A standard ranking algorithm for robust iris template protection

Mohammed Ali Hameed Yassir[1,2], Rudzidatul Akmam Dziyauddin[1,2], Norshaliza Kamaruddin[1], Norulhusna Ahmad[1]
[1]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
[2]Wireless Communication Center, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

Article Info

Article history:

Received Dec 15, 2023
Revised Feb 6, 2024
Accepted Feb 9, 2024

Keywords:

Biometrics
Cancelable
Iris
Protection
Recognition
Security

ABSTRACT

In iris biometric recognition systems, protecting the storage and transmission of iris templates is crucial, and template protection techniques are pivotal for ensuring their security. A prevalent approach involves using indexing methods as an effective algorithm for iris template protection, leveraging the index or rank of the extracted iris code to generate a secure iris template. Meantime, many privacy threats to biometric data have emerged, necessitating heightened protection measures. Specifically, protecting the privacy of iris data is imperative within the context of iris template protection during recognition processes. As stipulated by the international standard ISO/IEC 30136, effective iris template protection must concurrently meet the criteria of irreversibility, revocability, and unlinkability. Nevertheless, existing indexing methods on iris template protection faced the formidable challenge of simultaneously fulfilling these three privacy requirements while maintaining the efficacy of iris recognition. This paper introduces a standard ranking (standardR) algorithm, named standardR, designed to enhance the security of iris templates by transforming each iris template into an irreversible representation. The experimental results on the benchmarked Casia-Iris-interval dataset, along with two additional iris datasets MMU1 and UBRIS 1, demonstrate the efficacy of the proposed algorithm. The proposed standardR algorithm achieves an equal error rate (EER) of 0.1695% and an area under the curve of 0.93011% with the Casia-Iris-Interval dataset. Furthermore, the algorithm maintains efficient recognition with a reduced iris code length of 1280 bits, a time complexity of O(n log n), and satisfies the biometric template protection (BTP) requirements in irreversibility, unlinkability, and renewability.

Corresponding Author:

Mohammed Ali Hameed Yassir
Razak Faculty of Technology and Informatics, University Technology Malaysia
Sultan Yahya Petra St. (Street of Semarak), 54100 Kuala Lumpur, Malaysia
Email: ali-1984@graduate.utm.my

1. INTRODUCTION

Biometric template protection (BTP) techniques play a pivotal role in fortifying the security and privacy of biometric data, aiming to render stored templates cancelable, revocable, and protected. Cancelable biometrics (CB) involves transforming original biometric data into an irreversible representation, dictated by random parameters, ensuring that the stored template cannot be reverse-engineered. These techniques, including those applied to irises [1], have become integral in contemporary stringent security systems, necessitating user authentication based on cancelable biometrics methods.

Iris biometrics, owing to its unique and stable physiological traits, has garnered significant interest over the past decade [2]. Its application in authentication systems stands out as a preferred alternative to traditional methods, reducing reliance on passwords and tokens [3], especially given its irrevocable nature. The implementation of the general data protection regulation (GDPR) in 2018 has underscored the importance of secure handling, leading to the establishment of ISO/IEC 30136 as an international standard for biometric technologies [4]. Four critical considerations must be taken into account concerning iris template protection for both performance and security:

- Irreversibility: the original iris template should be challenging to analogize from the IrisCodes generated during enrolment and matching stages.
- Un-linkability: it is crucial to maintain the privacy of the iris template to prevent tracking the user and matching templates in different authentication systems.
- Diversity (renewability/revocability): the protection mechanism should ensure that the iris template is safeguarded from generating identical iris codes for re-registration, and it should allow for the discarding of leaked IrisCodes.
- Performance: the matching process should not degrade while satisfying the three aforementioned requirements.

Typically, when employing non-inversion transformation algorithms to secure stored iris templates from disclosure, user-specific keys should be incorporated to create a distorted iris template [5]. BTP uses various methods like hash functions and indexing methods to protect the iris templates, drawing inspiration from fuzzy recognition systems for user authentication [1]. One-way hash functions, employed as mathematical transformations, take variable-length inputs and produce fixed-length outputs [6]. Initially facing challenges due to intraclass variations, hash functions evolved into robust hash functions to address intraclass variability while maintaining privacy and discrimination [7]. Indexing methods represent significant approaches of cancelable biometrics, particularly renowned for their low equal error rate (EER) in iris recognition [8]. The term “IrisCode” refers to a binary feature characterized by fixed dimensions, derived from the iris image [9]. Indexing-based BTP methods rely on helper data in two scenarios: firstly, user-specific keys that are unique and independent for each user, and secondly, common user-specific keys when all users share this information to improve discrimination through the management of random keys [10].

However, the use of helper data in both scenarios can increase discrimination while potentially leading to heightened complexity, computational costs, and storage requirements requirements [11]–[13]. An efficient local rank transformation algorithm, as presented in [14], follows indexing approaches to protect iris templates. This algorithm utilizes user-specific keys to transform the extracted iris code after applying the local rank, generating transformed templates. Notably, according to [15], the proposed algorithm in [14] did not fulfill the irreversibility and non-linkability requirements of BTP. In another indexing method explored in valuable research [16], a row-wise scheme with decimal encoding-based look-up table (LUT) mapping is suggested to transform the iris code into an irreversible representation. However, the authors of [16] acknowledge the possibility of reversing the iris templates if an attacker gains access to the LUT table. Moving on to a study recommended in [17], which proposes partial sort and alignment-free techniques based on column-wise and LUT mapping for coding the extracted iris simultaneously, the suggested method [17] does not achieve accuracy and efficiency while meeting the security requirements at the same time. Furthermore, the research in [18] introduces a confidence matrix to enhance performance in iris datasets with noise masks, utilizing the index first one (IFO) approach. However, a pre-image attack conducted by [19] succeeded in breaking the IFO approach. Despite the proposed indexing methods attempting to satisfy the efficiency in recognition, these attempts did not maintain the tradeoff between the BTP security requirements and the efficiency in iris recognition at the same time. The leakage of iris templates and the succeeded attacks on the indexing BTP methods emphasize the need for robust security measures [8]. Iris template protection, therefore, aims not only to secure templates by transforming them to irreversible representation but also to prevent linking among databases or applications, contributing to a comprehensive BTP strategy [20], ensuring that the proposed methods remain effective in iris recognition while concurrently meeting the essential BTP requirements of irreversibility, unlinkability, and renewability. So, in this study we propose a cancelable iris template algorithm called standard ranking (standardR) based on standardR to protect iris templates. The main benefits of the proposed algorithm can be listed:

- A robust indexing algorithm to the evolving challenges of iris template leakage and satisfying the security BTP requirements in irreversibility, unlinkability, and renewability.
- Substantial enhancements in authentication accuracy, evidenced by a reduction in EER, an increase in AUC, and an improved genuine acceptance rate (GAR).
- Efficiency improvements were achieved by reducing the iris code length to 1,280 bits and optimizing time complexity to O(n log n).

