Section: Ophthalmology

Review Article

ADVANTAGES OF IRIS AS A BIOMETRIC TOOL OVER OTHER BIOMETRIC SYSTEMS

Simi Zaka ur Rab[1]

[1]*Professor, Institute of Ophthalmology, J. N. Medical College, Aligarh Muslim University, Aligarh, India.*

Received : *05/07/2025*
Received in revised form : *22/08/2025*
Accepted : *11/09/2025*

Corresponding Author:
Dr. Simi Zaka ur Rab,
Professor, Institute of Ophthalmology, J. N. Medical College, Aligarh Muslim University, Aligarh, India.
Email: s_zrab@yahoo.co.in

DOI: 10.70034/ijmedph.2025.3.461

Source of Support: Nil,
Conflict of Interest: None declared

Int J Med Pub Health
2025; 15 (3); 2507-2515

ABSTRACT

“Biometrics” is the science of establishing the identity of an individual based on physical, chemical or behavioural attributes of the person. Biometrics-based authentication systems are security technologies, which use human characteristics for personal identification.

Automated biometric systems have only become available over the last few decades, because of the significant advances in the field of computer processing. The biometric iris recognition is based on multiple advantages as compared to other biometric systems like fingerprints, retinal scans, voice typing, signature analysis, DNA analysis, gait and odour analysis: it is a noncontact, real-time measurement and with very quick recognition of a person's identity by mathematical analysis of the random patterns that are visible and constant within the iris structure of the individual eye. The iris recognition system has also been used to empower residents of India with a unique identity and a digital platform to authenticate anyone, anytime and anywhere. Government of India launched “Aadhaar” which is a 12-digit unique-identity number issued to all Indian residents based on their biometric and demographic data.

With the advancement in microsurgical techniques and early rehabilitation, people are now opting for early cataract surgeries. Though many studies have previously shown that iris scanning system cannot be fooled by artificial or dead eyes, or by the use of high definition contact lenses, there are studies that have observed a failure in recognition by the iris scanning system after undergoing surgical interventions for cataract or after iatrogenic topical dilation

Keywords: Biometrics, fingerprints, iris patterns, retinal patterns.

INTRODUCTION

There goes a historical English saying that “eyes are the window to your soul”, and in today’s era this saying has become more accurate than ever. With the development of technology and new innovations, identification of a person through various characteristics has become a reality. Identifying characteristics of a person can either be physical or behavioural. Physical parameters include fingerprint, palm, face, cornea, iris or retina, and behavioural features include signature, voice, typing dynamics, odour and walk pattern. But this is only a partial as new means of identification are in developmental process all the time. Identification can be done by using any of the above biometric characteristics, but only if they satisfy the five basic requirements which are: robustness, distinctiveness, availability, accessibility and acceptability. Each of these above mentioned features has been described in detail below. A characteristic is said to be “robust” if it does not change over a due course of time; By “distinctiveness” it means that it should present with variations in the entire population; “Availability” is defined as universal presentation of the feature in over whole spectrum of population; “Accessibility” shows that the feature is easy to be used with the technological innovations and last but not the least is “Acceptability” which indicates the extent to which people are giving consent for this feature of theirs to be used for identification.[1]

“Biometrics” is the science of establishing the identity of an individual based on physical, chemical or behavioural attributes of the person.[2] Biometrics-based authentication systems are security technologies, which use human characteristics for personal identification. [3,4]

History of biometric technology

The earliest accounts of biometrics can be dated as far back as 500BC in Babylonian empire.[5] There is evidence of Babylonian business transactions that were recorded in clay tablets that included fingerprints. [6-10]

There are historical evidences, that early Chinese merchants used fingerprints for settling business transactions. Chinese parents also used fingerprints and footprints to differentiate their children from one another. [11,12]

By 702 BC, Japan also allowed the use of fingerprints as the signature in divorce papers. [13-14].

Various books, treatise and papers were written on fingerprints and many observations by different anatomists and historians in different parts of the world reported the details of friction skin ridges and their uniqueness. [15-18]

Fingerprinting followed suite in the 1880s, as not only the means of identifying criminals but also as a form of signature on contracts. It was recognized that a fingerprint was symbolic of a person's identity and one could be held accountable by it. The Europeans first began using fingerprints in July 1858 when Sir William James Herschel, Chief Magistrate of the Hooghly District in Jungipoor, India, first used fingerprints on native contracts.[19,20] Faulds, a Scottish physician, suggested that bloody finger marks or impressions could lead to scientific identification of criminals.[21] In 1870, Alphonse Bertillon,[22] developed "Bertillonage" or anthropometries, a method that was used to identify individuals based on detailed records of their body measurements, physical descriptions and photographs.

In 1892 Sir Francis Galton,[23] wrote a study of fingerprints in which he presented a new classification system, which involved prints from all the ten fingers. The characteristics that Galton used to identify individuals are still used till date and these details are referred to as Galton's details.

