving protected biometric templates is proposed. We show that the proposed approach is agnostic across BCs and cancelable biometric schemes. Focusing on unprotected biometric systems, some published works have reported results in terms of WR that go beyond the approach presented [7]. Nevertheless, most of these systems are custom-built for specific biometric systems and are not expected to be applicable to other systems. In contrast to these schemes, the proposed system can be used to merge different BCs, such as face, fingerprint and iris, while protecting the privacy of the subjects. Experimental evaluations compliant with international standards showed that a protected multi-biometric identification system can reduce the computational workload to approximately 57% (indexing up to three types of BCs) and 53% (indexing up to two types of BCs). This can be achieved while simultaneously improving the biometric performance at the high-security thresholds of a baseline biometric system.

REFERENCES

[1] L. Pascu. *Global Biometrics Market to Surpass $45b by 2024, Reports Frost & Sullivan*. Accessed: Mar. 2020. [Online]. Available: https://www.biometricupdate.com/202003/global-biometrics-market-to-surpass-45b-by-2024-reports-frost-sullivan

[2] B. Beranek. *How Banks and Retailers Fight a Rising Tide of Fraud With Multimodal Biometrics*. Accessed: Jan. 25, 2023. [Online]. Available: https://www.biometricupdate.com/202301/how-banks-and-retailers-fight-a-rising-tide-of-fraud-with-multimodal-biometrics

[3] C. Burt. *Combined Iris and Face Biometrics Solution Launched by Thales for Efficient Border Checks*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.biometricupdate.com/202212/combined-iris-and-face-biometrics-solution-launched-by-thales-for-efficient-border-checks

[4] *Information Technology-Vocabulary—Part 37: Biometrics*, Standard ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 2382-37:2022, International Organization for Standardization, 2022.

[5] Unique Identification Authority of India. *Aadhaar Dashboard*. Accessed: 2018. [Online]. Available: https://www.uidai.gov.in/aadhaar_dashboard/

[6] J. Nash. *Clear Must Re-Enroll 48k Members After it's Found They Weren't Biometrically Checked*. Accessed: Jan. 11, 2023. [Online]. Available: https://www.biometricupdate.com/202301/clear-must-re-enroll-48k-members-after-its-found-they-werent-biometrically-checked

[7] P. Drozdowski, C. Rathgeb, and C. Busch, "Computational workload in biometric identification systems: An overview," *IET Biometrics*, vol. 8, no. 6, pp. 351–368, Nov. 2019.

[8] *Regulation of the European Parliament and of the Council on the Protection Of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, European Council, Brussels, Belgium, Apr. 2016.

[9] 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.

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

[11] V. Krivokuca Hahn and S. Marcel, "Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 639–666, 2022.

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

[13] A. Juels and M. Sudan, "A fuzzy vault scheme," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 237–257, Feb. 2006.

[14] X. Dong, S. Kim, Z. Jin, J. Y. Hwang, S. Cho, and A. B. J. Teoh, "Open-set face identification with index-of-max hashing by learning," *Pattern Recognit.*, vol. 103, Jul. 2020, Art. no. 107277.

[15] C. Rathgeb and C. Busch, "Multibiometric template protection: Issues and challenges," in *New Trends and Developments in Biometrics*. Rijeka, Croatia: InTechOpen, 2012, pp. 173–190.

[16] D. Osorio-Roig, C. Rathgeb, H. O. Shahreza, C. Busch, and S. Marcel, "Indexing protected deep face templates by frequent binary patterns," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2022, pp. 1–8.

[17] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[18] 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.

[19] P. Drozdowski, C. Rathgeb, B.-A. Mokroß, and C. Busch, "Multi-biometric identification with cascading database filtering," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 2, no. 3, pp. 210–222, Jul. 2020.

