Cancelable Iris Template Generation using Weber Local Descriptor and Median Filter Projection

Ilaiah Kavati
Department of Computer Science & Engineering
National Institute of Technology Warangal
India - 506004
ilaiahkavati@nitw.ac.in

Venkatesh Akula
Department of Computer Science & Engineering
National Institute of Technology Warangal
India - 506004
avenkatesh@student.nitw.ac.in

Erukala Suresh Babu
Department of Computer Science & Engineering
National Institute of Technology Warangal
India - 506004
esbabu@nitw.ac.in

Ramalingaswamy Cheruku
Department of Computer Science & Engineering
National Institute of Technology Warangal
India - 506004
rmlswamy@nitw.ac.in

***Abstract*—In recent years, the growing use of biometric recognition systems in various applications has increased the need to protect the biometric templates recorded in multiple databases. Due to their consistency and uniqueness, iris recognition systems have significantly outperformed other biometrics. Directly stored Iris templates on a central server constitute a privacy and security risk. To address this, we will generate a cancelable template that can be stored instead of the original. In the event of a security breach, we will discard the stored template and generate a new iris template. This research employs the Weber Local Descriptor (WLD) technique to create a multi-instance iris biometric system. Left and right iris images are initially acquired and normalized using the USIT toolkit. We generate a feature vector from the normalized image using WLD. The obtained feature vector is then normalized using L1 normalization. The vector of normalized features is then projected onto a median filter to generate a cancelable template. Experiments are conducted on the IIT Delhi iris database, and the results are optimistic compared to previously published research.**

***Index Terms*—Biometrics, Iris, Template Protection, Weber Descriptor, Security**

I. Introduction

Biometric recognition systems outperform traditional token-based and knowledge-based authentication methods such as passwords and PINs. The iris is the most frequently used biometric due to its uniqueness and dependability among all biometric characteristics. Even in identical twins, the essence of the iris results from its morphogenesis, which occurs during the seventh month of gestation. The body's systems maintain these texture patterns over a person's lifetime. Due to the unpredictability of the iris pattern, it is exceedingly uncommon to forge or copy a person's iris pattern. Iris recognition identifies individuals based on patterns in the innermost circular area encompassing the eye's pupil.

However, the threat to stored and in-transit iris templates has increased with iris recognition systems in various applications. This necessitates protecting these templates from unauthorized access and regenerating them in the event of fraudulent activity, similar to how we generate new credentials and passwords in case of a compromise [1]. To accomplish this, the original iris image is converted into a cancelable iris template, which is irreversible. If this stored template is lost or compromised, our algorithm will generate a new template for the iris.

This work utilized the Weber Local Descriptor (WLD) proposed by Jie Chen et al. [2]. WLD is a new feature-discriminative descriptor derived from Weber's Law, founded on human perception. By capturing both differential excitations and orientations at specified points, organized WLD characteristics are used to generate a histogram. Arnab Banerjee et al. comprehensively evaluated numerous image classification techniques based on WLD [3]. Their report demonstrated WLD's theory, principles, characteristics, and resistance to noise, rotational changes, illumination changes, and scale variations compared to Local Binary Patterns(LBP), Scale Invariant Feature Transform (SIFT), Speed Up Robust Features (SURF), etc. The WLD's computation is considerably quicker than SIFT and SURF and comparable to LBP.

II. Related Work

Recently, cancelable biometric recognition technology has gained interest from researchers, resulting in the development of several robust algorithms [4]. Gurjit Singh Walia et al. presented a multimodal biometric system based on real-time Deep Feature Unification to achieve high performance while protecting against attacker threats [5]. The suggested key-based generic feature extraction approach ensures revocability by generating a dimensionally reduced feature from any type and dimension of the modality. As a result of this, the suggested system has low computational and space requirements. The Query Deep Features are randomly projected onto the key deep Features, resulting in non-invertible and resilient cancelable templates.

Ajish S et al. provides a double-bloom filter-based iris feature transformation that exponentially reduces the size of the converted iris template [6]. A double-bloom filter-based feature transformation improves the data compression ratio, template protection, matching response time, and matching

979-8-3503-0219-6/23/$31.00 ©2023 IEEE

accuracy. The double bloom filter minimizes the size of the converted iris template while increasing the quality.

