Indexing Protected Deep Face Templates by Frequent Binary Patterns

Dailé Osorio-Roig[1], Christian Rathgeb[1], Hatef Otroshi Shahreza[2,3],
Christoph Busch[1,4], and Sébastien Marcel[2,5]

[1]Hochschule Darmstadt, Germany
[2]Idiap Research Institute, Switzerland
[3]École Polytechnique Fédérale de Lausanne (EPFL), Switzerland
[4]Norwegian University of Science and Technology (NTNU), Norway
[5]Université de Lausanne (UNIL), Switzerland

Abstract

In this work, we present a simple biometric indexing scheme which is binning and retrieving cancelable deep face templates based on frequent binary patterns. The simplicity of the proposed approach makes it applicable to unprotected as well as protected, i.e. cancelable, deep face templates. As such, this approach represents to the best of the authors' knowledge the first generic indexing scheme that can be applied to arbitrary cancelable face templates (of binary representation).

In experiments, deep face templates are obtained from the Labelled Faces in the Wild (LFW) dataset using the ArcFace face recognition system for feature extraction. Protected templates are then generated by employing different cancelable biometric schemes, i.e. BioHashing and two variants of Index-of-Maximum Hashing. The proposed indexing scheme is evaluated on closed- and open-set identification scenarios. It is shown to maintain the recognition accuracy of the baseline system while reducing the penetration rate and hence the workload of identifications to approximately 40%.

1. Introduction

Face recognition technologies are deployed in many personal, commercial, and governmental identity management systems around the world, *e.g*. border control, national ID systems. The rapid growth in the number of subjects enrolled in these systems can lead to high monetary costs, *e.g*. investments in hardware. In a response to this, biometric *workload reduction* (WR) methods [4], *a.k.a*. biometric indexing schemes, have been introduced as algorithmic methods with the goal of processing of large amounts of biometric data with reasonable transaction times.

Current state-of-the-art, face recognition technologies employ deep learning and large training databases to embed face images as discriminative representations in the latent space [9]. At the same time, deep learning-based techniques allow developing reconstruction techniques that have shown impressive results for reconstructing facial images from their corresponding embeddings [15, 21]. Also, privacy regulations, *e.g*. the European Union (EU) General Data Protection Regulation 2016/679 (GDPR) [7], usually define biometric information as sensitive data. That is, in the context of a biometric system, an unprotected storage of biometric references could lead to different privacy threats such as identity theft, linking across databases, or limited renewability [8].

As a consequence of the aforementioned privacy issues, *biometric template protection* (BTP) schemes have been proposed for various biometric characteristics, including the face. Biometric template protection methods are commonly categorised as *cancelable biometrics* and *biometric cryptosystems*. It is worth noting that only a few approaches have combined computational WR strategies with BTP for biometric identification systems. Complex comparison strategies in these schemes have limited their applicability in identification systems where typically an exhaustive search (*i.e*. one-to-many comparison) of a biometric probe is carried out against all stored biometric references in order to find and return the biometric reference identifier(s) attributable to a single individual. Here, the workload is dominated by comparison costs.

In the context of face biometrics, researches have mainly focused on cancelable biometrics for biometric identification systems, *e.g*. [19, 1, 16]. However, the computational costs in these schemes, which apply a typical exhaustive search-based identification, tend to grow linearly with the number of enrolled subjects. In addition, most of the cancelable schemes introduce the randomness to fulfill BTP requirements defined by the ISO/IEC 24745 standard [12]

Table 1: Overview of most relevant published approaches combining BTP schemes and WR schemes in face-based identification systems (results are reported for best configurations and scenarios).

