International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

Biometric Accreditation Adoption using Iris and Fingerprint: A Review

Ojasvi Dere[1], Srushti Gaikwad[2]

[1]*Department of Electronics and Telecommunication, Ramrao Adik Institute of Technology, DY Patil University, Navi Mumbai, India*
[2]*Department of Electronics and Telecommunication, Ramrao Adik Institute of Technology, DY Patil University, Navi Mumbai, India*

Abstract - *Safety is a major concern in our lives today. Whether within an organization or in a restricted area; With the growing need for security measures in everyday life, biometrics has become a hot topic of research targeting its potential value in personal identification. This is because biometric systems are classified as more secure than other security systems. This paper focuses on iris and fingerprint as one of the best biometric features for identity management. Iris recognition possesses properties that make it a quintessential biometric system. The point of this venture is to distinguish an individual without a blunder, burning through less time, and keep away from mistakes in confined regions. The recognition of Iris for dealing with Indian weapons is the most powerful innovation related to the security of our country. The method used for fingerprint authentication divides the identification into stages and eliminates many fake fingerprints at different stages. This saves a lot of time by maintaining a high recognition rate. Although Minutiae-based technology is widely used, it is difficult to extract features if the fingerprint image quality is poor. This paper aims to understand how the characteristics of fingerprints can be inferred. Significant advances in this field show that iris and fingerprint biometrics still require fast, real-time, reliable, and powerful algorithms for higher recognition.*

Key Words: **Iris, Hough Transform, Daugman Method, Fingerprint, Minutiae, Image Processing.**

1. INTRODUCTION

Biometric is a reliable, secure authentication tool where controlled access is given by identifying the individual using the physiological or behavioral characters [5]. Physiological properties are contained in the physical parts of the body such as fingerprints, fingerprints, iris, face, DNA, the shape of the hand, retina, etc. The behavioral characteristics of the are based on human actions such as (voice recognition, key scan, signature scan). The commonly used physiological characters are iris, signature, voice, fingerprint, DNA, and palm [6]. Biometric recognition methods are predicated on properties that cannot be stolen or lost or replicated, in contrast to other methods. The Biometric system can run in two modes identification or verification. It consists of rudimental modules which consist of a sensor module, feature extraction module, matching module, and decision-making module.

Iris is a significant piece of the natural eye. The two eyes have autonomous and uncorrelated iris designs [1,2]. No two irises of a person are alike; Indeed, the indistinguishable twins have distinctive iris designs [7]. Even though the irises of a similar individual appear to be comparative yet they contain exceptional examples [6]. Iris is a slim, roundabout design in the eye that is an ensured interior organ, hence it's anything but influenced by natural variables. Iris acknowledgment is an interaction of perceiving an individual dependent on textures and patterns in an iris [4]. It is a strategy for biometric confirmation in which the highlights of the iris of an individual eye are extricated. The Iris acknowledgment framework gets the picture, extricates the iris region to decide the extraordinary texture for distinctive identification during the check interaction, and matches it with the database made during the enrolment cycle. It is quite possibly the most exceptional and dependable quick access biometric framework. Iris acknowledgment is a promising arrangement because of its dependability, soundness, uniqueness, and wide scope of utilizations [5].

The fingerprint is one of the most common authentication methods for its accuracy, low cost, and varied applications used to identify people. The fingerprint identification system stores a set of fingerprints in its database, then it tries to identify a fingerprint by matching it with the fingerprints already existing in the database. All different applicable methods for fingerprint recognition attempt to reach the proper accuracy and speed. The effectiveness of the fingerprint recognition system is well established in terms of uniqueness and permanence.

2. IRIS RECOGNITION

2.1 Principle

The Iris is an important fragment of the eye. It is the colored tissue at the front of the eye which contains the pupil in the center [2]. Iris decides the structure of the eyeball [4]. Iris controls the amount of light penetrating the eye. The principle of iris recognition is the same as capturing an image. The process of iris recognition is capturing the iris patterns and then the captured image is converted into computational frames using image processing techniques. The image processing converts the iris pattern from one form to another without a change in its original composition.

The iris patterns are extracted from the captured images. These patterns are then stored in the database suitable for retrieving.