The subsequent sections of this study are structured as follows. Section 2 delves into the existing body of literature concerning iris template protection methods, providing a comprehensive overview of related works. In section 3, we elucidate the details of our proposed algorithm designed for cancelable iris template protection. The experimental findings are thoroughly examined in section 4, shedding light on the outcomes of our research efforts. Finally, section 5 encapsulates the entirety of this research, encompassing conclusions drawn from our work and delineating avenues for future research endeavors.

2. RELATED WORKS

Indexing methods, particularly those employed in iris recognition systems [21], stand out as a promising avenue for protecting biometric templates. These methods generate binary vectors for individual iris features based on their indexes within the iris code, leveraging inherent feature variability to establish secure binary representations. Despite their demonstrated success in enhancing security and recognition performance, indexing methods face a challenge stemming from limited variability among generated binary vectors, making them susceptible to potential exploitation [22]. To address this challenge, various approaches have been introduced to enhance the security of indexing methods.

A notable algorithm utilizing local rank transformation is proposed by [14], transforming iris templates through XOR operations with user-specific keys, yielding local rank decimal values for partitioned blocks and groups based on decimal values. The local rank transformation algorithm emerges as an efficient means to ensure privacy and security in iris template protection. However, challenges arise in meeting specified string length requirements, ranging from 196,608 bits in basic methods to 1,536 bits in the shift technique, potentially compromising irreversibility. According to Ouda [15], the local rank algorithm did not fulfill the irreversibility and unlinkability requirements of BTP

Another research from Dwivedi *et al.* [16] suggested a row-wise scheme with decimal encoding-based look-up table mapping (LUT), advocating for decimal encoding and LUT, presenting a deterministic approach but demanding secure LUT generation. Despite ensuring that extracted bits originate from the same input data, the methodology's reliance on a 32,768-bit iris length and the need for 4 iris images per subject pose constraints, echoing accuracy concerns in poor-quality image scenarios. The authors refer to the possibility of the attacker reversing the leaked iris templates if the attacker has the LUT.

To achieve improved accuracy, a study from Jeong and Jeong [17] recommended partial sort and alignment-free techniques based on column-wise and LUT mapping for coding four iris codes simultaneously. While these techniques exhibited enhanced accuracy, concerns were raised about template inversion risks and the need for the attacker to possess the LUT, potentially impacting accuracy due to preprocessing issues in iris feature extraction for low-quality images. Additionally, column-wise partial sort and alignment-free techniques [17] proved efficient in reducing EER for verification, particularly in on-body wearable wireless networks. However, challenges persist, including the need for a secure LUT and reliance on four iris images per person, resulting in a total iris length of 9,600 bits. Furthermore, the proposed method does not achieve accuracy and efficiency while meeting the security requirements at the same time

Meanwhile, another study [18] proposed a confidence matrix to enhance performance in iris datasets with noise masks, utilizing the IFO hashing method. Nevertheless, the methodology faces challenges linked to intra-user variability resulting from aging and fluctuating lighting conditions, potentially impacting accuracy within the Casia-Iris-Interval dataset. However, a pre-image attack conducted by [19] succeeded in breaking the IFO approach. In summary, while these studies contribute valuable advantages in enhancing authentication efficiency, the common issue is that these methods did not satisfy the BTP requirements while achieving efficient iris recognition at the same time.

Hence, this study introduces an algorithm for iris template protection called standardR, incorporating a standardR for each iris code. The proposed algorithm is proposed to enhance the iris recognition efficiency while maintaining the BTP security requirements in irreversibility, unlinkability, and renewability. Then extended the algorithm's efficiency to reduce the iris code length and time complexity. The experiment will be conducted on the renowned Casia-Iris-Interval dataset [23] and will be validated using two additional iris datasets, MMU1 [24] and UBRIS 1 [25].

3. THE PROPOSED BTP-BASED STANDARD RANKING ARCHITECTURE

The StandardR algorithm, rooted in BTP, is strategically designed to elevate performance in CB while ensuring robust protection for iris templates. In pursuit of heightened authentication accuracy, the BTP-based StandardR algorithm integrates multiple stages, encompassing preprocessing through to the decision-making stage. The architectural depiction of the BTP-based standardR algorithm is elucidated in Figure 1. The ensuing sections delve into the intricacies of the algorithm's crucial steps, shedding light on its comprehensive approach of BTP-based standardR algorithm.

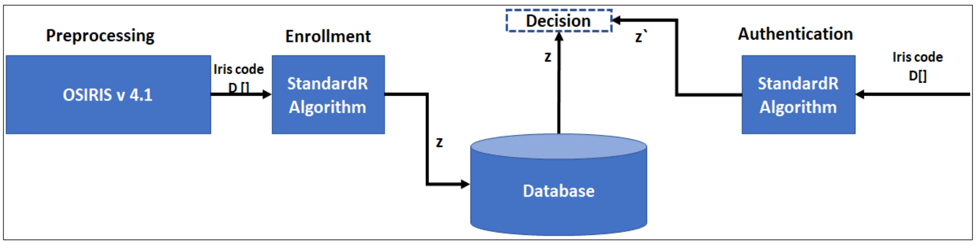

Figure 1. An architecture of BTP-based standardR

3.1. The preprocessing stage

The OSIRIS system, utilized for iris recognition and cited in [26], draws inspiration from the Daugman algorithm and consists of four processing sub-modules in its latest version 4.1. The initial module centers on segmentation, employing the Viterbi algorithm to distinguish boundaries and identify both the iris and pupil regions. Subsequently, Daugman’s rubber-sheet model, integrated with the Viterbi algorithm, is employed for normalization, precisely detecting coarse contours. In the final stage, 2D Gabor filters are applied to extract binary iris code images after encoding the transformed features in both real and imaginary parts. Figure 2 shows the utilizing of OSIRIS v4.1 for preprocessing stage. For comprehensive guidance on utilizing OSIRIS version 4.1, refer to the installation and configuration instructions provided in the system documentation. These instructions outline the steps necessary to effectively employ the system tools within the biometric reference system for iris recognition [27].