Avantika Singh et al. propose a re-enrollable cancelable iris biometric authentication system that stores a transformed version of the original iris template [7]. A novel deep architecture based on aggregate learning was presented for extracting discriminative iris characteristics. The use of ordinal measurements in this work allows a good representation of unique iris features. Biohashing and $2N$ discretized BioPhasor are used to preserve the iris characteristics.

Marta Gomez-Barreroa et al. present a basic methodology for assessing unlinkability in biometric template protection techniques and an enhanced, unlinkable, and irreversible Bloom filter-based system [8]. The suggested approach is demonstrated to preserve the unprotected system's biometric performance. Furthermore, in adversary models where potential attackers have access to protected biometric templates and secret credentials, cross-matching resistance is accomplished in the presence of current attacks.

Mahesh Kumar Morampudi et al. [9] propose secure iris authentication technology based on the classification. To achieve privacy-preserving (PP), they used the Nearest Neighbor and Multi-class Perceptron model for training and classification. The fully homomorphic technique ensures the iris templates' anonymity, and the aggregate verification vector helps verify the computed classification result. Experimental results on benchmark iris databases show that this method gives iris templates security without sacrificing accuracy.

The rest of the paper is organized as follows: Section 3 describes the proposed method of enrolling the cancelable iris templates into the database and how authentication will be performed in the transformed domain. The experimental setup and results are discussed in Section 4, along with the comparative, security, and computational analyses. The concluding remarks are given in Section 5.

III. Proposed Methodology

This section outlines the proposed architecture and its implementation on a benchmark dataset. The proposed system consists of two fundamental phases: registration and authentication.

A. Registration

Fig. 1 depicts the enrollment system being proposed. Initially, the iris is captured and preprocessed, and a WLD-generated feature vector is created. Using L1 normalization, the extracted feature template is normalized column-by-column and row-by-row. In addition, the normalized template is projected to a 2D median filter to achieve total irreversibility, and the resulting cancellable template is saved in the database.

1) Image Prepossessing : The user's right and left iris images are captured and preprocessed. The iris region is then normalized using the University of Sazalburg Iris-Toolkit (USIT), which implements Daughman's rubber sheet model. Fig. 2 depicts the normalized and preprocessed iris.

2) Weber Local Descriptor(WLD): According to the nineteenth-century theory of Ernest Weber, the ratio between the increment threshold and background intensity is constant.

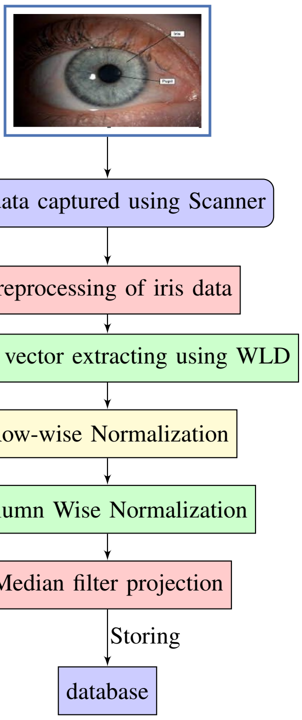

Iris data captured using Scanner
Preprocessing of iris data
Feature vector extracting using WLD
Row-wise Normalization
Column Wise Normalization
Median filter projection
Storing
database

Fig. 1. Enrollment Phase

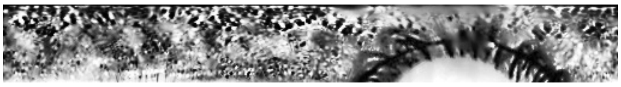


Fig. 2. Preprocessed and Normalized Iris Image

Since then, this relationship has been referred to as Weber's Law and is depicted as follows:

$$\frac{\delta I}{I} = k \tag{1}$$

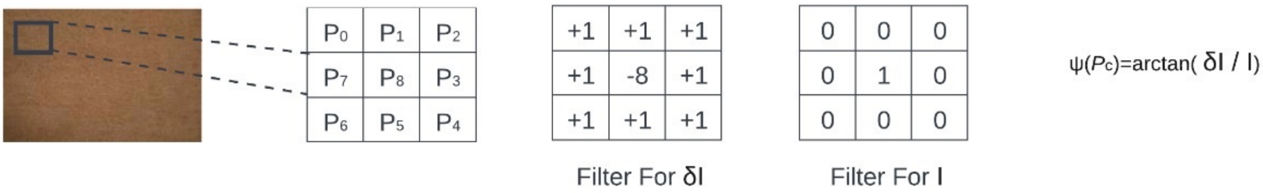
where δI represents the increment threshold (just a noticeable difference for discrimination); I represents the initial stimulus intensity, and k signifies that the proportion on the left side of the equation remains constant despite variations in the I term. Jie Chen et al. [2] state that Webber Local Descriptor (WLD) performs better than Local Binary Pattern (LBP) [10] and Scale Invariant Feature Transform (SIFT) [11].

WLD is formed using the differential excitation and orientation concepts. The small variation within an image can be computed by considering the intensity difference (δI) between the neighboring pixels and expressed as follows:

$$\delta I = \sum_{x=0}^{i-1} (I(p_x) - I(p_c)) \tag{2}$$

where $I(p_c)$ represents the intensity of current pixel, $I(p_x)$ represents the intensity of the neighbored pixels and i represents total number of neighbors in a region. The differential excitation $\psi(p_c)$ for the current pixel can be expressed as follows:

$$\psi(p_c) = arctan\left(\frac{\delta I}{I}\right) = arctan\left(\sum_{x=0}^{i-1} \frac{((I(p_x) - I(p_c)))}{(I(p_x))}\right) \tag{3}$$



P_0	P_1	P_2
P_7	P_8	P_3
P_6	P_5	P_4

+1	+1	+1
+1	-8	+1
+1	+1	+1

Filter For δI

0	0	0
0	1	0
0	0	0

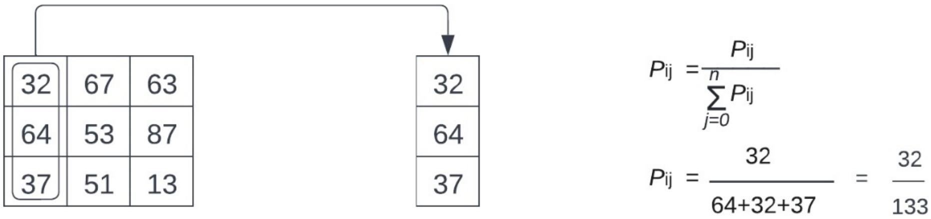
Filter For I

Fig. 3. Differential Excitation Illustration [12]

32	67	63
64	53	87
37	51	13

$$\psi(P_c) = \frac{(32 - 53) + (67 - 53) + \dots\dots\dots + (64 - 53)}{53} = -\frac{10}{53} = -0.188$$

Fig. 4. Computation of Differential Excitation [12]



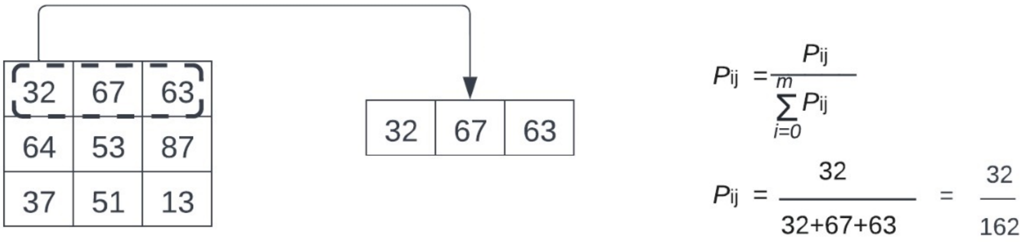
32	67	63
64	53	87
37	51	13

32
64
37

$$P_{ij} = \frac{P_{ij}}{\sum_{j=0}^{n} P_{ij}}$$

$$P_{ij} = \frac{32}{64+32+37} = \frac{32}{133}$$

Fig. 5. Row-wise L1 Normalization



32	67	63
64	53	87
37	51	13

32	67	63

$$P_{ij} = \frac{P_{ij}}{\sum_{i=0}^{m} P_{ij}}$$

$$P_{ij} = \frac{32}{32+67+63} = \frac{32}{162}$$

Fig. 6. Column Wise L1 Normalization

The process of computing differential excitation $\psi(p_c)$ for the current pixel in a 3×3 neighborhood is shown in Fig. 3 and Fig. 4, respectively. This process is repeated for all the pixels of the image.

