Morton Filters for Superior Template Protection for Iris Recognition

Kiran B. Raja†‡ R. Raghavendra† Sushma Venkatesh‡ Christoph Busch‡
† The Norwegian Colour and Visual Computing Laboratory, NTNU - Gjøvik, Norway
‡ Norwegian Biometrics Laboratory, NTNU - Gjøvik, Norway

{kiranj.raja; raghavendra.ramachandra; sushma.venkatesh; christoph.busch} @ntnu.no

Abstract—In this work, we address the fundamental performance issues of template protection for iris verification. We base our work on the popular Bloom-Filter templates protection and address the key challenges like sub-optimal performance and low unlinkability. Specifically, we focus on cases where Bloom-filter templates results in non-ideal performance due to presence of large degradations within iris images. Iris recognition is challenged with number of occluding factors such as presence of eye-lashes within captured image, occlusion due to eyelids, low quality iris images due to motion blur amongst many other. All of such degrading factors result in obtaining non-reliable iris codes and thereby provide non-ideal biometric performance. These factors further directly impact the protected templates derived from the iris images when classical Bloom-filters are employed. To this end, we propose and extend our earlier ideas of Morton-filters for obtaining better and reliable templates for iris. Morton filter based template protection for iris codes is based on leveraging the intra-class and inter-class distribution by exploiting the low-rank iris codes to derive the stable bits across the iris images for a particular subject and also analyzing the discriminable bits across various subjects. Such low-rank non-noisy iris codes enables realizing the template protection in a superior way which not only can be used in constrained setting, but also can be used in relaxed iris imaging. We further extend the work to analyze the applicability to visible spectrum iris images by employing a large scale public iris image database - UBIRIS (v1 and v2), captured in a unconstrained setting. Through a set of thorough experiments, we demonstrate the applicability of proposed approach and yet the strengths and weaknesses. Yet another contribution of this work stems in assessing the security of the proposed approach where factors of Unlinkability is studied to indicate the antagonistic nature to relaxed iris imaging scenarios.

1 INTRODUCTION

With the growing need for secure access control in many domains, biometrics has been employed as an ubiquitous way to identify and verify the identity of subjects. Among the well used biometric characteristics such as face, fingerprint, iris, palmprint etc., iris recognition has been preferred way for highly secure applications. The iris patterns begins to form during the third month of gestation and the structures creating it’s striking patterns are developed by the eighth month [24], [46]. Despite the pigment accretion continuing in the postnatal years, the layers of the iris have both ectodermal and mesodermal origin, consisting of dilator and sphincter muscles, a vascularized stroma, and an anterior layer with a genetically determined density of melanin pigment granules.
in biometric systems is therefore to compare the biometric features in protected domain in the modern day systems.

Considering such a demand within biometric systems, ISO/IEC JTC1 SC27 committee [19] has standardized the need to protect the biometric features under Biometric Template Protection [32, 39, 38, 42, 13, 14]. This standard is further aligned to the newer guidelines from the European General Data Protection Regulations (EU-GDPR) [43] which demands the strict need for privacy preservation and data protection. The three fundamental requirements of template protection respecting the ISO standards and GDPR are irreversibility, unlinkability and revokability which are briefly discussed below. The concept of irreversibility is to ensure that the biometric features in the protected domain will not lead to reconstruction of biometric sample that can lead to either direct or indirect association with a subject. Number of works have underlined this need by demonstrating ability to reconstruct biometric samples when the features are not stored in protected manner for iris [10], face [20] and fingerprint [9]. Secondly, the unlinkability ensures that any subject using two different services with same biometric modality should not be identified by linking the protected features. The specific challenge of linking of biometric templates across two services compromises the integrity of biometric systems as shown in recent work [14]. Thirdly, the concept of revokability ensures the mitigation measure when the biometric systems are compromised. It is therefore required that the template protection scheme can revoke and replace the protected templates if a such a need should arise. Apart from the three regulations, it is also needed to ensure that the performance of biometric system is not degraded due to template protection mechanism itself.

Motivated by such factors, a number of works have been reported in the recent past for achieving biometric template protection for various modalities [32, 39, 38, 42, 13]. Given the focus of this work, we limit ourselves to template protection schemes for iris recognition. We first note a number of template protection schemes proposed for iris recognition considering the wide scale deployment [33, 39, 38, 42, 13] and then briefly review the existing template protection schemes for the iris recognition. Subsequently, we identify the set of unsolved challenges for template protection within iris recognition in the section below.

1.1 Related Works

A brief overview of the state-of-art template protection schemes proposed in the recent works is first reviewed in this section. As it can be noted from the Table 1, most of the works on the iris template protection are focused on the Near-Infra-Red (NIR) domain and further the data employed for validating the previously proposed template protection corresponds to constrained capture setting (a summary of state-of-art works are presented in the Appendix of this article). While noting these two factors, we also note that the accuracy of most of the proposed approaches are very high as a direct consequence of data stemming from constrained setting. In another direction, we make another observation that a number of recent works have been inspired by the recently proposed Bloom-Filter based template protection schemes [39], [38], [42], [13]. Given the wide popularity of the Bloom-Filter based template protection schemes, we identify the key limitations of the Bloom-Filter based template protection, especially in scaling up to unconstrained iris template protection where a higher false accepts and false rejects are noted. Secondly, the previously proposed approaches have limited the validation to iris images captured in NIR spectrum and no work has been reported in Visible Spectrum (VIS) iris recognition. In an effort to address such limitations, we present a new framework for template protection which not only is able to scale up to unconstrained iris images, but also across capture spectrum.

1.2 Challenges and Our Contributions

From the number of works listed above it can be noted that most of the works focus on constrained iris data captured in close proximity. The challenge for template protection in unconstrained iris images lies in the fact that there is a need to scale to wide capture spectrum. Additionally, a need should arise, to revoke and replace the protected templates if a such a need should arise. Apart from the three regulations, it is also needed to ensure that the performance of biometric system is not degraded due to template protection mechanism itself.