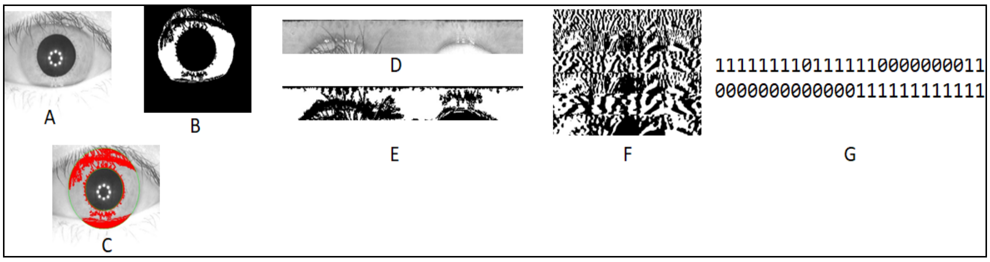

Figure 2. Iris preprocessing using OSIRIS v4.1, A: original iris image, B: mask, C: segmented iris, D: normalized iris, E: normalized mask, F: IrisCode, and G: Binary IrisCode

The resulting binary image undergoes the transformation into binary values based on a predetermined threshold, where pixel values equal to or exceeding the threshold (thr) are assigned 1, and those below are designated as 0. The conventional threshold value is set at 128 as shown in 1. After this, the converted iris code undergoes XOR operation with randomly generated keys, leading to the generation of decimal values stored in the array D[]. It is imperative to note that the threshold-based conversion and XOR operation introduce variability to the iris code, contributing to enhanced security and privacy protection, while simultaneously ensuring the renewability of the iris code generation in the event of loss or enrollment of a new user in the system.

$$P_i = \begin{cases} 0 & if\ Image\ Pixel\ [i] < thr = 128 \\ 1 & if\ ImagePixel\ \ [i] \geq thr = 128 \end{cases} \tag{1}$$

The assignment of values to the variable p_i based on the condition of the binary image pixel at index i. If the pixel value is less than 128, p_i is assigned the value 0; otherwise, if the pixel value is greater than or equal to 128, p_i is assigned the value 1.

3.2. The proposed standardR algorithm

The proposed standard rank algorithm assigns ranks to elements based on their sorted order in the input vector D[i]. Elements with the same value get the same rank, and the next rank is incremented by the number of tied elements. Algorithm 1 presents the proposed standardR algorithm pseudocode and Figure 3 presents the standardR algorithm flowchart, respectively. Let *D* be the input vector of the decimal values, and

x be the sorted vector of distinct elements from D. Then, the standard rank of the elements in $D[m]$, Let m=n is given by (2).

$$\text{Standard Rank}(D[m]) = \text{Position of } D[m] \text{ in vector } x + (\text{Number of tied elements before } D[i]) \quad (2)$$

The standardR algorithm offers a systematic method to assign standardized ranks to a given sequence of decimal values represented by the array *D*[]. The primary goal of this algorithm is to establish a consistent and uniform ranking scheme that accurately reflects the relative positions of the values within the sequence. The algorithm receives as input an array *D*[] containing decimal values. Each value in *D*[] is associated with an index i that ranges from 1 to n, where n represents the length of the set. The output of the algorithm is an array *Z*[], which holds the calculated standard ranks for each value in the set. The algorithm initiates the rank calculation process by creating an auxiliary array *x*[], which mirrors the values in the input array *D*[]. This copy facilitates the sorting and analysis of the values without altering the original set.

The subsequent step involves sorting the *x*[] array in non-decreasing order. This action allows for the identification of distinct values and their sequential arrangement, which is essential for determining their respective ranks. A pivotal aspect of the standard rank calculation involves addressing tied elements, which are values that occur more than once in the set. The algorithm introduces an unordered map named rank_map, which serves as a repository for the calculated ranks. Additionally, two integer variables are initialized: rank and count.

As the algorithm iterates through the sorted *x*[] array, the count variable increments with each step. The algorithm also checks for instances where the current element *x*[i] is not equal to the previous element *x*[*i*-1]. This verification identifies a transition from tied elements to a new set of values. Upon detecting such a transition, the algorithm increments the rank by the current value of count. This action effectively assigns the appropriate rank to the tied elements based on their grouping. The algorithm subsequently resets the count to 1, as it now pertains to the new set of tied elements. As the algorithm concludes the rank computation phase, it creates an empty array *Z*[], ready to accommodate the standardized ranks. For each index i in the range from 1 to n, the algorithm retrieves the rank associated with the corresponding value *D*[*i*] from the rank_map. This rank is then assigned to the respective position in the array *Z*[]. The standardized ranks generated by the algorithm embody an equitable and coherent ranking scheme for the input set. By considering the ordering of elements in the sorted array *x*[] and accounting for tied elements, the algorithm ensures that equivalent values share the same rank, and subsequent ranks are adjusted according to the number of tied elements. The resulting array *Z*[] encapsulates this standardized ranking scheme, making it invaluable for various analytical and comparative purposes.

