EasyChair Preprint

№ 11568

Biometric Authentication Using Invariant Gray Level Co-Щccurrence Matrices (GLCM)

Mokhtari Aicha and Hadj Slimane Zine-Eddine

December 19, 2023

Biometric Authentication Using Invariant Gray Level Co-occurrence Matrices (GLCM)

Mokhtari Aicha

Biomedical Engineering Department

Faculty of Technology

University of Abou Bekr Belkaid

Tlemcen 13-000, Algeria

aicha.mokhtari@univ-tlemcen.dz

Hadj Slimane Zine Eddine

Biomedical Engineering Department

Faculty of Technology

University of Abou Bekr Belkaid

Tlemcen 13-000, Algeria

zineeddine.hadjslimane@univ-tlemcen.dz

***Abstract*— Biometric authentication plays a crucial role in ensuring security, access control and identity verification, with applications in various sectors and contexts. Biometric authentication in the context of access control is a resilient security technique employed to oversee and manage entry to physical locations, digital platforms, or valuable assets. It verifies the identities of individuals by assessing their distinct biological or behavioral attributes. This approach ensures that it enhances security and accountability by granting access only to authorized individuals. This article introduces an authentication method centered on retinal images, enhancing security levels through the utilization of the Invariant Gray Level Co-occurrence Matrices (GLCM) technique for feature extraction and employing a Random Forest classifier for classification. Our evaluation, conducted on the RIDB database, yielded highly favorable results, achieving a flawless accuracy of 100%.**

***Keywords*——Authentication, retina, GLCM, Random Forest.**

I. INTRODUCTION:

Advances in information and communication technologies (ICT) open wider doors to the accessibility of information and knowledge, resulting in a significant transformation of the institutional framework of society. Digital platforms, services and technologies have transformed societies into interconnected ecosystems, facilitating monitoring, data collection and analysis. Globalization and the rapid pace of change accelerate this development, affecting various aspects of public life and disrupting traditional norms.

Innovation is exponentially growing and driving an increase in the speed of technological advancements. These advancements include new technologies like the Internet of Things, artificial intelligence, biometric authentication, and other digital technologies.

Biometric authentication is an access control and management system.

This system ensures security and controls the entry and exit of premises or territory.

Biometric authentication involves the verification or identification of individuals through their distinct physical or behavioral attributes. This method ensures secure access control and identity verification by leveraging unique biological traits that are challenging to duplicate or counterfeit.

These systems analyze and compare specific features such as fingerprints, iris or retinal patterns, facial characteristics, voiceprints, or behavioral traits like typing patterns or gait. The collected biometric data is securely stored in a database or on a device for future reference.

When someone seeks access to a system, facility, or device, the system compares their biometric information to the stored data to verify their identity. If the biometric traits match the stored template, the authentication is successful, granting access. Conversely, if there is a significant mismatch, the system denies access. Figure 1 illustrates biometric system authentication

These systems find applications in various industries and contexts, including physical access control to buildings or restricted areas, unlocking devices like smartphones or laptops, authorizing financial transactions, and ensuring secure identification for government or law enforcement purposes.

Among the biometric modalities, retinal recognition is a very accurate and reliable method of biometric identification. In the current state of the art, the field of biometric retina has witnessed significant advancements. Many studies have focused on the use of retinal vascular network as biometric keys. For instance, Sadeghpour et al. [1] introduce and assess

a cohort-based dissimilarity vector representation for safeguarding retinal vascular templates in biometric systems, emphasizing irreversibility and unlink ability of the protected reference templates. The proposed approach achieved a mean AUC of over 98% in classifying cohort-based dissimilarity vectors, with a maximum accuracy drop of 1-2% compared to unprotected templates across three datasets: ESRID, VARIA, and Messidor-2.