[20] A. Ross, K. Nandakumar, and A. Jain, *Handbook of Multibiometrics*, vol. 6. Springer, 2006. [Online]. Available: https://cased-dms.fbi.h-da.de/literature/RossNandakumarJain-HandbookOfMultibiometrics-2006.pdf

[21] *Multimodal and Other Multibiometric Fusion*, Standard ISO/IEC JTC1 SC37 Biometrics, ISO/IEC TR 24722, Intl. Organization for Standardisation, 2015.

[22] J. Merkle, T. Kevenaar, and U. Korte, "Multi-modal and multi-instance fusion for biometric cryptosystems," in *Proc. BIOSIG Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2012, pp. 1–6.

[23] P. P. Paul, M. L. Gavrilova, and R. Alhajj, "Decision fusion for multimodal biometrics using social network analysis," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 44, no. 11, pp. 1522–1533, Nov. 2014.

[24] L. M. Dinca and G. P. Hancke, "The fall of one, the rise of many: A survey on multi-biometric fusion methods," *IEEE Access*, vol. 5, pp. 6247–6289, 2017.

[25] M. Singh, R. Singh, and A. Ross, "A comprehensive overview of biometric fusion," *Inf. Fusion*, vol. 52, pp. 187–205, Dec. 2019.

[26] J. Daugman, "Biometric decision landscapes," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Tech. Rep. TR482, 2000.

[27] I. Kavati, M. V. N. K. Prasad, and C. Bhagvati, "Search space reduction in biometric databases: A review," in *Computer Vision: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2018, pp. 1600–1626.

[28] P. Drozdowski, F. Struck, C. Rathgeb, and C. Busch, "Benchmarking binarisation schemes for deep face templates," in *Proc. 25th IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2018, pp. 191–195.

[29] Y. Wang, J. Wan, J. Guo, Y.-M. Cheung, and P. C. Yuen, "Inference-based similarity search in randomized Montgomery domains for privacy-preserving biometric identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 7, pp. 1611–1624, Jul. 2018.

[30] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio, and K. Takahashi, "Cancelable permutation-based indexing for secure and efficient biometric identification," *IEEE Access*, vol. 7, pp. 45563–45582, 2019.

[31] P. Drozdowski, C. Rathgeb, and C. Busch, "Bloom filter-based search structures for indexing and retrieving iris-codes," *IET Biometrics*, vol. 7, no. 3, pp. 260–268, May 2018.

[32] S. K. Choudhary and A. K. Naik, "Protected biometric identification with multiple finger vein," in *Proc. 2nd Asian Conf. Innov. Technol. (ASIANCON)*, Aug. 2022, pp. 1–6.

[33] A. Sardar, S. Umer, C. Pero, and M. Nappi, "A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template," *IEEE Access*, vol. 8, pp. 105263–105277, 2020.

[34] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, and C. Busch, "On the application of homomorphic encryption to face identification," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2019, pp. 1–5.

[35] J. J. Engelsma, A. K. Jain, and V. N. Boddeti, "HERS: Homomorphically encrypted representation search," 2020, *arXiv:2003.12197*.

[36] D. Osorio-Roig, C. Rathgeb, P. Drozdowski, and C. Busch, "Stable hash generation for efficient privacy-preserving face identification," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 4, no. 3, pp. 333–348, Jul. 2021.

[37] P. Drozdowski, F. Stockhardt, C. Rathgeb, D. Osorio-Roig, and C. Busch, "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection," *IEEE Access*, vol. 9, pp. 139361–139378, 2021.

[38] J. Kolberg, P. Bauspies, M. Gomez-Barrero, C. Rathgeb, M. Durmuth, and C. Busch, "Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2019, pp. 1–6.

[39] P. Bauspieß, J. Kolberg, P. Drozdowski, C. Rathgeb, and C. Busch, "Privacy-preserving preselection for protected biometric identification using public-key encryption with keyword search," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 6972–6981, May 2023.

[40] J. J. Engelsma, K. Cao, and A. K. Jain, "Learning a fixed-length fingerprint representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 6, pp. 1981–1997, Jun. 2021.

