ISSN (ONLINE) : 2045 -8711
ISSN (PRINT) : 2045 -869X

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING

March 2024
Vol - 14 No. - 03
@IJITCE Publication

UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.

India: Editor
International Journal of Innovative Technology & Creative Engineering
36/4 12th Avenue,
1st cross St,
VaigaiColony
Ashok Nagar
Chennai, India 600083

Email: editor@ijitce.co.uk

www.ijitce.co.uk

IJITCE PUBLICATION

International Journal of Innovative Technology & Creative Engineering

Vol.14 No.03

March 2024

www.ijitce.co.uk

Dear Researcher,

Greetings!

Articles in this issue discusses about study endeavors to recent trends in iris image.

We look forward many more new technologies in the next month.

Thanks,
Editorial Team
IJITCE

Editorial Members

Contents

BIOMETRIC IDENTIFICATION SYSTEM USING IRIS RECOGNITION TECHNOLOGY

Dr. V.K. NARENDIRA KUMAR
Assistant Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
Dr.R.TAMILSELVI
Assistant Professor & Head, School of Computer Science,
VET Institute of Arts and Science (Co-Edu) College, Erode, Tamil Nadu, India.
Dr.K.S.MOHANASATHIYA
Assistant Professor, School of Computer Science,
VET Institute of Arts and Science (Co-Edu) College, Erode, Tamil Nadu, India.
Dr. S. PRASATH
Assistant Professor, School of Computer Science,
VET Institute of Arts and Science (Co-Edu) College, Erode, Tamil Nadu, India.

ABSTRACT--Biometrics is a multifaceted discipline combining many scientific fields including computational biology, statistics, mathematics, molecular biology, and genetics. Biometrics enables biomedical investigators to exploit existing and emerging computational technologies to seamlessly store, mine, retrieve, and analyze data from genomics and proteomics technologies. The main objective of the paper is the determinations of an individual identify in order to avoid threat to the security. In this paper we are discussing about secure biometric identification system using iris technology. There has been a significant surge in the use of biometrics for authentication in recent years because biometrics-based authentication offers several advantages over other authentication methods. It is important that such biometrics-based authentication system be designed to withstand attacks when employed in security-critical applications. Biometrics, identification based on distinctive personal traits, has the potential to become an irreplaceable part of any identification system. Iris patterns have now been tested in many field and laboratory trials, producing no false matches in several million comparison tests. The recognition principle is the failure of a test of statistical independence on iris phase structure encoded by multi-scale wavelets. Most popular application in biometrics is eye scanning, face reorganization and finger print scanning. The proposed method generates better results than other available methods. Eye scan security system and its implementation are discussed in this paper.

Keywords: - Biometrics, Iris, Pupil, Acquisition, Template, Recognition, Database and Security.

I. INTRODUCTION

Biometrics comes from the Greek words bios (Life) and metrics (Measure). It is basically a pattern-recognition system that is used to identify or verify users based on his or her unique physical characteristics. Several identification and verification schemes that exist today but the most accurate identification is in the area of biometrics. Biometrics is the emerging area of deals with recognition of a person through something the person has (e.g., iris, finger print, retina, face, etc.) or produces (e.g., voice, handwriting, gait, etc.). Biometric Technology Comparison as shown in Table 1. The importance of biometric research has increased significantly in the new century due to its potential impact to boost security efforts. Biometric identification would also be useful in areas such as banks, advanced human-computer interfaces, criminal identification, etc.

Biometric technologies vary in complexity, capabilities, and performance, but all share several elements. They use acquisition devices such as cameras and scanning devices to capture images, recordings, or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics. Because the process is automated, biometric decision-making is generally very fast, in most cases taking only a few seconds in real time.

A. Security Assumption

Enrollment is performed at a trusted Certification Authority (CA). The database is vulnerable to attacks as well from the outside as from the inside (malicious verifier). During the authentication phase an attacker is able to present artificial biometrics at the sensor. All capturing and processing during authentication is tamper resistant and reveals no information. The communication channel between the sensor and the verification authority is assumed to be public and authenticated.