Algorithm 1. The pseudocode of the standardR algorithm

```
Start
Input: D[]: An array of integers representing decimal values (i = 1 to n), where n is the
set length.
Output: Z[]: An empty array to store the standard ranks (1 to n) for each value in D[].
1. Create an array x[] with the same size as D[].
2. for i = 1 to n do
     2.1. x[i] = D[i]
    end for loop
3. Sort x[] in ascending order.
4. Create an empty unordered_map called rank_map.
5. Initialize an integer variable rank to 1.
6. Initialize an integer variable count to 0.
7. for i = 1 to n do
     7.1. count++
     7.2. if i > 1 and x[i] != x[i-1] then
         7.2.1. rank += count
         7.2.2. count = 1, reset count to 1
       end if condition
     7.3. rank_map[x[i]] = rank
   end for loop
8. Initialize an empty array Z[].
9. for i = 1 to n do
     9.1. Z[i] = rank_map[D[i]]
   end for loop
Output: Z[]
End
```

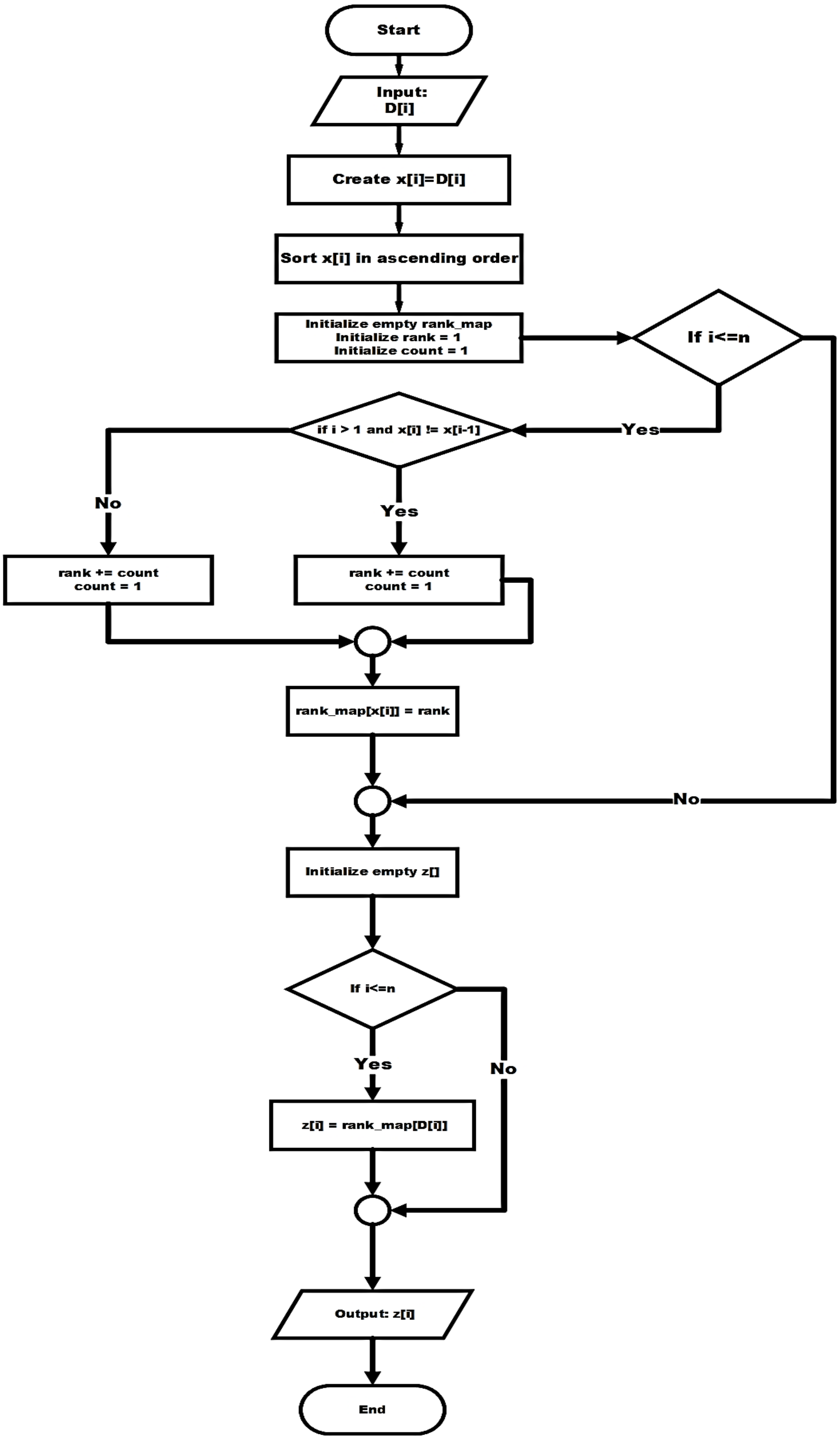

Figure 3. The flowchart of the proposed standardR algorithm

3.3. Decision stage

In the decision stage, also known as the matching phase, the objective is to calculate the similarity or dissimilarity by identifying the cumulative disagreements between any two corresponding pairs of converted iris codes, denoted as $z=z_1$ ......z_n and z_1^{-} ....z_n^{-}. The dissimilarity distance in the fundamental algorithm is determined in (3):

$$Dis(Z, Z^{-}) = \sum_{i=1}^{n} |Z_i - Z^{-}{}_i| \quad (3)$$

this formula computes the sum of absolute differences between individual elements Z_i and Z_i^-, providing a measure of dissimilarity for the given pair of iris codes. Manhattan distance [28], is calculated as the sum of the absolute differences between corresponding elements of two sets. Distance measure is used to quantify the dissimilarity between pairs of converted iris codes.