Motivated by such factors, a number of works have been reported in the recent past for achieving biometric template protection for various modalities [32, 39, 38, 42, 13]. Given the focus of this work, we limit ourselves to template protection schemes for iris recognition. We first note a number of template protection schemes proposed for iris recognition considering the wide scale deployment [33, 39, 38, 42, 13] and then briefly review the existing template protection schemes for the iris recognition. Subsequently, we identify the set of unsolved challenges for template protection within iris recognition in the section below.

### TABLE 1: State-of-art approaches for template protection in iris recognition

| Previous Work | Approach | Contribution | Dataset Type | Database | Accuracy |
|---------------|----------|--------------|--------------|----------|----------|
| Yang and Verbauswede [47] | Error Correcting Code (ECC) based BTP | Bose-Chaudhuri-Hochquenghem (BCH) code of a random bit-stream | Constrained NIR Iris | – | – |
| Nandakumar and Jain [11] | Fuzzy-vault scheme to derive private keys from iris patterns. | Fixed-length binary vector representation of iriscode into an unordered set representation | Constrained NIR | CASIA v1 Iris | – |
| Maiorana et al. [28] | Turbo codes with soft-decoding for iris | High performance in terms of both verification rates and security | Constrained NIR | CASIA-Iris V4 database | – |
| Zhang et al. [45] | Concatenated coding scheme and bit masking scheme | A bit masking scheme was proposed to minimize and randomize the errors | Constrained Internal | CASIA Interval | 0.52% EER |
| Rathgeb et al. [50] | Bloom-filter based biometric template protection | Alignment free template creation | Constrained NIR | CASIA-v3 Interval Iris | 1.19 % EER |
| Rathgeb and Busch [51, 52] | Adaptive Bloom filter-based transforms | The irreversible mixing transform generating alignment-free templates | Constrained NIR | ITTD Iris Dataset | 0.5% EER |
| Gomez-Barrero et al. [13] | Generic framework for generating an irreversible representation | Feature level fusion of different biometrics (face and iris) to a single protected template | Constrained NIR | ITTD Iris Database version 1.0 | 0.5% EER |
| Lai et al. [26] | Cancellable iris template with Jaccard similarity matcher | Low error rate and attack resistance | Constrained NIR | CASIA v3 iris database | 0.16% EER |
| This work [23] | Morton-Filter Template Protection | Very low error rate and high attack resistances | Constrained and Unconstrained | CASIA v4 Distance Dataset (NIR and VIS), UBIRIS v1, UBIRIS v2 (Equivalent to Unprotected domain) | 0% EER for NIR, 15 % EER on VIS |
cooperation. While the practical iris recognition systems need to operate at within a stipulated time, they often relax the constraints for the capture. Under such relaxed capture conditions, the iris recognition suffers from number of quality degrading factors such as motion blur, reflection from ambient light, reflection of eyelashes on iris and partial iris capture due to partial closure of lids [13, 14, 5, 6]. These factors are further aggravated in the iris-on-the-move systems where not just the quality is impacted, but also the details of the captured iris by itself is substantially low. As observed from the Figure 2, the capture in unconstrained settings results in quality par-below the one captured in constrained and fully-cooperative scenario. Secondly, the capture of iris images in Near-Infra-Red (NIR) results in superior iris features while the capture in visible spectrum results in iris features that are often with even lower iris pattern details.

![Iris Images](image)

Fig. 2: The degradation of iris quality from constrained capture to iris-on-move capture. (a) presents the iris captured in constrained setting as provided in IITD v1 Iris Dataset [25] and (b) presents the iris captured from on-the-move scenario as provided by UBIRIS Dataset [36]. (b) and (d) represent the corresponding segmented and normalized iris image for (a) and (c).

Such inherent challenges arising out of capture problems pose challenge in obtaining a reliable representation of iris codes subsequent to feature extraction (for instance, 2D/1D Gabor features). The direct impact of such inferior quality iris codes can be witnessed through low performance reported in many earlier works [15, 14, 5, 6]. A number of strategies have been proposed in earlier works to handle the problems of inferior quality iris codes to improve the recognition performance [15, 14, 5, 6]. The sub-optimal quality iris data can impact not only the recognition accuracy but also the subsequent operations based on iris code, specifically iris template protection. This specific aspect of degraded performance of template protection schemes with Bloom-Filter due to unconstrained iris capture and inferior quality iriscodes was noted and illustrated in our recent work [23].

With a detailed analysis of Bloom-filter based template protection for iris recognition in unconstrained setting, we established the limitations of classical Bloom-filter based template protection in scaling for unconstrained setting where the data is significantly noisy. As it can be noted from the Figure 1, the iriscodes in unconstrained iris capture from CASIA.v4 distance dataset [11] results in unreliable iriscodes that differ for the same subject across captures. This implicitly impacts the Bloom Filter based template protection where similar locations are set in the protected templates leading to high number of false accepts. High number of false accepts therefore defeats the purpose of high security in iris biometrics systems.

Driven by such problem, specifically for creation of protected templates even under noisy representation, we present a new approach employing the recently proposed Morton Filters [3]. Morton Filters introduces several key improvements to currently well employed Bloom-Filters simply by creating multiple buckets with a predetermined logic. With such an architecture, Morton Filter approach supports compressed format that permits a sparse template that can be stored compactly in memory. Further, the multi-bucket architecture of Morton Filters reduces the False Accepts and False Rejects considerably over the traditional Bloom Filters with minimal computational overhead. Motivated by the architecture facilitating such improvements over Bloom Filters [2, 3], we propose a new protected template creation mechanism using the Morton Filter approach on iriscodes.