B. Security with Biometrics

The qualities of a useful biometric trait include [6]:

Universality: Prevalent in the entire population.

Permanence: Does not vary significantly over time.

Uniqueness: Unique to each individual.

However, for a biometric trait to be implemented in a real world scenario, it must have practical qualities, including:

Performance: Provide sufficient identification accuracy.

Efficiency: The trait must be amenable to efficient and automatic collection/implementation.

Security: Secure against impostors and forgeries (fraudulent access).

Acceptability: Non-intrusive, non-harmful and accepted by users.

Two interesting properties of biometric identification are:

1. The person to be identified is required to physically be present at the point of identification.

2. Identification is based on the biometric technique that does not depend on the user to remember a password or to carry a token.

The biometric system either automatically cross checks the enrolled characteristics for duplicates, or otherwise does not allow a person to register their biometric under two different names [2].

C. Biometric System Consists of Four Basic Modules

Figure 1 illustrates enrollment, verification, and identification tasks are shown using the four main modules of a biometric system.

1) Enrollment Unit: The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual’s biometric characteristic to produce its digital representation.

2) Feature Extraction Unit: This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

3) Matching Unit: This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user’s master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching).

4) Decision Maker: This module accepts or rejects the user based on a security threshold and matching score, as shown in figure 1 [1].

III. IRIS RECOGNITION

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the appearance of dividing the iris radically, with striations, rings, furrows, a corona, and freckles. Iris recognition technology uses about 173 of these distinctive characteristics. Formed during the 8^{th} month of gestation, these characteristics reportedly remain stable throughout a person’s lifetime, except in cases of injury. Iris recognition can be used in both verification and identification systems. Iris recognition systems use a small, high-quality camera to capture a black and white, high-resolution image of the iris. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system [3].

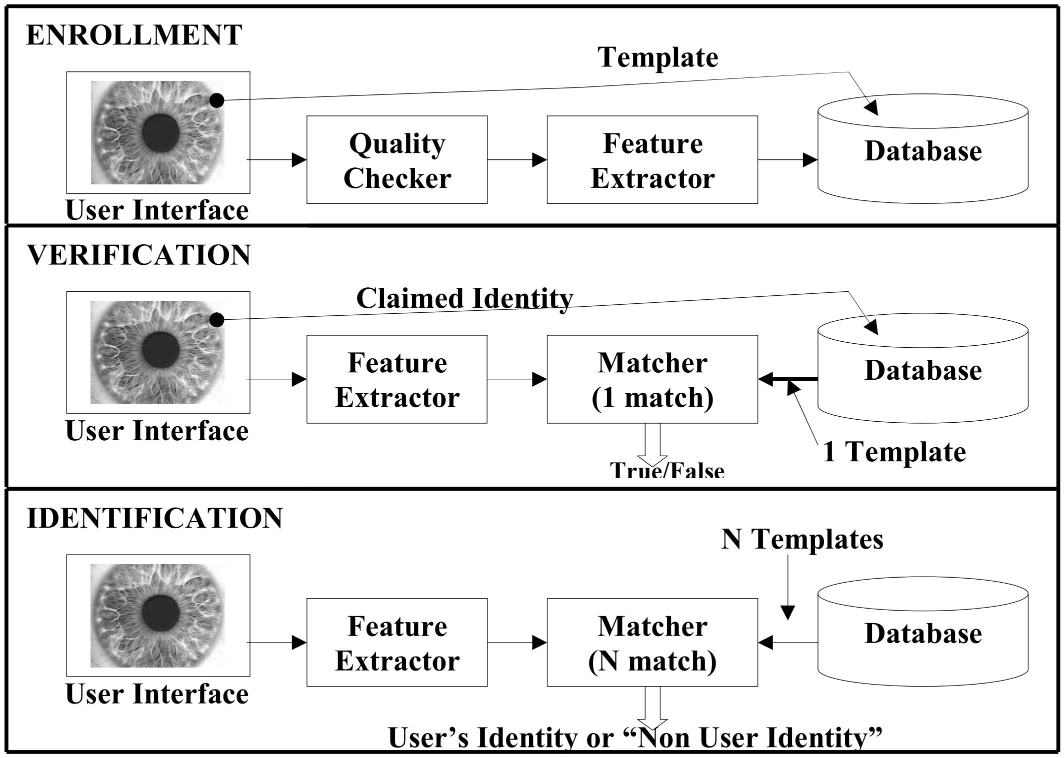

Figure 1: Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system.