[41] X. Dong, S. Kim, Z. Jin, J. Y. Hwang, S. Cho, and A. B. J. Teoh, "Secure chaff-less fuzzy vault for face identification systems," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 17, no. 3, pp. 1–22, Aug. 2021.

[42] *Information Technology Security Techniques—Biometric Information Protection*, Standard ISO/IEC JTC1 SC27 Security Techniques, ISO/IEC 24745:2022, Intl. Organization for Standardization, 2022.

[43] 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.

[44] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[45] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 108–117, Mar. 2013.

[46] L. Sperling, N. Ratha, A. Ross, and V. N. Boddeti, "HEFT: Homomorphically encrypted fusion of biometric templates," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2022, pp. 1–10.

[47] P. Indyk and R. Motwani, "Approximate nearest neighbors: Towards removing the curse of dimensionality," in *Proc. 30th Annu. ACM Symp. Theory Comput.*, 1998, pp. 604–613.

[48] U. Jayaraman, S. Prakash, and P. Gupta, "Indexing multimodal biometric databases using kd-tree with feature level fusion," in *Proc. Int. Conf. Inf. Syst. Secur.*, 2008, pp. 221–234.

[49] A. Gyaourova and A. Ross, "A coding scheme for indexing multimodal biometric databases," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2009, pp. 93–98.

[50] 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.

[51] M. Lim, A. B. J. Teoh, and J. Kim, "Biometric feature-type transformation: Making templates compatible for secret protection," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 77–87, Sep. 2015.

[52] Z. Cao, M. Long, J. Wang, and P. S. Yu, "HashNet: Deep learning to hash by continuation," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Oct. 2017, pp. 5609–5618.

[53] 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.

[54] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Deep hashing for secure multimodal biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1306–1321, 2021.

[55] A. Jain, B. Klare, and A. Ross, "Guidelines for best practices in biometrics research," in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 541–545.

[56] *Information Technology—Performance Testing of Biometric Template Protection Schemes*, Standard ISO/IEC JTC 1/SC 37 Biometrics, ISO/IEC 30136:2018, International Organization for Standardization and International Electrotechnical Committee, 2018.

[57] H. Al-Assam, H. Sellahewa, and S. Jassim, "Accuracy and security evaluation of multi-factor biometric authentication," *Int. J. Inf. Secur. Res.*, vol. 1, no. 1, pp. 11–19, Mar. 2011.

[58] P. Bauspieß et al., "HEBI: Homomorphically encrypted biometric indexing," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2023, pp. 1–10.

[59] *Information Technology—Biometric Performance Testing and Reporting—Part 1: Principles and Framework*, Standard ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 19795-1:2021, International Organization for Standardization, Jun. 2021.

[60] G. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," in *Proc. Workshop Faces 'Real-Life' Images, Detection, Alignment, Recognit.*, Marseille, France, 2008, pp. 1–14.

[61] J. Ortega-Garcia et al., "MCYT baseline corpus: A bimodal biometric database," *IEE Proc.-Vis., Image Signal Process.*, vol. 150, no. 6, pp. 395–401, Dec. 2003.

[62] (2004). *Chinese Academy of Sciences Institute of Automation. Casia Iris Image Database*. [Online]. Available: https://www.kaggle.com/datasets/achampetasonali/casia-iris-thousand, http://biometrics.idealtest.org

[63] J. Ortega-Garcia et al., "The multiscenario multienvironment BioSecure multimodal database (BMDB)," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 6, pp. 1097–1111, Jun. 2010.

[64] *Information Technology—Biometric Sample Quality—Part 6: Iris Image Data*, Standard ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 29794-6, Int. Organization for Standardization, 2015.

[65] T. Rohwedder, D. Osorio-Roig, C. Rathgeb, and C. Busch, "Benchmarking fixed-length fingerprint representations across different embedding sizes and sensor types," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2023, pp. 1–6.

[66] F. Boutros, O. Kaehm, M. Fang, F. Kirchbuchner, N. Damer, and A. Kuijper, "Low-resolution iris recognition via knowledge transfer," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2022, pp. 1–5.