In this version of our work, we extend the Morton Filter based iris template protection by specifically modelling inter-class and intra-class distribution of iris codes which is known to provide well separated comparison scores following statistical distribution motivated by earlier works [6, 5]. The key motivation is to explore class distribution to make the template protection roost for unconstrained iris capture which typically suffers performance degradation in general iris recognition [8, 44, 15, 44, 8, 17]. We specifically exploit the inter-class and intra-class distribution to extract robust iriscodes to the benefit of template protection such that multiple buckets can be easily composed. Such buckets facilitate optimal template creation through Morton Filter principles. To this extent, we employ low rank iriscodes that correspond to relatively non-noisy iriscodes, discriminable codes that differ from iriscodes of other subjects and a combination code using both representation of iriscodes.

Our initial assertion of such an idea was validated in our earlier work [23] where the biometric performance was significantly improved by optimizing both the false accepts and false rejects simultaneously. While noting the previous works limiting to constrained iris data [8, 22, 13, 14], we validated the approach slightly unconstrained data [23]. In this work, we take a step further to extend the approach to truly unconstrained iris recognition. Further, the approach is validated on the visible spectrum iris recognition through an evaluation on large scale public visible spectrum iris database. The key contributions of this extended work therefore are listed as below:

- Proposes a new approach for template protection of iris codes using Morton Filters in a multi-bucket approach exploiting various stable bits and discriminable bits within the iriscodes [23].
- Presents the key idea behind modelling the intra-class and inter-class distribution to the advantage of biometric template protection along with the theoretical background.
- An extensive analysis of the proposed approach is presented to validate the scalability of proposed approach by employing both constrained and unconstrained iris databases. Further, the approach is analyzed on both NIR spectrum and VIS spectrum iris recognition. To the best of our knowledge, this is the first work attempting to study the template protection scheme on large scale unconstrained iris database in both VIS and NIR spectrum.
- Additionally, the security analysis using unlinkability framework is provided to validate the applicability of proposed template protection scheme while benchmarking it with the Bloom-Filter based template protection scheme.

In the remainder of this paper, we present the principles and theory of Morton Filters in Section 2. Section 3 presents the
approach of template protection using Morton Filters mechanism. Section 1 provides the experimental results along with the details of databases employed for evaluation. Section 5 discusses the security analysis for linkability issues followed by the conclusions and potential future works in Section 7.

2 MORTON FILTERS

Morton Filters were originally proposed for the Approximate Set Membership Data Structures (ASMDs) in the field of computing to make the storage efficient[3]. Specifically, Morton Filters were designed to facilitate the lookups, insertions, and deletions unlike the Bloom-Filters which do not allow the dynamic changes. The key improvements come from the introduction of compressed format permitting logically sparse filter and leveraging metadata to prune unnecessary memory accesses. As a third major improvement over the Bloom-Filters, Morton-Filters heavily bias insertions through the use of a single hash function for primary bucket while allowing multiple buckets. As it can be deduced, Bloom-Filters set the same bit over and again for multiple various entries due to inherent design limitation of using single bucket operation. A significant drawback of this is that it does not allow efficient querying of false negatives due to absence of locality of reference[3]. Although, this can be handled by adding extra number of hash functions, at a particular point the hash functions by themselves will overshadow actual length of original data or have high collision rate when few hashes are employed. Another alternative is to move the set bits to a different location based on the empty slots by constant look-up. While the former strategy can reduce false rejects, the later strategy can result in high number of false accepts both of which are not ideal in any operational scenario. This being the primary reasons, Morton-Filters formulated the multi-bucket approach to handle the problem efficiently. Through realization of multiple buckets set membership can be queried effectively leading to lower false negatives and false positives[3].

Thus, with the paradigm of multiple buckets (say for instance $H_1, H_2, \ldots, H_n$) within the Morton-Filters, the primary bucket $H_1$ is favoured heavily for insertions before proceeding with the rest of buckets. For negative lookups, the Morton-Filter employs an Overflow Tracking Array (OTA), a simple bit vector that tracks when data cannot be placed within $H_1$ and moves to other available buckets. Negative lookups only require accessing a single bucket (i.e., OTA), in most cases even when the filter is heavily loaded. This unique architecture makes the lookup (positive, false positive, or negative) to access one bucket and at most 2 leading to query efficiency of upto 50%[3].

In terms of implementation, Morton filters build upon the concepts of the Bloom Filters which operate by employing $k$ number of hash representations corresponding to number of blocks. The final representation $T$ in a Bloom-Filter of a predetermined size is first initialized to 0. For every chosen block within $n$ number of blocks, a particular location $x, y$ is set which corresponds to the final hashed representation $T$.

$$T(x, y) = 1 \quad \text{if } h^n_k = (y)$$

for a given column $x$ in chosen block $n$ (2)

While in the Morton Filters, filling of each bucket relies on the fingerprint of previous hash value as denoted by Eqn. 2 and the output position within a new template given $T(x, y)$ is set to 1. If the $T_1(x, y)$ is already set, another bit at a different location is set within a new template corresponding to $T_2(x, y)$. The process progresses for the number of designed buckets if all the bits in the previous buckets are already set. A detailed theory of the Morton-Filters is further provided in the original article [3] and we limit at this point to diverge into the details of how Morton-Filters are employed for template protection in the upcoming sections.

3 MORTON FILTER IRIS TEMPLATE PROTECTION

Intrigued by the design considerations of multi-bucket approach proposed in Morton-Filters to handle the false accepts and false rejects (or false positives and false negatives), we adapt the framework for template protection of iriscodes. The details of the template protection scheme based on Morton-Filters are presented in this section.