3) Cancelable Template Generation: After extracting the feature vector using WLD, a cancelable template is generated

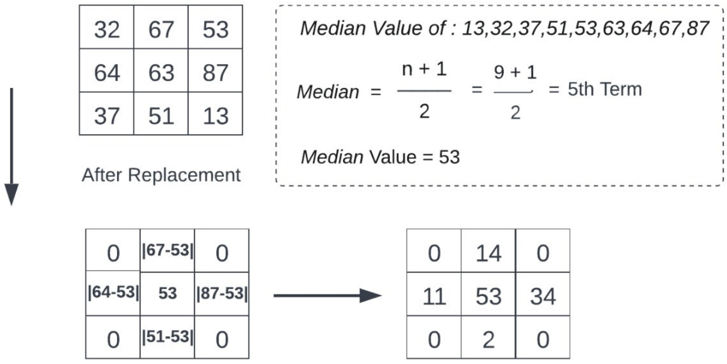


Fig. 7. Median Filter Projection

by row- and column-wise normalizing the feature vector using L1 normalization, as depicted in Fig. 5 and Fig. 6. Then, the normalized feature vector is projected to the median filter to achieve irreversibility property (Fig. 7).

B. Authentication Phase

The query iris image is subjected to several phases: preprocessing, feature extraction, and cancelable template generation and matching. Using Hamming distance, the query input template is matched to the previously stored template (Fig. 8). The Hamming distance is compared to a predetermined threshold to determine whether the input query is genuine or fraudulent.

IV. Results and Experimental Setup

We used the IIT Delhi Iris Database (Version 1.0) to test the effectiveness of our proposed technique. This dataset contains 2240 images covering 224 different subjects. Each subject has ten images (five right and five left eyes). All subjects in the database are between the ages of 14 and 55, with 48 girls and 176 males. These images have a resolution of 320 x 240 pixels. Out of ten images (five on the left and five on the right), eight images (four on the left and four on the right) are used to enroll four cancelable templates, and the remaining two images (one on the left and one on the right) are used for authentication. The experiment is carried out with the help of PYTHON 3.9.5, and the machine specifications are shown in Table I.

TABLE I
Machine Specification

Manufacturer	Apple
Model	FVFYK4UZJ1WK
Hard Drive	1600 MHz DDR3
RAM	8 GB
Processor	1.8 GHz Dual-Core intel Core i5
System type	64 bit
Operating System	macOS Monterey

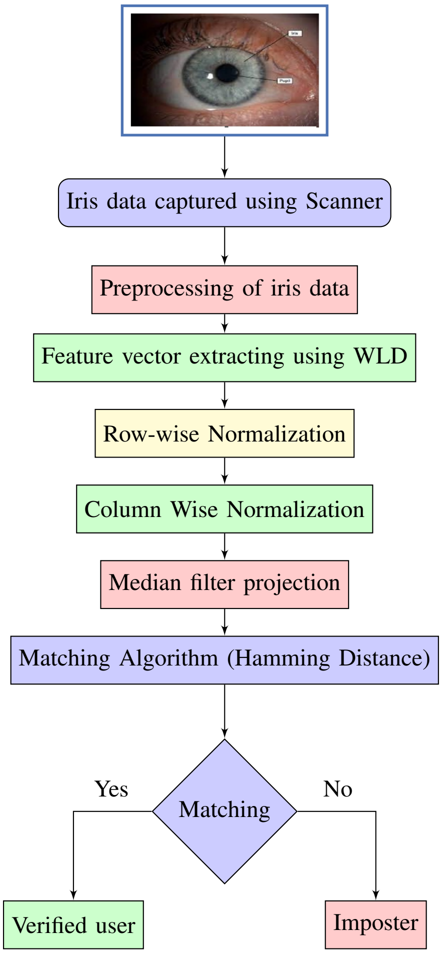

Iris data captured using Scanner
Preprocessing of iris data
Feature vector extracting using WLD
Row-wise Normalization
Column Wise Normalization
Median filter projection
Matching Algorithm (Hamming Distance)
Matching
Yes
No
Verified user
Imposter

