IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

Biometric Authentication: Iris Recognition

Jyoti.Sarambale[1], Rama Bansode[2]

P.G. Student, Department Master of Computer Application, Modern College of Engineering , Shivaji Nagar, Pune, India[1]

Associate Professor, Department of Computer Application, Modern College of Engineering, Shivaji Nagar, Pune, India[2]

ABSTRACT: Humans recognize one another per their various characteristics for ages. We recognize others by their face once we meet them and by their voice as we speak to them. to realize more reliable verification or identification we should always use something that basically characterizes the given person. Biometrics offer automated methods of biometric authentication or identification on the principle of measurable physiological or behavioral characteristics. looking on the context, a biometric system will be either a verification (authentication) system or an identification system. Biometrics could be a rapidly evolving technology which has been widely employed in forensics like criminal identification and prison security. This research has information of Iris recognition with working principal & application.

I. INTRODUCTION

Biometric authentication can be a security process that relies on the unique biological characteristics of a private to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Typically, biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices.

The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. Once an intruder acquires the user ID or network access. Many other applications in everyday life also require user authentication, such as banking, e-commerce, and physical access control to computer resources, and could benefit from and the password, the intruder has total access to the user's resources.

User authentication methods can be broadly classified into three categories as shown in Table 1. Because a biometric property is an intrinsic property of an individual, it is difficult to surreptitiously duplicate and nearly impossible to share. Additionally, a biometric property of an individual can be lost only in case of serious accident

Table I Authentication Methods

Method	Examples	Properties
What you know?	User ID Password PIN	Shared Many passwords easy to guess Forgotten
What you have?	Cards Badges Keys	Shared Can be duplicated Lost or stolen
What you know and what you have?	ATM card + PIN	Shared PIN a weak link (Writing the PIN on the card)
Something unique about the user	Fingerprint Face Iris Voice print	Not possible to share Repudiation unlikely Forging difficult Cannot be lost or stolen

Biometric authentication works by comparing two sets of data: the first one is preset by the owner of the device, while the second one belongs to a device visitor. If the two data are nearly identical, the device knows that "visitor" and "owner" are one and also the identical and provides access to the person.

The important thing to note is that the match between the two data sets must be **nearly identical** but not **exactly identical**. This is because, it's close to impossible for 2 biometric data to match 100%. For instance, you'd possibly have a slightly sweaty finger or a touch, tiny scar that changes the print pattern.

Designing the process so that it doesn't require an exact match greatly diminishes the chance of a false negative (the device doesn't recognize your fingerprint) but also increases the odds that a fake fingerprint might be considered genuine

II. LITERATURE REVIEW

Wencheng Yang et.al [1] has done a comprehensive review to shed light on the latest developments in the study of fingerprint-based biometrics covering these two aspects with a view to improving system security and recognition accuracy. Based on a thorough analysis and discussion, limitations of existing research work are outlined and suggestions for future work are provided. It is shown in the paper that researchers continue to face challenges in tackling the two most critical attacks to biometric systems, namely, attacks to the user interface and template databases. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is a hot research topic currently, as well as in the foreseeable future. Moreover, recognition accuracy under non-ideal conditions is more likely to be unsatisfactory and thus needs particular attention in biometric system design. Related challenges and current research trends are also outlined in this paper.

NehaKak et.al [2] has mentioned Iris Recognition and its application. In a biometric system a person is identified automatically by processing the unique features that are posed by the individual. Iris Recognition is regarded as the most reliable and accurate biometric identification system available. In Iris Recognition a person is identified by the iris which is the part of eye using pattern matching or image processing using concepts of neural networks. The aim is to identify a person in real time, with high efficiency and accuracy by analysing the random patters visible within the iris if an eye from some distance, by implementing modified Canny edge detector algorithm. The major applications of this technology so far have been substituting for passports (automated international border crossing); aviation security and controlling access to restricted areas at airports; database access and computer login.

Marcos Faundez et.al [3] has presented an overview of the main topics related to biometric security technology, with the main purpose to provide a primer on this subject. Biometrics can offer greater security and convenience than traditional methods for people recognition. Even if we do not want to replace a classic method (password or handheld token) by a biometric one, for sure, we are potential users of these systems, which will even be mandatory for new passport models. For this reason, to be familiarized with the possibilities of biometric security technology is useful.