3.4. Performance metrics

Authentication accuracy can be measured using many parameters as following [8]:

a. GAR: the probability that a genuine user is correctly accepted. It is the complement of false rejection rate (FRR) and can be calculated in 4.

$$\mathrm{GAR} = 1 - FRR \tag{4}$$

Where: FRR is the probability that a genuine user is incorrectly rejected as an imposter. It is calculated as the number of false rejections (FR) divided by the total number of genuine attempts (GA) given by FRR = FR / GA.

b. False acceptance rate (FAR): The probability that an imposter is incorrectly accepted as a genuine user. It is calculated as the number of false acceptances (FA) divided by the total number of impostor attempts (IA). FAR can be calculated in 5.

$$\mathrm{FAR} = \mathrm{FA}/\mathrm{IA} \tag{5}$$

c. EER: The point at which FAR and FRR are equal. It represents a compromise between security and convenience. A lower EER indicates better system performance. GA and IA, and then use these values to compute FAR, FRR, and GAR. GA = TA + FR, IA = FA + TR

d. The receiver operating characteristic (ROC) curve is a graphical representation that illustrates the diagnostic ability of a binary classification system across various thresholds. It is created by plotting the true positive rate (Sensitivity) against the false positive rate (1-Specificity) at different threshold settings. The ROC curve provides a visual tool for assessing the trade-off between sensitivity and specificity.

e. The area under the ROC curve (AUC) is a quantitative measure of the classifier’s ability to distinguish between positive and negative classes.

f. Interclass correlation coefficient (ICC) or pearson correlation coefficient (PCC): measures a relation between two variables of different classes (types).

g. ICC: according to the Ronald fisher ICC is the quantitative measurements on the units which are organized into groups.

h. The irreversibility index serves as a valuable metric in gauging the efficacy of a protection technique in preventing the reversal of templates to their original state.

i. Time complexity of an algorithm is a measure of the amount of time it takes for the algorithm to complete as a function of the size of the input. It provides an estimate of the computational efficiency of the algorithm.

4. EXPERIMENT RESULTS AND DISCUSSION

This section provides an extensive account of our experiments, focusing on a meticulous comparison of results, particularly emphasizing various parameters concerning established literature indexing methods. A critical aspect of this study involves an in-depth analysis of the security implications associated with the proposed algorithm. For our evaluations, we utilized the benchmarked Casia-Iris-Interval iris dataset, which includes 249 subjects and 1,332 images of left irises. The primary emphasis centers on securing iris data, employing an advanced iris processing system OSIRIS-V4.1. This system is utilized for tasks such as iris localization, normalization, and the transformation of iris images into binary strings as presented in previous section.

Employing OSIRIS v4.1, we extracted iris codes and conducted rigorous testing. This process involved preprocessing and template generation using the standardR algorithm for both enrollment and matching stages. Our comprehensive approach ensures a robust examination of the algorithm’s performance against established benchmarks, contributing to a thorough evaluation of its security implications.

Upon acquiring the binary strings from iris images, our methodology proceeds to convert these strings into templates. For our experiments, we default to utilizing the Casia-IrisV3-Interval dataset with a specific focus on left-eye iris images. Notably, all iris strings undergo conversion into templates, yet only one template is selected as the enrolled data for the valid user in each test. The ensuing comparison involves evaluating each template against the chosen template. This process entails intraclass matching when comparing templates from the same user and interclass matching when comparing templates from different users against the chosen template. Each iris, in turn, is treated as the valid user during a test, with an iris image randomly chosen for enrollment. Additionally, application-specific strings, comprised of randomly generated binary strings with matching lengths to the iris strings, are introduced. Each test is iteratively conducted 30 times by default.

Upon completion of the processing for all irises, we derive the GAR, FAR, and EER as the primary metrics for evaluating the recognition performance. These metrics collectively provide a comprehensive assessment of the algorithm's effectiveness in distinguishing between genuine and false acceptance scenarios. The results of the standardR algorithm are presented in Table 1 for the Casia-Iris-Interval dataset, UBRIS 1, and MMU1, respectively. Furthermore, Figures 4 illustrates the ROC curves for the standardR algorithm with the Casia-Iris-Interval, UBRIS 1, and MMU 1 datasets, respectively.

Table 1. The performance results of the denser algorithm using Casia-Iris-Interval, UBRIS 1 and MMU1 datasets

Metric	Values of Casia-Iris-Interval	Values of UBRIS 1	Values of MMU 1
EER	0.1695	0.2349	0.2361
GAR at FAR = 0.1	0.8074	0.5759	0.5602
GAR at FAR = 0.01	0.7071	0.5627	0.5398
GAR at FAR = 0.001	0.6288	0.5313	0.5288
AUC	0.93011	0.6288	0.7071

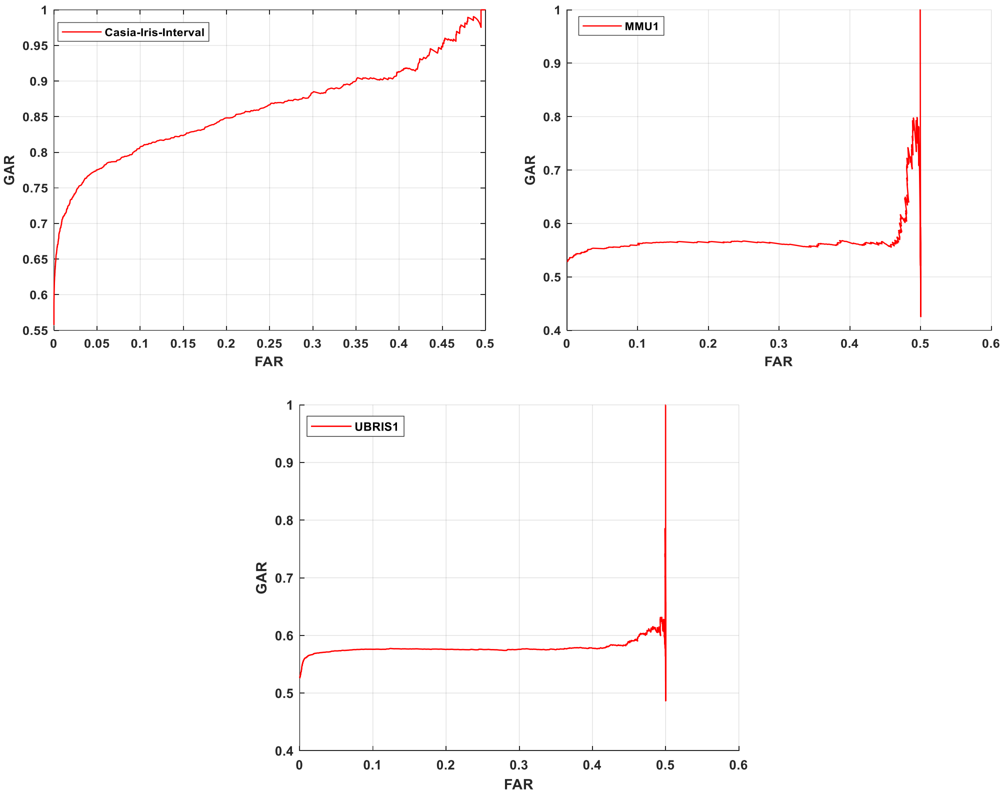

Figure 4. ROC of the standardR algorithm using Casia-Iris-Interval, UBRIS 1, and MMU 1 datasets