To improve existing methods for identifying retinal images, Noori. A [2] proposes an innovative approach for evaluating such images. The suggested method relies on the histogram of Hue matrix values in the HSC color format, along with the LBP and HOG algorithms. According to the DRIVE database, the mean precision of the proposed method is 98.5%. Betaouaf et al. [3] have developed an automated identity verification algorithm based on the complex vascular network structure in the human retina. Their approach involves using watershed transformation for retinal vasculature segmentation and a hit or miss transform for detecting bifurcation and intersection points. Additionally, they utilize automatic image registration and compare biometric data models through the Iterative Closest Point (ICP) algorithm.

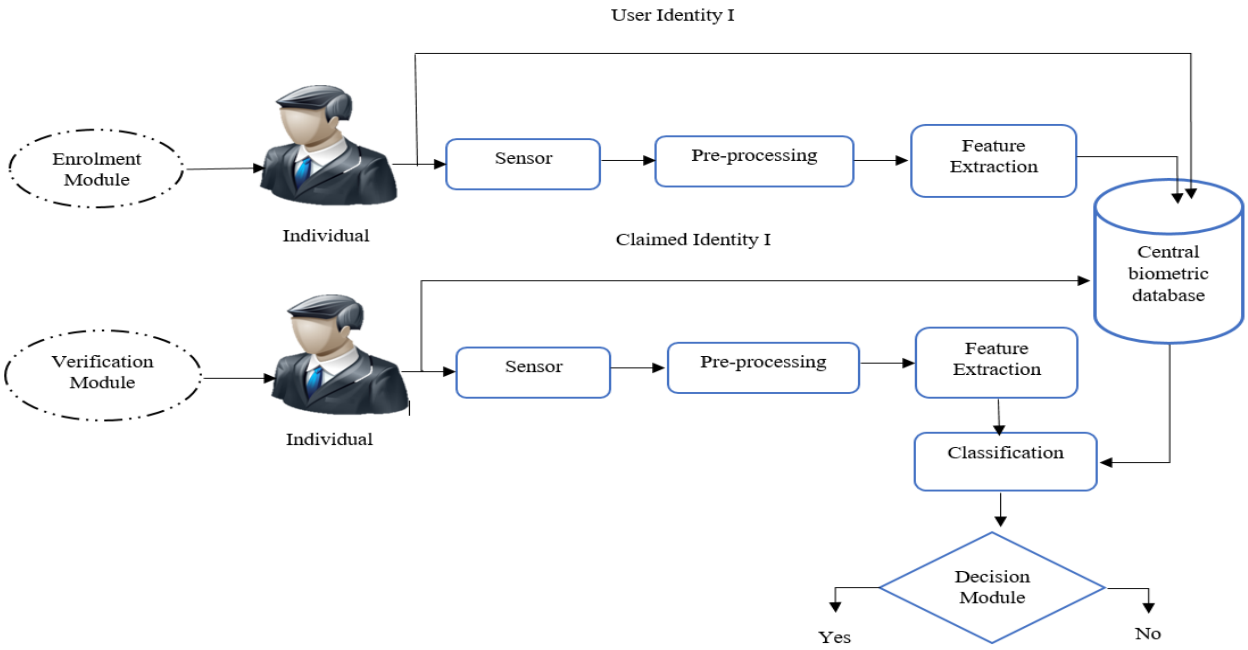

Fig. 1. Biometric system authentication.

Vignan's Nirula and co-authors [4] have developed a biometric verification system for personal identification on mobile devices. The system uses adaptive histogram equalization, Gaussian filtering, top-hat transformation, binary morphological reconstruction, and the KNNRF classifier. The system achieves a 60% false acceptance rate, 90% false rejection rate, and 94% accuracy on the Drive database.

Saba A. Tuama and Loay E. George present a distinctive method centered on retinal vascular patterns and personal recognition [5]. This innovative technique employs the Euclidean distance metric during the matching phase and leverages the spatial distribution of local vascular density as a feature vector. The system evaluates its efficacy using two databases, DRIVE and STARE, and it reveals a remarkable 100% accuracy rate for both datasets.