In 1896, Sir Edward Henry,[24] Inspector General of the Bengal Police developed a fingerprint classification system which was enhanced by one of his workers, Azizul Haque, so that searching could be performed easily and efficiently. Sir Henry later established the first British fingerprint files in London. The Henry classification system, as it came to be known later, was the foundation to the classification system used later by the Federal Bureau of Investigation and other criminal justice organizations that perform ten print fingerprint searches. [25-27]

The fingerprint matching system seemed to dwindle with time and the need for other modalities came into existence. In 1981, the first prototype of retinal scanning device was developed that used infrared light for illumination.[28] It was in 1936, when Bruch proposed an idea that iris could be used as a mode of identification. In 1985, Dr. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irises are alike. They were awarded a patent for their concept that the iris could be used for identification.[29] Dr. Flom approached Dr. John Daugman who developed an algorithm to automate the identification of the human iris for which the latter was awarded a patent in 1994. Owned by Iridian Technologies, the successor to lriScan, Inc. – this patent is the cornerstone of most commercial iris recognition products to date.[30]

One of the most recent advancements is an idea of fusion of iris and retinal biometric systems. Based on this idea Retica Inc. launched Cycolps in 2006 (a retinal scanner that used also iris patterns to derive its own set of codes) that is supposed to be the best candidate at the moment with best false match and false non match odds of any other biometric security identifier in the industry.[31]

Advantages and disadvantages of different biometric systems

There are various biometric identification methods; some of the common used means of identifying a person have been: face, voice, signatures and fingerprints, but even they are amenable to changes. The skin grows old, face changes with time and lots of people look very similar which makes face recognition even less reliable. Signatures can be changed and forged very easily; also the error rates can be very high due to inconsistencies in one's signature.[32] Identification mechanisms using fingerprints have shown high matching accuracy rates for past many years.[3] But even they're not infallible: illnesses and injuries, like basic wear-and-tear, cuts and bruises which are more common in certain occupational areas (manual workers are more prone to injuries on their fingers), genetic factors, ageing and environmental causes can alter the fingers in time, which make it unsuitable for automatic identification.[3] It may even be difficult to collect the data after amputations. It has also been demonstrated that even replica fingerprints or gummy fingers (generated from silicone) or inked fingerprints on a paper are capable of fooling certain kinds of recognition systems.[33]

Modern criminal behaviour is significantly determined by science and modern technology. As the perpetrators in committing criminal acts increasingly resorted to sophisticated methods and techniques using the latest tools, the need for high quality protection of persons, objects and systems became imperative. For these reasons, scientifically advanced methods of identification system were developed like DNA profiling, iris scans, retina scans. One of the most revolutionary discoveries of 20th century in the field of forensic investigation was DNA profiling. It was established as a mechanism for identification of an individual later by Dr. Alec Jeffreys at the University of Leicester, in UK.[34] Because of its high accuracy it has since then been used in various fields, ranging from forensic evaluation in criminal investigations and genealogical and medical research. It is currently the most accurate and advanced technology for parentage

Testing.[35] But issues like contamination and sensitivity, cumbersome chemical methods needed for automatic real time recognition and privacy concerns make it a high cost and time consuming process,[3] rendering it less approachable and infrequently used method of identification.

Eye biometrics on the other hand seem to be a complete package offering highest level of uniqueness, universality, permanence and accuracy.[31] The human eye contains numerous individual characteristics that make it particularly suitable for the process of identifying a person. Today, the eye is considered to be one of the most reliable body parts for human identification. Especially suitable for identification is the iris and the retina of the eye. The retina is a thin layer of sensory neural cells with abundant blood vessels located in the posterior part of the eye which helps form images by converting the light rays into electric pulses. Based on a major studies, by Simon and Goldstein in 1935, it was confirmed that pattern of retinal blood vessels is individual and unique for each person.[36] Retinal pattern recognition methods have been suggested to be better and more promising biometric systems than iris patterns.[31] The detection is performed by scanning the eye. Retinal scan takes 10–15 seconds. This method requires that the eye is closest to the scanner, and the spectacles have to be removed, otherwise the light reflecting back from the lens of the spectacles will interfere with the signals of the scanning device.[31] During the scanning, the eye is illuminated with an infrared light beam which is absorbed by the retinal blood vessels at a quicker rate than other tissues in the eye and reveals their pattern in the retina.[37] This is also the most expensive method of identification because the equipment used to scan the retina is very costly; therefore this method is not commonly used, although it has the best results.[38] Like other biometric recognition systems, the retinal recognition system has its own strength and weakness. Despite being inaccessible to tampering, its unique features, stable retinal blood vessel patterns over lifetime, identification ability between genetically identical twins and small feature vector size that fastens the processing speed, it has various weaknesses like, need of high cooperation of the subjects, close eye contact to eyepiece, and exploitation of the data to reveal the medical conditions deciphered on seeing the retinal blood vessel pattern.[37,39] The retinal measurements change due to various pathological developments (for example in diabetic retinopathy). [40] High cost of this biometric method and its above-mentioned weaknesses limits its applications in military facilities and areas of high-level security (police stations, prisons, nuclear plants, laboratories, etc.) where the price of equipment is not the determining factor. Faster, cheaper and thus more used method is a method of identifying a person through the iris.

