JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IRIS BIOMETRICS: A REVIEW OF CURRENT TRENDS AND FUTURE PROSPECTS

Pooja Biswal[1], Gurajala Abbulu[2], Tabbussum Parveeni[3]

UG II Year Student, Department of Forensic Science, GIET Degree College, Rajahmundry.

UG II Year Student, Department of Forensic Science, GIET Degree College, Rajahmundry.

Assistant Professor, Department of Forensic Science, GIET Degree College, Rajahmundry.

ABSTRACT

Biometrics is an advanced technology that provides authentication to system access through a sensor because they are unique to each and every person. There are various types of biometrics like fingerprint, face recognition, voice, iris, palm, etc. However, in present days, we need a strong biometric to protect our belongings and data. One example of such secured and strong biometric is iris pattern recognition. Iris pattern biometrics is a highly reliable and secure technology for personal identification. It leverages the unique and intricate patterns found in the human iris to establish individual identity. The iris pattern remains relatively stable over time, and it is difficult to reverse-engineer an individual's identity from iris data. Iris pattern biometrics has emerged as a robust and secure means of identity verification. Its high accuracy, non-intrusive nature, and resistance to fraud make it a valuable technology in various fields, contributing to enhanced security and privacy in a world where digital authentication is of paramount importance.

KEYWORDS: Authentication, Acquisition, Encoding, DNA amplification

1. INTRODUCTION

Passwords have historically been the main keys to the digital world, providing theoretical strength because they are stored only in the user's memory. But when people find it difficult to remember complicated passwords, they turn to unsafe methods like writing them down or sharing them, which creates practical problems. Hackers now often use these human weaknesses as a means of attack. Password security is further jeopardized by automated attacks like keyloggers. Companies are faced with a conundrum when it comes to human security and compliance, as they require strong authentication.

Because of all these disadvantages of using passwords there is a need for safe and efficient way to safeguard one’s data. To surmount the drawback of passwords, biometric technology emerged as an innovative way to protect any device from unauthorised access.[1]

DEFINITION:

The term biometric is adopted from the Greek literature in which Bio means “life” and Metric refers to “measure”. Biometric is a measurable feature of a person's physical attributes or behaviour that is used to confirm or establish an applicant's claimed identification.[2]

Biometrics, or biometric recognition, is a dynamic field that is rapidly advancing and finds applications in everything from computer access to passport admission. These systems use behavioural or physical characteristics, like voice, hand geometry, face features, and fingerprints, to verify an individual's identity.[3]

1.2. History and evolution of Biometrics

Though the first recorded use of biometrics dates to the Babylonian empire in 500 BC, the first biometric identification system was documented in Paris, France in the 1800s. Alphonse Bertillon invented a system for categorizing and contrasting criminals using particular body measurements. Bertillon's technique represented the first steps toward using distinguishing biological characteristics for identification verification, notwithstanding its flaws.

Fingerprinting became widely used in the 1880s as a means of contract signatures as well as a way to identify offenders. Although it is acknowledged that a fingerprint serves as a representation of a person's identify and accountability, there is ongoing discussion regarding who invented fingerprinting as a method of identification. However, Edward Henry is recognized for creating the first standardized system for fingerprint-based identification, the Henry Classification System.

The field of biometrics had tremendous expansion as a research area over the next century. There were many innovations in the 1900s, and although it would be impossible to list them all, the following are notable breakthroughs from the last quarter of the century:

1960s: Before the advent of automated phone security systems, administrators had to manually evaluate facial features in an image and extract useable feature points. This was due to the birth of semi-automatic facial recognition algorithms.

1969: The FBI made the decision to invest in automated fingerprint and face recognition technology due to its wide-ranging application in law enforcement. The creation of more advanced sensors for biometric data extraction and capture was sparked by this effort.

The National Institute of Standards and Technology was founded in the 1980s.