Approach	WR category	BTP category	Dataset	Biometric performance	Exhaustive search
Wang *et al.* [24]	Pre-selection, Feature transformation	Non-traditional BTP	FERET LFW	89% H-R 95% H-R	Yes
Murakami *et al.* [16]	Feature transformation	Cancelable biometrics	NIST BSSR1 SET3	0.1% FRR, 0.022% FAR	Yes
Dong *et al.* [1]	Feature transformation	Cancelable biometrics	LFW (closed-set) LFW (open-set) VGG2 (closed-set) VGG2 (open-set) IJB-C (closed-set) IJB-C (open-set)	99.75% R-1 97.99% DIR, 1% FAR 99.03% R-1 96.03% DIR, 1% FAR 80.57% R-1 56.80% DIR, 1% FAR	Yes
Sardar *et al.* [19]	Feature transformation	Cancelable biometrics	CASIA-V5 IITK CVL FERET	99.85% CRR-1 100% CRR-1 100% CRR-1 100% CRR-1	Yes
Drozdowski *et al.* [3]	Feature transformation	Homomorphic encryption	FERET	$\sim$5% FNIR, 1% FPIR	Yes
Engelsma *et al.* [6]	Feature transformation	Homomorphic encryption	MegaFace	81.4% R-1	Yes
Osorio-Roig *et al.* [17]	Pre-selection	Homomorphic encryption	FEI FERET LFW	0.0% FPIR, 0.0% FNIR 0.0% FPIR, 0.2% FNIR 1.0% FPIR, 2.5% FNIR	No
Drozdowski *et al.* [5]	Pre-selection	Homomorphic encryption	MORPH	0.42% FPIR, 0.1% FNIR	No
Dong *et al.* [2]	Feature transformation	Fuzzy vault	LFW VGG2 IJB-C	99.86% R-1 99.77% R-1 81.36% R-1	Yes
Ours	Pre-selection	Cancelable biometrics	LFW(Closed-set) LFW(Open-set)	$\sim$99.00% H-R $\sim$19% FNIR100	No

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

(*i.e.* renewability, unlinkability, irreversibility) yielding binary representations-based features. Therefore, based on this fact, authors are inspired to explore whether the most frequent binary patterns over cancelable templates could be most stable and sufficient for indexing.

The main contribution of this paper is (to the best of the authors' knowledge) the first proposal of search space-reducing WR scheme for deep face templates protected by well-known cancelable biometric schemes. To this end, we introduce a new approach based on the search of frequent binary patterns for indexing and retrieval of protected binary templates obtained through different cancelable schemes. Experimental results showcase that the proposed scheme is agnostic w.r.t. the applied cancelable schemes. Evaluations are conducted for a challenging identification scenario, *i.e.* open-set scenario on a database exhibiting a high intra-class variability (LFW). It is shown that the proposed system reduces the number of required comparisons per identification transaction w.r.t. the baseline (exhaustive search).

This paper is organised as follows: section 2 briefly introduces the related work. In section 3, the proposed system is described in detail. Section 4 presents the experimental setup and the achieved results, while a summary and concluding remarks are given in section 5.

2. Related work

This section provides a brief overview of the WR schemes applied to protected deep face templates. For a summary of state-of-the-art techniques for WR the reader is referred to [4]. According to Drozdowski *et al.* [4], WR methods can be categorised as: pre-selection, focusing on the reduction of the number of necessary template comparisons, *i.e.* reduction of the search space, and feature transformation (*e.g.* binarisation methods) approaches, concentrating on decreasing the computational cost at the individual template comparison level. It should be noted that the former are of interest in the context of this article.

Table 1 compares the most relevant related works in face identification for indexing protected templates. As it can be noted, WR schemes that employ homomorphic encryption have recently been employed in face identification in order to show its applicability, *e.g.* [5]. However, these approaches require specific optimizations for WR according to their encoding schemes (*e.g.* [6]). In other words, encoding schemes are limited to the feature representation, *e.g.* float-, binary-, integer-values. In this context, each optimisation (*e.g.* dimensionality reduction) can lead to different number of operations or computational costs depending on the encoding scheme. As done *e.g.* in [6], a packing

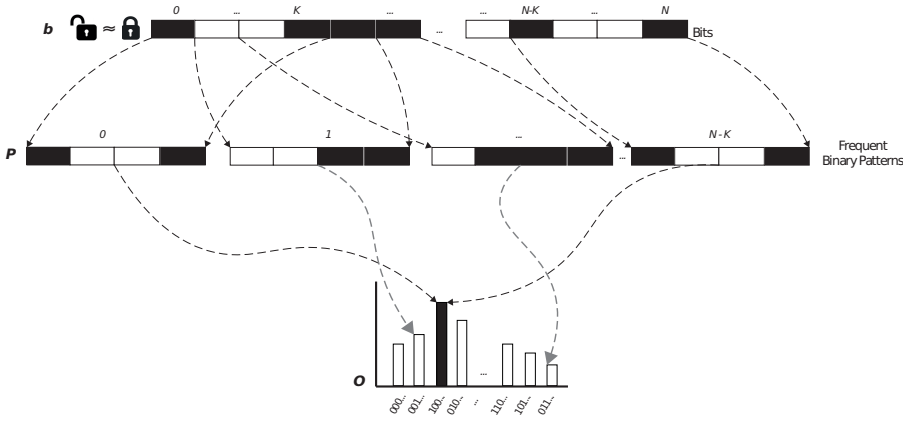


Figure 1: Frequent binary pattern extraction: a set $\mathbf{P}$ of binary patterns are extracted from N bits; subsequently, frequent patterns are defined according to their corresponding number of occurrences in N.

technique is applied on polynomial optimizations as Fan-Vercauteren schemes are represented as a polynomial ring.