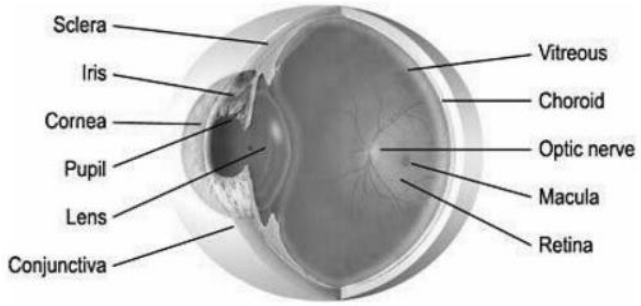

Fig- 1: The internal structure of the eye [4]

During identification, if the pattern recognized is stored in the database, then the database manager indicates the match of iris pattern to evident. The patterns are authenticated or unauthenticated by a recognizer. The captured pattern is recognized by the iris recognition device and checked to see if it is authenticated or fraudulent. The iris recognizer recognizes and computes the iris patterns even when the eyeball is affected by a disease or an infection. Only the authenticated patterns are converted into unique binary representations using image processing.

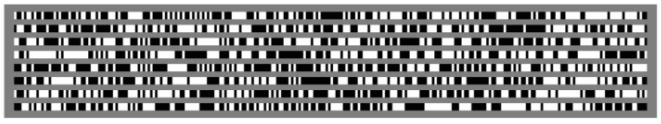

Fig- 2: Iris pattern with its Unique binary representation [4]

2.2 Methods

The framework comprises a few subsystems which compare to each phase of the iris acknowledgment [1]. The image acquisition stage captures an image using sensors. High-quality images are captured using specialized iris cameras. High resolution and good sharpness and good lighting conditions are taken into consideration. The Iris localization is completed utilizing the circular Hough transform that recognizes the circular boundaries from the edge map of the eye image. Image segmentation relies upon image quality. The methodologies, for example, Hough transform, Integrodifferential constitute a significant part in image segmentation.

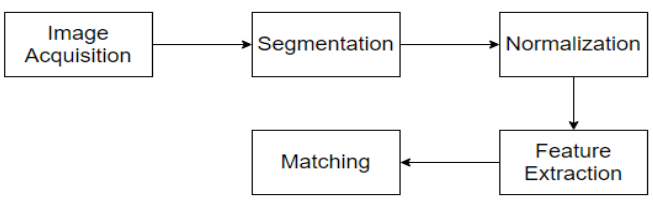

Fig- 3: Block diagram of Iris Recognition system

Daugman proposed an algorithm to find both inner and outer limits of the iris using the integrodifferential operator [5,6]. The transform even detects the upper and lower boundaries of the iris. It acts as a circular edge finder, assuming the pupil and edge are essentially circle. The circular path is detected when there is a most extreme change in pixel esteem by fluctuating the radius of the circular contour.

Daugman implemented the system using a 2-D Gabor wavelet filter for localization of iris, Gaussian transform for feature extraction and 256-byte iris code for computation [3]. The significant commitment of Daugman's is to give statistical theories for the degree of iris code agreement [3].

Hough Transform is the algorithm that was introduced by Paul Hough in 1962 for the detection of features like lines, circles. The exemplary method uses a standard algorithm for the detection of lines and circles. The advantage of this transform is that it is tolerant to gaps feature boundary portrayal and moderately unaffected by image noise, unlike edge detectors, and provides segmentation exactness up to a degree. It does not give regard to eyelid localization, reflection, eyelashes, shadows which is a downside of this transform.

The image normalization stage normalizes the part to generate iris code and their comparisons. The process involves unwrapping the iris and converting it into its polar equivalent [1]. Normalization was performed using Daugman's rubber sheet model, in which the circular region of the iris was transformed into a rectangular block of fixed size [5]. The phase information is encoded by 2D Gabor and hamming distance is used for template matching.

For feature encoding, the discriminative feature of the iris pattern is extracted. V. Garagad et al proposed an identification technique where the iris region is radially followed to extract the feature [5]. This method is invariant to tilt and scale variation. Iris feature is extracted using 2D Gabor, 1D Log-Gabor wavelets, and 2D Log Gabor wavelets. Feature matching is performed using Hamming distance, Elastic similarity metric, and Euclidean distance. The feature extraction algorithm employs the complex-valued 2D Gabor wavelets to produce the iris codes which are then matched using the hamming distance.

Another feature extraction method based on the extraction of statistical features in an iris was presented by Sowmya B. et al [5]. After the iris localization, concentric circles of different radii are drawn with the focal point of the pupil as the center. The mean, standard deviation, variance, and mode for each circle are determined. The image is viewed as a feature vector having the above-calculated values and number of circles drawn. Hamming distance is used for template matching [1,5]. The principal objective of template matching is to evaluate the two iris images [1].