3.1 Morton Filters for Iris Template Protection

While the implementation of the Bloom-Filter based template protection for iris recognition is relatively straight forward, it has to be noted that Morton-Filter template protection differs in certain aspects. The core of Morton-Filters relies on having multiple buckets and in the very least case, more than one bucket is needed as discussed in previous sections. It can therefore be deduced that to make the template protection compatible to Morton-Filters, number of buckets need to be designed for iriscodes. A trivial idea for this can be to divide the iriscodes into blocks and thereafter consider them as separate buckets. While this may seem feasible at the first instance, it has to be noted that the iris imaging is impacted number of factors and thereby resulting in unreliable blocks for certain segments of the iris/iriscodes. Secondly, the iriscodes do not provide any correlational factors across different blocks due to the random structure of iris owing to biological factors[7]. Thus a more apprehensible manner of bucket formulations remains the first task. Therefore, we first focus on principles for suitable bucket design in an effort to obtain optimal templates.

3.1.1 Bucket Creation for Iriscodes

Within various deployed iris recognition systems, it is commonly observed that iris images are captured in multiple attempts or as a stream of video. The general idea behind using multiple captures or video of any particular iris is to obtain the non-noisy part of iriscodes to minimize the error in comparison. In an analogy within the signal (or image) representation, the non-noisy iriscodes lie within the subspace of the complete iriscodes consisting of both noisy and non-noisy parts. Thus, obtaining the subspace corresponding to non-noisy iriscodes can provide us with at-least one bucket for the realization of Morton-Filters based template protection.

For $k$ capture attempts of an iris image, the iriscodes ($I$) consisting of noisy and non-noisy parts can be represented as:

$$I = [I_1, I_2, \ldots, I_k]$$

where each iriscode is of dimension $x, y$ pixels. Given the task at hand is to obtain a non-noisy iriscodes from the complete iriscode, it can be represented as composite of non-noisy part and noisy part as below:

$$I_m = S_m + E_m$$

1. An ASMDs like a set data structure answers set membership queries (i.e., is an item $e$ an element of the set $S$?)
where $S_m$ is low-rank non-noisy part and $E_m$ is sparse error part within the iriscode corresponding to noisy data. As the capture conditions can vary across multiple captures, it can be easily deduced that both non-noisy part and the noisy part of iris code can vary in spatial locations. Thus, to obtain a stable non-noisy subspace of iriscode, one can explore multiple approaches such as obtaining Principal Component Analysis (PCA) or a median weighted approach [30], [16]. Given the recent formulation for obtaining the superior non-noisy subspace using tensor formulation from our recent work [22], we employ the same in this work.

Thus, by stacking the iriscodes obtained from multiple ($k$) capture attempts, a tensor of iriscodes can be represented as $I \in \mathbb{R}^{x \times y \times k}$. The tensor formulation thus leads to easy recovery within the tensor space which corresponds to common bits across iriscodes across capture attempts. In an alternative interpretation, the solution to low-rank recovery of tensor space provides the iriscodes which are relatively non-noisy. Recovering non-noisy iriscodes from the tensor space thus translates to obtaining $S_m$, low-rank non-noisy component and $E_m$, sparse error component (i.e., low tubal rank component [21]) from set of noisy iriscodes represented as $I = S_m + E_m \in \mathbb{R}^{x \times y \times k}$:

$$\min_{S, E} \|S\|_* + \lambda\|E\|_1, \text{ s.t. } I = S + E,$$

where $\|S\|_*$ is the tensor nuclear norm. However, the challenge of obtaining a sensible solution still remains in Eqn. 5 and in order to address this challenge, we express the $\lambda = 1/\sqrt{\max(x, y) \times k}$ [21] such that non-noisy subspace of iriscodes can be obtained. Given the formulation in Eqn. 5 and a reasonable expression of $\lambda$, we employ the software package provided by [27] to solve the Eqn 5 with no additional parameter tuning. Thereby, with the obtained non-noisy subspace, we derive one bucket ($B_k^l$) of $k^{th}$ iriscode for a particular subject by simply using it as a weight map as given below:

$$B_k^l = I_k \ast S$$ (6)

While the first bucket is created from the above steps, the Morton-Filter architecture needs at-least another additional bucket. Thus, we explore the intra-class discriminablility of iriscodes exploring the findings from statistical trials provided in earlier works [3]. Under the assumption that binomial distribution of iriscodes, all the bits within the iriscodes corresponding to 0 and 1 are equi-probable and randomly distributed [5]. Thus, if the probability of $i^{th}$ bit equalling to 1 is given by $p_i^*$ and the probability of $i^{th}$ bit equalling to 0 is given by $q_i^*$, it can be safely written that $p_i^* + q_i^* = 1$ for the $i^{th}$ bit within an iriscode. Thus, discriminablility of a particular bit $d_i$ for a particular iriscode from the rest of the iriscodes can be formulated as:

$$d_i = p_i q_i^* + q_i p_i^*$$ (7)

where $p_i$ is the probability of $i^{th}$ bit equalling to 1 and $q_i$ is the probability of $i^{th}$ bit equalling to 0 for any other iriscode [16] in an ideal case. Expressing, $q_i^* = 1 - p_i^*$, the Eqn 7 becomes

$$d_i = (1 - 2p_i) p_i^* + p_i^*$$ (8)

It can therefore be noted that if the $p_i = 0.5$, the $d_i = 0.5$ and the implication is that intra-class value of the $i^{th}$ bit is highly uncertain being equi-probable. An alternative formulation leads to the fact discriminablility $d_i$ of one subject will be lower when the

![Fig. 3: Morton Filtering based protected template creation.](image-url)
that many early works on iris template protection have employed the same. While the architecture can improve the performance of the template protection, we note that this may suffer from the same challenge of linkability issues as indicated earlier\textsuperscript{[14]}. In order to mitigate any such potential linkability issues, we adapt the private keys for creation of protected templates as described in recent work\textsuperscript{[13], [4]} along with a bijective function on all the three buckets such that the unique bits within the iris template is retained.