In Figure 5, the represented overlap area between intraclass and interclass kernel density estimation (KDE) curves, achieved through cross-matching, holds a calculated value of 0.9770. This substantial overlap indicates a scenario where an attacker, upon obtaining and attempting to reverse-engineer leaked iris templates to their original state, would face considerable difficulty in distinguishing between genuine and impostor templates. The high value of 0.9770 underscores the effectiveness of the applied protection technique, emphasizing the robust security and privacy measures in place for the biometric information contained within the iris templates. This feature reinforces the algorithm’s capability to resist template reversal, contributing to a strong defense against unauthorized access or malicious exploitation of sensitive biometric data.

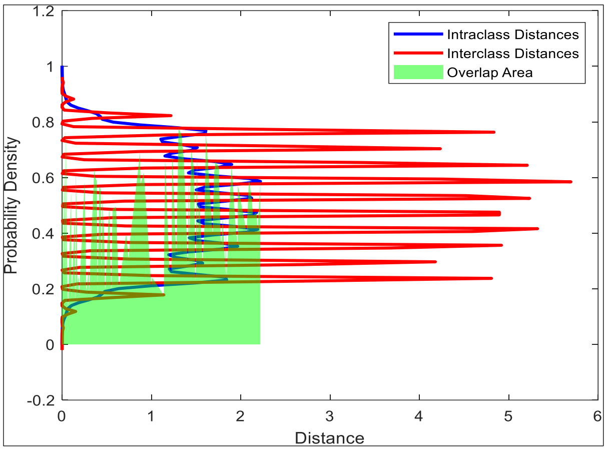

Figure 5. illustrates the overlap area between intraclass and interclass through cross-matching

An irreversibility value approaching 1 signifies robust security and privacy for biometric information, indicating the effectiveness of the applied protection technique. The irreversibility index is measured at 1.0180, indicating a robust level of security and privacy in the biometric information. A value exceeding 1 suggests a strong resistance to the reversal of templates to their original state, underscoring the effectiveness of the applied protection technique. The results of the standardR algorithm are meticulously compared with those of literature indexing methods, as detailed in Table 2. This comparative analysis offers comprehensive insights into the relative performance and effectiveness of the proposed algorithm in contrast to existing methodologies.

Table 2. Comparative analysis of results with literature indexing methods

Method	Dataset	EER (%)	Bit cost
[14]	Casia-Iris-Interval	1.32	1536
[16]	Casia-Iris-Interval	0.43	32768
[17]	Casia-Iris-Interval	0.97	9600
[18]	Casia-Iris-Interval	1.08	297000
standardR	Casia-Iris-Interval	0.1695	1280

The performance evaluation of the standardR algorithm across multiple datasets reveals its efficacy in iris recognition systems. The algorithm demonstrates robust results in terms of EER, GAR at different FAR, and AUC. The EER values for the Casia-Iris-Interval (0.1695%), UBRIS 1 (0.2349%), and MMU 1 (0.2361%) datasets indicate a high level of accuracy in distinguishing between genuine and impostor matches. The low EER values underscore the algorithm’s effectiveness in achieving a balance between false acceptance and false rejection rates. The GAR values at different FAR levels (0.1%, 0.01%, and 0.001%) demonstrate the algorithm’s ability to maintain high recognition rates while controlling false acceptance. Notably, the GAR remains consistently above 50%, even at stringent FAR levels, showcasing the algorithm's reliability in authenticating genuine users. The AUC value of 0.93011 for the Casia-Iris-Interval dataset affirms the algorithm’s strong classification performance.

In comparison with literature indexing methods (Table 2), the standardR algorithm consistently outperforms in terms of EER, showcasing its superiority in achieving a balance between false acceptance and false rejection. The algorithm’s bit cost of 1,280 bits is favorable in terms of computational efficiency, ensuring effective performance without excessive computational overhead. The ROC curves visually represent the trade-off between true positive and false positive rates, consistently exhibiting a desirable upward trend and confirming the algorithm’s discriminative power.

Moreover, the time complexity T(n) of the standardR algorithm in Algorithm 1 can be analyzed by considering the dominant factors that contribute to the overall running time. The standard algorithm could be break down the algorithm step by step:

- Creating the array x[] (Lines 1-2): the T(n): *O(n)*, a linear loop that iterates through each element of D[] and copies it to the array x[]. The loop runs for n iterations, where n is the length of the array D[].
- Sorting the array x[] (Line 3):the T(n): *O(n log n)*, sorting the array x[] is the most time-consuming operation. Standard sorting algorithms like quicksort or mergesort have an average time complexity of *O(n log n).*
- Creating the unordered_map rank_map (Line 4): T(n): *O(1)*, creating an empty unordered_map is a constant time operation.
- Calculating ranks and populating rank_map (Lines 5-7): T(n): *O(n)*, another linear loop that iterates through the sorted array x[] and assigns ranks to distinct elements. The loop runs for n iterations.
- Creating the array Z[] (Lines 8-9): T(n): *O(n)*, a linear loop that iterates through each element of D[] and assigns the corresponding rank from rank_map to the array Z[]. The loop runs for n iterations.

The overall time complexity is dominated by the sorting operation, so the total time complexity of the algorithm is *O(n log n)*, where n is the length of the array D[].

$$T(n) = (logT(n) = O(n) + O(nlogn) + O(1) + O(n) + O(n) = O(nlogn)$$

The sorting operation is the most significant factor, and other operations contribute linearly or with constant time complexities.