Table- 1: Overview of different methods used for Iris Recognition

Method	Features	Advantages	Disadvantages	Application
Hough Transform	Detects lines, circles, and other parametric curves	Tolerant to gaps and unaffected by image contamination.	It is computationally intensive and therefore not appropriate for real-time applications. Does not give any consideration to eyelid localization, eyelashes, and shadows.	Traffic & Transport, biometrics, underwater, medical, industrial
Daugman	Detects pupil and iris boundaries, employs 2D Gabor wavelet transform to extract phase structure of iris.	Provide the statistical theories for the degree of iris codes. Gives the most extreme proficiency as compared to other methods.	The segmentation of an iris may result in an error if the image is contaminated or contains noise. It suffers from bright spots of illumination inside the pupil.	Image localization, segmentation, and extraction.
Hamming distance	Gives a degree of dissimilarity between two templates.	Fast matching speed because the templates are in binary format.	Bandwidth utilization is more.	Used in different sorts of error correction and assessment of contrasting data, telecommunication industry, nanosatellites, computer memory, and embedded processors.
Daugman's rubber sheet model	Remaps each point within the iris locale to a pair of polar coordinates.	It considers pupil dilation, imaging distance & non- concentric pupil displacement.	Does not account for rotational disjointedness.	Image normalization.
Gabor Filter	Gives optimum localization in both spatial and frequency domains.	Does not depend on unessential factors such as imaging contrast, illumination, and camera gain.	Takes too high time for performing features due to the dimension of the feature vector is exceptionally long.	Used for texture analysis and image processing.

With the development of the biometric system, iris recognition will bestow global protection to the armed forces in future warfare [4]. It likewise discovers applications in rail infrastructure. It is implemented for aviation security, for controlling access to confined regions at airports, premises access control, and database access. Iris Recognition is employed in Indian armed weapons, ID distinguishing pieces of proof cases, border management, and defense and mobile authentication with special IR-enabled cameras. War weapons are authenticated and secured using the biometric system. Armed services require a biometric system for the recognizable proof and anticipation of early indications of agroterrorism [4].

3. FINGERPRINT RECOGNITION

3.1 Principle

Fingerprints are a graphic form of ridges and grooves on the surface of the fingertips, and the ends of ridges and cracks in the ridge are called ridges. The fingerprints differ from person to person. The fingerprint identification is predicated on two basic assumptions, Invariance, and Singularity. Invariance means the fingerprint characteristics don't change alongside life. Singularity means that the

fingerprints are unique and two people don't have the same fingerprint pattern.

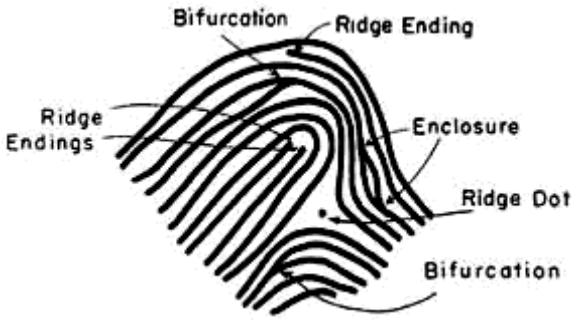

Fig- 4: Fingerprint image showing different Ridge Feature [8]

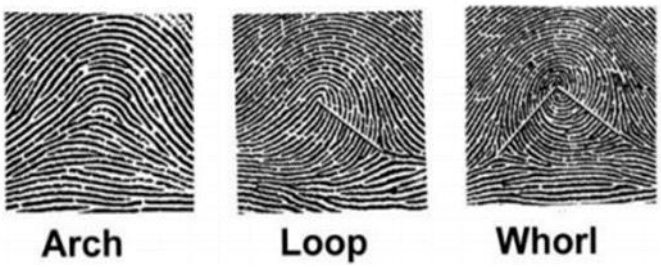

Fig- 5: Types of Fingerprints [9]

The ridges are declared as black lines and the valleys are declared as white lines [8]. The minutiae points are the points where the ridge structure changes like bifurcation and endpoint. There are three types of fingerprint patterns the arches, the loops, and the Whorls [9]. This categorization is predicated on the range of ridges found within the fingerprint from person to person. The principle of fingerprint recognition includes image extraction in this case fingerprint, using a biometric reader or scanner. The information obtained from the scanner is converted from analog to digital format and using image processing its noise elements are extracted. There are various stages involved to achieve this principle.