Therefore, cancelable BTP schemes seem to be more suitable in an identification scenario. This is because cancelable BTP schemes usually allow retaining efficient biometric comparators of the corresponding unprotected systems [18], in contrast to biometric cryptosystems (*e.g.* [2]) that enable biometric comparison by verifying the correctness of a retrieved key [23].

The current state-of-the-art of cancelable BTP schemes for face identification systems usually focuses on feature transformations that lead to compact binary representations (*e.g.* BioHashing in [19]) which allow for a rapid one-to-one comparison. Also, recently, special instances of the Locality Sensitive Hashing (LSH) [11] (*e.g.* Index-of-Maximum (IoM) Hashing in [1, 2]), have been applied on facial deep features to yield compact non-invertible features. Based on the nature of LSH, it is expected that in cancelable schemes, similar facial protected templates are more likely to have the same hash collision compared to dissimilar ones. Also, in the current state-of-the-art of biometric template protection, these IoM Hashing-based instances contribute to hashed codes with a strong concealment to the biometric information which are insensitive to the features magnitude [14]. These representations are more robust against intra-class variation of biometric features.

In summary, it is important to note that until to date, all published works on cancelable BTP schemes for face identification employ an exhaustive search.

3. Proposed system

The proposed approach can be applied on any cancelable BTP scheme where the protected template is represented as binary vector. Also, the proposed scheme exhibits a search based on frequent binary patterns which in turn makes it possible to find them in protected and unprotected templates, respectively. The following subsections describe the main processing steps of the proposed approach as part of the indexing (enrolment) and retrieval (authentication) processes.

3.1. Frequent binary pattern extraction

Let $b \in \{0,1\}^N$ be a bit-string of size N and $K < N$ a given frequent pattern length. A set of unique binary patterns $\mathbf{P} = \{p_1, \ldots, p_M\}$, each of length K can be computed over b by sampling in a sliding window the consecutive K bits starting from positions $[0, \ldots, N-K]$ with stride 1, *i.e.* $M = N-K$. Let $\mathbf{O} = \{o_1, \ldots, o_M\}$ be the set of occurrences of each $p_i \in \mathbf{P}$. This means, for each $p_i \in \mathbf{P}$ there exists a $o_i \in \mathbf{O}$ which denotes the number of occurrences of p_i in b. Figure 1 depicts a conceptual overview of the process of frequent binary pattern extraction.

3.2. Indexing based on frequent binary patterns

In the enrolment step, cancelable face templates are extracted from deep face embeddings. Subsequently, the enrolment database (*i.e.* the set of protected biometric references) is organised as follows: let $\mathbf{B} = \{b_1, \ldots, b_T\}$ be the set of cancelable face templates of all the subjects to be enrolled. For each $b_i \in \mathbf{B}$, frequent binary patterns $\mathbf{P}$ of size K are extracted as explained in Section 3.1. The enrolment database is then binned into a set of $\mathbf{L} = \{l_1, \ldots, l_R\}$, where each l_i represents the frequent binary pattern $p_i \in \mathbf{P}$ with the maximum number of occurrence in a single protected template b_i, *i.e.* $l_i = p_i : p_i \rightarrow \text{argmax}\, \mathbf{O}$. In other words, each $b_i \in \mathbf{B}$ is assigned to the bin l_i that corresponds to its most frequent binary pattern. Therefore, as expected, different cancelable templates could yield the same frequent binary pattern and hence the same bin. Also, each bin could group more than one cancelable template. It should be noted that if a new subject (template) needs

to be enrolled, then, the bin corresponding to its most frequent binary pattern will be updated by including the new cancelable template. Otherwise, the cancelable template is assigned to its corresponding new bin generated in the enrolment databse. Note that for different frequent patterns with equal number of occurrences, the binary pattern with the minimum corresponding integer value is selected as a bin.

3.3. Retrieval by frequent binary patterns

In contrast to the indexing step, a set of frequent binary patterns are extracted from a given probe as explained in Section 3.1. Then, frequent binary patterns $\mathbf{P}$ are ordered in descending order, according to their corresponding number of occurrences $\mathbf{O}$. Subsequently, for an identification transaction, the proposed approach starts searching at the bins corresponding to the most frequent patterns of the probe. If the corresponding reference is not found, *i.e.* none of the references reaches a similarity score exceeding the defined threshold, the search will be continued at the second most frequent pattern in $\mathbf{P}$ and so on and so forth. In other words, the process of search for a probe will follow the order of the frequent binary patterns in $\mathbf{P}$ until a match is found or a pre-defined maximum number of visited bins is reached.