Ravi Subban et.al [4] has presented an overview of fingerprint technique. Fingerprint (FP) serves to identify that the person authenticating is who he/she claims to be. FP identification is popular biometric technique due to easiness in acquiring, availability of plenty sources (i.e. ten fingers) for collecting data and their established use. This paper summarizes the research work carried out in FP matching techniques, recognition methods and their performance analysis.

III. WHAT IS BIOMETRIC AUTHENTICATION

Biometric authentication asks the question "can you prove who you are" and is predominantly related to proof of identity in digital scenarios. A system will challenge someone to prove their identity and the person has to respond in order to allow them access to a system or service.

Traditionally, the response involves presenting an authenticator, or factor, that is bound to that person. The system would then ask for a secret that the person knows, like a PIN/Password or a one-time-password (OTP) generated by a cryptographic process, or something the person has, such as a private key stored on a smartcard that is used as part of Public Key Infrastructure (PKI) authentication.

Biometric authentication involves use of a factor that is something a person is – a biometric identifier from a person can include a fingerprint, their voice, face, or even their behavior. This biometric is indexed against other identifiers, such as a user id or employee number, with the identifier being matched against a single stored biometric template – one-to-one match.

IV. BIOMETRIC PROCESS

Two different stages are involved in the biometric system process
I) Enrollment,
II) Verification.

I. Enrollment: As shown in Figure I, the biometric image of the individual is captured during the enrollment process (e.g., using a sensor for fingerprint, microphone for voice verification, camera for face recognition, scanner for eye scan). The unique characteristics are then extracted from the biometric image to create the user's biometric template. This biometric template is stored in a database or on a machine-readable ID card for later use during an identity verification process.

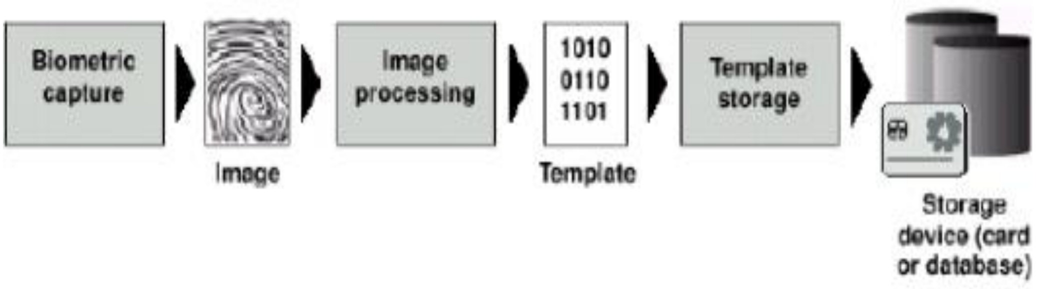

Figure 1 Enrollment Process

II. Verification: Figure II illustrates the identity verification process. The biometric image is again captured.

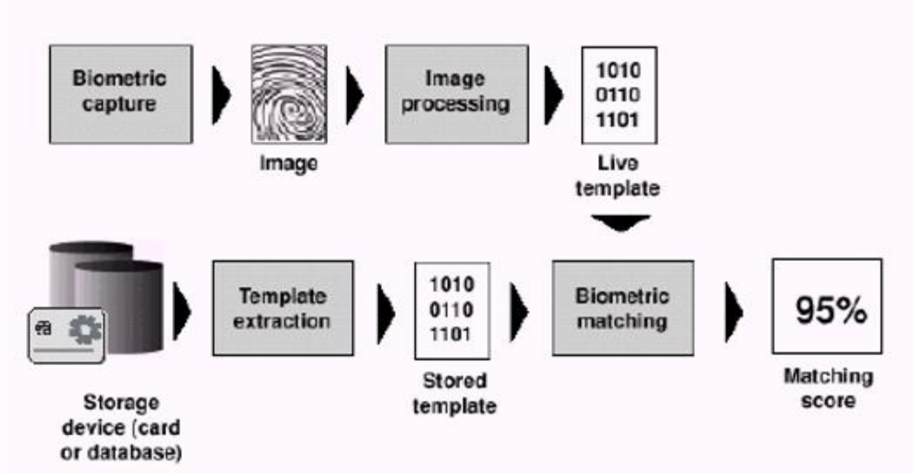

Figure 2 Verification Process

The unique characteristics are extracted from the biometric image to create the user's "live" biometric template. This new template is then compared with the template previously stored and a numeric matching score is generated, based on the percentage of duplication between the live and stored template. System designers determine the threshold value for this identity verification score based upon the security requirements of the system.