As noted from Eqn\textsuperscript{[11]} the bits in the final template are activated based on bits of other buckets. Such an architecture not only results in robust templates, but also makes the guessability attacks harder if not fully eliminate given only sparse number of bits are activated across the protected iris template. As it can be seen from the Figure\textsuperscript{3} the protected template is created by iteratively checking the bit location indicated by hash function and set if it is empty. If not, the hash value is carried forward to next bucket by determining the location based on the values in block under consideration and the previously obtained location for earlier bucket. It can be observed that fewer number of bits are set in the last bucket while more number of bits are set in the first bucket from Figure\textsuperscript{[3]}

![Multiple templates of iris code using low rank non-noisy representation, discriminative representation, and combined representation of the same binarized iris code (partial iris code) for a sample iris from IITD Iris Dataset\textsuperscript{[49]}]

\begin{equation}
T^1_k = I_k \oplus T^2_k \oplus T^3_k \quad (12)
\end{equation}

In order to diffuse the arrangement of bits, we further introduce a random ordered interleaving within the above Eqn\textsuperscript{[12]} to avoid any correlation based guessability attacks.

In the second variant, we simply employ a bijective XOR function to eliminate the bits within the protected template which are not common across all the three individual protected templates. The operation can therefore be given by:

\begin{equation}
T^\text{XOR}_k = T^1_k \oplus T^2_k \oplus T^3_k \quad (13)
\end{equation}

The two variants of the proposed template protection can be further seen in the illustrated Figure\textsuperscript{4} As observed, the XOR
variant of the template protection provides the template of the size that is equal to the three independent templates resulting in a compact protected template size. As a second observation, it can be evidently seen that the size of the template triples for the IV version of the protected template. As a direct implication of this, one can deduce the high performance of the IV version as compared to it’s XOR variant.

4 Experiments and Results

We present the experimental evaluation on four different datasets and the corresponding results along with an analysis of the results. The first set of experiments relate to constrained iris acquisition by employing IITD Iris Database version 1.0 [25] and the second set of experiments relate to unconstrained iris acquisition using CASIA.v4 distance dataset [1]. While the former is captured in highly cooperative setting, the latter is captured at various stand-off distance resulting in non-ideal iris images with significant degradation. Both of these datasets are captured in NIR spectrum mimicking the deployment iris systems. In another set of experiments, we employ the iris images captured in the visible spectrum by employing the UBIRIS v1 [35] and UBIRIS v2 [36] dataset. The key motivation behind such experiments on the unconstrained visible spectrum iris data is to evaluate scalability of the proposed approach for capture domain independence. Further, this set of experiments also establishes the robustness on degraded data stemming from unconstrained capture setting with significant degradations.

We further provide the comparison of performance from proposed approach against unprotected version and protected template using Bloom-Filter. For each of iriscode in unprotected domain and protected domain, we employ a simple Hamming Distance measure [6] to obtain the compare score.

Performance Metrics

All the results in Detection Error Trade-off (DET) curves along with indication of Genuine Match Rate (GMR) where GMR is (1 - False Non Match Rate (FNMR)) at a False Match Rate of 0.01%. In addition to the DET graphs, we also present the results in Error Rate (EER%) to indicate the symmetric error rates.

4.1 IITD Iris Database version 1.0

IITD Iris Database version 1.0 [25] is a constrained iris database consisting of data captured from 224 subjects and 5 images per iris. We employ the set of left iris images in the lines of earlier work and to provide fair comparison to earlier works [42], [4]. Thus, in our work, we employ data from 1120 iriscodes from 224 subjects with 5 iris codes per subject. We employ 1D Log-Gabor encoding [29] for the unprotected iris templates and the subsequently, use the same encoding to obtain protected templates in the lines of earlier works on Bloom-filter based template protection [39], [4], [13]. Further, it can be noted that the our approach does not heavily depend on feature space and thus allowing the freedom to employ any other binary encoding scheme for iris feature encoding. In order to consistent with the earlier works, we also present the comparison to earlier works [4], [13], we present the results in various size of block widths $\ell \in \{4, 8, 16, 32\}$.

### Table 2: Results of proposed template protection schemes compared to other schemes on IITD Iris Dataset.

| Iris code   | EER | GMR @ 0.01% FMR | EER | GMR @ 0.01% FMR |
|-------------|-----|-----------------|-----|-----------------|
| **Unprotected** |     |                 |     |                 |
| Log-Gabor    | 0.36 | 99.11           | 0.36 | 99.11           |
| Bloom - 4    | 0.38 | 99.33           | 0.62 | 99.38           |
| Bloom - 8    | 0.39 | 99.38           | 0.44 | 99.55           |
| Bloom - 16   | 0.40 | 99.15           | 0.26 | 98.84           |
| Bloom - 32   | 0.83 | 98.57           | 0.34 | 98.08           |
| **Protected** |     |                 |     |                 |
| Proposed - 4 | 0.00 | 100.00          | 0.00 | 100.00          |
| Proposed - 8 | 0.00 | 100.00          | 2.34 | 90.63           |
| Proposed - 16| 0.00 | 100.00          | 1.42 | 94.98           |
| Proposed - 32| 0.01 | 99.67           | 1.10 | 96.32           |

Fig. 5: Comparison of biometric performance using DET for IITD Iris Dataset. Proposed approach is depicted with 4 blocks and 5 bits alongside similar configuration with Bloom-filter template protection. It has to noted that the EER being close to 0 for proposed approach, the curves do not appear on the DET curves.

4.2 Results on IITD Iris Dataset

The empirical results of the proposed template protection scheme along with the comparison to unprotected templates and protected templates using Bloom Filter approach are presented in Table 2. From the Table 2, the following observations can be made on the proposed approach:

- The proposed approach is antagonistic to block size unlike the approach based on Bloom Filter which is fairly robust in smaller block sizes and degrades in performance with increasing block size. A similar observation for Bloom-Filter based template protection was reported in earlier work [4] which noted the degradation of biometric with increasing block width and higher bits within each blocks.

- A near ideal performance from proposed approach with IV version of the protected template. As a direct implication of this, one can deduce the high performance of the IV version as compared to it’s XOR variant.