Furthermore, the algorithm’s robust performance across diverse datasets, including Casia-Iris-Interval, UBRIS 1, and MMU 1, underscores its adaptability and generalization capabilities. Consistent performance across datasets indicates the algorithm’s potential for real-world applications and its resilience to variations in iris images. The standardR algorithm exhibits strong performance across various metrics and datasets, positioning itself as a reliable and effective solution for iris recognition. The balance between accuracy, efficiency, and adaptability makes it a promising candidate for practical deployment in secure authentication systems.

5. CONCLUSION AND FUTURE WORKS

In conclusion, the proposed StandardR algorithm represents a significant stride in advancing iris template protection for biometric recognition systems. Successfully meeting the main objective of enhancing security while preserving recognition accuracy, the algorithm, employing a cancelable approach grounded in standardR, transforms iris templates into irreversible representations, surpassing the limitations of indexing BTP methods. Comprehensive experimental evaluations across benchmarked datasets-Casia-Iris-Interval, UBRIS 1, and MMU 1-underscore the algorithm’s exceptional performance, achieving an EER of 0.1695% and an AUC of 0.93011% for the Casia-Iris-Interval dataset.

Furthermore, the algorithm’s adaptability and generalization across diverse datasets are evident in consistent performance. The meticulous balance between false acceptance and rejection rates, exemplified by high GAR at different FAR levels, positions the algorithm as a reliable and secure solution for iris recognition. This research not only offers a promising resolution to current challenges in iris template protection but also lays the foundation for ongoing advancements in biometric recognition technology, fostering a more secure and reliable authentication landscape. Key features include a reduced iris code length of 1,280 bits and optimized time complexity $O(nlogn)$. In analyzing the results, the significance of time complexity underscores the algorithm’s efficiency. Additionally, the combined emphasis on irreversibility and unlinkability is integral to fortifying the algorithm’s robust security measures. The measured IR value of 1.0180 signifies a robust resistance to the reversal of templates to their original state, while the substantial overlap area of 0.9770 between intraclass and interclass achieved through cross-matching, underscores the algorithm’s efficacy in resisting template reversal and enhancing security against unauthorized access or malicious exploitation of sensitive biometric data. Looking ahead, future work will focus on integrating the standardR algorithm with cutting-edge technologies in edge computing, with specific attention to incorporating additional biometric modalities.

ACKNOWLEDGEMENTS

Authors acknowledge the Fundamental Research Grant Scheme (FRGS) grant number FRGS/1/2019/ICT03/UTM/02/3 funded by the Ministry of Higher Education (MOHE), Malaysia. Also, we extend our heartfelt appreciation to Dr. Jianwen Xiang and Dr. Dongdong Zhao of Wuhan University of Technology for their invaluable guidance, insightful suggestions, and unwavering support.

REFERENCES

[1] R. D. Labati, V. Piuri, and F. Scotti, "Biometric privacy protection: guidelines and technologies," In *E-Business and Telecommunications: International Joint Conference, ICETE 2011*, 2011, pp. 3-19.

[2] A. Hameed, Y. Mohammed, R. A. Dziyauddin, and L. A. Latiff, "Current multi-factor of authentication: approaches, requirements, attacks and challenges," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, pp. 166–178, Feb. 2023, doi: 10.14569/IJACSA.2023.0140119.

[3] L. Masek, "Recognition of human iris patterns for biometric identification," Journal of Engineering and Applied Science-Cairo, vol. 54, no. 6, p. 635, 2003.

[4] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004, doi: 10.1109/TCSVT.2003.818350.

[5] S. K. S. Modak and V. K. Jha, "Multibiometric fusion strategy and its applications: a review," *Information Fusion*, vol. 49, no. January 2018, pp. 174–204, 2019, doi: 10.1016/j.inffus.2018.11.018.

[6] 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, no. May, pp. 45563–45582, 2019, doi: 10.1109/ACCESS.2019.2908456.

[7] S. D. Patil *et al.*, "Robust authentication system with privacy preservation of biometrics," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/7857975.

[8] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega, "A review on protection and cancelable techniques in biometric systems," *IEEE Access*, vol. 11. Institute of Electrical and Electronics Engineers Inc., pp. 8531–8568, 2023. doi: 10.1109/ACCESS.2023.3239387.

[9] M. J. Lee, Z. Jin, S. N. Liang, and M. Tistarelli, "Alignment-robust cancelable biometric scheme for iris verification," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3449–3464, 2022, doi: 10.1109/TIFS.2022.3208812.

[10] M. Osadchy and O. Dunkelman, "It is all in the system's parameters: privacy and security issues in transforming biometric raw data into binary strings," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 5, pp. 796–804, Sep. 2019, doi: 10.1109/TDSC.2018.2804949.

[11] V. Subha and Mariammal G, "Comparative analysis of palmprint matching techniques for person identification," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, [Online]. Available: www.ijarcs.info.

[12] M. Statistician, E. Applications, M. K. Nalini, and K. R. Radhika, "Article info page number," *Publication Issue*, vol. 71, pp. 1797–1804, 2022, [Online]. Available: http://philstat.org.ph

[13] D. Keller, M. Osadchy, and O. Dunkelman, "Fuzzy commitments offer insufficient protection to biometric templates produced by deep learning," *arXiv preprint arXiv*, Dec. 2020, [Online]. Available: http://arxiv.org/abs/2012.13293

[14] D. Zhao, S. Fang, J. Xiang, J. Tian, and S. Xiong, "Iris template protection based on local ranking," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/4519548.

[15] O. Ouda, "On the practicality of local ranking-based cancelable iris recognition," *IEEE Access*, vol. 9, pp. 86392–86403, 2021, doi: 10.1109/access.2021.3089078.

[16] R. Dwivedi, S. Dey, R. Singh, and A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping," *Computers and Security*, vol. 65, pp. 373–386, Mar. 2017, doi: 10.1016/j.cose.2016.10.004.