TABLE I

Biometric Technology Comparison

Method	Coded Pattern	Misidentification rate	Security	Applications
Iris Recognition	Iris pattern	1/1,200,000	High	High-Security Facilities
Finger Printing	Fingerprints	1/1,000	Medium	Universal
Hand Shape	Size, length and thickness of hands	1/700	Low	Low-Security Facilities
Facial Recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-Security Facilities
Signature	Shape of letters, writing order, pen pressure	1/100	Low	Low-Security Facilities
Voice Printing	Voice characteristics	1/30	Low	Telephone Service

II. IRIS STRUCTURE

The iris is the colored part of the eye behind the eyelids, and in front of the lens. It is the only internal organ of the body, which is normally externally visible. These visible patterns are unique to all individuals and it has been found that the probability of finding two individuals with identical iris patterns is almost zero. Although the human eye is slightly asymmetrical and the pupil is slightly off the center [2], for the most practical cases we think of the human eye is symmetrical with respect to line of sight. The iris controls the amount of light that reaches the retina. Due to heavy pigmentation, light pass only through the iris via pupil, which contracts and dilates according to the amount of available light. Iris dimensions vary slightly between the individuals. Its shape is conical with the papillary margin located more interiorly than the root. A thickened region called the collarete divides the anterior surface into the ciliary and pupil zones.

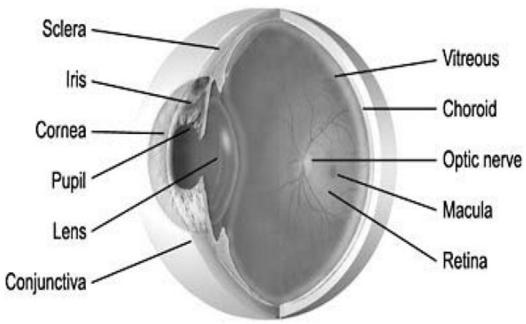

Figure 2: Structure of the eye

Iris is made up of four different layers. The back layer is heavily pigmented and makes iris opaque so that light only reaches the eye through the pupil. The next layer contains the sphincter and the dilator muscles that allows for contraction and dilation. The third layer is the stroma, which is loosely connected tissue containing collagen, melanocytes, most cells and macrophases. The exterior layer is called the anterior border layer and is denser than the previous layer with more pigmentation. The color of the iris is created by different levels of light absorption in the anterior border layers, little pigmentation in this layer results in a blue appearance because light reflects from the back layer of the iris. The more pigmentation a person has in the anterior border layer, the darker is the iris.

IV. IRIS CAMERA

The iris camera is the monochrome Cooke PixelFly QE, which is equipped with a 2/3" format Sony ICX 285AL CCD sensor, and has boosted sensitivity in the NIR spectrum. High NIR sensitivity is desirable to reduce the required level of illumination. The sensor resolution is 1394 by 1024 pixels, with a frame rate of 12 Hz. The sensor elements of this camera are relatively large at 6.45 by 6.45 mm, limiting the adverse effects of diffraction and thus allowing for high image contrast.

The iris camera lens is the potentiometer-equipped Fujinon D16x73A-Y41. This lens provides programmable motorized focus and zoom (focal length 10–160 mm). A study of the trade-off between diffraction effects and depth of field resulted in an aperture setting of f/9.5, where the system is (just) diffraction limited. The depth of field is about 30 mm, making clear the need for accurate focal distance control. The lens is equipped with a 715 nm long-pass filter that blocks most of the ambient light and allows most of the LED NIR illumination. The iris camera and lens are configured to capture iris images at a resolution of approximately 200 pixels across the iris, with a field of view of 76 mm at a subject distance of 1.5 m.