For a long time iris recognition biometric system technology did not advance, until two ophthalmologists; Flom and Safir, were awarded a patent in 1987 for describing the methods and apparatus for iris recognition.[29] Sarode and Patil (2014),[41] described the iris of the eye as an ideal part of the human body for biometric identification for reasons stated below:

1. It is an internal organ that is well protected against damage and wear and tear, by a very sensitive and transparent (the cornea). This differentiates it from fingerprints, which can undergo changes overtime due to manual labour or trauma.
2. The iris is mostly flat, and its geometric configuration is controlled by only two muscles; the sphincter pupillae and the dilator papillae. They control the diameter of the pupil.[42] This makes the iris shape far more predictable than, for instance, that of the face.
3. The human iris has an intricate structure with many minute characteristics such as furrows, freckles, crypts, and coronas,[43] and like fingerprints, it is determined randomly during embryonic gestation. The iris patterns of the two eyes of an individual or those of identical twins are completely independent and uncorrelated.[44] Also many factors go into the formation of these textures (the iris and fingerprint) that make the chances of false matches for either extremely low.
4. An iris scan is similar to clicking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the subject to touch any equipment that has recently been touched by a stranger, thereby eliminating any objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece.

The system for identification based on iris cannot be fooled by lenses, glasses or eyes removed from a dead body. Modern biometric systems have measures to ensure that the subject is alive and that the sample which undergoes testing is not a photograph or a removed eye from the cadaver.

There are algorithms that register the changes in a living eye like contraction and dilation of pupil when eye is illuminated by light; which are not present in glass eyes or the eye of a dead person. This method is non-invasive because it requires no physical contact between the eye and the scanner. The iris scanning can be done with a simple camera with a gap of two feet distance and to search the database takes just few seconds, that makes the process reasonably quick.[38]

Every biometric system consists of four main parts. First is an "Input unit" that measures and registers the biometric features. Then comes in action the "extractor unit", which extracts certain specific features from the registered data collected initially during registration process. Then there are units for verification and comparison that certify the quantity and quality of contentious characteristics and compare them with previously stored database.[38]

History of development of iris scanning technology

- 1936: US ophthalmologist Frank Burch suggested the idea of recognizing people from their iris patterns long before technology for doing so was invented.[45]
- 1981: American ophthalmologists Leonard Flom and Aran Safir described the methods and apparatus of iris recognition biometric system.[29]
- 1987: Leonard Flom and Aran Safir gained, US patent (US Patent number 4,641,349) for describing the basic concept of an iris recognition system.[29]
- 1994: US-born mathematician John Daugman worked on the idea of Dr. Flom and Dr. Safir and developed the algorithms (mathematical processes) that turned digitalised photographs of iris of the eyes into unique numeric codes. For this he was granted US patent (US patent number 5,291,560) for a "biometric personal identification system based on iris analysis" in the same year.[30] Daugman has widely been credited as the inventor of practical iris recognition since his algorithms were used in most iris-scanning systems.

Principles of Working of Iris Scanner

The principal steps of the iris scanning process developed in the 1994 by computer scientist John G. Daugman were as follows.[33]

1. The camera scans the person's eye and produces a digitalised image.
2. Image processing software isolates the iris by drawing two circles, one at its inner boundary (between the pupil and the iris) and the other at its outer boundary (known as the limbus, between the iris and the white, outer sclera). The inner boundary is relatively easy to detect, because it has a circular edge, which changes in brightness at the margin of pupil and iris (as iris is generally lighter and pupil is darker). Though this relation can be reversed in eyes with dark iris or in eyes with cloudy lens giving pupil a lighter contrast as compared to iris. A series of “exploding circles” (steadily increasing in radii) are positioned and the one which has the maximum spike of change in luminance is summed as its perimeter with centre corresponding with the true centre of the pupil. A broadly similar process is used to find the outer boundary but with two “exploding pie wedges” in the horizontal meridian, which allows compensation of parts of iris blocked by the eyelids superiorly and inferiorly and for the asymmetrical left and right limbic distance from pupil margin.
3. Polar coordinates (concentric circles and radial lines with origin at the centre of pupil) are then added to the image to define separate "zones of analysis," so that the key features of the iris can be accurately located and compared in two-dimensional space. This dimensionless coordinate system accommodates for the iris changes as the pupil grows (dilates) and shrinks (constricts) in different light conditions and also for image acquisition from distance which allows the generation of an approximately similar iris code.
4. This pattern of light and dark areas in the iris is then converted into digital form using bandpass filters, such as 2-D Gabor filter, and through the mathematical calculations inside the system, a unique digital 2048 bits of Iris code is generated with the significant iris texture in the image reduced to 256 byte size. Each bit in an iris code can be regarded as a coordinate of a vertice in a unit square of the complex plane from the coordinate system as described above, forming a 256 bytes code, which is used for comparisons.[46]
5. To get past an iris-scanning system, the unique pattern of the eye has to be recognized so that the person can be identified correctly. Which means there have to be two distinct stages involved in iris-scanning: enrolment (the first time when the system stores the database of the enrolled eye) and verification/recognition (where the subject eye is matched with the previously stored database in the system). Each time this recognition process is conducted, a different template of iris code is generated and the difference between the two templates is measured as a value termed as Hamming distance, which is simply the sum of total number of times the two presented iris codes disagree.