3.4. Computational workload reduction

The computational workload W of an identification transaction (measured in terms of the number of necessary template comparisons), can be expressed as follows:

$$W = \sum_{i=1}^{z} |l_i|, \tag{1}$$

where $|l_i|$ denotes the number of biometric references stored in bin l_i, $z \leq R$ denotes a threshold for the maximum number of bins visited, and R refers to the total number of bins which the enrolment database is organised. It should be noted that computational WR can be easily controlled by the number of bins visited z.

4. Experiments

In this section, we report on the evaluation of the computational workload reduction by indexing deep protected face templates. To that end, we analysed whether the search of frequent binary patterns on protected face templates can be used for indexing. Generic cancelable BTP schemes (*e.g.* BioHashing, IoM-GRP, IoM-URP) representing the current state-of-the-art for biometric template protection have been taken into account for this evaluation.

On the other hand, it is worth noting that WR methods proposed in the literature (Table 1) for indexing protected templates are commonly designed for specific biometric template protection schemes. Therefore, a comparison with state-of-the-art methods in these experiments is deliberately avoided as it might be misleading.

Table 2: Selected configurations to generate the hashed codes from IoM-GRP and IoM-URP, respectively.

IoM-hashing	IoM-length	q	m	p	k	#bits	Hash-length (bits)
IoM-GRP	512	16	512	-	-	4	2,048
IoM-URP	512	-	512	10	50	6	3,072

q: maximum number of gaussian random projection vectors, p: Hadamard product order, m: number of Gaussian random matrices (for IoM-GRP) and number of hashing functions (for IoM-URP) respectively, k: window size, #bits: represents the maximum count of bits that can be represented each discrete index, *i.e.* q (for IoM-GRP) and k (for IoM-URP) respectively, Hash-length: represents the final hashed code resulting from the IoM Hashing-based instances.

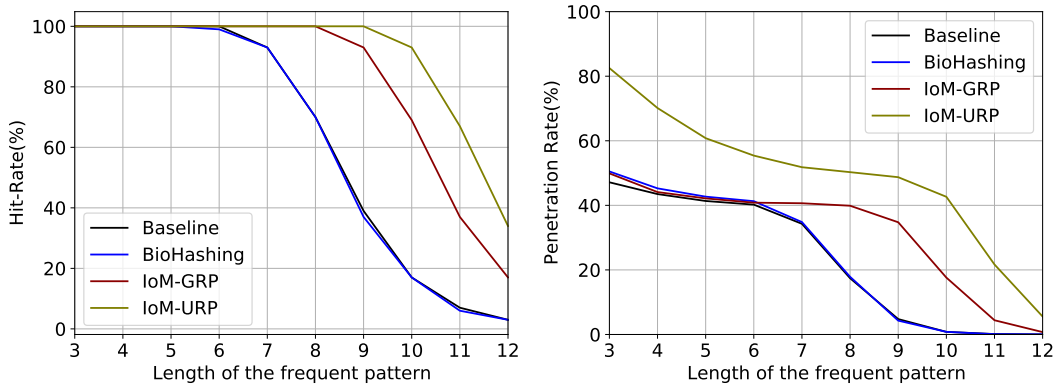
4.1. Experimental setup

A single face recognition system (ArcFace) is selected to extract face embeddings from face images. The resulting representation is a 1-dimensional feature vector containing 512 float values. Here, the pre-trained[1] model has been employed. In order to generate a binary representation suitable for the search of frequent binary patterns in the indexing scheme, 512 float-values feature vectors extracted from ArcFace are binarised by using a simple sign function with threshold 0. It should be noted that binary vectors from original face embeddings are used as a baseline (*i.e.* unprotected system) in our identification system.

Cancelable biometric template protection schemes used in this work are employed to generate feature vectors consisting of 512 bits for BioHashing and 512 integer indexes for the different IoM Hashing variants. For the latter, we employ IoM with Uniformly Random Permutation (IoM-URP) and Gaussian Random Projection (IoM-GRP). For IoM Hashing-based techniques, each integer index value is represented by its binary representation. The number of bits representing an integer is determined by the maximum number of bits (with a power of two) that can be represented each integer value in the feature vector. This maximum number of bits is depending on the maximum number of gaussian random projection vectors, *i.e.* **q**, for IoM-GRP, and the window size, *i.e.* **k**, for IoM-URP. Table 2 shows in detail the configurations corresponding to the hashed codes generated from IoM-GRP and IoM-URP, respectively. Note that different parameters are utilised for each IoM Hashing-based instance. Overall, for BioHashing- and IoM Hashing-based vectors, configurations suitable for face recognition are selected from [20] and [22], respectively.