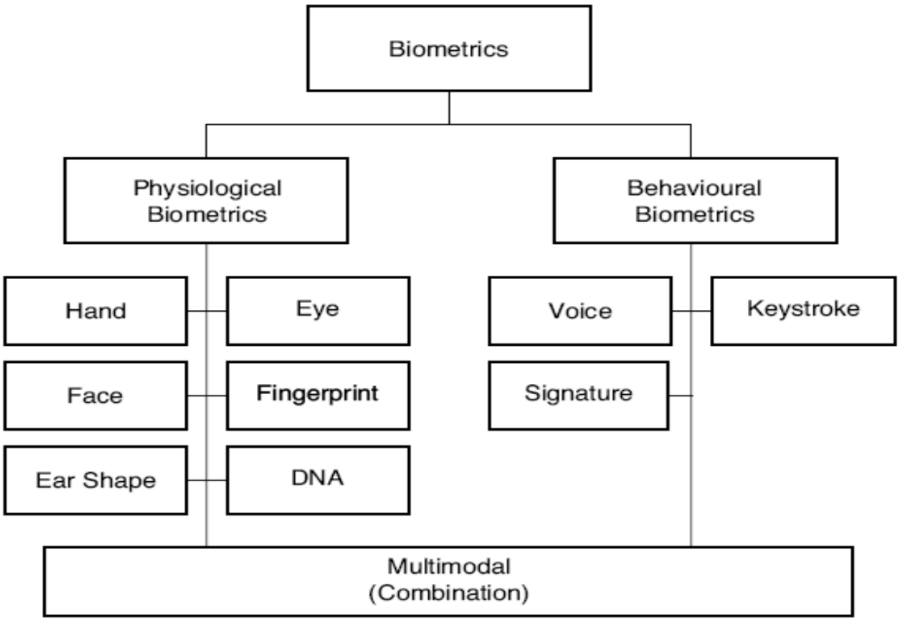
1985–1994: In response to the 1985 hypothesis that iris patterns were distinctive, akin to fingerprints, the first iris identification algorithm was patented by 1994. The utilization of eye blood vessel patterns for identification was made possible by the simultaneous revelation that these patterns were distinct.

1991: Despite its inherent shortcomings, real-time recognition was made possible by the advancement of facial detection technology. This increase in demand drove additional developments in face recognition technology.

2000s: Several biometric authentication recognition algorithms were functioning and patented in the United States during the start of the twenty-first century. The usage of biometrics has evolved from being restricted to use in government and large business contexts to being incorporated into commercial items and utilized at major events, such as the 2001 Super Bowl.

Biometric technology has advanced significantly over the last ten years, with new developments coming on the scene almost every day. What was formerly thought to be innovative has now become a necessary component of our everyday existence. When Apple introduced fingerprint technology to unlock iPhones in 2013, it marked a turning point in this trajectory by encouraging the general public to adopt biometrics as the primary means of authentication. Many mobile phones on the market now include biometric features, and many applications use biometrics as a regular way to authenticate daily operations.[4]

2. TYPES OF BIOMETRICS



Physiological characteristics, such as hand shapes, retinal blood vessel patterns, iris pattern, DNA fingerprints, and facial features, show extraordinary stability and constancy across time. On the other hand, behavioural traits might change as a result of age, trauma, or even changes in mood. The following data lists numerous methods divided into seven categories, which include these:

2.1. Hand Recognition Technology

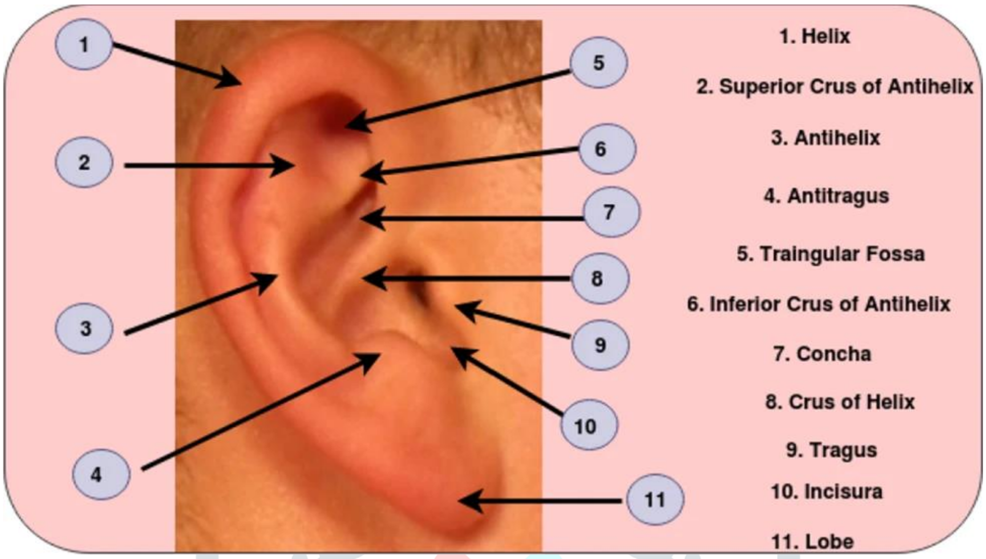
PALM RECOGNITION [27]