Jarina B. and her team [6] present a three-step procedure for individual identification utilizing color retinal images: initial vessel extraction through parabolic model fitting, subsequent feature extraction, and matching based on Euclidean distance. The performance of their proposed method is comprehensively assessed using a variety of pathological images, a local hospital database, two authentication databases (RIDB and VARIA), and three standard databases (DRIVE, HRF, and Messidor).

Biometric retina technology extends beyond vascular patterns to encompass other unique features of the retina for identification and verification purposes. This approach in retinal biometrics focuses on aspects other than blood vessels to establish identity. By analyzing aspects of the retina beyond blood vessels, including the overall retinal texture. Our research methodology comprises three distinct phases:

1. In the first stage, we employ CLAHE to preprocess the data.
2. Following the data preprocessing, the next step involves the extraction of unique features using the Gray-Level Co-occurrence Matrix (GLCM) analysis with invariance properties.

3. Subsequently, the features extracted in the previous phase undergo a classification process, utilizing a Random Forest algorithm.

The outcomes of our investigation demonstrate an exceptional accuracy rate of 100% during rigorous testing conducted on the RIDB (Retinal Identification Data Base) database. This paper comprises three principal sections: the methodology, where we elaborate on our approach; the experimental results and subsequent discussion; and, finally, a concluding section that encapsulates our findings and insights.

II. METHODOLOGY:

Within this section, we outline our methodology, commencing with image preprocessing, followed by the extraction of characteristics using GLCM, and concluding with the classification process.

A. Preprocessing :

In this step, we convert the input image to gray level and apply adaptive histogram equalization to eliminate contrast and brightness problems Fig.2 present results of this step.

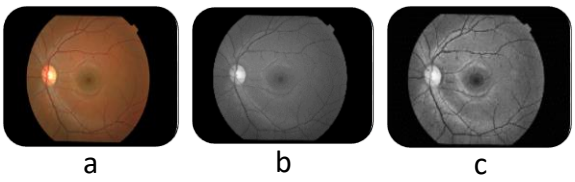

Fig.2.Preprocessing step: a: input image, b: gray image, c: image preprocessed.

B. Feature extraction:

The Gray-Level Co-occurrence Matrix (GLCM) is a widely used method for texture feature extraction in image processing. It characterizes the spatial relationship of pixel intensity values in an image by computing the occurrence of pairs of pixel values at various pixel displacements or offsets.
Gray-level invariant Haralick features constitute a collection of statistical metrics employed to assess the textural characteristics of an image. These features hold substantial significance in the domains of image analysis and computer vision, finding extensive utility in diverse applications such as image categorization, segmentation, and the comprehensive analysis of textures.

When computing the GLCM, one can incorporate various measures or statistics derived from the matrix to extract features. These features are commonly used to describe the texture properties of an image. However, the GLCM itself is invariant to certain transformations such as rotation, translation, or scaling [7]. To address the lack of invariance, we employ in combination with the GLCM based features. A combination of these approaches can significantly enhance the invariance of GLCM based features and improve the robustness of texture analysis in image processing tasks.

The texture features computed from GLCMs are:

1. Autocorrelation: Measures the similarity between an image and a shifted version of itself.
2. Contrast: Gauges the variation in intensity between adjacent pixels in the image.
3. Correlation: Measures the linear dependency between the intensity values of neighboring pixels.
4. Difference Average: Calculates the mean absolute difference among pixel intensities in the image
5. Difference Entropy: Measures the randomness or disorder of the differences between pixel intensities.
6. Difference Variance: Measures the variance of the differences between pixel intensities.
7. Dissimilarity: Determines the mean absolute difference between pixel intensities.
8. Energy: Also referred to as Angular Second Moment, quantifies the uniformity or smoothness of the image.
9. Entropy: Measures the randomness or disorder of pixel intensities in the image.
10. Homogeneity (Inverse Difference Moment): Assesses the proximity of the element distribution in the GLCM to the diagonal.
11. Maximum Correlation Coefficient: Measures the maximum correlation coefficient between intensity values at different pixel distances and orientations.
12. Maximum Probability: Measures the highest probability of occurrence of pixel pairs in the GLCM.
13. Sum Average: Measures the average sum of the pixel pairs at different distances and orientations.
14. Sum Entropy: Measures the randomness or disorder of the sum of pixel pairs at different distances and orientations.
15. Sum of Squares: Measures the sum of squared elements in the GLCM.
16. Sum Variance: Measures the variance of the sum of pixel pairs at different distances and orientations.

C. Classification :

This step involves feature matching. Initially, we collected various variables to train the random forest model for classification. Furthermore, we assigned a unique identifier (ID) to each individual. In a binary classification approach, label chosen ID with the value 1, while assigning zero to other IDs. This method makes it

possible to predict and distinguish the chosen ID from other identifiers.

A random forest serves as a meta-estimator that trains multiple decision tree classifiers on different subsets of the dataset and employs averaging to enhance predictive accuracy while mitigating the risk of over fitting .It is a popular choice in many machine-learning applications due to its effectiveness and ease of use. Through experimentation and thorough evaluation on our specific dataset, we choose a number of trees to 100.

III. RESULTS AND DISCUSSION:

To verify the effectiveness of our algorithm, we utilize a publicly dataset called RIDB [8]. The Retina Identification Database (RIDB) consists of Retinal Fundus Images taken using the TOPCON-TRC camera. It comprises 100 images, each with a resolution of 1504 x 1000 pixels, stored in JPEG format. These images were captured from 20 individuals, with five samples per person, and none of the individuals had any retinal diseases. We employed RIDB for training and testing purposes in developing a retinal recognition system. retinal recognition is one of the most precise biometric methods used to authenticate and identify individuals.. We carried out all tests using MATLAB 2016 on a personal computer with an Intel Celeron CPU N3050.

I based the evaluation of the system's performance on the following performance criteria:

1) False Acceptance Rate (FAR):
   This probability refers to the likelihood of wrongly identifying an unknown user as a known user. This rate is essential to evaluate the security of the biometric system. Its calculation is as follows:

$$FAR = \frac{the\ number\ of\ false\ acceptances}{he\ number\ of\ identification\ attempts} \times 100$$

2) False rejection rate (FFR):
   The probability that a known user will be rejected by the biometric system. This rate is the probability that a known user will be rejected by the biometric system. This rate helps to evaluate the level of comfort of use of the biometric system. Its formula is as follows:

$$FRR = \frac{the\ number\ of\ false\ recognitions}{the\ number\ of\ identification\ attempts} \times 100$$

3) Equal Error Rate (EER) :
   Represents the point at which the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are equal. In other words, the Equal Error Rate is the threshold or operating point where the system's performance reaches a balance between incorrectly accepting impostors and incorrectly rejecting legitimate users. It is a critical metric for assessing the overall accuracy and usability of a biometric authentication system.
4) The ROC curve:
   Serves as a valuable tool to visualize and evaluate the effectiveness of binary classification models. It enables informed decision making regarding the balance between correctly identifying true positives and the occurrence of false positives, achieved through the adjustment of the classification threshold.

In this part, we present the results for two identifiers 2 and 10 (we choose the IDs numbers) as an example of classification. This method makes it possible to increase the precision.Fig.3 and Fig. 4 shows the ROC curve, false acceptance rate and false rejection rate of the proposed system using the RIDB database. It shows a good separation distance between the genuine and imposter classes.

Additionally, we calculate the average accuracy across various IDs and proceed to evaluate the performance of our proposed method against established state-of-the-art techniques. The table presented below presents both the outcomes of our suggested approach and those of existing methods. This table provides a summary of the release year for several approaches and their respective performances on the RIDB dataset. Our findings indicate that our method has the highest accuracy, along with a substantial confidence interval.