Identification experiments are conducted on closed-set (*i.e.* all searched subjects are enrolled in the system) and open-set (*i.e.* some searched subjects are enrolled in the system and some not) scenarios. In closed-set scenario, a

[1] https://github.com/deepinsight/insightface/wiki/Model-Zoo/resnet_v1_101.



(a) H-R – Normal scenario

(b) P-R – Normal scenario

Figure 2: Effect of the length of the frequent patterns (*i.e.* K) over closed-set evaluation for normal scenario. Baseline represents the unprotected system.

single sample per subject was randomly selected as biometric reference and a single sample from the remaining samples was randomly selected as probe sample in the search over a sub-sampling of 10 rounds. For open-set scenario, a sub-sampling over 10 rounds is applied on the set of biometric references utilised in closed-set scenario, while including subjects containing a single sample as impostor comparisons.

Experiments for closed-set scenario are evaluated in the normal scenario where each users' key is assumed to be secret. While for open-set scenario, as expected, normal and stolen-token scenarios have been evaluated. In the context of stolen-token scenario, the impostor has access to the genuine users' secret key and uses this key with the impostors' own face features. It is important to note that the baseline workload of an identification system is considered to be an exhaustive search, *i.e.* a biometric probe is compared against all references enrolled in the database.

4.1.1 Database

LFW [10] is a dataset 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. Hence, we considered 1,680 samples at enrolment for closed-set scenario and an evaluation of open-set scenario consisting of 1,680 mated comparison trials and 4,069 non-mated comparison trials transactions per round.

4.1.2 Metrics

The experimental evaluation is conducted according to the ISO/IEC 19795-1:2021 [13] standard methods and metrics:

- **Biometric performance**: for closed-set scenario, the hit-rate (H-R); for 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**: penetration rate (P-R), *i.e.* computational workload as the necessary number of comparisons per identification transaction compared to the exhaustive search baseline. It is worth noting that P-R is theoretically defined in section 3.

4.2. Results

Figure 2 and Table 3 show the effect of the length of the frequent pattern (K) in relation to the hit-rate (H-R), the average number of comparisons (#Comp), and the penetration rate (P-R) empirically computed for a set of identification transactions over closed-set scenario. It should be noted that the #Comp is totally dependent on the parameter z defined in equation 1. However, for closed-set scenario evaluation, this parameter will be named as #Visited-patterns. This parameter refers to z which is known and easy to compute in this scenario as subjects are known to have a reference in the enrolment database. In contrast to open-set scenario, where potential subjects are not enrolled in the system. Evidently, the latter needs to find empirically a threshold (*i.e.* z) in terms of the number of visited patterns/bins. Therefore, authors preferred to differentiate this parameter in terms of names on both scenarios. Therefore, #Visited-patterns and z will be employed on closed-set and open-set scenario, respectively.

Note that for the baseline workload (*i.e.* exhaustive search), the P-R is 100% for a set of identification transactions. Therefore, a protected frequent binary patterns

Table 3: Closed-set scenario evaluations over normal scenario. Results are shown with a 95% of confidence interval. Baseline represents the unprotected system for both scenarios.