- As anticipated, the compact size of XOR variant of the
The DET curves in Figure 5 depicts the performance of proposed approach. Further, to illustrate the antagonistic nature of proposed approach towards various block sizes, the DET curves are presented in Appendix in Figure B. As it can be noted, various configurations of the proposed approach for a bit length of 5 provides near ideal performance for protected templates.

4.3 CASIA V4 Distance Iris Dataset

Considering the earlier works focusing on the constrained iris recognition, we evaluate the proposed approach on unconstrained capture setting by employing CASIA.v4 distance dataset. CASIA.v4 capture includes parts of the face image due to stand-off distance of 3 meters in the acquisition setting from a total of 1-2 subjects. Further, it has to be noted that the captured iris images suffers from degradation unlike ideal iris images due to blinking, occlusion due to eye-lids, specular reflection, presence of eye-glasses and motion blur all leading to real-life iris acquisition. We therefore employ classical Viola-Jones eye detector to detect the eye region alone and then correct the errors manually for any undetected/wrongly detected eye regions. Further to eye region localization, we segment and normalize the iris region using Morton Filters. When such a operation a carried out, the collision of the bits across multiple protected templates starts to happen. The collision rate along with the low number of activated bits in final template jointly degrade the performance in XOR variant.

The DET curves in Figure 5 depicts the performance of proposed approach. Further, to illustrate the antagonistic nature of proposed approach towards various block sizes, the DET curves are presented in Appendix in Figure B. As it can be noted, various configurations of the proposed approach for a bit length of 5 provides near ideal performance for protected templates.

Table 3 presents the results of proposed template protection along Bloom Filter approach. Noting the low performance of naive Bloom-Filter on CASIA v4 dataset, we also employ the stable bits to extract the Bloom-Filter template. Specifically, we employ the Eqn 6 provided in the Section 3.1.1 to extract the stable bits from iriscodes. As it can be noted from Table 3 there is an marginal performance improvement over naive Bloom-Filter templates but much below the required operational performance in a practical biometric system. Further, in the lines of our experiments on IITD Iris dataset, we also present the results on both IV and XOR variant of the proposed approach on CASIA v4 dataset. The clear improvement of the proposed approach can be seen from the Table 3 and impelled by such a improvement, we note the following points:

- While in the case of Bloom-Filter templates, same set of bits are activated due to noisy nature of the iriscodes. This in turn results in sub-optimal protected template results validating the motivation and initial assertion for this work. It can be noted from Fig. 1 that for the iris template across sessions for the same subject, bloom filter approach results in dissimilar protected templates for the same subject across different captures leading to a significant false rejections.
- While in the proposed approach, the creation of multiple buckets and further activation of bits based on the predecessor buckets leads to a unique template even for different captures for a same subject. Adding the uniqueness of the template, both Interleaved variant (IV) makes the templates unique due

### Table 3: Results from proposed approach on CASIA v4 Dataset

| Configurations | 5 Bits | 10 Bits |
|----------------|--------|---------|
|                | EER    | GMR @ 0.01% FMR | EER    | GMR @ 0.01% FMR |
| Bloom - 4      | 36.24  | 0.65     | 38.52  | 0.20    |
| Bloom - 8      | 40.00  | 0.24     | 41.65  | 0.08    |
| Bloom - 16     | 41.70  | 0.24     | 43.77  | 0.08    |
| Bloom - 32     | 40.07  | 0.08     | 44.87  | 0.12    |
| Bloom - 4      | 27.12  | 29.27    | 31.87  | 14.63   |
| Bloom - 8      | 31.83  | 11.38    | 36.09  | 4.07    |
| Bloom - 16     | 34.31  | 8.94     | 39.92  | 2.44    |
| Bloom - 32     | 32.92  | 18.29    | 42.12  | 3.66    |
| Interleaved (IV) |       |          |        |         |
| Proposed - 4   | 0.13   | 99.51    | 0.53   | 96.63   |
| Proposed - 8   | 0.37   | 98.37    | 2.40   | 82.07   |
| Proposed - 16  | 0.04   | 99.96    | 1.96   | 86.87   |
| Proposed - 32  | 0.04   | 99.88    | 1.92   | 88.66   |
| XOR            |        |          |        |         |
| Proposed - 4   | 0.00   | 100.00   | 0.00   | 100.00  |
| Proposed - 8   | 6.27   | 52.93    | 6.61   | 39.88   |
| Proposed - 16  | 3.40   | 69.88    | 11.21  | 18.70   |
| Proposed - 32  | 2.11   | 86.18    | 8.37   | 27.93   |
to large size and the XOR variant eliminates the inconsistent bits. Both of these variants further lead to lower false rejects needing further investigation into design considerations of Morton-Filters for template protection.

- Despite the degradations of iriscodes owing the unconstrained setting, it can be noted that the proposed approach on CASIA.v4 distance dataset is significantly stable in IV variant of proposed approach while the XOR variant produces the templates that have slightly higher collisions.

We further present the DET curves of proposed approach as shown in Figure 6 for both variants and do not present the DET curves for the Bloom-Filter templates owing to the low performance. Supporting our initial assertion, the proposed approach through employing multiple buckets results in lower false accepts and false rejects as shown in Figure 6.

4.5 UBIRIS v1 Dataset

We further evaluate the proposed approach on the visible spectrum iris recognition, especially captured in unconstrained setting. To this end, we evaluate the proposed approach on UBIRIS.v1 database composed of 1877 images collected from 241 persons in two distinct sessions in visible spectrum at a stand-off distance. Unlike the other existing public and free databases for iris recognition, UBIRIS v1 incorporates images with several noise factors, thus permitting the evaluation of robustness proposed template protection scheme. The enrollment set consists of minimized noise factors, specially those relative to reflections, luminosity and contrast, having installed image capture framework inside a dark room as compared to the second session. While in the second session, the iris images are captured with the introduced natural luminosity factor. Thus, we employ the images from the first session for the enrolment template creation and second session for template verification. Given the database has number of noise factors, we have eliminated the images that have severe segmentation errors and completely off-angled iris images. The segmentation and the normalization of the iris region is performed using the recent approach of Total-variation based segmentation to derive the iris images of size $100 \times 360$ pixels which is then used to extract the features by employing 1D Log – Gabor representation.