Of all the biometric modalities, hand geometry systems have the longest implementation history. David Sidlauskas created and patented the idea of hand geometry in 1985, and the following year saw the release of the first professional hand geometry recognition devices. When hand geometry systems were used to control and secure physical entrance to the Olympic Village during the 1996 Games, the importance of this technology was highlighted.[5]

It's based on a fact that the shape of hand is different for everyone and it doesn't change after a certain age. This methodology involves the estimation of thickness, width, length and surface area of the hand [6,7]

It involves measuring of physical dimensions from a 3D image. The prospect places hid hand on the sensor in exact position and the camera captures required details which doesn't include any surface details like skin colour, injuries etc. [8,9,10,11]

2.2: EAR BIOMETRICS



EAR BIOMETRICS [28]

This biometric recognition method uses both 2D and 3D methodologies to examine the form of the outer ear, the ear lobes, and the bone structure. After obtaining a side profile image from a sensor, the system separates the ear from surrounding features such as clothing, facial hair, and facial regions. In order to identify the ear pit, define the visible ear region, and account for changes in skin tone, ear size, shape, hair occlusion, and the presence of earrings, the algorithm integrates colour and depth analysis.[11]

2.3. FACIAL RECOGNITION

FACE RECOGNITION BIOMETRIC [28]

A facial recognition system compares a user's facial traits with a pre-designated database to identify or authenticate people from digital photos or video frames. For unique identification, this biometric artificial intelligence program uses pattern analysis based on facial textures and forms. It was first created as a computer program, but it has now been extended to mobile devices and other technological fields, such as robotics.

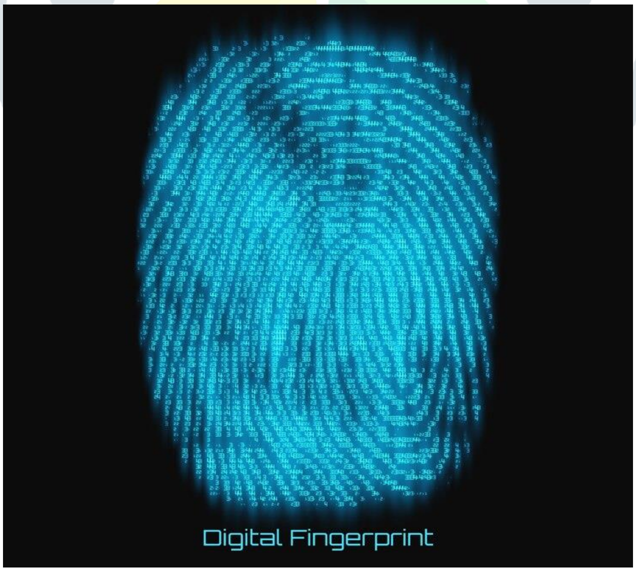
Despite having a lower accuracy rate than other biometrics like fingerprint and iris recognition, it is nonetheless widely used in security systems for access control. Its non-invasive and contactless operation features are responsible for its wide acceptance.[12]

2.4. IRIS BIOMETRIC

IRIS RECOGNITION TECHNOLOGY [29]

The actual concept of utilising iris for the purpose of recognition was put forward in 1930s, but a perfect algorithm for automated iris recognition was not developed until early 1990's. [11]. The process which involves recognising a person by analysing the irregular or random iris pattern is known as iris recognition. The iris is a muscular structure that controls the size of the pupil, which in turn controls the amount of light that enters the eye. The quantity of melatonin pigment in the muscle gives this coloured portion of the eye its unique colour.[13]

2.5. FINGERPRINT RECOGNITION



FINGERPRINT BIOMETRIC [Garry Killian]