Fig. 8. Authentication Phase

A. Performance Metrics

The following evaluation metrics are used to assess the performance of the proposed system: The False Acceptance Rate (FAR), the False Rejection Rate (FRR), and the Equal Error Rate (EER). The process of computing FAR and FRR are given in Equation 4 and Equation 5, respectively.

$$FAR = \frac{\text{Number of successful imposter attempt}}{\text{Total number of imposter attempt}} \tag{4}$$

$$FRR = \frac{\text{Number of unsuccessful genuine attempt}}{\text{Total number of genuine attempt}} \tag{5}$$

Finally, the Equal Error Rate (EER) is the point at which the false acceptance rate (FAR) and false rejection rate (FRR) are equal. An ideal biometric system should have low EER.

B. Experimental Results

The experimental results on the left Iris and right Iris datasets are shown in Fig. 9 and Fig. 10, respectively. It can be observed that as the Threshold increases, false rejections decrease and false acceptances increase. Further, the Equal Error Rate for the left Iris and right Iris datasets is 0.14% and 0.12%, respectively. To decrease the error rate further, we fused the left iris and right iris images. It can be observed that from Fig. 11, the fusion results in a lesser error rate (0.08%) of the system. We can also observe from Fig. 12 that, for the fusion method, both the error rates (FAR and FRR) are less compared to individual methods.

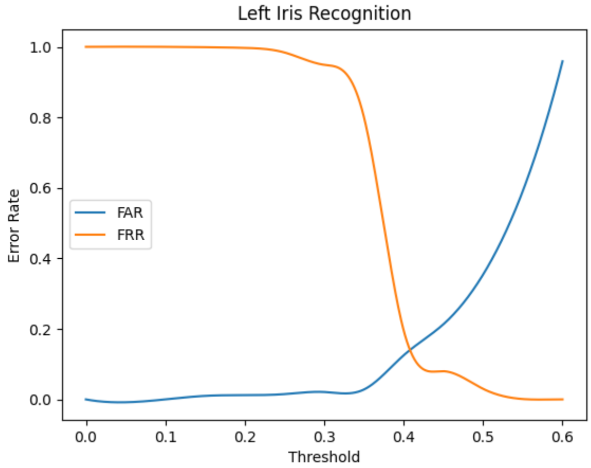


Fig. 9. Threshold vs FAR/FRR for Left Iris dataset

C. Security Analysis

1) Irreversiblity: In the experiment, the irreversibility of the feature vector is achieved using L1 normalization and median filter projection on the extracted feature vector. In [12], the feature vector is unprotected and stored in its original form, which is subjected to a high risk of unauthorized access.

2) Non Invertibility: Noninvertibility of the system is achieved by projecting the median filter on the extracted feature vector. The median filter alters the pixel intensity values by replacing the center pixel with the median value. To retrieve the original vector, unauthorized users need to know the exact neighboring values of the center pixel.

3) Revocability: Revocabilty refers to the fact that even in hacking or data loss, the newly generated templates have no relation with the lost one. In this study, even if a new template is generated from the same iris, it will ultimately differ from the existing one as the neighborhood size is selected randomly.