Table: Result of our method and other methods.

Method	application	Dataset	Accuracy (%)
Our method	authentication	RIDB	100
[3]	authentication	DRIVE	100
[9]	identification	DRIVE	97.5
[10]	identification	DRIVE, RIDB	100
[11]	authentication	DRIVE	0.999
[12]	authentication	VARIA	97.16

IV. CONCLUSION

In our pursuit of developing trustworthy digital retinal templates for identity verification, we concentrated on identifying unique and dependable retinal characteristics. We focused on textural features extracting by invariant GLCM. To validate the efficacy of our proposed method, we subjected it to rigorous testing using the RIDB dataset. The results were exceptionally impressive, achieving a remarkable accuracy rate of 100%. This accomplishment underscores the resilience and reliability of our approach in accurately confirming individuals' identities based on their retinal biometrics.

By harnessing these distinctive retinal features, we have paved the way for the creation of highly reliable digital retinal templates. This breakthrough carries significant

potential for improving identity verification systems across various domains, including security applications.

Leveraging such unique retinal characteristics empowers us to construct precise and secure identity authentication systems, instilling confidence in the realm of biometric authentication.

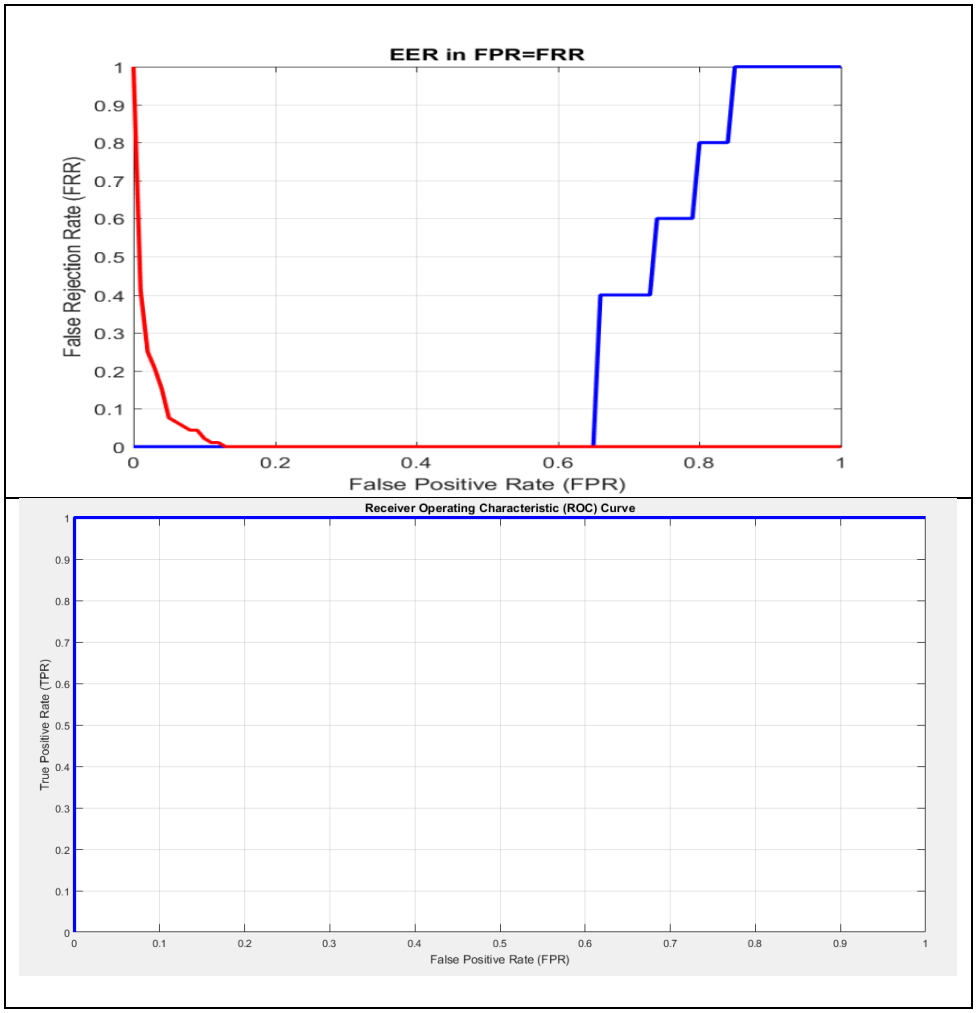

Fig.3. the ROC curve, false acceptance rate, and false rejection rate of the proposed system when employing the RIDB database for ID 2.