The theory that fingerprints are personal to each person and mostly unchanged throughout life gained acceptance in the 19th century. Due to this recognition, fingerprints are now widely used for personal identification. Raised ridges and valleys make up the unique pattern of fingertip skin, which is utilized in biometric identification. The three main fingerprint features—arches, loops, and whorls—as well as maybe other elements like the core and delta, contribute in the recognition of patterns. A fingerprint pattern's centre is called the core, and the point where three patterns diverge is called the delta. It is noteworthy that while the core and delta can function as corresponding landmarks, they are not present in all fingerprints.[12]

2.6. DNA (De-oxyribonucleic Acid)

DNA as biometric [30]

Although identical twins have the same DNA sequence, each person has a unique identity based on the genetic differences found in their De-oxyriboNucleic Acid (DNA), a one-dimensional code that is specific to each individual. In forensic applications, DNA is often used for personal identification. The first step in forensic processes is to gather a DNA sample from the crime site, which might be blood or hair. After that, the targeted loci in the extracted DNA are amplified. Next, the DNA is sliced and sorted according to size, which is connected with the number of repeating units. The resultant transcribed DNA profile, which includes information on the number of repeat units at each locus, offers a digital depiction of variability in certain regions.

3. IRIS BIOMETRIC TECHNOLOGY:

Iris recognition is the process of determining someone by seeing their distinct, random pattern on their iris. Only since 1994 has this automated system been patented, making it relatively new. The iris, a muscular component in the eye, controls the size of the pupil, which in turn controls the amount of light that enters the eye. It is the coloured portion of the eye, and the amount of melatonin pigment in the muscle determines the colour of the area. The iris functions as an externally visible object that may be evaluated from a distance with the use of an automated machine vision system for iris recognition.

A. Computer vision, pattern recognition, statistical inference, and optics are all combined into the iris recognition technology.

B. Every individual has a different set of unique spatial patterns in their iris.

3.1. WORKING MECHANISM OF IRIS TECHNOLOGY

Iris recognition system is composed of numerous sub-systems, they correspond to each stage of this system. The stages are:

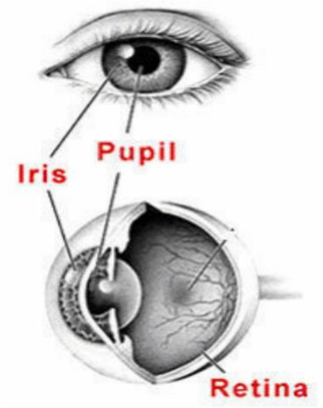
- Image capture-which involves taking a picture of an eye
- Segmentation- which involves locating the iris area in an image of an eye
- Normalization- which involves creating a dimensionally consistent representation of the iris region.

- Feature encoding- involves creating a template that solely comprises the most notable characteristics of the iris. [14,15]

The system generates an iris template as an output after receiving a picture of an eye as input. The iris region is represented mathematically by the iris template.[14]

Let us study each and every sub-stage of iris recognition technology in detail

3.1.1. IMAGE ACQUISITION



Because the success of the feature extraction step depends on the quality of the image, the iris image needs to have a strong iris texture. A 3CCD camera is used to accomplish this, and it is placed about 9 cm from the user's eye. The user and the light source are separated by about 12 centimeters. For the image acquisition setup, see Figure. The following factors were noted when taking pictures:

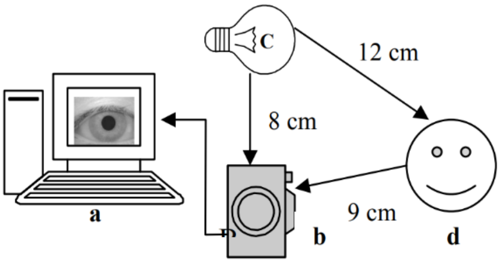
• High sharpness and resolution: necessary for precise identification of the boundaries between the inner and outer circles.

• Sufficient lighting: To avoid the spotlight effect, the system uses diffused light.

3.1.2. SEGMENTATION

Isolating the genuine iris region from a digitized eye image is the first step in iris recognition. Two circles can be used to represent the iris region, as shown in the above figure. The first circle shows the line separating the iris from the sclera, while the second, inside the first, shows the line separating the iris from the pupil. [16,17]

The quality of ocular image capture is a determining factor in segmentation efficiency. The outside radius of iris patterns can be detected by using the pupil's centre. The Canny edge detector is used to locate the inner and outer constraints of the iris in order to identify the edge picture.[17]



3.1.3. MODIFIED CANY EDGE DETECTOR

The algorithm of this detector runs in 5 different stages:

Smoothing: Filtering and blurring techniques are used to the picture in an effort to remove noise, which in turn reduces the number of pixels that contribute to unwanted artifacts.