V. SYSTEM METHODOLOGY

Iris recognition leverages the unique features of the human iris to perform identification and, in certain cases, verification. Iris recognition is based on visible (via regular and/or infrared light) qualities of the iris. A primary visible characteristic is the orbicular meshwork (permanently formed by the 8th month of gestation), a tissue which gives the appearance of dividing the iris in a radial fashion. Other visible characteristics include rings, furrows, freckles, and the corona, to cite only the more familiar [8].

A. Iris Scan

The user places him or her so that he can see his own eye's reflection in the device. The user may be able to do this from up to 2 feet away or may need to be as close as a couple of inches depending on the device. Verification time is generally less than 5 seconds, though the user will only need to look into the device for a couple moments. To prevent a fake eye from being used to fool the system, these devices may vary the light shone into the eye and watch for pupil dilation.

Iris scans analyze the features that exist in the colored tissue surrounding the pupil which has more than 200 points that can be used for comparison, including rings, furrows and freckles. The scans use a regular video camera style and can be done from further away than a iris scan. It will work through glasses fine and in fact has the ability to create an accurate enough measurement that it can be used for identification purposes, and not just verification.

The uniqueness of eyes, even between the left and right eye of the same person, makes iris scanning very powerful for identification purposes. The likelihood of a false positive is extremely low and its relative speed and ease of use make it a great potential biometric.

B. Iris Code

Expressed simply, iris recognition technology converts these visible characteristics as a phase sequence into a 512 byte IrisCode(tm), a template stored for future identification attempts. From the iris' 11mm diameter, Dr. Daugman's algorithms provide 3.4 bits of data per square mm. This density of information is such that each iris can be said to have 266 'degrees of freedom', as opposed to 13-60 for traditional biometric technologies. A key differentiator of iris-scan technology is the fact that 512 byte templates are generated for every iris, which facilitates match speed (capable of matching over 500,000 templates per second).

C. Iris Image Acquisition

An important and difficult step of an iris recognition system is image acquisition. Since iris is small in size and dark in color (especially for Asian people), it is difficult to acquire good images for analysis using the standard CCD camera and ordinary lighting. We have designed our own device for iris image acquisition [5], which can deliver iris image of sufficiently high quality.

D. Preprocessing

The acquired image always contains not only the 'useful' parts (iris) but also some 'irrelevant' parts (e.g. eyelid, pupil etc.). Under some conditions, the brightness is not uniformly distributed. In addition, different eye-to-camera distance may result in different image sizes of the same eye. For the purpose of analysis, the original image needs to be preprocessed. The preprocessing is composed of three steps.

1) Iris Localization: White outlines indicate the localization of the iris and eyelid boundaries. Both the inner boundary and the outer boundary of a typical iris can be taken as circles. But the two circles are usually not co-centric. The inner boundary between the pupil and the iris by means of threshold, as shown in figure 3.

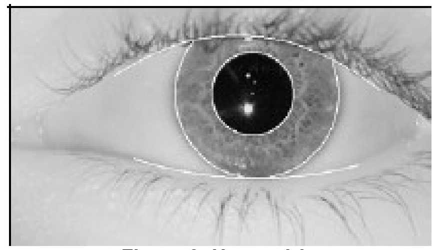

Figure 3: Human iris

The outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. We detect the outer boundary by maximizing changes of the perimeter-normalized sum of gray level values along the circle. The technique is found to be efficient and effective.

2) Iris Normalization: The size of the pupil may change due to the variation of the illumination and the hippus and the associated elastic deformations in the iris texture may interfere with the results of pattern matching. For the purpose of accurate texture analysis, it is necessary to compensate this deformation. Since both the inner and outer boundaries of the iris have been detected, it is easy to map the iris ring to a rectangular block of texture of a fixed size.