V. TYPES OF BIOMETRICS

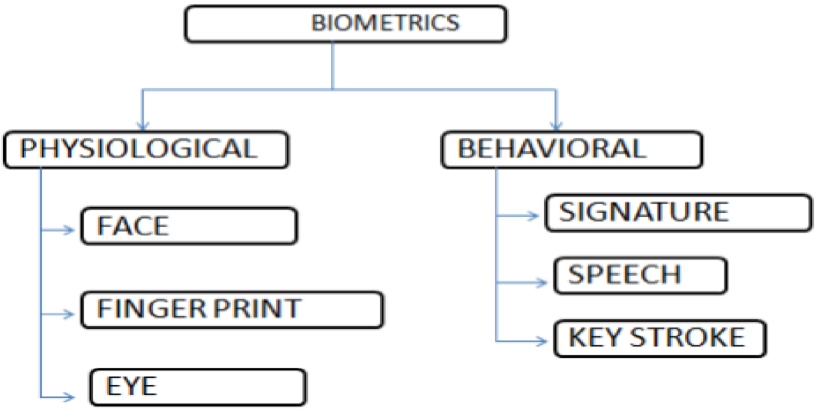

Figure 3 Types Biometrics

- **Physical Biometrics**

  A physiological characteristic type of biometric measurement is usually unchanging and unalterable without significant duress to the individual.

i. **Fingerprint-** Fingerprint recognition, which measures a finger's unique ridges, is one of the oldest forms of biometric identification. After capturing the print, sophisticated algorithms use the image to produce a unique digital biometric template. The template is then compared to new or existing scans to either confirm or deny a match.

ii. **Facial Recognition-** Facial recognition is, by far the oldest form of biometric authentication. Even infants use facial recognition to identify the people closest to them. Biometric facial recognition software works much the same way, albeit with more precise measurements. Specifically, facial recognition software measures the geometry of the face, including the distance between the eyes and the distance from the chin to the forehead (just to name a few). After collecting the data, an advanced algorithm transforms it into an encrypted facial signature.

iii. **Hand Geometry-** Hand geometry biometrics refer to the measurement of hand characteristics like the length and width of fingers, their curvature, and their relative position to other features of the hand. Though once a dominant method of biometric measurement, modern advances in fingerprint and facial recognition software have replaced its relevance in most advanced applications.

iv. **Iris recognition-** The iris, or the colored part of the eye, consists of thick, thread-like muscles. These muscles help shape the pupil to control the amount of light that enters the eye. By measuring the unique folds of these muscles, biometric authentication tools can confirm identity with incredible accuracy. Liveness detection (like requiring a user to blink for the scan) adds an additional layer of accuracy and security

v. **Vascular Patterns-** Veins are considerably harder to hack than other biometric scans because they occur deep within the skin. Infrared lights pass through the skin surface where they absorb into deoxygenated blood. A special camera captures the image which digitizes the data then either stores it or uses it to confirm identity.

vi. **Retinal Scan-** Retinal scans capture capillaries deep within the eye by using unique near-infrared cameras. The raw image is first preprocessed to enhance the image then processed again as a biometric template to use during both enrollment and verification.