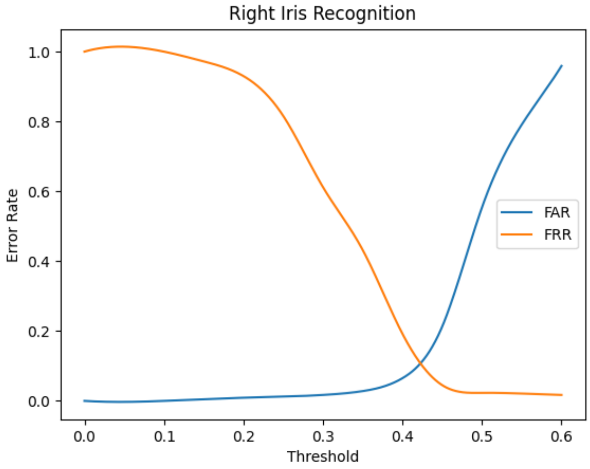


Fig. 10. Threshold vs FAR/FRR for Right Iris dataset

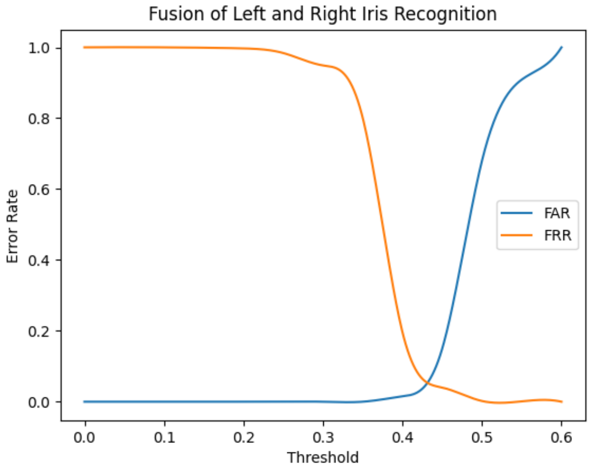


Fig. 11. Threshold vs. FAR/FRR for fused Iris dataset

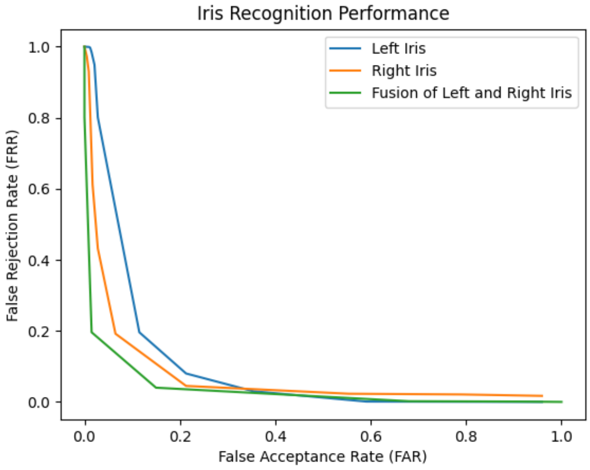


Fig. 12. FAR vs. FRR for Left Iris, Right Iris, and fusion of both

V. Conclusion

The IIT Delhi database evaluates a method for cancelable template protection for multi-instance iris biometrics.

Extracted the feature vector using Weber Local Descriptor, further normalized it for irreversibility, and then projected it to the median filter for cancelable template generation. The model also achieved lesser error rates without compromising the security of the biometric templates. In the future, this preliminary work will extend to other benchmark datasets with thorough analysis.

References

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

[2] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikäinen, X. Chen, and W. Gao, "Wld: A robust local image descriptor," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, no. 9, pp. 1705–1720, 2009.

[3] A. Banerjee, N. Das, and K. Santosh, "Weber local descriptor for image analysis and recognition: a survey," *The Visual Computer*, pp. 1–23, 2022.

[4] I. Kavati, G. K. Kumar, M. V. Gopalachari, E. S. Babu, R. Cheruku, and V. D. Reddy, "Non-invertible cancellable template for fingerprint biometric," in *International Conference on Hybrid Intelligent Systems*, pp. 615–624, Springer, 2021.

[5] G. S. Walia, K. Aggarwal, K. Singh, and K. Singh, "Design and analysis of adaptive graph-based cancelable multi-biometrics approach," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 54–66, 2020.

[6] S. Ajish and K. AnilKumar, "Iris template protection using double bloom filter based feature transformation," *Computers & Security*, vol. 97, p. 101985, 2020.

[7] A. Singh, A. Arora, and A. Nigam, "Cancelable iris template generation by aggregating patch level ordinal relations with its holistically extended performance and security analysis," *Image and Vision Computing*, vol. 104, p. 104017, 2020.

[8] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Information Sciences*, vol. 370, pp. 18–32, 2016.

[9] M. K. Morampudi, M. V. Prasad, M. Verma, and U. Raju, "Secure and verifiable iris authentication system using fully homomorphic encryption," *Computers & Electrical Engineering*, vol. 89, p. 106924, 2021.

[10] J. Chen, V. Kellokumpu, G. Zhao, and M. Pietikäinen, "Rlbp: Robust local binary pattern.," in *BMVC*, 2013.

[11] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, pp. 91–110, 2004.

[12] V. Bharadi, D. Shah, N. Thapa, B. H. Pandya, and G. Cosma, "Multi-instance iris recognition," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 1–6, IEEE, 2018.