3) Image Enhancement: The original iris image has low contrast and may have non-uniform illumination caused by the position of the light source. These may impair the result of the texture analysis. We enhance the iris image and reduce the effect of non-uniform illumination by means of local histogram equalization [4].

VI. TESTING BIOMETRIC SYSTEM

All biometric tests are accuracy based. A summary of the more common of these tests is described below:

A. Acceptance Testing

The process of determining whether an implementation satisfies acceptance criteria and enables the user to determine whether or not to accept the implementation. This includes the planning and execution of several kinds of tests (e.q., functionality, quality, and speed performance testing) that demonstrate that the implementation satisfies the user requirements.

B. Conformity

Fulfillment by a product, process or service of specified requirements.

C. Conformity Evaluation

Systematic examination of the extent to which a product process or service fulfils specified requirements.

D. Interoperability Testing

The testing of one implementation (product, system) with another to establish that they can work together properly.

E. Performance Testing

Measures the performance characteristics of an Implementation Under Test (IUT) such as its throughput, responsiveness, etc., under various conditions.

F. Robustness Testing

The process of determining how well an implementation processes data which contains errors.

VII. BIOMETRIC PERFORMANCE MEASUREMENTS

The performance of biometric system is tested usually in terms of False Rejection Rate (FRR), False Acceptance Rate (FAR), Failure to Enroll Rate (FER), Enrollment Time, and Verification Time. The false acceptance rate is most important when security is a priority whereas low false rejection rates are favored when convenience is the priority [3].

The biometric system employed in the flight deck must have a low false acceptance rate since security is the priority. If the false acceptance rate is a low as possible then we have better chance of not allowing unauthorized subjects into the system. The point at which the FAR and FRR meet or crossover is known as the equal error rate. This rate gives a more realistic measure of the performance of the biometric system rather than using either the FAR or FRR individually.

VIII. IMPLEMENTATION OF SYSTEM

In order to implement this iris system efficiently, ASP.NET program is used. This program could speed up the development of this system because it has facilities to draw forms and to add library easily [6].

The researchers presented a system based on phase code using Gabor filters for iris recognition and reported that it has excellent performance on a diverse database of many images. A system for personal verification based on automatic iris recognition. It relies on image registration and image matching, which is computationally very demanding. An algorithm for iris feature extraction using zero crossing representation of 1-D wavelet transforms. All these algorithms are based on grey images, and color information was not used. Grey iris image can provide enough information to identify different individuals. The iris identification is basically divided in four steps.

A. Capturing the Image

A good and clear image eliminates the process of noise removal and also helps in avoiding errors in calculation. In practical applications of a workable system an image of the eye to be analyzed must be acquired first in digital form suitable for analysis.

B. Defining the Location of the Iris

The next stage of iris recognition is to isolate the actual region in a digital eye image. The part of the eye carrying information is only the iris part. Two circles can approximate the iris image, one for the iris sclera boundary and another interior to the first for the iris pupil boundary. The segmentation consists of binary segmentation, pupil center localization, circular edge detection and remapping.

1) Binary Segmentation: For finding the pupil and limbus circular edges in the location of the pupil center is required. The segmentation is such that only pupil part is extracted.

2) Pupil Center Location: The binary-segmented image the row gradient is taken in one direction. The pixel location corresponding to maximum gradient is found out. Then row gradient is taken in the reverse direction. And the pixel

location corresponding to maximum gradient is found out. Then maximum of all these distances is the distance corresponding to diameter of the pupil circle. The row corresponding to diameter gives us x_0 co-ordinate for pupil center. In the same way above procedure is repeated for column gradients and y_0 co-ordinate for pupil center.

3) Circular Edge Detection: Iris analysis begins with reliable means for establishing whether an iris is visible in the video image, and then precisely locating its inner and outer boundaries (pupil and limbus). Because of the felicitous circular geometry of the iris, these tasks can be accomplished for a raw input image.