The general framework the iris recognition system involves following steps (Das, 2012),[47]

1. Image acquisition

In the first step of this identification system, a high resolution black and white image of the eye is acquired with a small high quality camera that uses infrared scans.[48] Infrared helps to show up the unique features of darkly coloured eyes that do not stand out clearly in ordinary light.

2. Segmentation

The next part of iris recognition system is to isolate or localize the actual iris region from the digital eye image. Daugman (1994) explained the algorithm of iris recognition system, which defines the boundary of the iris (inner and outer boundaries of the iris), sets the coordinate system over the iris, and defines an area for analysis.[33] Segmentation excludes the disturbances like eyelids, eyelashes, specular reflections corrupting the iris pattern. The segmentation step is very important as the data that has not been correctly localized will result in poor recognition rates.

3. Normalisation

Dimensional inconsistencies in eye images generally arising due to; dilation of the pupil that depends on the varying levels of illumination falling on the eye, varying imaging distance, camera rotation, head tilt, and rotation of the eye within the socket are eliminated by this normalization process that produces iris regions having constant dimensions such that two images of the same iris taken at different conditions and time will have the same characteristics features at the same locations spatially.

4. Feature extraction

It is the process of generation of iris codes. To provide for an accurate method of recognition of individuals, the features which are most distinctive in an iris pattern are extracted. Only the significant parts are extracted so that they can be encoded into biometric templates which are used for comparisons. For feature extraction a number of filters are adopted that decompose the segmented image into different components and detects the local feature points. The system identifies around 240 unique features (about five times more "points of comparison" as fingerprint systems use). These features, unique to every eye, are then turned into 512-digit number called an "Iris code" that is stored alongside the enrolled name and other details in a computer database.

4. Classification and matching

The eye is photographed again. The system quickly processes the image and extracts the new Iris code. For identification (one-to-many template matching) or verification (one-to-one template matching), a template created by imaging an iris is compared to stored template(s) in the database.

Hamming distance is used as a matching algorithm that compares the two biometric templates, giving us the information, if the new pattern that is generated is from the same iris or from different irises.

Hamming distance

The verification template when compared to the enrolment template computes a mathematical difference between the two iris codes. This mathematical difference is called the Hamming distance (HD).[49] The Hamming distance between the identification and enrolment codes is used as a score and is compared to a confidence threshold for a specific equipment or use, giving a match or non-match result. Systems may be highly secure or not secure, depending on their confidence threshold settings. If the Hamming distance is below the decision threshold, a positive identification is made because of the statistical extreme improbability that two different persons could agree by chance in so many bits, due to the high entropy of the iris templates. [41]

The decision made by the algorithm may be either correct or incorrect. The four outcomes, are consequently a correct accept, false accept, correct reject and false reject.

Uses of iris recognition biometric technology:

Iris pattern recognition systems have been deployed at airports, border crossings (as in certain European nations), and individual points of entry or exit for buildings in several countries across the globe.[50] Iris recognition devices can either be wall-mounted (for use in airports and other buildings) or hand-held and portable (as in the iris scanners deployed by the US Army and AADHAR system in India).[51]

1. In 1996 the U.S. District Lancaster prison in Louisiana introduced the first experimental identification system using iris scanning.[38]
2. In 2000, Douglas International Airport in North Carolina and Flughafen Frankfurt Airport in Germany became two of the first airports to use iris scanning in routine passenger checks.
3. In June 2001 iris recognition technology was used at the Heathrow airport London. The technology made it possible to avoid the passport control, which shortened the waiting in line for passport control.[38]
4. The Amsterdam Schiphol Airport also uses iris scanning for passenger's identification. Banks such as the Japanize Suruga Bank also use iris identification for internal security matters, such as for opening and accessing the vault.[38]
5. Mexico was the first country that placed a picture of the iris on the identity card.[38]

Iris recognition systems for personal use are available for protecting laptops and other equipment, while a number of mobile apps are available for providing access control and anti-theft protection on smartphones and other devices fitted with front-facing cameras. A small portable iris-scanning device is available on the consumer market for personal applications such as logging onto secure websites without having to use a password or pin.