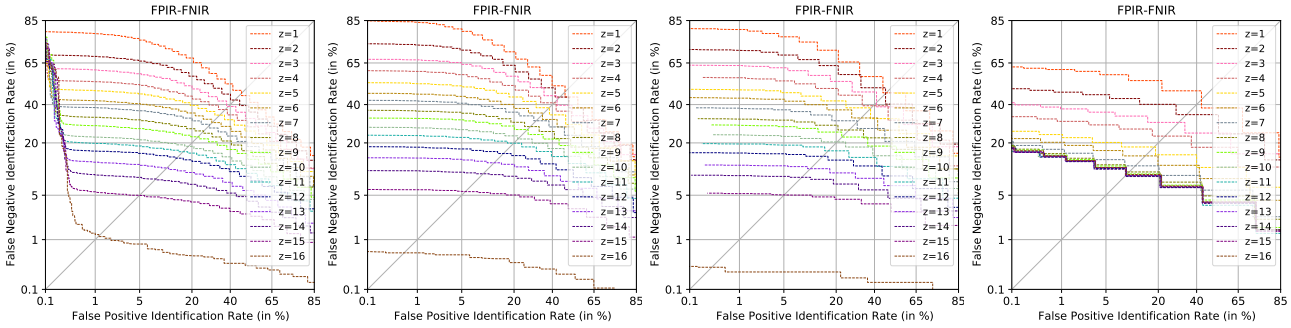
Approach	K	#Comb	#Bins-e	#Patterns-p	#Visited-patterns	H-R(%)	#Comp	P-R(%)
Baseline	3	8	8	8.00	3.38±0.05	100.00	794.73±10.99	47.31
	4	16	16	16.00	6.44±0.10	100.00	734.91±12.60	43.74
	5	32	32	32.00	12.38±0.21	99.96	695.30±8.30	41.39
	6	64	63	63.75	24.05±0.42	99.50	665.35±17.80	39.60
	7	128	126	116.11	44.03±0.75	93.43	575.05±17.26	34.23
	8	256	251	150.58	57.35±1.11	70.31	299.78±6.43	17.84
	9	512	451	132.28	48.74±1.23	39.37	82.24±2.23	4.90
	10	1024	698	89.15	29.38±1.25	17.71	14.45±1.37	0.86
	11	2048	940	51.83	16.21±1.24	7.02	2.19±0.36	0.13
BioHashing	3	8	8	8.00	3.74±0.05	100.00	848.35±10.33	50.50
	4	16	16	16.00	6.95±0.10	100.00	760.38±7.43	45.26
	5	32	32	32.00	13.10±0.20	100.00	717.23±7.86	42.69
	6	64	64	63.77	25.97±0.41	99.44	693.69±11.41	41.29
	7	128	126	116.57	46.32±0.75	93.31	584.98±5.75	34.82
	8	256	250	151.16	59.09±1.10	69.94	300.25±9.44	17.87
	9	512	442	132.15	47.37±1.26	36.96	72.11±1.96	4.29
	10	1024	690	88.80	29.48±1.26	17.32	13.53±0.51	0.81
	11	2048	953	51.65	16.24±1.40	5.64	1.62±0.39	0.10
IoM-GRP	3	8	8	8.00	3.59±0.05	100.00	838.18±6.07	49.89
	4	16	16	16.00	6.57±0.10	100.00	741.13±15.68	44.11
	5	32	32	32.00	13.03±0.21	100.00	708.07±9.89	42.15
	6	64	63	64.00	25.27±0.41	100.00	686.01±16.01	40.83
	7	128	126	128.00	50.81±0.81	100.00	682.96±4.49	40.65
	8	256	253	255.13	100.33±1.60	99.52	670.03±8.35	39.88
	9	512	464	464.69	186.91±2.98	93.46	583.97±9.07	34.76
	10	1024	749	606.46	241.55±4.42	68.80	296.00±6.66	17.62
	11	2048	991	537.52	189.30±5.00	37.24	74.08±3.52	4.41
IoM-URP	3	8	4	8.00	1.40±0.01	100.00	1386.36±5.98	82.52
	4	16	8	16.00	2.72±0.04	100.00	1178.34±15.77	70.14
	5	32	17	32.00	4.94±0.10	100.00	1021.50±6.98	60.80
	6	64	32	63.94	10.70±0.21	100.00	930.87±15.85	55.41
	7	128	59	126.95	23.79±0.48	100.00	870.48±14.04	51.81
	8	256	123	250.69	53.91±1.03	100.00	844.78±4.08	50.28
	9	512	213	472.70	121.03±2.31	99.51	818.50±8.41	48.72
	10	1024	385	751.19	221.53±57.54	92.94	716.43±11,83	42.65
	11	2048	593	874.20	192.66±32.49	66.52	364.18±11.76	21.68

K: length of the frequent binary pattern, #Comb: Number of possible combinations to be generated given a K, #Bins-e: Number total of bins in enrolment (L), #Patterns-p: Average number of binary patterns generated from the probe, #Visited-patterns: Average number of binary patterns visited from the probe, #Comp: Average number of comparisons, P-R: Average penetration rate.

search-based face identification system should yield an average workload, *i.e*. P-R, of less than 100%.