[17] J. Y. Jeong and I. R. Jeong, "Efficient cancelable iris template generation for wearable sensors," *Security and Communication Networks*, vol. 2019, 2019, doi: 10.1155/2019/7473591.

[18] T. Y. Chai, B. M. Goi, and W. S. Yap, "Towards better performance for protected iris biometric system with confidence matrix," *Symmetry (Basel)*, vol. 13, no. 5, 2021, doi: 10.3390/sym13050910.

[19] X. Dong, Z. Jin, A. B. J. Teoh, M. Tistarelli, and K. Wong, "On the security risk of cancelable biometrics," *arXiv preprint arXiv*, 2019.

[20] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," *Journal of Information Security and Applications*, vol. 58, p. 102704, 2021, doi: 10.1016/j.jisa.2020.102704.

[21] X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems, BTAS 2019*, 2019, doi: 10.1109/BTAS46853.2019.9185997.

[22] B. Z. H. Zhao, H. J. Asghar, and M. A. Kaafar, "On the resilience of biometric authentication systems against random inputs," *arXiv e-prints*, no. February, 2020, doi: 10.14722/ndss.2020.24210.

[23] "Center for biometrics and security research national laboratory of pattern recognition institute of automation, Chinese academy of sciences." Accessed: Dec. 06, 2023. [Online]. Available: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp

[24] "MultiMedia University Iris database for biometric attendance system." Accessed: Dec. 06, 2023. [Online]. Available: http://pesonna.mmu.edu.my/ccteo/

[25] "SOCIA Lab. - Soft Computing and Image Analysis Group Department of Computer Science, University of Beira Interior." Accessed: Dec. 06, 2023. [Online]. Available: http://p-destre.di.ubi.pt/

[26] N. Othman, B. Dorizzi, and S. Garcia-Salicetti, "OSIRIS: an open source iris recognition software," *Pattern Recognition Letters*, vol. 82, pp. 124–131, 2016, doi: 10.1016/j.patrec.2015.09.002.

[27] O. Nadia, G. Sutra, D. *Bernardette, Garcia-Salicetti, Sonia, "A biometric reference system for iris OSIRIS version 4.1" BioSecure project, Telecom Sud Paris, 2013.*

[28] A. Golovanov, A. Kupavskii, and A. Sagdeev, "Odd-distance and right-equidistant sets in the maximum and Manhattan metrics," *European Journal of Combinatorics*, vol. 107, Jan. 2023, doi: 10.1016/j.ejc.2022.103603.

BIOGRAPHIES OF AUTHORS

Mohammed Ali Hameed Yassir holds a Master's degree in Computer Internetworking from Universiti Teknikal Malaysia Melaka (UTeM) and a Bachelor's degree from the College of Engineering. Currently, he is pursuing a Ph.D. at the Razak Faculty of Technology and Informatics, University Technology Malaysia (UTM). His research interests encompass image/signal processing, biometrics, edge computing, and pattern recognition. He can be contacted at email: ali-1984@graduate.utm.my.

Rudzidatul Akmam Dziyauddin is a highly accomplished academic and researcher specializing in the field of Wireless Communication Networks. As a Senior Lecturer at Universiti Teknologi Malaysia, Kuala Lumpur, she has been actively involved in shaping the academic landscape. Her expertise extends to areas such as Radio Resource Management, Vehicle/UAV Edge Computing, Machine Learning in IoT, and Energy Harvesting in Wireless Sensor Networks. Dr. Rudzidatul holds a Ph.D. in Electrical & Electronic Engineering from the University of Bristol, United Kingdom, with a thesis focus on the Quality of Service in WiMAX Network. Her dedication to research and innovation is evident in her various roles, including a Visiting Researcher Scientist at Nanyang Technology University (NTU) and a Research Engineer at Toshiba Research Europe Limited (TREL), Bristol, United Kingdom. With an illustrious career spanning over a decade, Dr. Rudzidatul has significantly contributed to academic committees, research management, and curriculum development, showcasing her leadership and commitment to academic excellence. Her international engagements, such as serving as a Committee Member in various conferences and editorial boards, highlight her global impact and recognition in the academic community. Dr. Rudzidatul's multifaceted contributions and continuous involvement in cutting-edge research underscore her as a prominent figure in the field of wireless communication networks. She can be contacted at email: rudzidatul.kl@utm.my.

Norshaliza Binti Kamaruddin holds a B.S. degree in Information Technology from Universiti Utara Malaysia, an M.S. degree in Computer Science, and a Ph.D. degree in Image Processing from the University of Malaya, obtained in 2003 and 2016, respectively. With a robust academic background, she served as a Lecturer in various private universities in Malaysia from 2001 to 2018. In 2019, Dr. Norshaliza joined Universiti Teknologi Malaysia as a Senior Lecturer. Her current research pursuits are focused on mental health issues using text analysis and real-time series data employing machine learning techniques. As of July 3, 2023, her research interests span across image processing, machine learning, and artificial intelligence. Driven by a commitment to advancing knowledge and addressing contemporary challenges, Dr. Norshaliza is a dedicated academic contributing significantly to the field of technology and informatics. She can be contacted at email: norshaliza.k@utm.my.

Norulhusna Ahmad is affiliated with the Ubiquitous Broadband Access Network (U-BAN) Research Group at the Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM), located in Kuala Lumpur. She obtained her B.Sc. degree in electrical engineering, followed by master's and Ph.D. degrees in electrical engineering, all from UTM, in 2001, 2003, and 2014, respectively. Beginning her journey at UTM as a staff member, Dr. Ahmad has evolved into her current role as a Lecturer at the Razak Faculty of Technology and Informatics. Her diverse research portfolio encompasses future wireless communication systems, massive Internet of Things (IoT) technologies, UAV communication, deep learning applications, multiple access techniques, and image processing. Recognized as a Professional Technologist by the Board of Technologists Malaysia, she is also a Graduate Member of the Institute of Engineers Malaysia (IEM) and the Board of Engineers Malaysia (BEM). Dr. Norulhusna Ahmad's commitment to advancing technology is evident through her contributions to various domains, from telecommunications to artificial intelligence and beyond. She can be contacted at email: norulhusna.kl@utm.my.