- **Behavioral Biometrics:**

  A behavioral characteristic is more a reflection of an individual's psychological makeup. A signature is the most common behavioral biometric used for identification. Because most behavioral characteristics vary over time, an identification system using these must allow updates to enrolled biometric references.

i. **Speaker Recognition-** Voice recognition technology falls under both the physiological and behavioral biometric umbrellas. Physically speaking, the shape of a person's vocal tract, including the nose, mouth, and larynx determines the sound produced. Behaviorally, the *way* a person says something – movement variations, tone, pace, accent, and so on – is also unique to each individual. Combining data from both physical and behavioral biometrics creates a precise vocal signature though mismatches due to illness or other factors can occur.

ii. **Signature-** Signature recognition is a behavioral biometric that measures spatial coordinates, pen pressure, inclination, and pen stroke in both "off-line" and "on-line" applications. A digital tablet records measurement then uses the information to automatically create a biometric profile for future authentication.

iii. **Keystroke-**Keystroke dynamics take standard passwords to the next level by tracking the rhythm used to enter a password. Measurements might include the time it takes to press each key, delays between keys, characters typed per minute, and so on. Keystroke patterns work in conjunction with passwords and PINs to improve security efforts.

VI. IRIS RECOGNITION

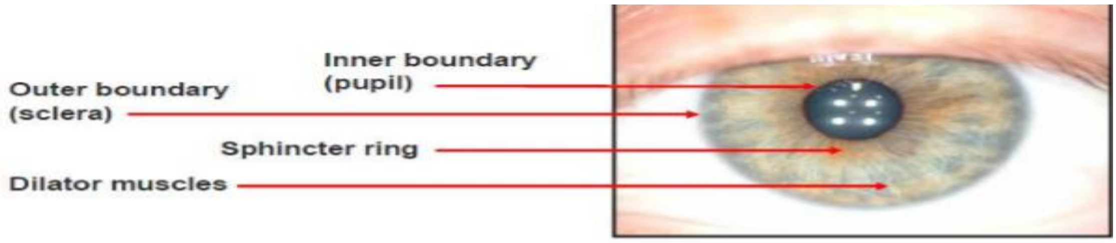

Figure 4 Iris Scan

- **Principal:** Iris recognition determines people's identity by comparing the similarities between iris image features. The core of iris recognition is to describe and match iris features of human eyes using pattern recognition and image processing methods, so as to realize automatic personal identity authentication.

- **Steps Of Recognition:**.

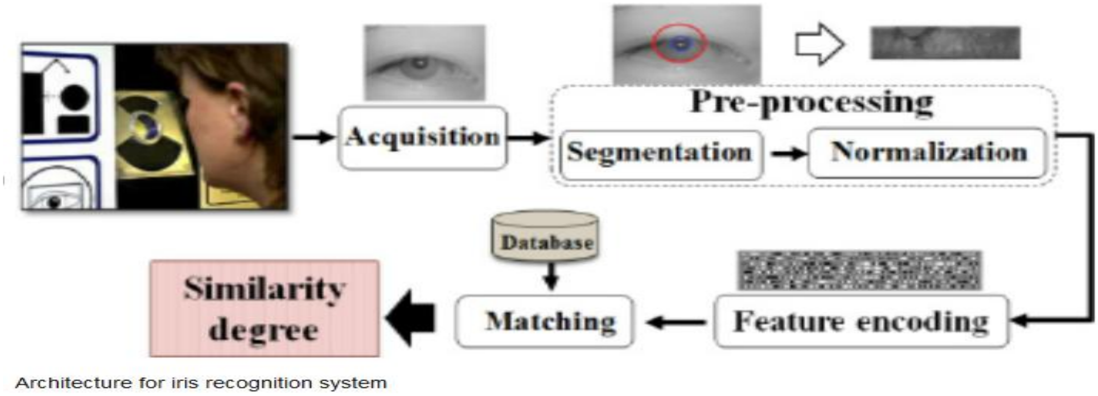

Figure 5 Architecture for this recognition system

The main steps of iris recognition include iris image acquisition, preprocessing, feature extraction, coding and classification.

i. **Iris Image Acquisition -**Iris image acquisition refers to the use of specific digital camera equipment to require pictures of the entire human eye, and also the captured image is transmitted to the computer through the image acquisition card for storage. The acquisition of iris image is the beginning in iris recognition, and its also a difficult step. It needs the comprehensive application of optical, mechanical and electrical technology. Because the area of people's eyes is small, if we want to meet the image resolution requirement of recognition algorithm, we must improve the magnification factor of optical system, which leads to a smaller depth of field of iris imaging. Therefore, the existing iris recognition system requires users to stop at the appropriate location, while the eyes stare at the lens (Stop and Stare). In additionally, the Oriental iris is darker and can not capture recognizable iris images with ordinary cameras. Different from image acquisition of biological features like face image and gait, iris image acquisition has to design an affordable optical system, equipped with the necessary light source and electronic control unit.

ii. **Image Preprocessing -** Image preprocessing refers to the necessity for image smoothing, edge detection, image separation and other preprocessing operations because the captured eye image contains a lot of redundant information and can’t meet the requirements in clarity and other aspects.
The process of iris image preprocessing usually includes iris localization, iris image normalization and image enhancement.