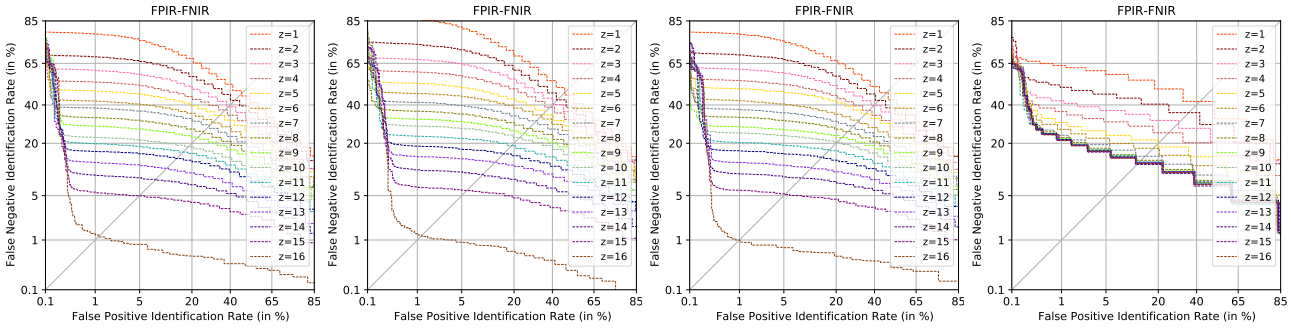
From the Figure 2, we can perceive that the curves can be maintained at almost 100% H-R up to a certain length of the frequent pattern depending on the BTP scheme: *e.g*. BioHashing, IoM-GRP, and IoM-URP for lengths down to 7, 9, and 10 bits, respectively. Also, in Figure 2 (b), a penetration rate can be reduced to approximately half (*i.e*. P-R $< 52\%$) of the baseline workload, while maintaining a high hit-rate (*i.e*. H-R $\simeq 100\%$). However, it should be noted that IoM-URP achieves this penetration rate for longer lengths (*e.g*. $K \geq 7$ bits). In other words, these trends mean that a reduced number of collisions in protected biometric references can be retained if the frequent pattern is longer up to a certain point. The lowest computational workloads (*e.g*. P-R $< 36\%$) are achieved by a drop in the H-R (H-R = 100% down to $\sim 93\%$), while fixing a length of the frequent pattern. The worst results can be observed for IoM-URP obtaining a P-R $< 43\%$ for a H-R = $\sim 92\%$. Current state-of-the-art BTP schemes (*e.g*. [22]) have also reported limited performance for IoM-URP. Overall, it should be noted that the search of frequent binary patterns over protected templates for different BTP schemes exhibits a trade-off between H-R and the workload reduction w.r.t. baseline (unprotected system), *i.e*. P-R.

From the Table 3 it can be noted that the number of comparisons (#Comp) varies according to the set of frequent binary patterns generated from the probe (#Patterns-p). In particular, the number of binary patterns visited from the probe (#Visited-patterns) leading to the most frequent binary patterns suitable for indexing, are computed empirically in order to find the earliest match, and hence the lowest workload. Thus, this confirms that this parameter can be employed as a fixed threshold (*i.e*. z) that controls the computational WR (as shown on the equation 1), specifically, for open-set scenarios.



(a) Unprotected baseline (b) BioHashing (c) IoM-GRP (d) IoM-URP

Figure 3: Open-set evaluation over normal scenario.



(a) Unprotected baseline (b) BioHashing (c) IoM-GRP (d) IoM-URP

Figure 4: Open-set evaluation over stolen-token scenario.

Table 4: Summary of the best results over open-set evaluation for normal and stolen-token scenarios, respectively.

BTP approach	**Normal-scenario**			**Stolen-token-scenario**		
	FNIR@FPIR=1.0%	**z**	**P-R(%)**	**FNIR@FPIR=1.0%**	**z**	**P-R(%)**
Unprotected baseline	19.76	11	66.08	19.76	11	66.08
BioHashing	23.30	11	66.27	23.14	11	66.44
IoM-GRP	19.57	11	66.28	20.37	11	66.61
IoM-URP	22.33	5	87.90	29.99	5	88.59

Figure 4 illustrates the effect of the parameter z over challenging open-set evaluations for stolen-token and normal scenarios, respectively. In order to avoid different results across different configurations shown in Table 3, we evaluated the indexing scheme for a fixed length of frequent pattern, *i.e.* $K = 4$, and z ranging in $[1, 16]$. From Figure 4, we can observe that the biometric performance improves as the maximum number of visited bins corresponding to the most frequent binary patterns from the probe (z) increases. Here, slight performance variations are perceived between the protected system (for different BTP schemes) w.r.t. the unprotected system (*i.e.* Unprotected baseline). The best results are shown in Table 4: for a FNIR@FPIR=1.0%, the system achieves a rejection rate for genuine identification transactions of less than 24%, while reducing to approximately 66% of the workload over open-set scenarios.