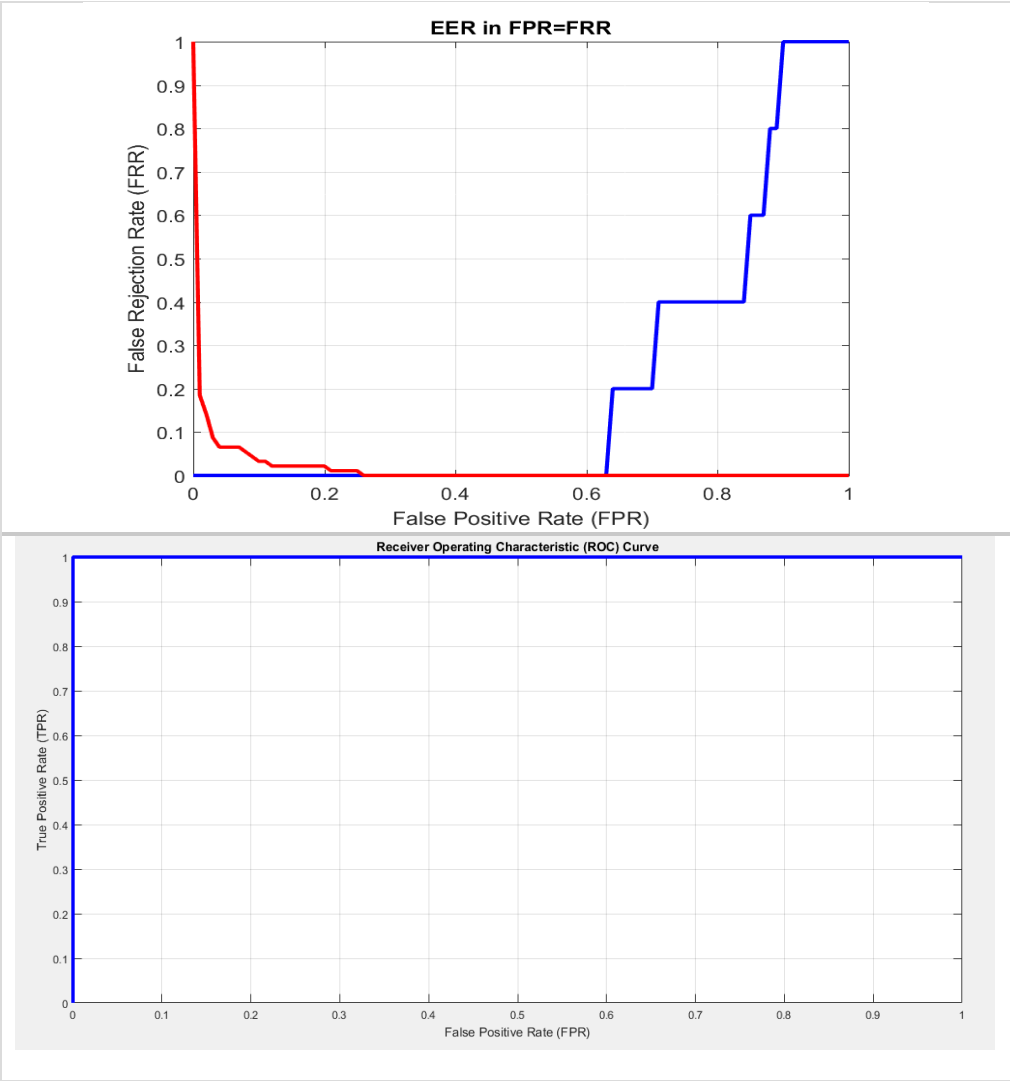

Fig.4. the ROC curve, false acceptance rate, and false rejection rate of the proposed system when employing the RIDB database for ID 10.

REFERENCES

[1] M. Sadeghpour, A. Arakala, S. A. Davis and K. J. Horadam, "Protection of Sparse Retinal Templates Using Cohort-Based Dissimilarity Vectors," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 2, pp. 233-243, April 2023, doi: 10.1109/TBIOM.2023.3239866.

[2] A Noori,"Retinal Vessels Combining LBP and HOG". arXiv preprint arXiv:2206.01658, Computer Science - Computer Vision and Pattern Recognition,2022, 10.48550/arXiv.2206.01658

[3] TH Betaouaf, E Decencière, A Bessaid. "Automatic biometric verification algorithm based on the bifurcation points and crossovers of the retinal vasculature branches". International Journal of Biomedical Engineering and Technology (2020), 32(1), 66-82, doi: 10.1504/IJBET.2020.104677.

[4] BMS Rani, AJ Rani. « Biometric retinal security system for user identification and authentication in smartphones". International Journal of Pure and Applied Mathematics (2018), 119(14), 187-202, doi: 10.21506/j.ponte.2018.2.3.

[5] SA Tuama, LE George. "Automatic Human Recognition Based on the Geometry of Retinal Blood Vessels Network", DOI: 10.9734/bpi/crst/v1.

[6] J Mazumdar, SR Nirmala. "Person identification using parabolic model-based algorithm in color retinal images", International Journal of Electrical and Electronic Engineering & Telecommunications (2019), doi: 10.18178/ijeetc.8.6.358-366.