- **Iris localization -** It is generally believed that the inner and outer boundaries of the iris is approximately fitted by circles. The inner circle represents the boundary between the iris and the pupil, and the outer circle represents the boundary between the iris and the sclera, but these two circles aren't concentric circles. Usually, the part of the iris near the upper and lower eyelids is usually covered by the eyelids, so it is necessary to detect the boundary between the iris and also the upper and lower eyelids, so as to accurately determine the effective area of the iris. The boundary between the iris and also the upper and lower eyelids can be represented by a two degree curve. The purpose of iris localization is to determine the location of these two circles and the two degree curves in the image. The commonly used location methods can be roughly divided into two categories: one is the combination of edge detection and Hough transform; the other is the method based on edge search. The common disadvantage of these two methods is that the operation time is long, so there are some improved methods supported the above two strategies, but the speed has not increased by an order of magnitude. Localization is remains one of the longest operation steps in iris recognition.
- **Iris image normalization -** The aim of iris image normalization is to regulate the iris to a fixed size. So far, the exact mathematical model of iris texture changes with illumination has not been obtained. Therefore, researchers engaged in iris recognition mainly use the mapping method to normalize iris images. If the method of iris texture changing with illumination intensity is modeled or simulated approximately, it will be helpful to boost the performance of iris recognition system.
- **Photographic enhancement -**The aim of image enhancement is to solve the problem of low contrast of normalized image caused by uneven illumination of human eye image. So as to boost the popularity rate, its necessary to boost the normalized image.

VIII. BENEFITS OF IRIS RECOGNITION

- **Accuracy**: Iris recognition is taken into account to be the most accurate biometric modality available. There is a 1 within the 10^{78} chance that the iris pattern of two individuals is identical.
- **Stability**: The iris pattern generally doesn't change throughout our lifetime.
- **Hygiene**: Iris recognition is contactless rendering it much more hygienic than other available modalities.
- **Speed**: The iris template size is tiny which helps facilitate fast matching.
- **Popularity/Acceptance**: Together with fingerprint, iris recognition technology is arguably one of the most popular and recognizable biometric technologies around the world because it contains a strong acceptance rate supported the non-invasive, non-contact, hygienic characteristics of the technology.

VIII. CONCLUSION

Iris recognition could be a very useful and versatile technique. Iris recognition is extremely accurate technique. This system has successful applications. This system increases both privacy and identity. Highly secure biometric method. Iris recognition could be a very easy process involving very less steps. Iris recognition consumes less time in comparison to other biometric recognition techniques. Iris recognition could be a quick and accurate way of identifying an individual. This system is now into use in fields involving high security concerns

REFERENCES

1. Wencheng Yang, "Security and Accuracy of Fingerprint-Based Biometrics", Received: 2 December 2018; Accepted: 23 January 2019; Published: 28 January 2019
2. Neha Kak, Rishi Gupta, Sanchit Mahajan, "Iris Recognition System", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, o. 1, 2010
3. Marcos Faundez, "Biometric security technology", Article in IEEE Aerospace and Electronic Systems Magazine · July 2006
4. Ravi Subban, "A Study of Biometric Approach Using Fingerprint Recognition", Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013
5. Anil Jain Michigan,Brendan Klare, Noblis Arun, "Guidelines for Best Practices in BiometricsResearch", Appeared in Proc. Of 8th IAPR International Conference on Biometrics, (Phuket,Thailand), May 2015
6. Mr. Rahul A.Patil[1], Mr.A.H.Karode[2], Mr.S.R.Suralkar[3], "Steps of Human Iris Detection for Biometric Application", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com