Privacy and security are also concerns. Critics have highlighted the risks of criminals compromising iris scanning security, either by using high resolution photographs of eyes or even a person's dead eyeballs. The latest iris-scanning systems attempt to get around this by detecting eye movements or seeing how a person's eyes change in different lighting conditions. There's also the matter of hacking and data breaches, which are potentially more serious if the stolen information is biometric. If the fingerprints are stolen, they can then be used to breach any other systems that use fingerprint access. On the other hand, it's important to remember that biometric systems don't generally store raw biometric information. Iris scans, for example, are using an encoded pattern derived from the iris, not the iris itself.

But with every new innovation, there are few drawbacks that need to be taken care of.

1. Many commercial iris scanners can be easily fooled by a high-quality image of an iris or face in place of the real thing.[41] There have even been reports of spoofing the iris recognition system using high quality photographs, contact lenses with iris pattern printed on it and with multilayered three dimensional artificial irises.[31]
2. The placement of the iris scanners are often tough to adjust and it can become bothersome for people of different heights to use them in succession.

3. Studies have shown that variation in pupil size decreases iris biometric performance by increasing the probability of false non matches and that light and medication may deform the iris differently. [41,52,53]
4. Iris scanners are slightly more expensive than some other forms of biometrics like password or prox-card security systems.[41]
5. Iris scanning is a relatively new technology and it is now difficult to substantially invest in them as the law and immigration authorities of some countries have already made huge investments in fingerprint recognition system.[41]
6. Iris recognition is very difficult to perform at a distance larger than a few meters and for people who are very uncooperative and cannot hold their head steady while looking into the camera.[41]
7. Like other photographic biometric technologies, iris recognition is susceptible to poor image quality, giving rise to high failure in enrolment rates. As with other identification systems like national residents' databases and ID cards, there are concerns that iris-recognition technology can help government track individuals beyond their will and consent.[41]
8. Eye pathologies like cataract, acute glaucoma, posterior and anterior synechiae, retinal detachment, rubeosis iridis, corneal vascularization, corneal grafting, iris damage and atrophy and corneal ulcers, haze or opacities have a high potential of impacting the false non match rate.[54]

Despite its high initial installation costs and relative newness of the technology, it's likely that it will continue to evolve to the stage where photography and digital image processing will be conducted with more clarity and at greater distances. This kind of evolution has the potential to raise issues over civil liberties, privacy concerns, and the ways in which recognition data is used and handled. Keeping these issues aside, in terms of its accuracy, uniqueness in identifying an individual and convenience over more conventional methods of verification and access control, iris pattern recognition has a lot to offer in security applications.

Effects of eye surgeries on iris

Eye surgeries in today's world continue to be a widely practiced group of surgeries, having developed various techniques to treat numerous eye diseases. Some of the common eye diseases to be named that require surgery include: cataract, glaucoma, strabismus, refractive errors, retinal detachment, diabetic retinopathies, orbital and adnexal mass etc.

Eye surgeries can be divided into intraocular and extraocular surgeries. Intraocular procedures are known to alter the iris texture, which can be evaluated by clinical examination on slit lamps. These surgeries are also known to decompensate cornea by producing corneal oedema, keratitis and hence raising the central corneal thickness,[55] leading to corneal haze, which can obscure the clear view of iris. Pachymeters are used to evaluate the degree of corneal oedema.[56] The commonly seen iris changes that occur after these surgeries are pupil ovalization, depigmentation, localized iris atrophy, loss of large areas of Fuchs' crypts, circular and radial furrows.[57] There is loss of iris tissue when iridectomy is performed in trabeculectomy for glaucoma. Direct trauma to the iris tissue in various ocular surgeries can also result in iris atrophy thereby modifying the iris patterns. The mechanism of iris changes in phacoemulsification surgery due to the probe is not clearly known, though it is known that iris tissue can be emulsified when the probe tip is pointed towards it and there is progressive atrophy after manipulation; also it is speculated that iris depigmentation can occur, even without any contact with the iris tissue, due to the energy dissipated in the anterior chamber. Nonelastic deformation and then loss in circularity also occur after pupillary dilation.[52] These changes in iris pattern challenge the core idea and concept of biometric iris recognition that is based on the stability and uniqueness of the iris texture.

Biometric iris recognition and eye surgery

Various studies have been done to study the reliability of biometric iris recognition system and cataract surgeries. Roizenblatt et al (2004),[57] conducted a prospective study in Brazil on fifty-five patients chosen for phacoemulsification type of cataract surgery done by trained residents under the supervision of experienced surgeon. Out of the 55 patients, 28 patients had cataract in right eye and 27 had cataract in left eye. Patients were properly positioned in front of the equipment and maximum ocular opening was instructed. The iris was separated in four quadrants and photographed with a slit lamp-attached camera. None of the patients in the study had undergone any other ocular surgery and did not have other associated ocular diseases. Patients were enrolled and three identification trials were done following which hamming distance and focal data were received. This was verified with the post operative iris scans, one month after the procedure (as the major iris changes occur in the first postoperative period due to surgical manipulation, and the acute healing with the chronic tissue retraction are usually complete by one month) and one week after the use of mydriatics was discontinued. At this time, each patient had his or her iris examined in the slit-lamp by an anterior segment specialist, who gave a score for the visible texture alterations. One point was given for each of the following alterations: focal atrophy without transillumination, depigmentation, focal atrophy with transillumination and pupil ovalization. A score of zero represented no visible alterations and a score of four meant all of these visible alterations were present. The result was non recognition of six out of fifty five eyes involved in the study and a correlation between visible subjective iris texture alteration and mathematical difference was verified. It also indicated prediction of cases in which iris recognition systems failed in identifying people based on slit-lamp examinations. They concluded that cataract procedures are able to change iris texture and that iris pattern recognition is no longer feasible or probability of false rejection is increased. Patients subjected to intraocular procedures may be advised to enrol again in biometric iris systems.