4.6 Results on UBIRIS v1 Iris Dataset

For the sake of brevity, we present the result of proposed approach on the UBIRIS v1 iris dataset in the Figure 7 and we do not report the performance of Bloom-Filter based template protection due to non-ideal performance. As it can be observed from the DET curves, the proposed approach has certain loss in terms of the biometric performance as compared to the unprotected templates as anticipated. Nevertheless, the performance is comparable in the IV version of the proposed approach as seen in Fig.7a. While a severe degree of performance loss is seen across the XOR variant, it is also interesting to note that the XOR version with a block length of 4 with 5 bits is performing close to unprotected template. This observation is consistent to our earlier observations where we have noted that the lower block widths perform superior as compared to the larger block widths. Further, the Receiver Operating
We present the security analysis to demonstrate the unlinkability of the proposed template protection using the recent Unlinkability Characteristics (ROC) to indicate the biometric performance is provided in supplementary material in Fig. C.2

4.7 UBIRIS v2 Dataset

We further evaluate the proposed approach on the visible spectrum iris recognition captured in unconstrained setting using the second set - UBIRIS v2. Similar to UBIRIS v1, this dataset has data with various non-ideal iris images, imaging distances, subject perspectives and lighting conditions. Further, the iris data is captured under both natural and artificial lighting sources along with a session interval of a weeks between the enrolment and probe. It has to be further noted that in the second session, the location and orientation of the acquisition device and artificial light sources was changing increasing the diversity in capture conditions with a total of 261 subjects totalling to 522 irises. The segmentation and the normalization of the iris region is performed using Total-variation based segmentation [49] to derive the iris images of size 100 × 360 pixels and then extract the features using 1D Log – Gabor representation.

4.8 Results on UBIRIS v2 Iris Dataset

Similar to the results obtained on UBIRIS v1 dataset, the results obtained on the UBIRIS v2 iris dataset is presented in Figure 9. The observations correlate to earlier observations and a slight degradation in performance can be noted as compared to the unprotected domain indicating the applicability of the proposed approach. It has to be noted that results of Bloom-Filter based template protection is not reported on this dataset due to non-ideal biometric performance.

4.9 Fine Tuned Experiments on UBIRIS v2 Iris Dataset

Seeking an answer to the low performance of the protected templates, we conducted an additional experiment where the segmentation masks were employed prior to deriving the stable and discriminable code corresponding to protected templates from iriscodes. As the masks eliminate the segmentation errors and thereby provide first level of reliable bits, our assertion was that such a refined iriscodes would improve the performance of proposed template protection. In order to validate the assertion, we report the following DET as show in the Figure 10. As seen from the Figure 10 the performance of protected template increases through the use of the masks prior to creation of multiple buckets.

5 Security Analysis: Unlinkability

We present the security analysis to demonstrate the unlinkability of the proposed template protection using the recent Unlinkability

4.10 Analysis Framework [11]. Under this framework, we measure the similarity of the mated imposter distribution versus non-mated imposter distribution. To maintain the terseness, we present the results on IITD Iris dataset in Figure 9 where a high degree of unlinkability can be observed along with the unlinkability metric by $D_{sys}^{pp}$. The lower $D_{sys}^{pp}$ indicates superior unlinkability. Further, one can observe the consistent unlinkability across different configurations for varying blocks and varying bits.

6 Future Works

Although the preliminary analysis of the security implications is carried out for unlinkability, this work has not investigated the potential threats with advanced attacks. While it can be noted that the analysis carried out for Bloom-Filter reliability can be generalized to the proposed approach and theoretical proof can be borrowed from the recent works [12], [13], it will be interesting to investigate the newer attacks. In the future works, we intend to analyse the robustness of proposed attacks towards such attacks. In the second direction, we shall explore the proposed approach for the other modalities to preserve the privacy of the biometric data.

7 Conclusions

We have addressed the problem of template protection for iris recognition in this work, specifically, we presented a novel approach for template protection employing Morton Filters on constrained and unconstrained iriscodes. Exploiting the intra-class and inter-class distribution of iriscodes, we have designed multiple buckets to realize Morton-Filter based template protection. The proposed approach has been evaluated for both performance and linkability challenges using four publicly available iris databases.
captured in NIR spectrum and VIS spectrum. Although these empirical validation on NIR domain demonstrate the feasibility and applicability of proposed approach, we have evaluated the approach on the unconstrained iriscodes captured in visible spectrum to measure the scalability and robustness. Along with providing security, the loss in the performance is observed to be marginal in visible spectrum iriscodes owing to noisy nature of images. The approach being robust in comparison to Bloom Filter, can be applied to other modalities with suitable adaptations in the future works.

REPRODUCIBLE RESEARCH

In order to facilitate the reproducible research, we intend to make the code of the proposed approach publicly available along with this article. Details on availing the code shall be provided in the final version of the manuscript.

ACKNOWLEDGEMENT

This work was carried out under the partial funding of the Research Council of Norway under Grant No. IKTPLUSS and applicability of proposed approach, we have evaluated the approach on the unconstrained iriscodes captured in visible spectrum to measure the scalability and robustness. Along with providing security, the loss in the performance is observed to be marginal in visible spectrum iriscodes owing to noisy nature of images. The approach being robust in comparison to Bloom Filter, can be applied to other modalities with suitable adaptations in the future works.

REPRODUCIBLE RESEARCH

In order to facilitate the reproducible research, we intend to make the code of the proposed approach publicly available along with this article. Details on availing the code shall be provided in the final version of the manuscript.