The complete operator behaves in effect as circular edge detector, that searches iteratively for maximum contour integral derivative with increasing radius at successively finer scales of analysis through three parameter space of center and radius (x_0, y_0, r) defining the path of the contour integration. The fitting contour to images via this type of optimization formulation is a standard machine vision technique, often referred to as active contour modeling [7].

4) Remapping of the Iris: To make a detailed comparison between two images, it is advantageous to establish a precise correspondence between characteristic structures across the pair. The system compensates or image shift, scaling, and rotation. Given the systems' ability to aid operators in accurate self-positioning, these have proven to be the key degrees of freedom that required compensation. Iris localization is charged with isolating an iris in a larger acquired image and thereby essentially accomplishes alignment for image shift. The system uses radial scaling to compensate for overall size as well as a simple model of pupil variation based on linear stretching. This scaling serves to map Cartesian image coordinates to dimensionless polar image coordinates.

C. Feature Extraction

We implement two well-established texture analysis methods to extract features from the normalized block of texture image, namely the multi-channel Gabor filter and the wavelet transform. The process of feature extraction starts by locating the outer and inner boundaries of the iris. The second step finds the contour of the inner boundary i.e., the iris-pupil boundary.

D. Matching

Comparison of bit patterns generated is done to check if the two irises belong to the same person. Calculation of Hamming distance (HD) is done for this comparison. The Hamming distance is a fractional measure of the number of bits disagreeing between two binary patterns. Two similar irises will fail this test since distance between them will be small. The test of matching is implemented by the simple Boolean Exclusive-OR operator (XOR) applied to the 2048 bit phase vectors that encode any two iris patterns. Letting A and B be two iris representations to be compared, this quantity can be calculated as with subscript 'j' indexing bit position and Θ denoting the exclusive-OR operator.

IX. CONCLUSION

This paper has presented a new approach to provide secure biometric identification systems using iris technology. Further, we have focused only on the core technology of iris capturing the image, location of the iris, feature extraction, and matching. Iris recognition has proven to be a very useful and versatile security measure. It is a quick and accurate way of identifying an individual with no room for human error. Iris technology is widely used in the transportation industry and can have many applications in other fields where security is necessary. Its use has been successful with little to no exception, and iris technology will prove to be a widely used security measure in the future.

ACKNOWLEDGEMENT

Over the last six months many people have contributed this research work. The authors would like to thank the Associate Editor and the anonymous reviewers, whose comments helped to improve for performing the training data and assisting with processing and analyzing the data. Finally authors would also like to thank each and every individual that the authors have not mentioned above, who gave even the slightest support through the lifetime of the research work.

REFERENCES

[1] J. Daugman, “High confidence personal identification by rapid video analysis of iris texture”, in Proceedings of the 1992 IEEE International Carnahan Conference on Security Technology, 1992.

[2] J. Daugman, “The importance of being random: Statistical principles of iris recognition”, in Pattern Recognition, Vol. 36, No. 2, pp. 279–291, 2013.

[3] T. Matsumoto, M. Hirabayashi, and K. Sato: “A Vulnerability Evaluation of Iris Matching (Part 3)”, in Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS), Institute of Electronics, Information and Communication Engineers, pp. 701 – 706, 2020.

[4] R.Wildes, “Iris recognition: an emerging biometric technology,” Proc. IEEE, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.

[5] Liu S. And Silverman M. “A Practical Guide to Biometric Security Technology”, January 2021.

[6] UK Biometrics Working Group,” Use of biometrics for identification and authentication: Advice on Product Selection”, November 2021.

[7] A.K. Jain, Ruud Bolle and Sharath Pankanti “Biometrics: Personal Identification in Networked Society” Publisher: Springer; 1st ed. 1999. 2nd Printing Edition 2005.

[8] Samir Nanavati, Michael Thieme and Raj Nanavati “Biometrics: Identity Verification in a Networked World” Publisher: Wiley; 1st Edition 2022.

March 2024
Vol - 14 No. - 03
@IJITCE Publication