5. Conclusion

We presented an indexing scheme for binning and retrieving (protected) deep face templates. We demonstrated the generalisability of the proposed approach by applying it to different cancelable biometric schemes as well as to an unprotected baseline system. Focusing on unprotected biometric systems, some published works have reported results in terms of workload reduction that outperform the presented approach, see [4]. However, these works are mostly custom-built for specific biometric systems and are not expected to be applicable within other systems. Moreover, these usually can not be applied to protected, *e.g.* cancelable, biometric templates.

Future work will be devoted to extend the proposed system to multi-biometrics where frequent binary patterns will be extracted from multiple biometric characteristics. By combining multiple frequent binary patterns, the number of databases bins and hence the overall workload in identification transactions is expected to further reduce.

Acknowledgements

This work has in part received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860813 - TReSPAsS-ETN and the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] X. Dong, S. Kim, Z. Jin, J. Hwang, S. Cho, and A. Teoh. Open-set face identification with index-of-max hashing by learning. *Pattern Recognition*, 103:107277, 2020.

[2] X. Dong, S. Kim, Y. J. Z-H. Jin, S. Cho, and A.-B.-J. Teoh. Secure chaff-less fuzzy vault for face identification systems. *ACM Trans. on Multimidia Computing Communications and Applications*, 17(3):1–22, 2021.

[3] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, and C. Busch. On the application of homomorphic encryption to face identification. In *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*, pages 1–8, September 2019.

[4] P. Drozdowski, C. Rathgeb, and C. Busch. Computational workload in biometric identification systems: An overview. *IET Biometrics*, 8(6):351–368, November 2019.

[5] 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*, 9:139361–139378, October 2021.

[6] J. Engelsma, A. Jain, and V. Boddeti. Hers: Homomorphically encrypted representation search. *arXiv preprint arXiv:2003.12197*, 2020.

[7] European Council. 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), April 2016.

[8] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Trans. on Information Forensics and Security*, 13(6):1406–1420, June 2018.

[9] G. Guo and N. Zhang. A survey on deep learning based face recognition. *Computer Vision and Image Understanding*, 189:102805, 2019.

[10] G. Huang, M. Ramesh, T. Berg, and E. Learned-Miller. Faces in the wild: a database for studying face recognition in unconstrained environments. *Technical Report*, pages 07–49, 2007.

[11] P. Indyk and R. Motwani. Approximate nearest neighbors: towards removing the curse of dimensionality. In *Proc. of the thirtieth Annual ACM Symposium on Theory of Computing*, pages 604–613, 1998.

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

[13] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19795-1:2021. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. Intl. Organization for Standardization and Intl. Electrotechnical Committee, 2021.

[14] 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. on Information Forensics and Security*, 13(2):393–407, 2017.

[15] G. Mai, K. Cao, P. C. Yuen, and A. K. Jain. On the reconstruction of face images from deep face templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 41(5):1188–1202, 2019.

[16] 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*, 7:45563–45582, 2019.

[17] D. Osorio-Roig, C. Rathgeb, P. Drozdowski, and C. Busch. Stable hash generation for efficient privacy-preserving face identification. *Trans. on Biometrics, Behavior, and Identity Science (TBIOM)*, 2021.

[18] V.-M. Patel, N.-K. Ratha, and R. Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65, 2015.

[19] 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*, 8:105263–105277, 2020.

[20] H. O. Shahreza, V. K. Hahn, and S. Marcel. On the recognition performance of biohashing on state-of-the-art face recognition models. In *2021 IEEE Intl. Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2021.

[21] H. O. Shahreza, V. K. Hahn, and S. Marcel. Face reconstruction from deep facial embeddings using a convolutional neural network. In *Proc. of the IEEE Intl. Conf. on Image Processing (ICIP)*. IEEE, 2022.

[22] H. O. Shahreza, V. K. Hahn, and S. Marcel. Mlp-hash: Protecting face templates via hashing of randomized multi-layer perceptron. *arXiv preprint arXiv:2204.11054*, 2022.

[23] U. Uludag, S. Pankanti, S. Prabhakar, and A.-K. Jain. Biometric cryptosystems: issues and challenges. *Proc. of the IEEE*, 92(6):948–960, 2004.

[24] Y. Wang, J. Wan, J. Guo, Y.-M. Cheung, and P. Yuen. Inference-based similarity search in randomized montgomery domains for privacy-preserving biometric identification. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 40(7):1611–1624, 2017.