Table- 2: Terms and Definitions of Fingerprint structure [8]

No.	Term	Definition
1	Termination	The location where a ridge comes to an end.
2	Bifurcation	The location where a ridge divides into two separate ridges.
3	Binarization	The method of converting the first grayscale image to a black-and-white image
4	Thinning	The method of reducing the width of every ridge to at least one pixel.
5	Termination Angle	The angle between the horizontal and therefore the direction of the ridge.
6	Bifurcation Angle	The angle between the horizontal and therefore the direction of the valley ending between the bifurcations.
7	Matching Score	The angle between the horizontal and therefore the direction of the valley ending between the bifurcations.
8	False Non-Matching Ratio	It's the probability that the system denies access to an approved user.

3.2 Methods

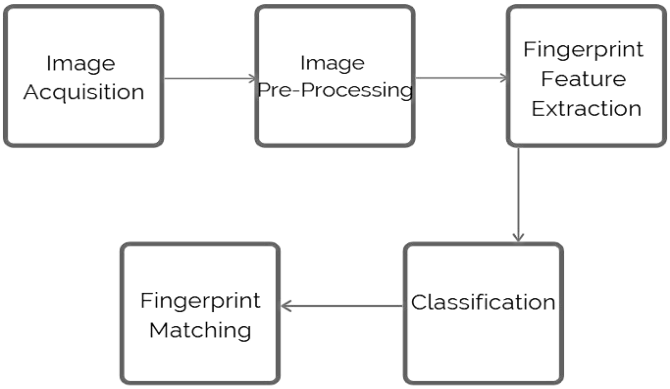

Fig- 6: Block diagram of Fingerprint Recognition System

1. Image Acquisition stage

Fingerprints of individuals can be obtained either by using a biometric reader/scanner or the traditional ink method [11]. Optical fingerprint sensors are used to image the friction ridge structure of the fingertip and then store them in the database with the help of computers. Fingerprint images are 260*300 pixels in size.

2. Image Pre-processing stage

This stage is critical and thought of as crucial during this process because it involves the removal of unwanted data like noise and reflection. Image Pre-processing is employed to amplify the clarity of ridge structure. Sub steps involved in accomplishing this are image segmentation, binarization, elimination, smoothing, and thinning. Gaussian filters and Short Time Fourier analysis also are wont to enhance image quality [12]. Fingerprint images contain various false minutiae which are removed using binarization. Jiao Ruili et. proposed an automatic fingerprint acquisition and pre-processing system with a troublesome and fast point DSP, TMS320VC5509A, and a fingerprint sensor, MBF200. The system is diminutive and versatile. Comparing various algorithms, suitable ones are selected for fingerprint identification pre-processing. These are Median Filtering, Directional Filtering Enhancement, Fixed Threshold Binarization, and Hilditch Thinning. The pre-processing is performed after distinguishing the fingerprint image quality consistent with its characteristics.

3. Fingerprint feature extraction

This stage is applied to the output obtained from the image pre-processing stage. Feature extraction mainly depends on sets of algorithms. Fingerprint feature extraction programs are used to find, measure, and code ridge edges and discrepancies. The minutiae extraction algorithm is a specific method to locate the minutiae points from the fingerprint and then map their relative placement on the finger. In an advanced fingerprint feature extraction, the minutiae are extracted directly from original gray-level fingerprint images without binarization and thinning. Gabor filter banks are also used to extract features from fingerprints.

4. Classification

Classification is taken into account a crucial step in the detection of fingerprints. Various factors like temperature and humidity affect the temperature of the skin causing the pictures of fingerprints to be blurred. Another factor that affects the capturing of fingerprints is that the way during which it's kept on the scanner and therefore the pressure applied thereto while taking the image. The most aim of classification is to assign a given fingerprint to a selected category consistent with its geometric properties. It also facilitates the management of huge fingerprint databases and accelerates the method of fingerprint matching. Different frameworks are used for various sets of properties. The system during which manual fingerprint classification is performed within a selected framework is named as Henry system. The classification is precisely supported ridge patterns, local ridge orientations, and minutiae. if these properties are often described quantitatively and extracted automatically from a fingerprint image then fingerprint classification will become a neater task. Different algorithms classify fingerprints into five to 6 categories with 90 percent classification accuracy.