Dhir et al (2010),[52] conducted a prospective, non comparative cohort study on the effect of cataract surgery and pupil dilation on iris pattern recognition for personal authentication. They took images of 15 subjects that were captured before (enrolment), and 5, 10, and 15 min after instillation of mydriatics before routine cataract surgery. After cataract surgery, images were captured 2 weeks in the follow up. Enrolled and test images (after pupillary dilation and after cataract surgery) were segmented to extract the iris. This was then unwrapped onto a rectangular format for normalization and a novel method using the Discrete Cosine Transform was applied to encode the image into binary bits. The numerical difference between two iris codes (Hamming distance, HD) was calculated. The HD between identification and enrolment codes was used as a score and was compared with a confidence threshold for specific equipment, giving a match or non-match result. The Correct Recognition Rate (CRR) and Equal Error Rates (EERs) were calculated to analyse overall system performance. They reported that matching reliability decreased considerably with increase in pupillary dilation. Cataract surgery had no effect on iris pattern recognition, whereas pupil dilation may be used to defeat an iris-based authentication system.

Seyeddain et al (2014),[58] conducted a prospective, nonrandomized, single centre, cohort study to investigate the reliability of a biometric iris recognition system for personal authentication after cataract surgery or iatrogenic pupil dilation. The study comprised of two groups. Group 1 constituted of 173 eyes which underwent cataract surgery and were evaluated by the iris recognition system 2 to 24 hours after phacoemulsification and intraocular lens implantation. Group 2 comprised of 184 eyes that were enrolled in miosis and were then evaluated before and after iatrogenic pupil dilation. The Biometric iris recognition system was installed in one of the examination rooms of the clinic. All image acquisitions were performed by one examiner using the same illumination conditions to reduce bias, due to the difference of pupil size under varying lighting conditions. Patients were properly positioned in front of the equipment and were instructed to maximally open their eyes for enrolment and postoperative/dilated re-examinations. They observed that in group 1 out of the 173 eyes that could be enrolled before cataract surgery, 164 (94.8%) were easily recognized postoperatively, whereas in 9 (5.2%) eyes this was not possible. However, these 9 eyes could be re-enrolled and afterwards recognized successfully. In 5 out of 9 eyes not recognized after surgical treatment, changes of iris texture (break in the continuity of the sphincter muscle of the iris, peripheral surgical coloboma, and segmental iris depigmentation) were obvious. Nevertheless, after re-enrolment, all eyes were recognized successfully. In group 2, of a total of 184 eyes that were enrolled in miosis, a total of 22 (11.9%) could not be recognized after dilation and therefore needed re-enrolment. No single case of false-positive acceptance occurred in either group. They reported that standard cataract surgery seems not to be a limiting factor for iris recognition in the large majority of cases. Some patients (5.2% in this study) might need “reenrolment” after cataract surgery. Iris recognition was primarily successful in eyes with medically dilated pupils in nearly 9 out of 10 eyes. No single case of false-positive acceptance occurred in either group in this trial.

Singh et al,[59] conducted a prospective, non-randomised, single centre cohort study to study the effect of pupil dilation on patients who reported for routine eye check up from November 2017 to November 2019 on biometric iris recognition system for personal authentication and identification. Iris scanning device “IRITECH-MK2120U” was used to initially enrol the undilated eyes. Baseline scans were taken after matching with enrolled database. All eyes were topically dilated and matched again with enrolled database. Hamming distance (measure of disagreement between two iris codes) and recognition status was recorded from the device output and eyes were evaluated by slit lamp ophthalmoscopy with special emphasis on pupil shape, size and texture. All 321 enrolled eyes matched after topical dilation. The pupil size had significant effect on Hamming distance with p value <0.05. There were no false matches. A correct recognition rate of 100% was obtained after dilation. No loss of iris texture or pupil shape was observed after dilation. They reported that Biometric iris recognition system is a reliable method for identification and personal authentication after pupil dilation. Topically dilated pupils are not a cause for non recognition of iris scans.

It seems therefore that iris recognition is a valid reliable biometric method in the majority of cases after cataract surgery or after pupil dilation.