[67] N. Othman, B. Dorizzi, and S. Garcia-Salicetti, "OSIRIS: An open source iris recognition software," *Pattern Recognit. Lett.*, vol. 82, pp. 124–131, Oct. 2016.

[68] H. O. Shahreza et al., "Benchmarking of cancelable biometrics for deep templates," *CoRR*, vol. abs/2302.13286, 2023, doi: 10.48550/ARXIV.2302.13286.

Dailé Osorio-Roig received the B.Sc. degree in computer science from the Technological University of Havana, in 2014. She is currently pursuing the Ph.D. degree with the Faculty of Computer Science, Hochschule Darmstadt (HDA), Germany. She joined the Advanced Technologies Application Center (CENATAV), Havana, Cuba, for computer science graduate training. She is also a member of the da/sec–Biometrics and Internet Security Research Group, National Research Center for Applied Cybersecurity (ATHENE), Germany. Her principal research interests are focused in the areas of pattern recognition, biometrics, and machine learning, specifically biometric indexing and privacy-enhancing technologies.

Lázaro Janier González-Soler received the B.Sc. degree in mathematics and computer science from the University of Havana in 2014 and the Ph.D. degree in applied computer science from Hochschule Darmstadt, Germany, in 2022. He is a Post-Doctoral Researcher with the da/sec Group, National Research Center for Applied Cybersecurity (ATHENE), Hochschule Darmstadt. He has been actively involved in national and European projects, such as Bio4ensics and Secure and Privacy-Friendly Mobile Authentication (RESPECT). His principal research interests are focused on improving the security of biometric systems through the development of biometric presentation attack detection (PAD) techniques. Further, his research interests are related to the development of algorithms for biometric recognition in forensic scenarios. He has been also granted several awards, such as the Best Ph.D. Thesis Award in Computer Science of German Universities of Applied Sciences, the Best Paper Award at the International Workshop on Information Forensics and Security (WIFS) 2021, and the Best-Performing Algorithm in the LivDet 2019 and 2021. He has served as a reviewer for different JRC journals and conferences.

Christian Rathgeb is currently a Professor with the Faculty of Computer Science, Hochschule Darmstadt (HDA), Germany. He is also a Principal Investigator with the National Research Center for Applied Cybersecurity (ATHENE). He has coauthored over 100 technical papers in the field of biometrics. His research interests include pattern recognition, iris and face recognition, security aspects of biometric systems, secure process design, and privacy enhancing technologies for biometric systems. He is a member of the European Association for Biometrics (EAB). He has served for various program committees and conferences, such as ICB, IJCB, BIOSIG, and IWBF. He is the Program Chair of the International Conference of the Biometrics Special Interest Group (BIOSIG) and an Associate Editor of *IET Biometrics* (IET BMT) and *Pattern Recognition* (Elsevier).

Christoph Busch (Senior Member, IEEE) is a member of the Norwegian University of Science and Technology (NTNU), Norway. He holds a joint appointment with Hochschule Darmstadt (HDA), Germany. Further, he has been lecturing biometric systems with Denmark's DTU, since 2007. On behalf of the German BSI, he has been the Coordinator of the project series BioIS, BioFace, BioFinger, BioKeyS Pilot-DB, KBEinweg, and NFIQ2.0. He was/is a partner of the EU Projects 3D-Face, FIDELITY, TURBINE, SOTAMD, RESPECT, TReSPsS, iMARS, and others. He is also a Principal Investigator with the German National Research Center for Applied Cybersecurity (ATHENE) and is a co-founder of the European Association for Biometrics (EAB). He has coauthored more than 500 technical papers and has been a speaker at international conferences. Furthermore, he chairs the TeleTrusT Biometrics Working Group and the German Standardization body on Biometrics and a Convenor of WG3 in ISO/IEC JTC1 SC37. He is a member of the Editorial Board of the *IET Biometrics* and formerly of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.