[7] T Löfstedt, P Brynolfsson, T Asklund, T Nyholm, A Garpebring, "Gray-level invariant Haralick texture features", PloS one, 2019, vol. 14, no 2, p. e0212110, https://doi.org/10.1371/journal.pone.0212110

[8] "RIDB: a dataset of fundus images for retina based person identification", Data in Brief, vol.33, p.106433, 2020, Elsevier, https://doi.org/10.1016/j.dib.2020.106433.

[9] F Sadikoglu, S Uzelaltinbulat," Biometric Retina Identification Based on Neural Network" Procedia Computer Science Volume 102, 2016, Pages 26-33 Elsevier, https://doi.org/10.1016/j.procs.2016.09.365.

[10] S Sultan, M Faris Ghanim," Human Retina Based Identification System Using Gabor Filters and GDA Technique", JOURNAL OF COMMUNICATIONS SOFTWARE AND SYSTEMS, VOL. 16, NO. 3, SEPTEMBER 2020, (DOI): 10.24138/jcomss.v16i3.1031

[11] MSA Malik, Q Zahra, IU Khan, M Awais, G Qiao, "An Efficient Retinal Vessel. Journal of Medical Imaging and Health Informatics, 10(10), 2481-2489, DOI: https://doi.org/10.1166/jmihi.2020.3180.

[12] R. Manjula Devi, P. Keerthika, P. Suresh, Partha Pratim Sarangi, M. Sangeetha, C. Sagana, K. Devendran, Chapter 5 - Retina biometrics for personal authentication, Machine Learning for Biometrics, Academic Press, 2022,p87-104,ISBN 9780323852098, https://doi.org/10.1016/B978-0-323-85209-8.00005-5.