Finding gradients: Groupings of points or pixels that fall within a threshold range and have a similar colour pattern are created. Edges that show notable magnitudes in the image's gradients are noted.

Non-maximum suppression: The part of the image that needs to be processed is circular or convex, and it is not linear. Thus, taking into account only local maxima, the boundary region that most closely resembles the form is retrieved and then recognized as an edge.

Double thresholding: Thresholding is determined by potential edges

Edge tracking by hysteresis: It entails suppressing all edges that are not linked to a particular (strong) edge in order to identify the final edges.[18]

3.1.4. HOUGH TRANSFORM

A well known computer vision algorithm called the Hough transform is used to extract the characteristics of simple geometric structures in an image, including lines and circles. To be more precise, the pupil and iris regions' radius and centre coordinates can be deduced using the circular Hough transform.

The process of creating an edge map begins with calculating the first derivatives of the intensity values in an eye image. The output is then subjected to a threshold. The parameters of circles that pass through each edge point are then determined by casting votes in Hough space, starting from the edge points. These parameters are the radius r, the centre coordinates y_c and x_c, these are used to define any circle according to the equation

$$Y^2_c + X^2_c - r^2 = 0$$

3.1.5. IMAGE NORMALIZATION

The next step once the iris region has been successfully segmented is to normalize this section so that it can be easier to generate iris codes and compare them later. Because individual differences include the iris's optical size, pupil location within the iris, and orientation vary from person to person, normalizing the iris image is necessary to create a standard representation with constant dimensions for every subject [21].

Through the use of Daugman's Rubber Sheet model, the iris is unwrapped and transformed into its polar equivalent as part of the normalization process. The reference point is the pupil's centre, and points are mapped from the Cartesian scale to the polar scale using a remapping formula.

The radial resolution was configured at 100, and the angular resolution was set to 2400 pixels. Each pixel within the iris corresponds to an equivalent position on the polar axes [8]. Subsequently, the normalized image is interpolated to match the size of the original image, utilizing the interp2 function. In cases where parts of the normalized image result in NaN (Not a Number), they are divided by the sum to obtain a normalized value.

3.1.6. FEATURE EXTRACTION [DIGITIZATION]

Digitalization of the iris's characteristic elements—such as stripes, coronas, and freckles—is necessary for iris recognition. These features together make up the iris's texture. Secure biometric identification is built on top of this material. Feature extraction, an essential step in the digitalization of iris images, uses a variety of algorithms to identify and measure these complex features.

One such feature extraction method is wavelet encoding, which uses wavelet transformations to extract fine-grained iris texture data. Recognized for their effectiveness in texture analysis, gabor filters concentrate on extracting particular elements that add to the overall distinctiveness of the iris. Because they function on a logarithmic scale, log-Gabor filters offer more versatility in identifying pertinent iris information. The signal processing technique known as Haar Wavelet. [22]

3.1.7. PATTERN MATCHING

The main goal is to determine an exact correlation between characteristic structures of two images in the systems under discussion. Both methods improve their robustness and flexibility by skillfully compensating for variables such as picture shift, scaling, and rotation.

Iris localization assumes the task of separating the iris from a broader obtained image in the context of these technologies. This procedure accomplishes alignment in the event of picture shift in addition to guaranteeing feature extraction correctness. The localization process is essential to getting the images ready for the next stage of pattern matching.

Comparing the collected image's pixels with database-stored ones is the process of pattern matching. The algorithm used here takes a novel approach by making use of Artificial Neural Networks (ANNs). These guidelines are known as Supervised Learning. [23]

4. ADVANTAGES AND APPLICAIONS

- Approximately thirty percent of the top airport operators globally have effectively incorporated biometric technology, particularly iris recognition systems, into their access control schemes.
- The iris is one of the most effectively used biometrics to improve security, efficiency, and speed up airport operations. It is thought to be the best portion of the human body for biometric recognition. For both landside and airside applications, iris recognition has proven to have special qualities that greatly increase security levels, speed up procedures, and improve user identification.
- The IRIS, which is a highly sensitive and transparent membrane, provides the iris, an interior organ, with a strong defence mechanism against wear and damage. This distinguishes it from fingerprints, which may experience difficulties with recognition after prolonged exposure to particular kinds of physical activity.