REFERENCES

1. Wayman J, Jain A, Maltoni D, Maio D. An introduction to biometric authentication system. In: Wayman J, Jain A, Maltoni D, Maio D, ed. by. Biometric systems. Springer; 2005. p. 1
2. Jain A, Flynn P, Ross A. Handbook of biometrics. New York, N.Y.: Springer; 2008
3. Jain A, Ross A, Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004; 14(1):4-20.
4. Rakshit S, Monro DM. An evaluation of image sampling and compression for human iris recognition. IEEE Trans Inform Forensics and Security 2007; 2(Issue 3), Part 2 605–612.
5. Grant C. A Brief History of Biometrics. Blog.bioconnect.com. 2019 .Available from: https://blog.bioconnect.com/a-brief-history-of-biometrics

6. Paul A, Eriksson SA. Fingerprints and archaeology 28. In: Studies in mediterranean archaeology series 1, 2. Goteborg, Sweden, 1980. ISBN- 9185058998
7. Ashbaugh DR. History of friction ridge identification. In: An introduction to basic and advanced ridgeology: quantitative qualitative friction ridge analysis. Florida: CRC Press Boca Raton, 1999: 11–38. ISBN: 978-0-8493-7007-6
8. Berthold L. History of the finger-print system. Smithsonian Institution Annual Report 1912. Reprinted in: The Print, Newsletter of South California Association of Fingerprint Officers 2000; 16(2): 1–13. 15.
9. Paul A. The study of ancient fingerprints. Journal of Ancient Fingerprints 2007; 1(1): 2–3. 16.
10. Bose PK, Kabir MJ. Fingerprint: A unique and reliable Method for Identification. Journal of Eman Medical College2017;7(1),29-34.
11. Laufer B. History of the Finger-Print System, Smithsonian Publication Washington: Government Printing Office.1912.p.1-22
12. Chavannes E. Les livres chinois avant l'invention du papier. (Chinese Books before the invention of paper). Journal Asiatique 1905; 10(5): 5–75.
13. Ashbaugh DR. History of friction ridge identification. In: An introduction to basic and advanced ridgeology: quantitative qualitative friction ridge analysis. Florida: CRC Press Boca Raton, 1999: 11–38. ISBN: 978-0- 8493-7007-6
14. Polson CJ. Finger prints and finger printing: an historical study. Journal of Criminal Law and Criminology 1951; 41(4): 495–517.
15. Laufer B. History of the Finger-Print System, Smithsonian Publication Washington: Government Printing Office.1912.p.1-22
16. Cummins, H. and Midlo, C. Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics. Philadelphia: Blakiston. 1943.
17. Lambourne G. The fingerprint story. 1st edn. London: Chambers, 1984: 1–208.
18. Stoney, DA. Fingerprint Identification. In: Faigman D, Kaye D, Saks M, Sanders J, ed. by. In Modern Scientific Evidence: The Law and Science of Expert Testimony. St. Paul: MN: West publishing; 1997. p- 78.
19. Herschel, W J. "Skin Furrows of the Hand." Nature.1880;23:76
20. Ed German F. The History of Fingerprints [Internet]. Onin.com. 2019 [cited 10 November 2019]. Available from http : //onin.com / fp / fphistory html
21. Faulds, H. "On the Skin Furrows of the Hand." Nature.1880; 22:605
22. Bertillon, A. Signaletic Instructions: Including the Theory and ractice of Anthropometrical Identification, trans. R.W. McClaughry.Chicago: Sharp and Smith.1896.
23. Galton F. Previous use of fingerprints. In: Finger Prints. New York: MacMillan & Co., 1892; 22–27.
24. Henry, Edward R. Classification and Uses of Finger Prints. London: Routledge.1900.
25. Hirsch WJ. Morphological evidence concerning the problem of skin ridge formation. J Ment Defic Res 1973; 17: 58–72.
26. 26. Tewari RK, Ravikumar KV. History and development of forensic science in India J Postgrad Med. 2000; 46(4): 303–308.
27. Eng A, Wahsheh LA. Look into My Eyes: A Survey of Biometric Security. In: 2013 10th International Conference on Information Technology: New Generations [Internet]. Las Vegas, NV, USA: IEEE; 2013 .p. 422–7. Available from: http://ieeexplore.ieee.org/document/6614344/
28. Vacca JR. Biometric Technologies and Verification Systems. Elsevier Inc., Burlington, MA, USA.2007
29. Flom L and Safir A. Iris recognition system.1987;U.S. Patent 4 641 349
30. Daugman JG. Biometric personal identification system based on iris analysis.1994; US patent 5,291,560. Available from:https: //patents. google. com/patent/US5291560
31. Zibran M. Eye Based Authentication: Iris and Retina Recognition. Semanticscholar. org. 2019.
32. Bubeck U, Sanchez D. Biometric Authentication-Technology and Evaluation-Term Project CS 574 Spring 2003 San Diego State University.