ACKNOWLEDGEMENT

This work was carried out under the partial funding of the Research Council of Norway under Grant No. IKTPLUSS.
[44] C.-W. Tan and A. Kumar. Adaptive and localized iris weight map for accurate iris recognition under less constrained environments. In Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on, pages 1–7. IEEE, 2013.

[45] P. Viola and M. Jones. Rapid object detection using a boosted cascade of simple features. In Computer Vision and Pattern Recognition, 2001, CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on, volume 1, pages I–I. IEEE, 2001.

[46] E. Wolff. The anatomy of the eye and orbit: including the central connections, development, and comparative anatomy of the visual apparatus. Blakiston, 1948.

[47] S. Yang and I. Verbauwhede. Secure iris verification. In 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP '07, volume 2, pages II–133. IEEE, 2007.

[48] L. Zhang, Z. Sun, T. Tan, and S. Hu. Robust biometric key extraction based on iris cryptosystem. In International Conference on Biometrics, pages 1060–1069. Springer, 2009.

[49] Z. Zhao and K. Ajay. An accurate iris segmentation framework under relaxed imaging constraints using total variation model. In Proceedings of the IEEE International Conference on Computer Vision, pages 3828–3836, 2015.
APPENDIX

STATE-OF-ART REVIEW FOR IRIS TEMPLATE PROTECTION

In this section we provide a brief overview of the state-of-art template protection schemes proposed and employed for the iris recognition. This section is supplementary to Table 1 with specifics of previously proposed approaches.

- Yang and Verbauwhede [47] proposed a iris template protection approach by employing Error Correcting Code (ECC) cryptographic technique with the reliable bits selection to improve the verification accuracy. In their work, Bose-Chaudhuri-Hocquenghem (BCH) code of a random bit-stream was introduced to eliminate the considerable differences between the features extracted from different scans of irises such that template protection was scheme reliable. The experiments were conducted on a a subset of CASIA iris data.

- Nandakumar and Jain [31] proposed another framework based on fuzzy-vault scheme to derive private keys from iris patterns. In the same work, they also proposed to fuse multiple biometric modalities, specifically fingerprint and iris. A salting transformation based on a transformation key was employed to indirectly convert the fixed-length binary vector representation of iriscode into an unordered set representation and further secured using the fuzzy vault. The performance for the iris template protection was reported on CASIA iris image database v1.0 consisting of 108 different eyes with 7 images per eye collected over two sessions and one image from each session was used for evaluation.

- Maiorana et al., [28] proposed a template protection framework inspired by the digital modulation paradigm where the properties of modulation constellations and turbo codes with soft-decoding were exploited to design a system. The approach was tested on the Interval subset of the CASIA-IrisV4 database where high performance in terms of both verification rates and security was reported.

- Zhang et al., [48] proposed a concatenated coding scheme and bit masking scheme to construct an iris cryptosystem. The concatenated coding scheme was proposed to embed long keys into the iris data and concatenated code combined with Reed-Solomon code and convolutional code. Further, a bit masking scheme was proposed to minimize and randomize the errors to make the error pattern more suitable for the coding scheme. The iris cryptosystem reported a FRR of 0.52% with the key length of 938 bits on a internal database of 128 iris images captured across 3 different sessions.

- Rathgeb et al. [39] proposed the popular Bloom-filter based biometric template protection. The iris codes were processed through K-hashes resulting in the protected templates through transformation. While the framework was later reported to be weak against linkability attacks, [44], the same was fixed by adding the private keys as proposed in [12]. The improved approach was evaluated on BioSecure Multimodal Database to demonstrate the robustness towards linkability and reversibility.

- Rathgeb and Busch [41], [40] proposed a framework based on adaptive Bloom filter-based transforms that were applied in order to mix binary iris biometric templates at feature level, where iris-codes are obtained from both eyes of a single subject. The irreversible mixing transform generating alignment-free templates obscured information present in different iris-codes. Further, the proposed transform was parameterized to achieveunlinkability resulting in implementing cancelable multi-biometrics. The experiments on IITD Iris Database version 1.0 resulted in EER below 0.5% for different feature extraction methods and fusion scenarios.

- Rathgeb et al. [38] further proposed a generic framework for generating an irreversible representation of multiple biometric templates extending the framework of adaptive Bloom filters from earlier work[41]. The technique enabled a feature level fusion of different biometrics (face and iris) to a single protected template, improving privacy protection compared to the corresponding systems based on a single biometric trait.

- Lai et al [26] recently proposed a new scheme to generate cancellable iris template with Jaccard similarity matcher by modifying the of Min-hashing to strengthen the privacy security in Indexing-First-One (IFO) hashing. The proposed approach was evaluated on CASIA v3 iris database and reported to result in 0.16% Equal Error Rate (EER). Further, it is worth noting that the approach is reported to be resistant against Single Hash Attack, Multi-Hash Attack, Attack via record multiplicity and Pre-image attack. Unlike many previous works, this work also reported the unlinkability and revocability analysis on the proposed approach.

2. Details on the dataset and number of images are not provided in the article.
B DET CURVES CORRESPONDING TO PROPOSED APPROACH AND INVARIANCE TO BLOCK SIZE IN NIR SPECTRUM

![Diagrams](image1.png)

Fig. B 1: Performance of multiple configurations for proposed Morton Filter on IITD Iris dataset for a bit length of 5 bits.

C RECEIVER OPERATING CHARACTERISTIC (ROC) CURVES CORRESPONDING TO PROPOSED APPROACH

![Diagrams](image2.png)

Fig. C 2: Performance of multiple configurations for proposed template protection on UBIRIS v1 dataset.
Fig. C 3: Performance of multiple configurations for proposed template protection on UBIRIS v2 dataset.
D Unlinkability Analysis

Fig. D 4: Unlinkability metrics obtained for proposed template protection scheme for various configurations