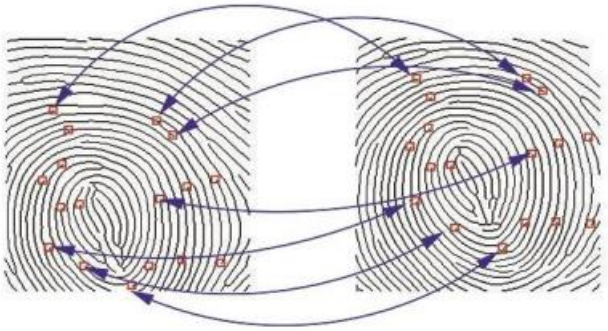

Fig- 7: Minutiae- Based Fingerprint matching [9]

5. Matching

The matching stage is that the method to match the acquired feature with the template within the database. In other words, the method of the matching stage is to calculate the degree of similarity between the input test image (for the user when he wants to prove his/her identity) and a training image from the database (the template created at the time of enrolment). Matching is often exhausted three methods: hierarchical approach, classification approach, and Coding approaches [11]. The hierarchical approach increases the matching speed at the value of accuracy. Classification approaches assign a category to every biometric during a database. There are many classification methods including the KNN classifier. Coding approaches use one matching function to look at entire databases. Arun Ross et. proposed the

hybrid fingerprint matcher which employs the mixture of ridge strengths and a gaggle of minutiae points. Johg Ku Kum et. al. presented a study on Hybrid fingerprint matching methods. They combine feature matching with image-based fingerprint verification methods.

4. CONCLUSIONS

The importance of this paper stems from the need that fingerprint and iris can be used in a variety of applications for authentication purposes. In the education system, business, banking systems, government official work. This method is easy as people can log in without having to remember any passwords. Also, it is reliable, accurate, inexpensive, low memory requirement, and is highly reliable. It is outstanding amongst other security strategies for confirmation because of its exactness and difficulty in engraving. Nowadays, security is one of the significant components in online business, data innovation, military, business, and so on. Most organizations use biometric validation to secure a high classified resource. Biometrics can be accustomed to enhance privacy since it yields a secure transaction and correct identification of the individual without any errors.

REFERENCES

[1] Bakti B. Bhagnagare, "Security System using Iris as Biometrics", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 7 (1), pp 399-401, 2016.

[2] Richard P. Wildes, Member, IEEE, "Iris Recognition: An Emerging Biometric Technology", Proceedings of the IEEE, Volume 85, No. 9, September 1997.

[3] Khattab M. Ali Alheeti, "Biometric Iris Recognition Based on Hybrid Technique", International Journal on Soft Computing (IJSC) Vol.2, No.4, November 2011.

[4] N. Prasanth, "Importance of Iris Recognition against Technology Failure", IOSR Journal of Computer Science (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014), pp 55-59.

[5] S. Kalaiselvi, R. Anandha Jothi, Dr. V. Palanisamy, "Biometric Security with Iris Recognition Techniques: A Review", International Journal of Pure and Applied Mathematics, Volume 118, No. 8, pp 567-572, 2018.

[6] S.S. Chowhan, G.N. Shinde, "Iris Biometrics Recognition Application in Security Management", International Conference on Communication and Electronics System (ICCES), vol.6, no.1, pp.1-12, June 2008.

[7] Suleiman Salihu Jauro, Raghav Yadav, "Review on Iris Recognition Research Directions- A Brief Study", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 13, Number 10, pp. 8728-8735, 2018.

[8] Mouad M. H. Ali, Ashok Gaikwad, "Multimodal Biometrics Enhancement Recognition System based on Fusion of Fingerprint and Palm Print: A Review", Global Journal of Computer Science and Technology(F), Volume XVI, Issue II, Version 1, 2016.

[9] Abdullah Saud1, Nazar Elfadil, "Biometric Authentication by Using Fingerprint Recognition System", International Journal of Scientific Engineering and Science, ISSN (Online): 2456-7361, Volume 4, Issue 5, pp 22-28, 2020.

[10] Fanglin Chen, Member, IEEE, Xiaolin Huang, Member, IEEE, and Jie Zhou, Senior Member, IEEE, "Hierarchical Minutiae Matching for Fingerprint and Palmprint Identification", IEEE Transactions on Image Processing, Volume 22, Issue No. 12, December 2013.

[11] Anil Jain, Fellow, IEEE, Lin Hong, and Ruud Bolle, Fellow, IEEE, "On-Line Fingerprint Verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 19, Issue No. 4, April 1997.

[12] Mouad. M. H. Ali, Vivek Mahale, Pravin Yannawar, A. T. Gaikwad, "Overview of fingerprint recognition", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016.