33. Matsumoto T, Matsumoto H, Yamada K, Hoshino S. Impact of artificial “gummy” fingers on fingerprint systems. In: van Renesse RL, editor. San Jose, CA; 2002. p. 275–289.
34. Roewer L. DNA fingerprinting in forensics: past, present, future. Investigative Genetics. 2013;4(1):22.
35. Rafi SM, Kumar NP, Kumar DJ. Survey for Interlinking of DNA Models with Aadhaar Real-Time Records for Enhanced Authentication. In: 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). Coimbatore, India: IEEE; 2019. p. 208–211. Available from: https://ieeexplore.ieee.org/document/8728512/
36. Simon C, Goldstein I. A new scientific method of identification. New YorkState Journal of Medicine; Sep 1935, 35 (18):901-906
37. Farzin H, Abrishami-Moghaddam H, Moin M-S. A Novel Retinal Identification System. EURASIP J Adv Signal Process. 2008 Dec; 2008(1):280635. Available from: https://aspeurasipjournals. springeropen.com/articles/10.1155/2008/280635
38. Marinovi□c D , Njiri□c S ,Coklo M , Muzi□c V. Personal Identification by Eyes, Coll. Antropol. 35 (2011); Suppl. 2: 347–350
39. Samples JR, Hill RV. Use of the Infrared Fundus Reflection for an Identification Device. American Journal of Ophthalmology.1984 Nov; 98(5):636–637.
40. Uludag U, Pankanti S, Prabhakar S, Jain AK. Biometric cryptosystems: issues and challenges. Proc IEEE [Internet]. 2004 Jun [cited 2019 Dec 9]; 92(6):948–60. Available from:http://ieeexplore.ieee.org/document/1299169/
41. Sarode NS, Patil AM. Review of Iris recognition: An evolving biometrics identification technology. International Journal of Innovative Science and Modern Engineering (IJISME) ISSN 2014 Sep; Volume-2 Issue-10: 2319-6386
42. Kong A, Zhang D, Kamel M. An Analysis of Iris Code. IEEE Transactions on Image Processing. 2010; 19(2):522-532.
43. Wolff E, Last RJ (ed). Anatomy of the Eye and Orbit, 6th ed. HK Lewis & Co. Ltd: London, 1968
44. Daugman J, Downing C. Epigenetic randomness, complexity, and singularity of human iris patterns. Proc R Soc Lond B Biol Sci. 2001; 268: 1737–1740
45. NSTC Subcommittee on Biometrics and Identity Management. Iris recognition. Biometrics.gov. 2006, March: p-1. Retrieved from www.biometrics.gov/Documents/IrisRec.pdf.
46. Daugman JG. High confidence visual recognition of person by a test of statistical significance. IEEE Trans Pattern Anal Machine Intell 1993: 1148- 6
47. Das A. Recognition of human iris patterns. Thesis, National Institute of Technology, Rourkela. 2012
48. Wildes RP. Proceedings of the IEEE, 85 (1997): 1348
49. Ronald AL, Duncan MW. In: "Signal analysis: time, frequency, scale, and structure." New York: IEEE Press, John Wiley & Sons Inc; 2004:338-351
50. Balzacq T. The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies. JCMS: Journal of Common Market Studies. 2007;46(1):75-100.
51. Pati R, Kumar V, Jain N. Analysis of Aadhaar: A Project Management Perspective. IIM Kozhikode Society & Management Review. 2015; 4(2):124-135.
52. Dhir L, Habib NE, Monro DM, Rakshit S. Effect of surgery and pupil dilation on iris pattern recognition for personal authentication. Eye 2010;24:1006 - 10;doi:10.1038/eye.2009.275
53. Rankin DM, Scotney BW, Morrow PJ, McDowell DR, Pierscionek BK. Dynamic iris biometry: a technique for enhanced identification. BMC Res Notes 2010;3:182.
54. Trokielewicz M ,Czajka A , Maciejewicz P. Database of iris images acquired in the presence of ocular pathologies and assessment of iris recognition reliability for disease-affected eyes. IEEE 2nd International Conference on Cybernetics (CYBCONF); 2015.
55. Aribaba O, Adenekan A, Onakoya A, Rotimi-Samuel A, Olatosi J, Kareem M et al. Central corneal thickness changes following manual small incision cataract surgery. Clinical Ophthalmology. 2015;151.
56. Sachdev MS, Honavar SG, Thakar M. Diagnostic tests for corneal diseases. Indian J Ophthalmol.1994;42:89-99

57. Roizenblatt R, Schor P, Dante F, Roizenblatt J, Belfort R Jr. Iris recognition as a biometric method after cataract surgery. Biomed Eng Online 2004;3:2.
58. Seyeddain O, Kraker H, Redlberger A, Dexl AK, Grabner G, Emesz M. Reliability of automatic biometric iris recognition after phacoemulsification or drug -induced pupil dilation. Eur J Ophthalmol. 2014 Jan-Feb; 24(1):58- 62. doi: 10.5301/ejo.5000343. Epub 2013 Jul 17.PMID:23873488
59. Singh T, Zaka ur rab S, Arrin S. Effect of pupil dilatation on biometric iris recognition systems for personal authentication. Indian Journal of Ophthalmology 2023; 71:57-61.