- Similar to fingerprints, the iris has a finely textured pattern that is randomly generated during embryonic gestation. Notably, iris textures are completely independent among genetically identical individuals, setting it apart from the non-uniqueness of DNA.
- From a structural perspective, the iris is primarily flat and is controlled by two complimentary muscles that determine the pupil's diameter. Because of this feature, the iris's geometric shape is significantly more predictable than face recognition.[23]

4.2.FEATURES OF IRIS BIOMETRIC

- Variability to Promote Personality: Biometric systems are made to distinguish between people according to their unique traits. The more intricate and varied these characteristics are, the better the system is at differentiating between people.
- Finding an Equilibrium Point Between Intra- and Interpersonal Variability: For accurate identification, it is critical to maximize variability across people, but it is also critical to decrease variability within the same individual under various temporal and environmental variables.
- Face Recognition Complexities: Faces are dynamic and capable of expressing a wide range of emotions, which makes it difficult to create a consistent identification template due to facial dynamics.
- Faces' Three-Dimensional Nature: Since faces are three-dimensional objects, their projected appearances can vary depending on the viewer's point of view, lighting, and other components like clothes.

4.3.CHALLENGES OF IRIS BIOMETRIC

There are several drawbacks associated with the use of iris scanning technology that should be taken into account. To begin with, iris scanning is a very recent technological development that presents compatibility issues. This phenomenon is especially noticeable in situations where specific nations' immigration and law enforcement agencies have made substantial investments in fingerprint recognition technology. The incompatibility of these newly developed infrastructures with the iris scanning technology might lead to significant financial losses and impede the smooth integration of these biometric identification techniques,

An other noteworthy disadvantage of iris recognition is its restricted working range. Beyond a few meters, the technology finds it difficult to operate efficiently. This restriction gets worse when the person being recognized refuses to comply by keeping their head steady and staring straight into the camera. These limitations make iris scanning less useful and effective, particularly in situations where a quick and uncooperative identification procedure is essential.

Moreover, like other photometric biometric methods, iris recognition is prone to image quality problems. Higher enrollment failure rates may result from poor image quality. This flaw jeopardizes the iris scanning system's overall dependability and precision because accurate identification primarily depends on sharp, clear images.

In summary, even though iris scanning technology has great potential for biometric identification, it is critical to recognize and resolve its present drawbacks. Concerns about operating limits, compatibility with current systems, and vulnerability to low image quality are some of the major obstacles that must be carefully taken into account in the continuous development and application of iris recognition technologies.

4.4.WHY IRIS…?

Iris scanning was selected as a biometric identification technique because of its distinct benefits, which make it stand out from other security options, biometric or not.

Above all, iris scanning is more accurate and dependable than a lot of other security procedures.

Iris recognition's stability and speed are other factors in its popularity. By the time a person is ten months old, their distinct iris pattern starts to form and doesn't change throughout the course of their lifetime. It takes less than two minutes to complete the enrollment process, which comprises taking an image of the iris pattern while following instructions. Its exceptionally quick authentication process—which takes less than two seconds to verify identity—makes it an effective and practical option for a range of applications.

Its exceptionally quick authentication process—which takes less than two seconds to verify identity—makes it an effective and practical option for a range of applications.

Iris scanning technology is made more attractive by its scalability, flexibility, and expandability. Iris recognition data templates require a mere 512 bytes of storage for each iris. Large databases can be created thanks to this storage efficiency without sacrificing search speed or performance accuracy. Iris scanning is a flexible solution that can be tailored to the requirements of various scenarios and organizations due to its ability to adapt to diverse database sizes. [31]

5. CONCLUSION

In conclusion, iris scanning is preferred as a biometric identification technique because of its unmatched stability, speed, accuracy, and scalability. Because of these unique qualities, iris scanning is a dependable and effective option for security applications, providing a degree of security that is difficult to match by other options. There are various biometrics which are capable of functioning as an efficient biometric technology but they have many disadvantages or changes of vulnerability. They just couldn’t beat iris biometric in terms of efficiency and accuracy. Though it requires a bit high maintenance and investment to set up iris biometric technology for recognition it can be made affordable by using some techniques. This biometric should be employed whenever someone have to safeguard some important data or files.

REFERENCES:

1. Encyclopedia of biometrics, By Stan Z.Li
2. bhttps://csrc.nist.gov/glossary/term/biometrics#:~:text=A%20measurable%20physical%20characteristic%20or,are%20all%20examples%20of%20biometrics.
3. Jain, Anil K., Patrick Flynn, and Arun A. Ross, eds. Handbook of biometrics. Springer Science & Business Media, 2007.
4. BCAdmin | Dec 8, 2021 | Blog

5. NSTC Subcommittee on Biometrics , 2006.

6. E. Kukula, S. Elliott, “Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance”, In Proc. of 35th Annual International Carnahan Conference on Security Technology, UK, Oct. 2001, pp. 83 –88.

7. A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, “Personal Verification using Palmprint and Hand Geometry Biometric”, In Proc. of 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, Jun. 2003, pp. 668 - 678.

8. Zunkel (1999) op. cit.

9. Jain et al. (2004) op. cit.

10. OECD, Working Party on Information Security and Privacy (2004) op. cit.

11. Irish Council for Bioethics , Dublin ISBN 978-0-9563391-0-2 ,2009

12. Petrescu, Relly Victoria. "Face recognition as a biometric application." Journal of Mechatronics and Robotics 3 (2019): 237-257.

13. NSTC Subcommittee, “Iris Recognition”, Aug. 2006, http://www.biometricscatalog.org/NSTCSubcommittee.

14.http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Iris%20Recognition.pdf

15. xpertsolutions.fortunecity.es/Technology/Biometrics/XprecEng.htm

.16 .W.W. Boles, B. Boashah: A Human Identification Technique Using Images of the Iris and Wavelet Transform. IEEE Transaction on Signal Processing Vol. 46 (1998) 1185-1188

17. T. Chuan Chen, K. Liang Chung: An Efficient Randomized Algorithm for Detecting Circles.Computer Vision and Image Understanding Vol. 83 (2001) 172-191

18. J. Canny: A Computational Approach to Edge Detection. IEEE Transaction on Pattern Analysis and Machine Intelligence Vol. 8 (1986) 679-714

19. http://www.csse.uwa.edu.au/~pk/studentprojects/libor/index.html

20. T. Chuan Chen, K. Liang Chung: An Efficient Randomized Algorithm for Detecting Circles. Computer Vision and Image Understanding Vol. 83 (2001) 172-191

21. Peter Kovesi, Matlab functions for Computer Vision and Image Processing. What are Log-Gabor filters?

22. Olatinwo, S.O., O. Shoewu, and O.O. Omitola. 2013. “Iris Recognition Technology: Implementation, Application, and Security Consi

23. Neha Kak, Rishi Gupta, Computer Science Engineering, Lingayas Institute of Technology and Management Faridabad, Haryana, INDIA

24. Sanchit Mahajan Information Technology Lingayas Institute of Technology and Management Faridabad, Haryana,INDIA

25. J. Daugman Two-dimensional spectral analysis of cortical receptive field profiles Vision Res.(1980)

26. A.N. Kolmogorov, Three approaches to the quantitative definition of information, Probl. Inform. Transm.(1965)

27. https://images.app.goo.gl/qvqBZ1m4NgRnMVFW8

28.https://www.google.com/url?sa=i&url=https%3A%2F%2Frecfaces.com%2Farticles%2Ffacial-recognition

29. https://d1sr9z1pdl3mb7.cloudfront.net/wp-content/uploads/2019/12/05172231/biometric-iris-recognition-for-healthcare.png

30. Image by <a href="https://www.freepik.com/free-photo/biotechnology-specialist-laboratory-conducting-experiments_44133702.htm#query=DNA%20sequence%20as%20biometric&position=0&from_view=search&track=ais&uuid=5cd68729-22de-4bad-81d4-084ad3526161">Freepik</a>

31. S.O. Olatinwo, Engr. Dr. Oluwagbemiga Omotayo Shoewu, Lagos State University, Olusegun O. Omitola, Afe Babalola University